



Dominion SX II User Guide ProCSS

Copyright © 2022 Raritan
DSX2-v2.5.0-0F-E
September 2022
v2.5.0

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without the express prior written consent of Raritan, Inc.

© Copyright 2022 Raritan, Inc. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

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

CS03 Certification - DSX2-16 and DSX2-48	5
<hr/>	
Features and Benefits	6
Package Contents	11
SX II Models	12
SX II Appliance Diagram	12
Supported Serial Devices	13
Access Clients	13
iOS Support	14
<hr/>	
Configure for the First Time	15
Default Login Information	15
Initial Configuration from the Remote Console	15
Connect a Laptop to Using a Cross-Over Cable (Optional)	16
Initial Configuration Using Command Line Interface (Optional)	16
Set Terminal Emulation on a Target	17
Set the CLI Escape Sequence	18
<hr/>	
Access and Use Remote Console Features	19
Allow Pop-Ups	20
Installing a Certificate	20
Example 1: Import the Certificate into the Browser	20
Example 2: Add the to Trusted Sites and Import the Certificate	21
Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)	22
Log In to and HSC	23
Security Warnings and Validation Messages	24
Java Validation and Access Warning	24
Additional Security Warnings	25
Log In to SX II Admin-Only Interface	25
Access SX II Using an iOS Device	25
Change Your Password from the Remote Console	26
Port Access Page	27
SX II Left Panel	28
Port Action Menu Options - Connect, Disconnect, Power On, Power Off and Power Cycle Targets	29
Connect to a Target	30
Disconnect from a Target	31
Power On a Target	31
Power Off a Target	32
Power Cycle a Target	32
Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets	33

Command Line Interface Protocols	35
Command Line Interface Partial Searches.	36
Command Line Interface Tips.	36
Command Line Interface Shortcuts.	36
Command Line Interface High-Level Commands.	37
HTML Serial Console (HSC) Help.	37
Emulator.	37
Copy and Paste and Copy All.	41
Send Text File.	42
Tools: Start and Stop Logging.	43
Power Status.	43
Power on a Target.	44
Power Off a Target.	44
Power Cycle a Target.	45
Browser Tips for HSC.	45
Connect a Rack PDU to and Configure Power Control Options	46
Connecting the to the PX PDU Serial Port.	46
Connecting the to the PX PDU FEATURE Port.	47
Specifications	48
SX II Dimensions and Physical Specifications.	48
Supported Remote Connections.	48
Supported Number of Ports and Remote Users per SX II Model.	49
Maximum Number of Users Session.	49
Maximum Number of Support Users Per Port.	49
Port Access Protocol Requirements.	49
Port Pins.	51
Port Ranges.	52
Network Speed Settings.	53
Default User Session Timeouts.	54
SX II Supported Local Port DVI Resolutions.	54
Appliance LED Status Indicators.	54
Target Cable Connection Distances and Rates.	55
Index	56

To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor.
- When using a backup UPS, power the computer, monitor and appliance off the supply.

CS03 Certification - DSX2-16 and DSX2-48

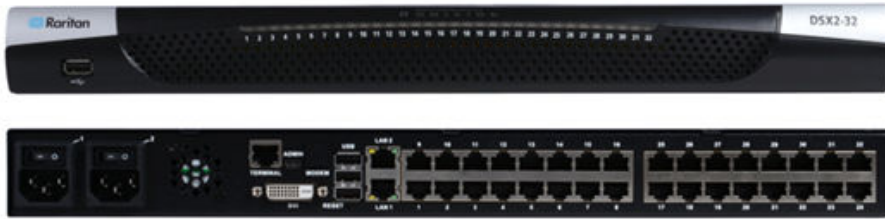
NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation IC, before the registration number, signifies that registration was performed based on a Declaration of Conformity, indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is 01. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

AVIS : Le présent matériel est conforme aux spécifications techniques d'Industrie Canada applicables au matériel terminal. Cette conformité est confirmée par le numéro d'enregistrement. Le sigle IC, placé devant le numéro d'enregistrement, signifie que l'enregistrement s'est effectué conformément à une déclaration de conformité et indique que les spécifications techniques d'Industrie Canada ont été respectées. Il n'implique pas qu'Industrie Canada a approuvé le matériel.

AVIS : L'indice d'équivalence de la sonnerie (IES) du présent matériel est de 01. L'IES assigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

Features and Benefits



Next-Generation Console Server

Raritan's Next-Generation Serial Console Server

The Dominion SX II is Raritan's next-generation Serial Console Server (also known as Terminal Server) that provides IT and network administrators secure IP access and control of serial devices, anytime, anywhere. The new SX II is the most powerful, secure, reliable, easy-to-use and manageable serial-over-IP console server on the market. SX II provides convenient and productive access to networking devices, servers, PDUs, telecommunications and other serial devices.

Ten Years of Serial Console Experience

For over ten years, thousands of customers have relied on the first generation Dominion SX for access and control of hundreds of thousands of serial devices, representing over 500 million hours of total operation. The SX II builds upon that experience with a wide range of advancements and innovations.

Dominion Platform, User Interface and Management

Starting with a powerful, Dominion hardware platform providing performance, reliability and security, the SX II includes virtually all the Serial-over-IP features of its predecessor, Dominion compatible user interfaces and management features, plus exciting new capabilities.

Full CLI-based Configuration and Auto-Configuration

The SX II offers complete CLI access and management via SSH, Telnet and web-based user interface, with convenient direct port access. Two script-based automatic configuration methods are available for a fast installation and for subsequent configuration changes.

Exciting New Features and Innovations

The SX II new features include: military grade security features with 256-bit AES encryption and FIPS encryption mode, automatic DTE/DCE serial port detection, innovative at-the-rack access options, wireless modem support, IPv6 networking, script based auto-configuration and Dominion compatible user interfaces and management.

CommandCenter Management & Scalability

With Raritan's CommandCenter, organizations can manage hundreds or even thousands of serial devices, spread across multiple locations, including branch offices.

Powerful Hardware Platform

Powerful New Hardware Platform

Powerful new hardware platform with 1GHz CPU engine, with an 8-fold increase in RAM. Increased flash memory, up to 8 GB, for storage and logging. Front panel LED's show port connection status.

Wide Variety of 1U Models

Rackable, 1U models available in 4, 8, 16, 32 and 48 ports. All have dual power supplies and dual Gigabit Ethernet LAN ports. Models are available with an optional built-in modem. At-the-rack access includes RJ-45/serial, USB and KVM console.

Powerful Serial Processing Engine	The Dominion SX II with its powerful hardware platform provides high-powered serial processing for the most extreme use cases. Up to 10 users can simultaneously connect to a serial device connected to a SX II port. Up to 200 simultaneous user sessions are supported by a given SX II console server. Port configuration time is up to 23 times faster than the original SX. Connection times are over 50 times faster.
Dual AC Power Supplies	All models have dual, 100-240 volt AC, auto-switching power supplies with automatic failover for increased reliability.
Dual DC Powered Models	Dual power and dual LAN, 8, 32 and 48 port DC powered models are available. These models provide the same features, serial access and performance as the AC powered models.
Dual Gigabit Ethernet LAN on all Models	Dual gigabit Ethernet LAN ports, which can be configured for simultaneous operation or automatic failover. Dual stack IPv4 and IPv6 networking.
Five USB Ports	The Dominion SX II has four USB 2.0 ports, three on the back panel and one on the front panel. These are available for local keyboard/mouse, 3G/4G cellular modem and for automatic configuration via USB drive. A USB 2.0 mini-B port is available for local laptop connection.
Optional Telephone Modem	All models have the option for an internal, 56K telephone modem with RJ11 connection for emergency access and disaster recovery.
Innovative Local Console	The Dominion SX II's local console provides multiple ways for at-the-rack access. The console includes a traditional RJ45 serial port, USB mini-B port, and even a DVI/USB KVM console.

Productive Serial-over-IP Access

Widest Variety of Serial-over-IP Access	The Dominion SX II supports the widest variety of serial-over-IP connections via SSH/Telnet Clients, web-browser, CommandCenter, telephony modem, cellular modem and at-the-rack access. This includes CLI, GUI and multiple Direct Port Access methods.
SSH/Telnet Client Access	SSH/Telnet client access from a desktop, laptop, or handheld device. Direct Port Access via SSH Client using a username/port string syntax. Customer can upload, view and delete SSH keys for greater security.
Web Browser Access	Web browser access via Dominion SX II or CommandCenter user interfaces.
Convenient Direct Port Access	Convenient Direct Port Access methods via SSH, Telnet & HTTP. IP address and TCP port-based access for Telnet and SSHv2 clients. Independent IP addresses or TCP port numbers can be assigned to access each SX II port. HTTPS-based direct access via URL. Com Port Redirection can be supported for third-party software redirectors.
Cellular and Telephone Modem Access	Optional external Cellular (3G/4G) modem and internal Telephone modem access for emergency access, business continuity and disaster recovery.
Innovative At-the-Rack Access	With the Dominion SX II, you get multiple types of local access at-the-rack. This includes: (1) Traditional RJ45 serial port, (2) Mini-USB port for laptop connection, and (3) DVI & USB-based KVM console for connection to a rackmount keyboard tray or even a KVM switch.
Port Keyword Monitoring and Alerting	Users can define up to 14 keywords per port. The SX II will scan the data coming from the port, and if one of the keywords is detected, it will send an alert via SNMP or e-mail. Serial devices are monitored, even when no user is connected! This results in faster notification that reduces Mean Time to Repair (MTTR).

Port Logging to Syslog, NFS and Local File	Port activity to and from serial devices can be logged to a Syslog server, Network File System (NFS) server or locally to the SX II device with up to 8 Gb of storage.
NFS Logging Features	Allows logging of all user keystrokes and server/device responses to NFS server(s). Can even be stored on the NFS server with user-defined encryption keys for greater security. Keep-alive messages in the NFS log allow easy monitoring if the managed server/device goes down.
SecureChat Instant Messaging	Allows for secure, instant messaging among SX II users. Enables collaboration of distributed users to increase their productivity, troubleshoot, reduce the time to resolve problems and for training purposes.
Automatic Serial Device Logoff	Once a user is timed out for inactivity, a user defined "logoff" command can be sent to the target. Improved security of user sessions results as serial sessions are automatically closed upon time out and not left open for possible un-authorized access.

Comprehensive Serial Device Access

Over Ten Years of Serial Device Management	The first generation Dominion SX has been serving customers for over ten years, with over 500,000 ports sold. This represents hundreds of millions of hours of operation across a wide variety of serial devices.
Automatic DTE/DCE Serial Port Detection	This feature allows for a straight Cat5 connections to Cisco equipment (and other compatible devices), without rollover cables. It also means that a SX II can replace the first generation SX with its existing serial device connections.
Support for the Widest Variety of Serial Devices	Supports the widest variety of serial equipment including: networking routers, Ethernet switches, firewalls, UNIX/LINUX servers, Windows Servers, virtual hosts, rack PDU's, UPS systems, telecom/wireless gear. Supports multiple operating systems including SUN® Solaris, HP-UX, AIX, Linux®, Windows® Server 2012, and UNIX®.
Up to 230,400 Baud Serial Connections	Supports operating speeds of 1,200 to 230,400 bits-per-second for serial connections.
Flexible Serial Port Options	Flexible per-port serial options, including BPS, emulation, encoding, parity, flow control, stop bits, character and line delays, always-active connections and more. Can define an exit command when the user times out, as well as enable an in-line menu for port commands and power control.
VT100/220/320/ANSI support	Increased choice of terminal emulation options, allows support of a broader range of devices. SX II supports the following code-sets: US-ASCII (ISO 646); ISO 8859-1 (Latin-1); ISO 8859-15 (Latin-9); UTF-8 and others.
Remote Power Control of Raritan PDU's (With Power Control Menu)	Raritan rack PDU's (PX, PX2, PX3, RPC) can be connected to the Dominion SX II for remote power control of the equipment connected to the PDU. Remote power control can be done via the SX II GUI, SSH/Telnet Client or CommandCenter. Outlet associations can be created for serial devices with multiple power supplies, such that these outlets can be controlled with a single power command. The SX II has "Control P" style menu commands for power control available during a serial session.

Security - Encryption

Strong 256 Bit AES Encryption	The SX II utilizes the Advanced Encryption Standard (AES) encryption for added security. 128- and 256-bit AES encryption is available. AES is a U.S. government-approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST) in the FIPS Standard 197.
--------------------------------------	---

Validated FIPS 140-2 Cryptographic Module

For government, military and other high security applications, the Dominion SX II utilizes a validated FIPS 140-2 Cryptographic Module for enhanced encryption. Modules tested and validated as conforming to FIPS 140-2 are accepted by federal agencies of the U.S. and Canada for the protection of sensitive information.

Enhanced Encryption Options

Support more encryption options: web-browser security through 256 and 128-bit SSL encryption; for SSHv2 connections, AES and 3DES are supported (client-dependent).

Security - Authentication

External authentication with LDAP, Radius, TACACS & Active Directory

Dominion SX II integrates with industry-standard directory servers, such as Microsoft Active Directory, using the LDAP, RADIUS and TACACS protocols. This allows Dominion SX II to use pre-existing username/password databases for security and convenience. SecureID is supported via RADIUS for added security.

Upload Customer-Provided SSL Certificates

Customers can upload to the Dominion SX II digital certificates (self-signed or certificate authority provided) for enhanced authentication and secure communication.

Configurable Strong Password Checking

The Dominion SX II has administrator-configurable, strong password checking to ensure that user-created passwords meet corporate and/or government standards and are resistant to brute force hacking.

Configurable Security Banner

For government, military and other security-conscious customers requiring a security message before user login, the SX II can display a user-configurable banner message and require acceptance before user login.

SSH Client Certificate Authentication

In addition to authentication via login/password, on the SSH interface users can be authenticated via SSH certificates. Each local user can be assigned up to 500 SSH keys. The key authentication takes the place of the login/password

Local Authentication with Users, Groups and Permissions

In addition to external authentication, the Dominion SX II supports local authentication. Administrators can define users and groups with customizable administration and port access permissions.

Login and Password Security

The SX II includes multiple login and password security features including password aging, idle timeout, user blocking and login limitations. Failed login attempts can be result in lockouts and user deactivation.

SHA-2 Certificate Support

Support for the more secure SHA-2 certificates.

Security - Networking

Dual Stack IP Networking – IPv4 and IPv6

The Dominion SX II provides dual-stack IP networking with simultaneous support of IPv4 and IPv6.

IPTables Firewall support

Fully configurable "iptables" firewall support. User selectable and customizable system security levels catering to wide range of security needs.

Selective Static Routing Support

Supports connections between modem and LAN 1, modem and LAN 2 or LAN 1 and LAN 2. This allows users to utilize two different networks (Public and Private) and modem access to KVM or Ethernet controlled devices. When used with the firewall function, secure access can be enabled.

TCP/IP Port Management	Can disable TELNET and SSH access if desired. Ability to change these ports in addition to HTTP, HTTPS and discovery ports
Prevent Man In The Middle Attacks	Enhanced security of communication channels by using client and server SSL certificates.
Modem Dial-Back Security	For enhanced security, Dominion SX supports modem dial-back.
Rejects SSHv1 Requests	Due to the many known security vulnerabilities of the SSHv1 protocol, the Dominion SX will automatically reject SSHv1 connections.

End User Experience

Multiple User Interfaces	The SX II supports multiple user interfaces giving the user the freedom to use the interface best suited for the job at hand. This includes remote access via Raritan or third party serial client via CLI, Raritan graphical user interface (GUI), Admin-only GUI, at-the-rack access or via CommandCenter. Convenient direct port access methods available.
Full Modern CLI – GUI Equivalence	Full CLI management and configuration, thereby allowing scripting of any command.
Broad Range of Supported Browsers	Offers broad range of browsers: Firefox, Safari, Internet Explorer, Chrome, Edge.
International Language Support	The web-based user interface supports English, Japanese and Chinese languages. The Raritan Serial Console can support four languages: English, Japanese, Korean and Chinese
PC Share Mode	Up to ten users can connect and remotely access each connected serial device up to a maximum of 200 serial sessions. Sharing feature is very useful for collaboration, troubleshooting and training.

Easy to Install and Manage

Full CLI-based Configuration and Management	The SX II offers complete CLI administration and management via SSH, Telnet and web-based user interface. Two script-based automatic configuration methods are available for a fast installation and for subsequent configuration changes.
Automatic Configuration via USB Drive	The SX II can be optionally configured via a CLI script on a USB drive connected to one of its USB ports. This can be used for initial configuration or subsequent updates.
Automatic Configuration via TFTP Server	The SX II can be optionally configured via a second method, i.e. via a CLI script contained in a TFTP server. This can be used for initial configuration or subsequent updates. The TFTP server address can be retrieved via DHCP or set by the administrator.
Dominion-Compatible Management	Dominion-compatible management features are available via a web-based user interface or CLI. This includes Dominion-style User Management, Device Settings, Security, Maintenance, Diagnostic and Help features. Firmware update via web browser without the use of an FTP server.
Easy to Install	Installation in minutes, with just a web browser, CLI or automatic configuration. Some competitive products require burdensome editing of multiple files to complete a basic installation.

Configurable Event Management and Logging

The SX II generates a large variety of device and user events including: device operation, device management changes, security, user activity and user administration. These can be selectively delivered to: SNMP, Syslog, email (SMTP) as well as stored on the SX II in the audit log. Support for SNMP v2 and v3,

Raritan CommandCenter® Management and Scalability

Raritan’s CommandCenter Centralized Management

Like the rest of the Dominion series, Dominion SX II features complete CommandCenter Secure Gateway integration, allowing users to consolidate all Dominion SX II and other Raritan devices into a single logical system, accessible from a single IP address, and under a single remote management interface.

Manage Hundreds of Serial Devices

When deployed with CommandCenter Secure Gateway, hundreds of Dominion SX II devices (and thousands of serial devices) can be centrally accessed and managed.

Single IP Address for Administration and Device Connection

Administrators and users can connect to a single IP address via CommandCenter Secure Gateway to manage the SX II or access the attached serial devices. This connection can be via web browser or through SSH. Option for SX II at-the-rack access while under CC-SG management.

Bulk Firmware Upgrades

Administrators can schedule firmware upgrades (and other operations) for multiple SX II devices from CommandCenter.

Remote Power Control via CommandCenter Secure Gateway

CommandCenter supports remote power control of Raritan PX rack PDU’s connected to serial ports on the Dominion SX II. For equipment with multiple power feeds, multiple power outlets can be associated together to switch equipment on or off with a single click of the mouse.

In This Chapter

Package Contents. 11

SX II Models 12

SX II Appliance Diagram. 12

Supported Serial Devices. 13

Access Clients. 13

iOS Support. 14

Package Contents

Each ships as a fully-configured stand-alone product in a standard 1U 19" rackmount chassis.

The package includes -

- 1 - appliance
- 1 - Rackmount kit
- 2 - AC power cords
- 1 - Set of 4 rubber feet (for desktop use)
- 1 - Quick Setup Guide

SX II Models

The following models are available.

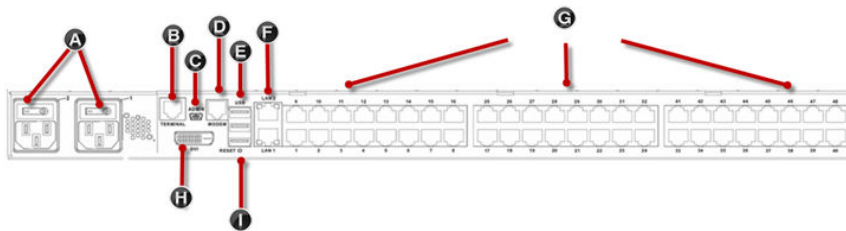
Models with an M include an internal modem in addition to the standard features that are provided on all models. For a list of standard features, see [Features and Benefits](#) (on page 6).

- DSX2-4 and DSX2-4M - 4-port serial console server
- DSX2-8 and DSX2-8M - 8-port serial console server
- DSX2-16 and DSX2-16M - 16-port serial console server
- DSX2-32 and DSX2-32M - 32-port serial console server
- DSX2-48 and DSX2-48M - 48-port serial console server

Model size, weight, temperature and other specifications are found in [SX II Dimensions and Physical Specifications](#) (on page 48).

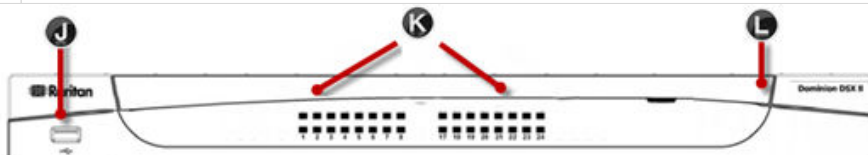
SX II Appliance Diagram

Note the image shown here is an example, so it may be different from your model.



Appliance diagram key

A	AC power outlet(s) 1 and 2 with independent power on/off switches
B	Terminal port/console port
C	Admin Mini-USB port
D	Modem port (based on model)
E	3 USB ports
F	LAN1 and LAN2 ports
G	Server ports
H	DVI-D port
I	Reset button



Appliance diagram key	
J	USB port
K	LED port indicators
L	Power status (Note 48 port models have their power status located above the front-panel USB port.)

Supported Serial Devices

- Routers
- LAN switches
- Rack PDUs
- Wireless modems
- Telecom modems
- Windows servers
- UNIX servers
- Linux servers
- Virtual hosts
- Firewalls

Access Clients

HTML Serial Client (HSC)

HSC is the default client and will launch when you connect to a serial device. The HSC is an HTML-based, Java-free Serial Client.

See [HTML Serial Console \(HSC\) Help](#) (on page 37)

Direct Port Access

Direct Port Access allows users to bypass having to use the 's Login dialog and Port Access page.

This feature also provides the ability to enter a username and password directly to proceed to the target, if the username and password is not contained in the URL.

Command Line Interface (CLI)

Connect using CLI via SSH or Telnet.

See Command Line Interface Help for SX II

Admin-Only Interface

Access the Admin Client at: <https://<SX2 IP/Hostname>/admin>.

The Admin Client does not allow target access. Use the Admin Client to perform administrator functions without using Java.

All admin functions available in the Remote Console are available in the Admin-Only Interface.

iOS Support

SX II supports iOS SSH apps, both with and without VPN, to allow users access via iOS mobile devices.

See [Access SX II Using an iOS Device](#) (on page 25)

Configure for the First Time

can be configured from the Remote Console or command line interface (CLI).

In This Chapter

Default Login Information.	15
Initial Configuration from the Remote Console.	15
Initial Configuration Using Command Line Interface (Optional).	16

Default Login Information

appliances are shipped with the following defaults. Use the defaults when you initially access .

- IP address - 192.168.0.192
- IP netmask - 255.255.255.0
- Username - admin (all lowercase)
- Password - raritan (all lowercase)

Important: For backup and business continuity purposes, it is strongly recommended you create a backup administrator username and password. Keep the information in a secure location.

Initial Configuration from the Remote Console

1. After you have installed the at the rack, connect the power cord(s) between the power connector on the and an external, AC or DC power source (depending on your model).
2. You can connect the second power connector to a backup power source.

Use the power cords that came with .



3. Connect an external modem to a USB port on the SX2 (optional). See [Connect and Enable Global Access to an External Broadband Modem](#) [Online Help](#)
4. Connect your target devices or other serially managed devices to the server ports on the .



Use a standard Cat5 cable to connect your target device to an available port on the back of .

Note: Check the pin definition of the RJ45 port on the target. It should match the pin definition on .

Or

If needed, connect a Raritan Nulling Serial Adapter to the serial port on your target, then plug a standard Cat5 cable into the adapter. Connect the other end of the cable to an available port on the back of .

5. Flip the power switch(s) to turn on.



Next, connect to your network and configure your network settings for the first time.

See [Initial Configuration Using Command Line Interface \(Optional\)](#) (on page 16) or Configure Network Settings from the Remote Console.

Connect a Laptop to Using a Cross-Over Cable (Optional)

The first time you configure , if you are connecting from the LAN port on laptop to the LAN1 port on using a crossover cable, do the following -

1. Use cross-over cable to connect between LAN1 and the laptop LAN port.
2. Set the Static IP of the LAN port that is connected to to 192 . 168 . 0 . 191 and Network Mask to 255 . 255 . 255 . 0.
3. Launch your browser and access via 192 . 168 . 0 . 192.

Initial Configuration Using Command Line Interface (Optional)

Ensure that the port settings (serial communication parameters) are configured as follows:

- Bits per Second (BPS) = 115200
- Data bits = 8
- Parity = None
- Stop bits = 1
- Flow Control = None

► To configure for the first time using CLI:

1. Connect to using any one of the following -
 - Connect a computer to the Terminal port for serial console access.



- Connect a keyboard tray or KVM console to the DVI-D and USB ports.



- Connect a laptop to the MiniUSB Admin port.



2. The emulator interface opens once you are connected to . Press the Enter key on your keyboard.
3. When the Login prompt appears, enter the default username `admin` and password `raritan`. Use all lowercase letters.
4. You are prompted to change the default password. When creating a password via CLI, it cannot begin with a space or end with a space. This does not apply to creating passwords in using the Remote Console.

By default, the network is configured for a static IP address.

5. At the `admin >` prompt, enter `config` and at the next prompt enter `network`.

6. At the `admin > config > network >` prompt, enter `interface if lan1 ipauto none ip <ip address> mask <mask> gw <gateway ip address>`

To use DHCP, enter `interface if lan1 ipauto dhcp`

7. Give the device a name to help identify it.

Enter `"name devicename <DSX2 name>"`.

Up to 32 characters are supported for the name. Spaces and special characters not supported.

8. At the `admin > config > network` prompt, enter `quit` to get into upper menu `admin > config`, then enter `time`.

9. At the `admin > config > time >` prompt, set the date and time on the .

- Enter `timezonelist` and find the number code that corresponds to your time zone.
- Enter `clock tz <timezone code> date <date string> time <time string>` where `<timezone code>` is the time zone code, `<time string>` is the current time in "HH:MM:SS" format and `<date string>` is the current date in "YYYY-MM-DD" format (quotes included, uses 24-hour time).

Example: `clock tz 9 date "2015-08-15" time "09:22:33"`

10. Enter `top` to return to the top level prompt.

11. Next, enter `config` and then enter `ports` at the next prompt.

You can now configure each server port that has a target device connected to it.

12. Enter `config port` then hit `?` to see the port parameters.

For example:

```
config port 1 name cisco1700 bps 9600 parity odd flowcontrol none
emulation vt100
```

You can also use port ranges or the wildcard asterisk `*`, such as `config port * bps 115200`

This configures all ports for a communications speed of 115200 bps.

Or

```
config port 3-7 bps 115200
```

This configures ports 3 through 7 for 115200 bps.

Or

```
config port 1,2,7-9 bps 115200
```

This configures ports 1, 2, 7 through 9 for 115200 bps.

Repeat this step for each port with a device connected to it.

13. When done, enter `top` to return to the top level prompt.

Set Terminal Emulation on a Target

The setting for terminal emulation on is a property associated with the port settings for a particular target device.

Ensure that the settings for terminal emulation in the client application, such as Telnet or SSH, are capable of supporting the target device.

Ensure that the encoding in use on the host matches the encoding configured for the target device.

For example, if the character set on a Sun™ Solaris™ server is set to ISO8859-1, the target device should also be set to ISO8859-1.

Ensure that the terminal emulation on the target host connected to serial port is set to VT100, VT220, VT320 or ANSI.

On most UNIX® systems, `export TERM=vt100 (or vt220|vt320|ansi)` sets the preferred terminal emulation type on the UNIX target device. So, if the terminal type setting on a HP-UX® server is set to VT100, the Access Client should also be set to VT100.

Set the CLI Escape Sequence

The escape key sequence is user-configurable and can be configured per port.

The escape sequence is programmable per port because different target operating systems and host applications may trap different escape key sequences.

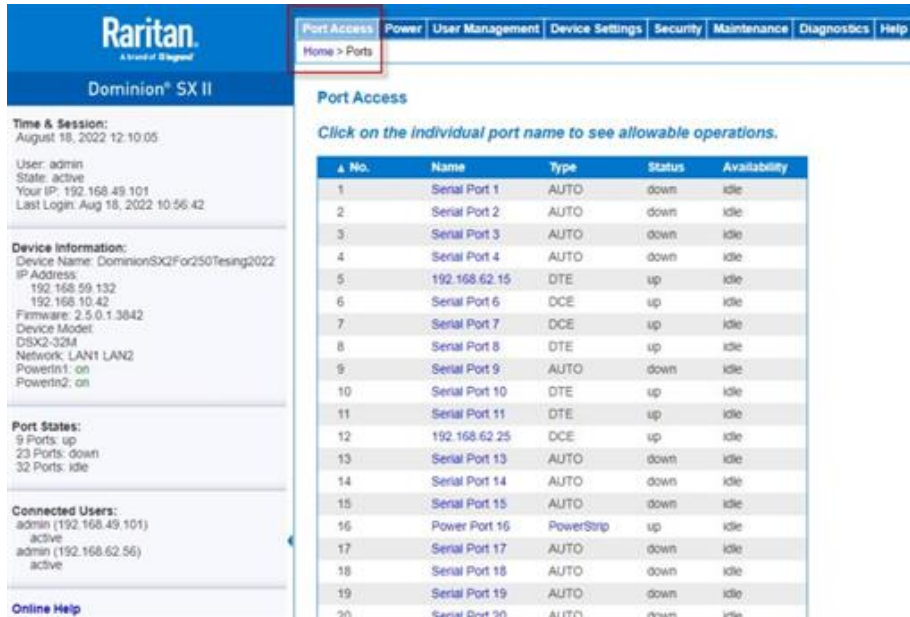
Ensure the default escape sequence set on the server does not conflict with a key sequence required by either the access application or the host operating system.

The console sub-mode should be displayed when the default escape key sequence `^]` is pressed.

Raritan recommends that you *do not* use `[` or `Ctrl-[`. Either of these may cause unintended commands, such as invoking the Escape Command unintentionally. This key sequence is also triggered by the arrow keys on the keyboard.

Access and Use Remote Console Features

The Remote Console is a browser-based interface accessed when you log in to via a network connection. See. [Log In to and HSC](#) (on page 23)



Administrator Functions in the Remote Console

Administrators perform configuration and maintenance functions from the Remote Console, such as configuring network access, adding and managing users, managing device IP addresses and so on.

Administrators can also use a version of the Remote Console that does not include any target access. See [Log In to SX II Admin-Only Interface](#) (on page 25).

End User Functions in the Remote Console

From the Remote Console, end users access targets, change passwords and so on. End users can choose HTML Serial Client. See [HTML Serial Console \(HSC\) Help](#) (on page 37)

Note that these functions can also be performed via command line interface.

In This Chapter

Allow Pop-Ups.	20
Installing a Certificate.	20
Log In to and HSC.	23
Security Warnings and Validation Messages.	24
Log In to SX II Admin-Only Interface.	25

Access SX II Using an iOS Device.	25
Change Your Password from the Remote Console.	26
Port Access Page.	27
SX II Left Panel.	28
Port Action Menu Options - Connect, Disconnect, Power On, Power Off and Power Cycle Targets.	29
Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets.	33
HTML Serial Console (HSC) Help.	37

Allow Pop-Ups

Regardless of the browser you are using, you must allow pop-ups in order to launch the Remote Console.

Installing a Certificate

You may be prompted by the browser to accept and validate the 's SSL certificate.

Depending on your browser and security settings, additional security warnings may be displayed when you log in to .

It is necessary to accept these warnings to launch the Remote Console. For more information, see Security Warnings and Validation Messages.

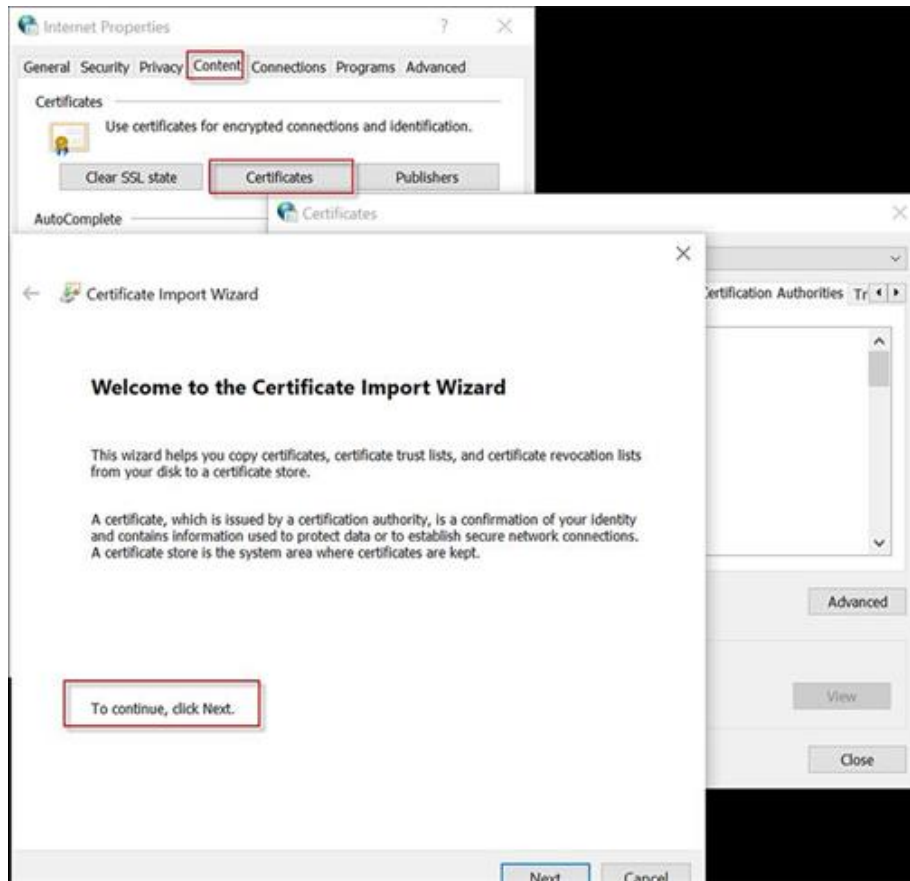
Two sample methods on how to install an SSL Certificate in the browser are provided here. Specific methods and steps depend on your browser and operating system. See your browser and operating system help for details.

Example 1: Import the Certificate into the Browser

In this example, you import the Certificate into the browser.

1. Open a browser, then log in to .
2. Click More Information on the first warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

Note: If you are not prompted by the browser, manually select the Settings or more tools for your browser, and import the certificate. The following example shows the Edge > more Tools > Internet Options method.



1. Click the Content tab.
2. Click Certificates.

The Certificate Import Wizard opens and walks you through each step.

- File to Import - Browse to locate the Certificate
- Certificate Store - Select the location to store the Certificate

3. Click Finish on the last step of the Wizard.

The Certificate is imported. Close the success message.

4. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

Example 2: Add the to Trusted Sites and Import the Certificate

In this example, the 's URL is added as a Trusted Site, and the Self Signed Certificate is added as part of the process.

1. Open an Edge browser, then select Settings > Launch the Internet Options settings by entering "Internet Options" in the search bar for Windows.
2. Click the Security tab.
3. Click on Trusted Sites.
4. Disable Protected Mode, and accept any warnings.
5. Click Sites to open the Trusted Sites dialog.

6. Enter the URL, then click Add.
7. Deselect server verification for the zone (if applicable).
8. Click Close.
9. Click OK on the Internet Options dialog to apply the changes, then close and reopen the browser.

Next, import the Certificate.

1. Open an Edge browser, then log in to .
2. Click More Information on the first Java™ security warning.
3. Click View Certificate Details on the More Information dialog. You are prompted to install the certificate. Follow the wizard steps.

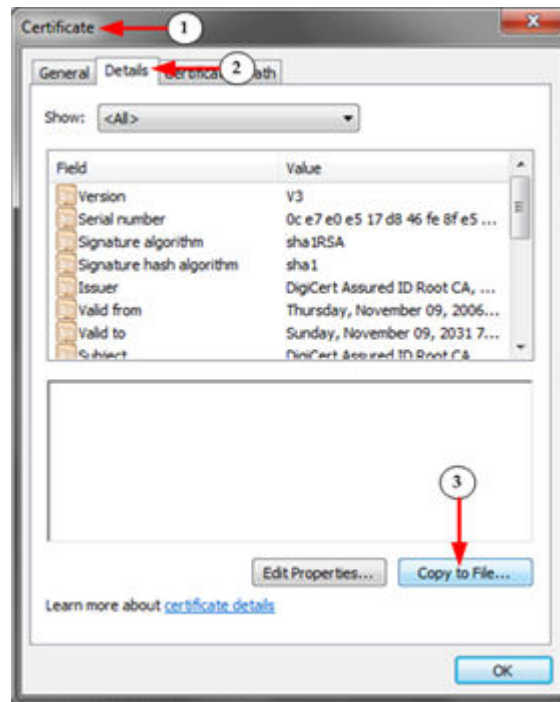
For details see, [Example 1: Import the Certificate into the Browser](#) (on page 20).

Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional)

requires an SSL certificate in either Base64-Encoded DER format or PEM format.

If you are using an SSL certificate in binary format, you cannot install it.

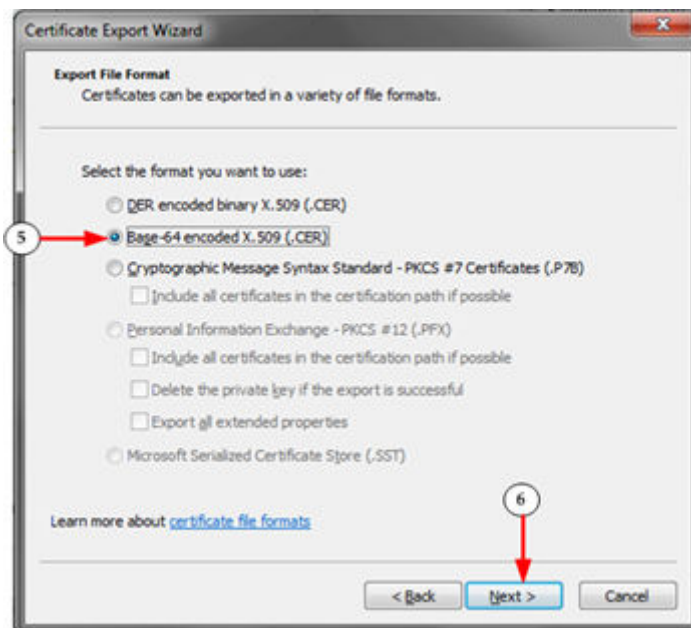
However, you can convert your binary SSL certificate.



1. Locate the DEGHKVM0001.cer binary file on your Windows machine. Double-click on the DEGHKVM0001.cer file to open its Certificate dialog.
2. Click the Detail tab.
3. Click "Copy to File..."



4. The Certificate Export Wizard opens. Click Next to start the Wizard.



5. Select "Base-64 encoded X.509" in the second Wizard dialog.

6. Click Next to save the file as a Base-64 encoded X.509.

You can now install the certificate on your .

Log In to and HSC

This login procedure gives you access to the default HTML Serial Client (HSC) for target connections.

1. Launch a supported web browser.
2. Enter the HTTP, HTTPS or DNS address provided to you by your Administrator.

Note: You are always redirected to the IP address from HTTP to HTTPS.

3. Enter your username and password, then click Login.
4. Accept the user agreement (if applicable).
5. If security warnings appear, accept and/or allow access.

Security Warnings and Validation Messages

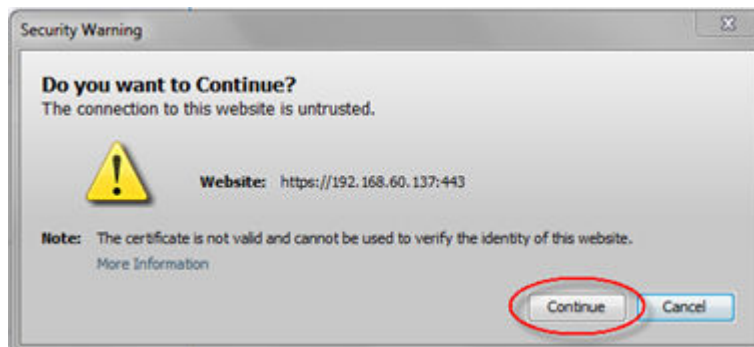
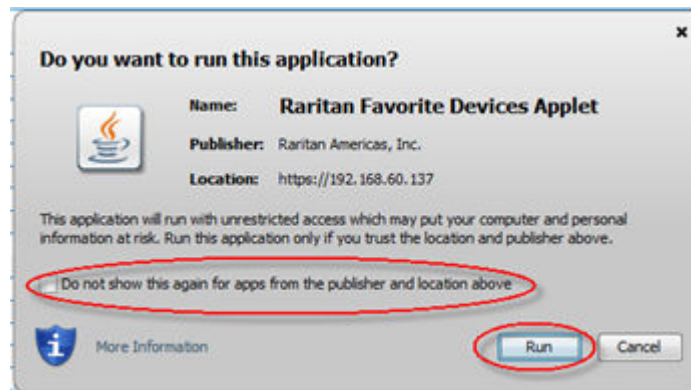
When logging in to , security warnings and application validation messages may appear. It is based on your browser and security settings: See [Additional Security Warnings](#) (on page 25)

Java Validation and Access Warning

When logging in to using the Java-based client, Java prompts you to validate , and to allow access to the application.

Installing an SSL certificate in each device is recommended to reduce Java warnings, and enhance security.

See SSL Certificates



Additional Security Warnings

Even after an SSL certificate is installed in the , depending on your browser and security settings, additional security warnings may be displayed when you log in to .

It is necessary to accept these warnings to launch the Remote Console.

Reduce the number of warning messages during subsequent log ins by checking the following options on the security and certificate warning messages:

- In the future, do not show this warning
- Always trust content from this publisher

Log In to SX II Admin-Only Interface

You cannot connect to targets using the admin-only interface.

1. Launch a supported web browser.
2. Enter the HTTP, HTTPS or DNS address provided to you by your Administrator, followed by /admin.
For example: IP Address/admin

Note: You are always redirected to the IP address from HTTP to HTTPS.

3. Enter your username and password, then click Login.
4. Accept the user agreement (if applicable).
5. If security warnings appear, accept and/or allow access.

Access SX II Using an iOS Device

You can access SX II using your iOS device when certificates are properly installed on the device. iOS requires that the certificate and all certificates in the certificate chain be installed on the device to connect properly. This can be done by emailing the certificates to the iOS device. When all certificates are installed, the Profile will be listed as Verified. If the profile is "Not Verified" for any reason, or if the certificate is not signed with the IP or DNS entry used to connect to the SX II, the connection will fail.

The following procedure shows how to generate and install valid certificates with openssl.

► *To access SX II using an iOS device:*

1. Create a simple CA.

```
openssl genrsa -out localCA.key 2048
```

```
openssl req -x509 -sha256 -new -key localCA.key -out localCA.cer -days  
356 -subj /CN="Local CA"
```

2. Generate key,CSR, and cer for SX II.

```
openssl genrsa -out sx2.key 2048
```

```
openssl req -new -out sx2.req -key sx2.key -subj /CN=<SX IP ADDRESS>
```

```
openssl x509 -req -sha256 -in sx2.req -out sx2.cer -CAkey localCA.key  
-CA localCA.cer -days 355 -CAcreateserial -CAserial serial
```

3. Email the localCA.cer and sx2.cer files created to an email account that can be opened on the iOS device.
4. Open the email through the iOS device mail app and click on the localCA.cer to install the certificate. Follow prompts and trust the certificate.
5. Repeat for the sx2.cer.
6. Install the sx2.key and then the sx2.cer onto the SX II.
7. Reboot the SX II.
8. Use any browser on the iOS device to connect to the SX II. If there is any error in the certificate or it is not trusted, the javascript client will immediately disconnect when attempting to connect.

Change Your Password from the Remote Console

Note: You can also update passwords using command line interface. See [Change Your Password Using CLI](#).

- To change your password, open the Change Password page by selecting User Management > Change Password.

A confirmation that the password was successfully changed is displayed after you change it.

If strong passwords are in use, this page displays information about the format required for the passwords.

For more information, see [Strong Passwords](#).

Port Access Power User Management Device Settings

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

OK Cancel

Important: If the administrator password is forgotten, must be reset to the factory default from the Reset button on the rear panel and the initial configuration tasks must be performed again.

Port Access Page

After a successful login, the Port Access page opens listing all ports along with their status and availability.

Note that target access is not enabled in the Admin-Only Interface version of the Remote Console.

Raritan
A brand of Legrand

Port Access | Power | User Management | Device Settings | Security | Maintenance | Diagnostics | Help

Home > Ports

Port Access

Click on the individual port name to see allowable operations.

No.	Name	Type	Status	Availability
1	Serial Port 1	AUTO	down	idle
2	Serial Port 2	AUTO	down	idle
3	Serial Port 3	AUTO	down	idle
4	Serial Port 4	AUTO	down	idle
5	192.168.62.15	DTE	up	idle
6	Serial Port 6	DCE	up	idle
7	Serial Port 7	DCE	up	idle
8	Serial Port 8	DTE	up	idle
9	Serial Port 9	AUTO	down	idle
10	Serial Port 10	DTE	up	idle
11	Serial Port 11	DTE	up	idle
12	192.168.62.25	DCE	up	idle
13	Serial Port 13	AUTO	down	idle
14	Serial Port 14	AUTO	down	idle
15	Serial Port 15	AUTO	down	idle
16	Power Port 16	PowerStrip	up	idle
17	Serial Port 17	AUTO	down	idle
18	Serial Port 18	AUTO	down	idle
19	Serial Port 19	AUTO	down	idle
20	Serial Port 20	AUTO	down	idle

Ports are numbered from 1 up to the total number of ports available for the . For example, Port_1 - Port_48, Port_1 - Port_32.

"SerialPort"_"Port #" are what make up the default name the physical port until a name is configured for the port. Once a name is designated for a port, the name stays with the port until the name is edited or SX II is factory reset.

Port type includes:

- Auto - No target connected
- DTE - DCE target is connected or this port is forced to be configured as DTE.
- DCE - DTE target is connected or this port is forced to be configured as DCE.

Sort by Port Number, Port Name, Status (Up and Down), and Availability (Idle, Connected, Busy, Unavailable, and Connecting) by clicking on the column heading.

Click on any port that listed and marked as Available to open its Port Action menu so you can then manage the target. For more information, see [Port Action Menu Options - Connect, Disconnect, Power On, Power Off and Power Cycle Targets](#) (on page 29).

Note that in the Remote Console, you can also quickly access a powerstrip's page from the Port Access page by clicking on the Powerstrip link in the Type column.



SX II Left Panel

The left panel contains the following information.

Note that some information is conditional - meaning it is displayed based on your role, features being used and so on. Conditional information is noted here.

Information	Description	Displayed when?
Time & Session	The date and time the current session started	Always
User	Username	Always
State	The current state of the application, either idle or active. If idle, the application tracks and displays the amount time the session has been idle.	Always
Your IP	The IP address used to access .	Always
Last Login	The last login date and time.	Always
Under CC-SG Management	The IP address of the CC-SG device managing the .	When is being managed by CC-SG.
Device Information	Information specific to the you are using.	Always
Device Name	Name assigned to the you are accessing.	Always
IP Address	The IP address of the you are accessing.	Always
Firmware	Current version of firmware installing on the .	Always
Device Model	The model of the you are accessing.	Always
Network	LAN1, or LAN1 and LAN2 if you are in dual LAN mode.	Always
PowerIn1	Status of the power 1 outlet connection. Either on or off, or Auto-detect off	Always
PowerIn2	Status of the power 2 outlet connection. Either on or off, or Auto-detect off	Always
Port States	The statuses of the ports being used by - up, down, idle.	Always
Connected Users	The users, identified by their username and IP address, who are currently connected to .	Always
Online Help	Links to online help.	Always
FIPS Mode	FIPS Mode: EnabledSSL Certificate: FIPS Mode Compliant	When FIPS is enabled

Port Action Menu Options - Connect, Disconnect, Power On, Power Off and Power Cycle Targets

Once you log in via a web browser, the Port Access page displays. For more information on the Port page, see [Port Access Page](#) (on page 27).

From the Port Access page, use the Port Action menu to connect, disconnect, or control power of targets and power strips that are connected to .

Once connected, you can manage a target with Serial Client, HSC See: [HTML Serial Console \(HSC\) Help](#) (on page 37)

Note that you must have permissions to a target or power strip in order to access it.

► *To access the Port Action menu for a target or power strip:*

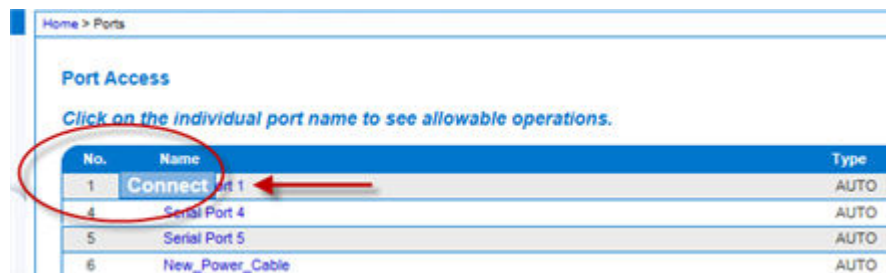
1. Hover your mouse over a target's port name in the list and click on your mouse.

The Port Action menu appears.

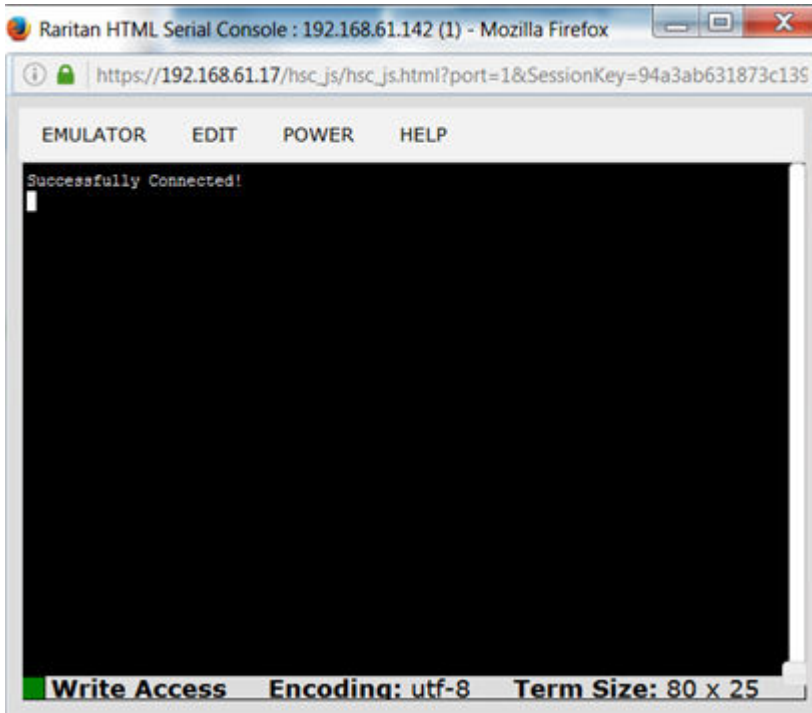
Note that only currently available options, depending on the port's status and availability, are listed in the Port Action menu.

2. Choose the desired menu option for that port to execute it.

- [Connect to a Target](#) (on page 30)
- [Disconnect from a Target](#) (on page 31)
- [Power On a Target](#) (on page 31)
- [Power Off a Target](#) (on page 32)
- [Power Cycle a Target](#) (on page 32)



You can then connect using the Serial Client. When you connect to a target, the serial client opens in a new window. This screenshot shows an HSC connection.



Alternatively, you can connect via Direct Port Access, if is configured for Direct Port Access.

Note that you can also connect to targets via command line interface. See [Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets](#) (on page 33).

Connect to a Target

Creates a new connection to the target device.

From the Remote Console, HSC opens in a new window and you manage the target from there.

If you are connected to the from the Local Console port, you access the target via command line interface. See [Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets](#) (on page 33).

Port Access

Click on the individual port name to see allowable operations.

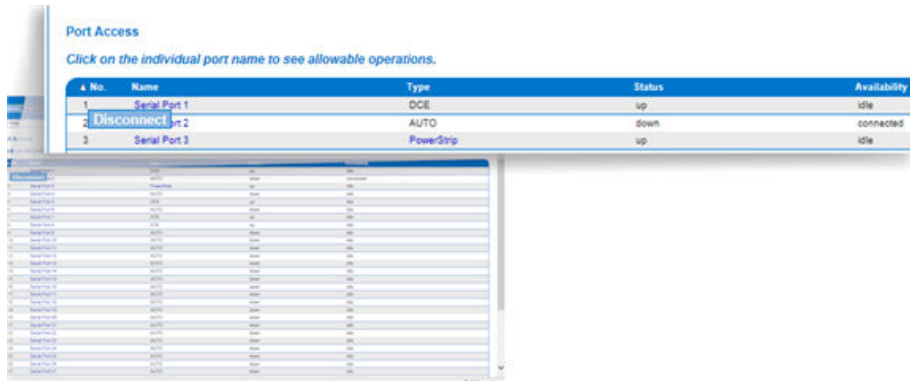
▲ No.	Name	Type	Status	Availability
1	Connect Serial Port 1	AUTO	down	idle
2	Serial Port 2	DCE	up	idle
3	Serial Port 3	AUTO	down	idle
4	Serial Port 4	AUTO	down	idle
5	Serial Port 5	AUTO	down	idle
6	Serial Port 6	AUTO	down	idle

Disconnect from a Target

Once connected to a target, the Disconnect menu option is available in the Port Action menu.

Clicking on the Disconnect option disconnects from a target, and closes the HSC window. You can also click the X icon on the window or use the Exit menu option.

See [Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets](#) (on page 33).

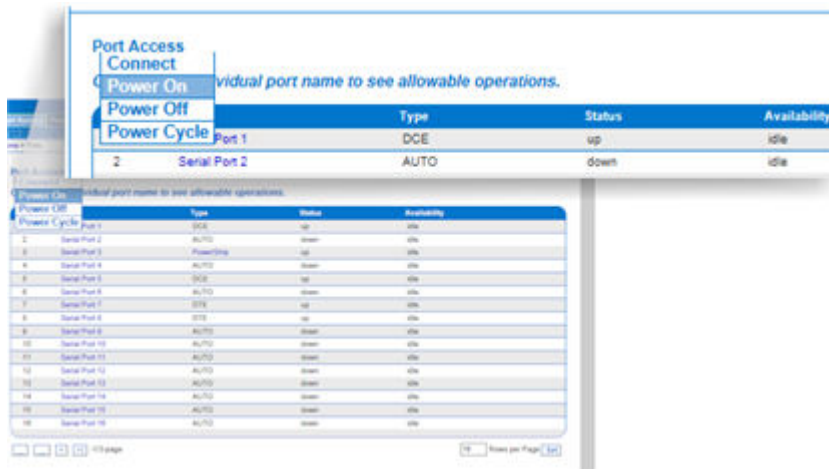


Power On a Target

Power on the target from the Remote Console through the associated outlet.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

You can also perform these actions through HSC, and command line interface. See [HTML Serial Console \(HSC\) Help](#) (on page 37), and [Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets](#) (on page 33).



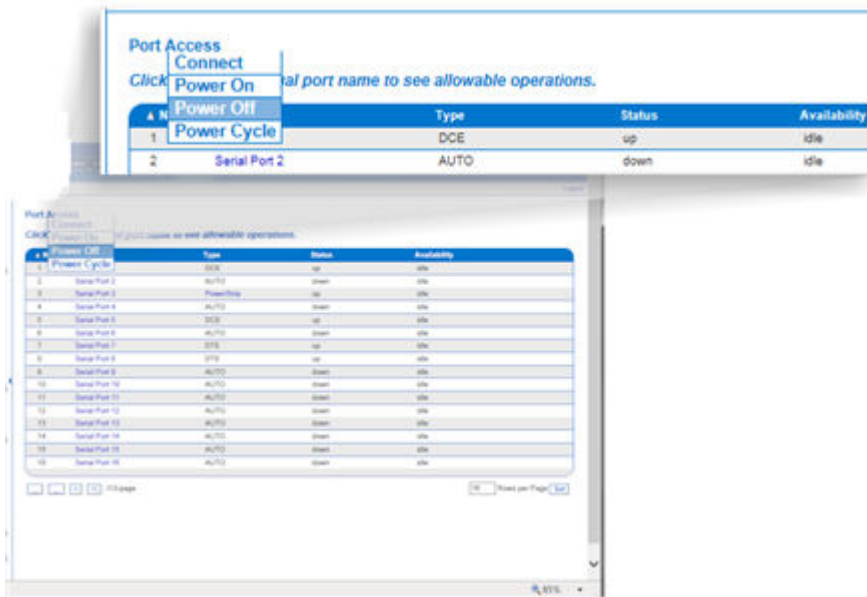
Power Off a Target

Power off the target through the associated outlet.

This option is visible only when -

- there are one or more power associations to the target or power strip
- you have permission to manage the power

You can also perform these actions through HSC, and command line interface. See [HTML Serial Console \(HSC\) Help](#) (on page 37), and [Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets](#) (on page 33).



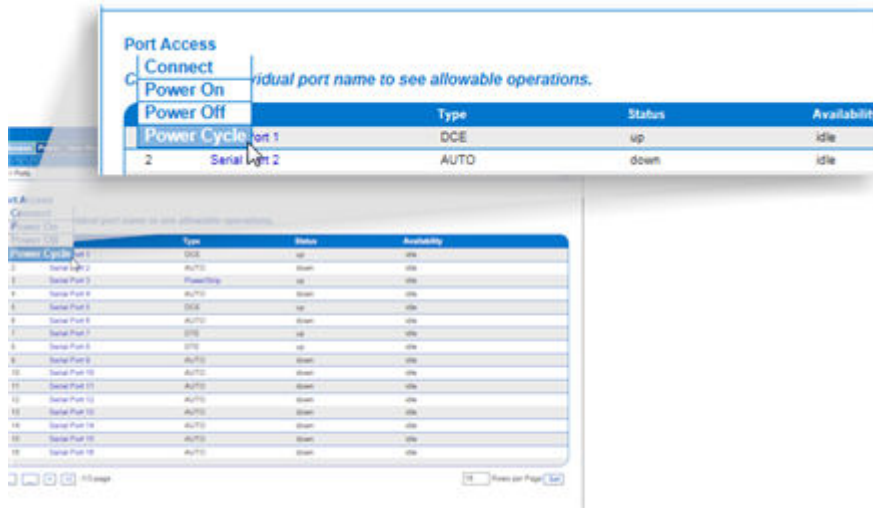
Power Cycle a Target

Power cycling allows you to turn a target off and then back on through the outlet it is plugged into.

This option is visible only when -

- The power strip is connected to SX II and configured properly.
- There are one or more power associations to the target.
- You have permission to manage the power.

You can also perform these actions through HSC, and command line interface. See [HTML Serial Console \(HSC\) Help](#) (on page 37), and [Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets](#) (on page 33).



Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets

Before connecting to a target, the terminal emulation and escape sequence must be configured. See [Set Terminal Emulation on a Target](#) (on page 17) and [Set the CLI Escape Sequence](#) (on page 18).

Connect the SX II While at the Rack

While at the rack, do one of the following depending on your needs -

- Connect a computer to the Terminal port with a CAT-5 cable and Raritan Adapter ASCSDB9F.



- Connect a keyboard tray or KVM console to the DVI-D and USB ports.



- Connect a laptop to the Mini-USB Admin port.



Note that connecting to the Local Console via the Local port is an independent access path to each connected target device.

Video Resolution

The default, Local Console port video resolution is 1024x768@60.

By default, monitors are typically set to the highest resolution they support.

Once a monitor is connected to the Local Port DVI, retrieves EDID information from the monitor, including its native, preferred resolution. uses the monitor's preferred, native resolution as long as it is a resolution that supports. If it is not, switches to a resolution it supports and that most closely matches the monitor's resolution.

For example, if a monitor with a native resolution of 2048x1600@60Hz is connected to , detects that it is not an supported resolution and selects a resolution it does support, such as 1280x1024@60Hz.

Note that you can connect to targets using the Remote Console and manage them using HTML serial console. See [HTML Serial Console \(HSC\) Help](#) (on page 37) and [Port Action Menu Options - Connect, Disconnect, Power On, Power Off and Power Cycle Targets](#) (on page 29) .

Connect Commands

Connect to a port using port number or port name. Use double quotes around port names that contain space symbols. For example: "Serial Port 1".

```
admin > connect <port number>
```

OR

```
admin > connect <port name>
```

Port Sub-Menu Commands

The port sub-menu can be reached using the escape key sequence.

Clear history buffer for this port.

```
admin > [portname] > clearhistory
```

Close this target connection. When a target is disconnected, the appropriate disconnect message appears.

```
admin > [portname] > close, quit, q
```

Display the history buffer for this port.

```
admin > [portname] > gethistory
```

Get write access for the port.

```
admin > [portname] > getwrite
```

Return to the target session.

```
admin > [portname] > return
```

Send a break to the connected target.

```
admin > [portname] > sendbreak
```

Lock write access to this port.

```
admin > [portname] > writelock
```

Unlock write access to this port.

```
admin > [portname] > writeunlock
```

Query Power status of this port.

```
admin > [portname] > powerstatus
```

Toggle Power On/Off of this port.

```
admin > [portname] > powertoggle
```

Power on the target.

```
admin > [portname] > poweron
```

Power off the target.

```
admin > [portname] > poweroff
```

Power cycle the target.

```
admin > [portname] > powercycle
```

Command Line Interface Protocols

- SSH (Secure Shell) via IP connection
- Telnet via IP connection
- Local Console via the Local Port and Mini-USB port
- Terminal port

If has an internal modem and console mode is enabled, the modem interface can also be accessed from CLI.

Many SSH/TELNET applications are available such as PuTTY, SSH Client and OpenSSH Client. These can be located and downloaded from the Internet.

Command Line Interface Partial Searches

Enter the first few characters of command and press the Tab key on your keyboard in order to locate a specific command.

The command line interface (CLI) completes the entry if the characters form an exact match.

For example entering

```
admin > Config > us
```

and then pressing the Tab key, returns the result `users`.

If an exact match is not found, all of the commands at the same level the CLI hierarchy that are potential matches are listed.

For example, entering

```
admin > Config > User > add
```

and then pressing the Tab key, returns results for `addgroup` and `adduser`.

If needed, enter additional text to make the entry unique and press the Tab key to complete the entry. Alternatively, use a command from the list.

Command Line Interface Tips

- When commands are displayed as a list, they are in alphabetical order.
- Commands are not case sensitive.
- Commands without arguments default to show current settings for the command.
- A command's parameters are usually parameter-value pairs in which the parameter name is followed by a space and the value.
- Typing a question mark (?) after a command displays help specific to the command.

Command Line Interface Shortcuts

- Press the Up arrow key to display the last entry.
- Press Backspace to delete the last character typed.
- Press Ctrl + C to terminate a command or cancel a command if you typed the wrong parameters.
- Press Enter on your keyboard to execute the command.
- Press Tab on your keyboard to complete a command. Tab also completes parameters and values (if the value is part of an enumerated set).

Command Line Interface High-Level Commands

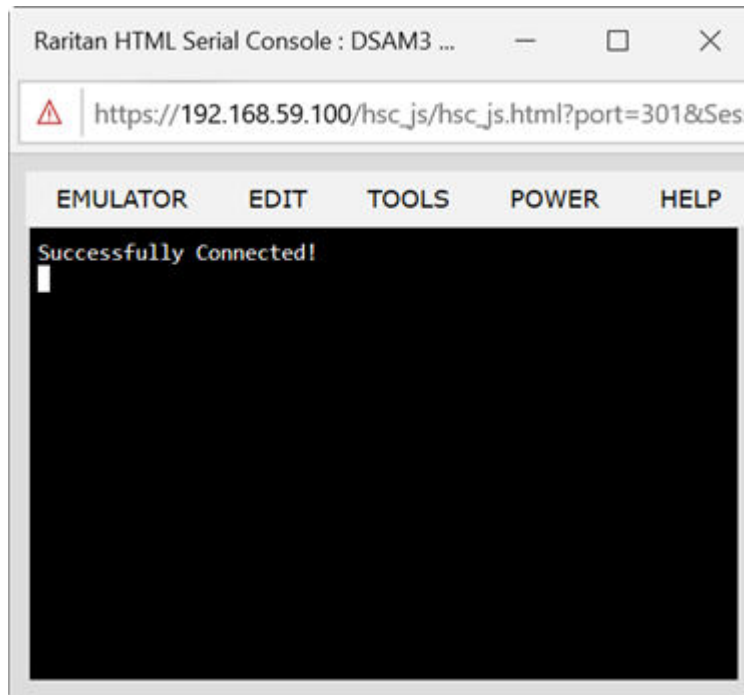
The CLI is menu based. Some commands move to a menu with a different command set.

The following common commands can be used at all levels of the command line interface (CLI):

- `top` - Return to the top level of the CLI hierarchy, or the `username` prompt.
- `history` - Displays the last 200 commands the user entered into the CLI.
- `logout` - Logs the user out of the current session.
- `quit` - Moves the user back one level in the CLI hierarchy.
- `help` - Displays an overview of the CLI syntax.

HTML Serial Console (HSC) Help

You can connect to serial targets using HSC. HSC is supported with several Raritan products that offer serial connections. Not all products support all HSC features. Differences are noted.



Emulator

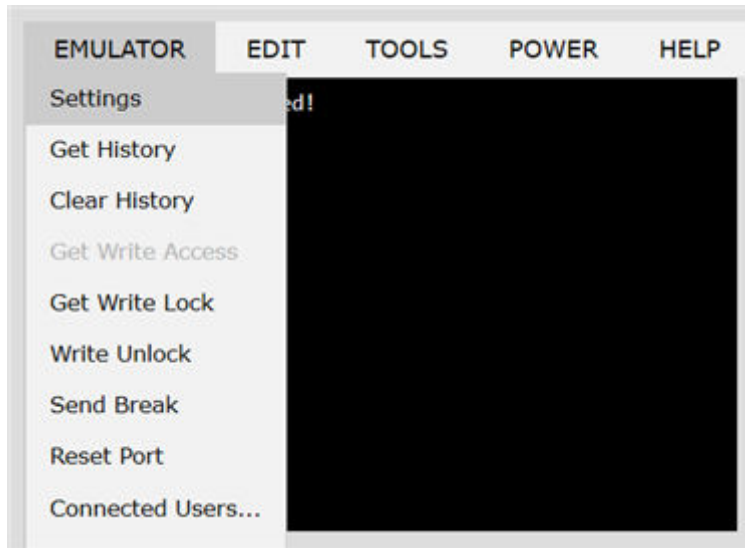
IMPORTANT: HSC sessions are affected by the Idle Timeout.

If you have not changed the Idle Timeout setting from the default, your session could be closed automatically if it exceeds the Idle Timeout period.

Change the default Idle Timeout setting and then launch the HSC. See Login Limitations for details on changing the Idle Timeout setting.

Access Emulator Options

1. Select the Emulator drop-down menu to display a list of options.



Settings

Note:

KX3 administrators can set Terminal emulation settings in Setup > Serial Port Configuration.

KX4-101 administrators can set terminal emulation settings in DSAM Serial Ports > Settings.

SX2 administrators can set terminal emulation settings in Device Settings > Port Configuration.

1. Choose Emulator > Settings. The Terminal Properties dialog displays the default settings.



2. Set the terminal size by selecting the number of Columns and Rows. Default is 80 by 25.
3. Set the Foreground and Background colors. Default is white on black.
4. Set the Font size. Default is 11.
5. Set the Scrollback number to indicate the number of lines available for scrolling.
6. Choose one of the following from the Encoding drop-down menu:
 - UTF-8
 - 8-bit ascii
 - ISO-8859-1
 - ISO-8859-15
 - Shift-JIS
 - EUC-JP
 - EUC-KR
7. Choose one of the following from the Language drop-down menu:
 - English
 - Japanese
 - Korean
 - Chinese
 - Bulgarian
8. The Backspace Sends default is ASCII DEL, or you can choose Control-H from the Backspace Sends drop-down menu.
9. Click OK to save. If you changed the Language setting, the HSC changes to that language when the Display Settings window is closed.

The emulator settings are saved on a per port basis in the browser used for HSC, so make sure your browser is not set to delete history on exit.

Get History

History information can be useful when debugging, troubleshooting, or administering a target device. The Get History feature:

- Allows you to view the recent history of console sessions by displaying the console messages to and from the target device.
- Displays up to 512KB of recent console message history. This allows a user to see target device events over time.

When the size limit is reached, the text wraps, overwriting the oldest data with the newest.

Notes: History data is displayed only to the user who requested the history.

To view the Session History, choose Emulator > Get History.

Clear History

- To clear the history, choose Emulator > Clear History.

Get Write Access

Only users with permissions to the port get Write Access. The user with Write Access can send commands to the target device. Write Access can be transferred among users working in the HSC via the Get Write Access command.

To enable Write Access, choose Emulator > Click Get Write Access.

- You now have Write Access to the target device.
- When another user assumes Write Access from you:
 - The HSC displays a red block icon before Write Access in the status bar.
 - A message appears to the user who currently has Write Access, alerting that user that another user has taken over access to the console.

Get Write Lock

Write lock prevents other users from taking the write access while you are using it.

1. To get write lock, choose Emulator > Get Write Lock.
2. If Get Write Lock is not available, a request rejected message appears.

Write Unlock

To get Write Unlock, choose Emulator > Write Unlock.

Send Break

Some target systems such as Sun Solaris servers require the transmission of a null character (Break) to generate the OK prompt. This is equivalent to issuing a STOP-A from the Sun keyboard.

Only users with Write Access privileges can send a break.

To send an intentional “break” to a Sun Solaris server:

1. Verify that you have Write Access. If not, follow the instructions in the previous section to obtain write access.
2. Choose Emulator > Send Break. A Send Break Ack (Acknowledgement) message appears.
3. Click OK.

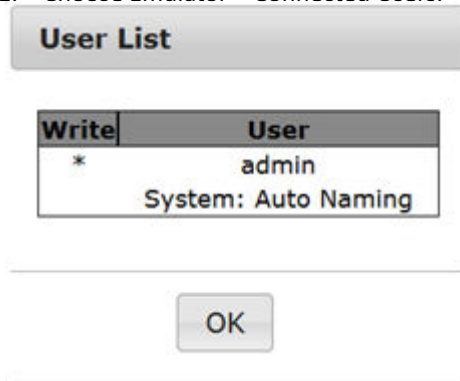
Reset Port

Reset Port resets the physical serial port on the SX2 and re-initializes it to the configured values regarding bps/bits, and so on.

Connected Users

The Connected Users command allows you to view a list of other users who are currently connected on the same port.

1. Choose Emulator > Connected Users.



2. A star appears in the Write column for the User who has Write Access to the console.

Exit

1. Choose Emulator > Exit to close the HSC.

Copy and Paste and Copy All

Data on the current visible page can be selected for copying. Copy and Paste are accessible in the HSC by right click in the terminal window. Select Copy or Paste in the context menu that appears.

To copy all text, use the Copy All option in the Edit menu.

If you need to paste a large amount of data, it is better to save the data in a file and use the Send a Text File function. Pasting a large amount of data in a browser windows can cause the browser to hang as it processes the data. See [Send Text File](#) (on page 42).

When pasting data to a port, the end of a line is sent as a carriage return.

The Cut option on the right-click menu is disabled.

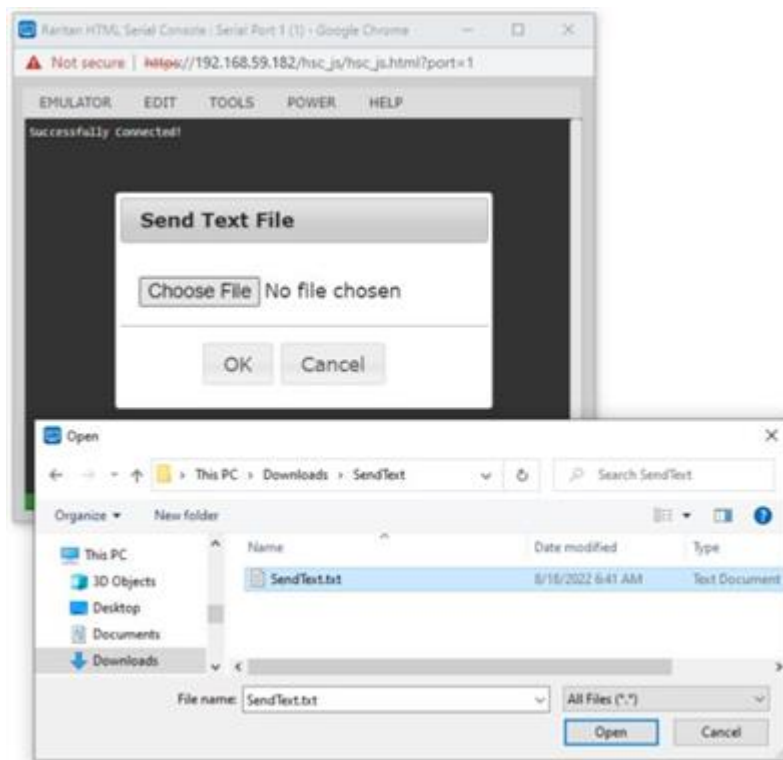
Do not use the Delete option that appears in the right-click menu of IE and some versions of Firefox. This Delete option will remove display lines entirely from the emulator window.

► *Browser-specific behaviors*

When copying from IE or Edge browsers, there are no end of line characters in the copied data. The pasted data appears to be all in one line and contains many spaces. When pasting back into a HSC window, the data may appear to be misaligned, but the data is complete.

Send Text File

1. Select Edit> Send Text File.
2. In the Send Text File dialog, click Browse to find the text file.
3. Click OK.
 - When you click OK, the selected file sends directly to the port.
 - If there is currently no target connected, nothing is visible on the screen.



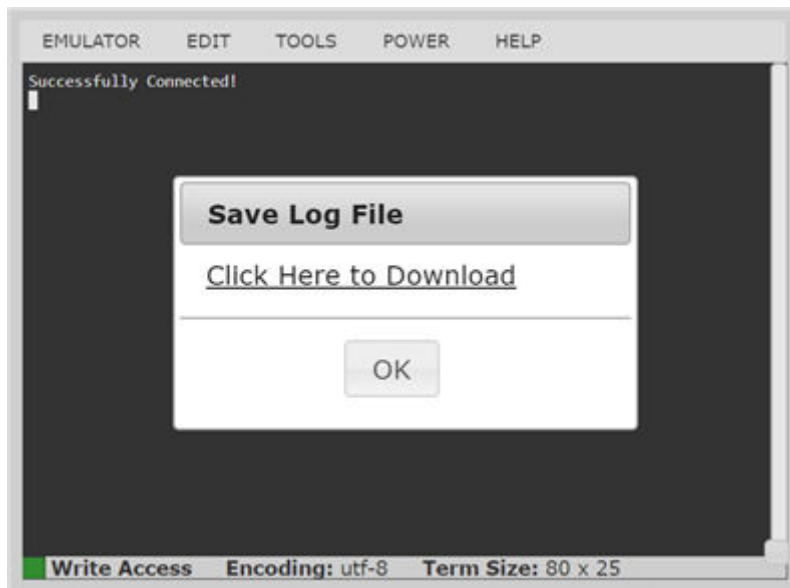
► *Note, if you are using a Mac® and/or Safari®, do the following in order to use this feature:*

1. In Safari, select Preferences.
2. Under the Security tab, select "Manage Website Settings"
3. Click on the website.
4. Select "Run in unsafe mode" from the drop-down box.
5. Restart Safari.

Tools: Start and Stop Logging

The Tools menu contains options for creating a data history file and downloading it.

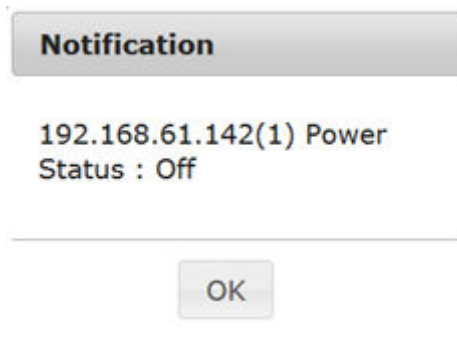
1. Choose Tools > Start Logging to start the storage of serial port data in memory.
2. Click Stop Logging to save the log file. A pop up message appears with a download link. Click to download the memory buffer into a text file.



Power Status

Power Status in HSC shows the status of the outlet the target is plugged into.

1. Choose Power > Power Status.
2. The Notification dialog shows the status of the outlet as ON or OFF. Status may also show no associated outlet, or no power permission to the port.



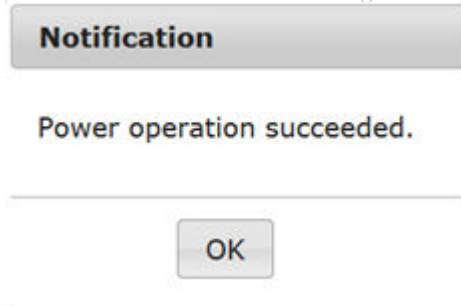


Power on a Target

Use this option to power on a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power On.
2. Click OK in the success message.

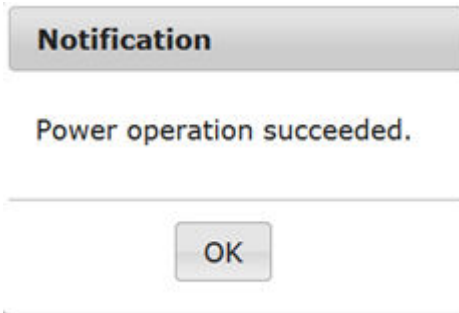


Power Off a Target

Use this option to power off a target from HSC.

This option is visible only when there are one or more power associations to the target, and when you have permission to manage the target's power.

1. Select Power> Power Off.
2. Click OK in the success message.



Power Cycle a Target

Power cycling allows you to turn a target off and then back on through the outlet it is plugged into.

This option is visible only when -

- there are one or more power associations to the target
- the target is already powered on (the port status is Up)
- you have permission to manage the target's power

1. Choose Power > Power Cycle.
2. Click OK in the success message.

Browser Tips for HSC

Some browsers have limitations that affect HSC.

- Edge & Chrome, disabling the background throttling to prevent background tabs from disconnecting after a certain amount of time. Go to `chrome://flags`, then search for "throttle". Set "Throttle Javascript timers in background" and "Calculate window occlusion on Windows" to "Disabled". Restart chrome to apply settings.
- Browser option to select certificate for authentication displayed on Edge and Chrome after session is idle for about 5 minutes, due to internal browser SSL caching and timeouts. If certificate is selected promptly, reconnection is successful. With longer idle times, authentication is not successful, and the browser should be restarted to reconnect. Issue is not observed in Firefox.
- Edge has an internal limitation on the number of websockets that are allowed to be created to a single server (6). This can be changed by modifying a registry variable as shown here : [https://msdn.microsoft.com/en-us/library/ee330736\(v=vs.85\).aspx#websocket_maxconn](https://msdn.microsoft.com/en-us/library/ee330736(v=vs.85).aspx#websocket_maxconn).
- Edge, and Safari have a limitation when connecting to IPv6 devices. Using the numerical URL will not work when it attempts to establish a websocket connection. In these browsers, use the device hostname or literal IPv6 as UNC to connect to the SX II. See https://en.wikipedia.org/wiki/IPv6_address#Literal_IPv6_addresses_in_UNC_path_names
- When using HSC in IOS Safari, the keyboard may not appear in some pages if the "request desktop website" setting is enabled. To change the setting, go to Settings > Safari > Request Desktop Website, then make sure All Websites is not selected, and the device address is not selected. You can also set this per address by clicking the "a" in Safari's URL pane when connected to the HSC port, then select "Website Settings" and make sure that "Request Desktop Website" is not selected.

Connect a Rack PDU to and Configure Power Control Options

provides the following options when connecting a Raritan PX PDU to a :

- Connect to the PX PDU Serial port.
In this configuration, access to the PX PDU is done through the PX PDU command line interface (CLI).
- Connect the to the Feature port on the PX PDU.
In this configuration, the PX PDU is managed from the interface like any other power strip.

Go to <https://www.raritan.com/support/product/px> for support on PX PDUs.

In This Chapter

Connecting the to the PX PDU Serial Port.	46
Connecting the to the PX PDU FEATURE Port.	47

Connecting the to the PX PDU Serial Port

In this configuration, after the PX is connected to the , *access the PX using the PX CLI.*

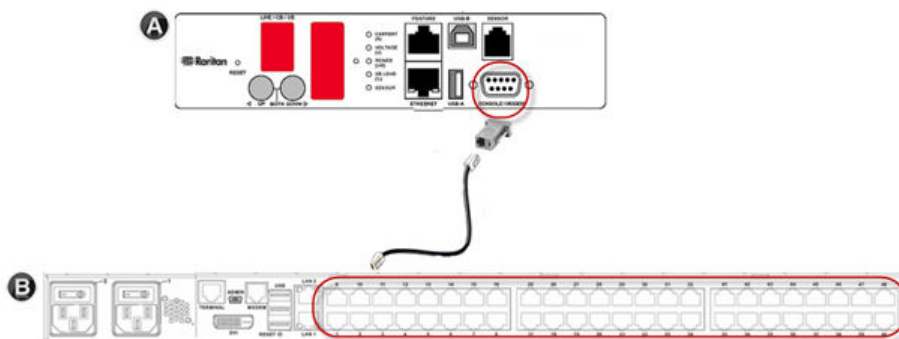
Note that the appliances used in the diagram may not match your specific models. However, the connections and ports used are the same across models.

► *To connect the to the PX:*

1. Connect an ASCSDB9F adapter to the PX2 DB9 console/modem port.

Note: The adapter is purchased from Raritan. It does not come with PX or appliances.

2. Plug a Cat5 cable into the ASCSDB9F adapter, then plug the other end of the cable in to the port on the .
3. Power on the PX (if it is not already). The command line interface (CLI) interface appears.



A	PX appliance
B	

Connecting the to the PX PDU FEATURE Port

In this configuration, the PX is managed from the interface like any other powerstrip. See Power Control.

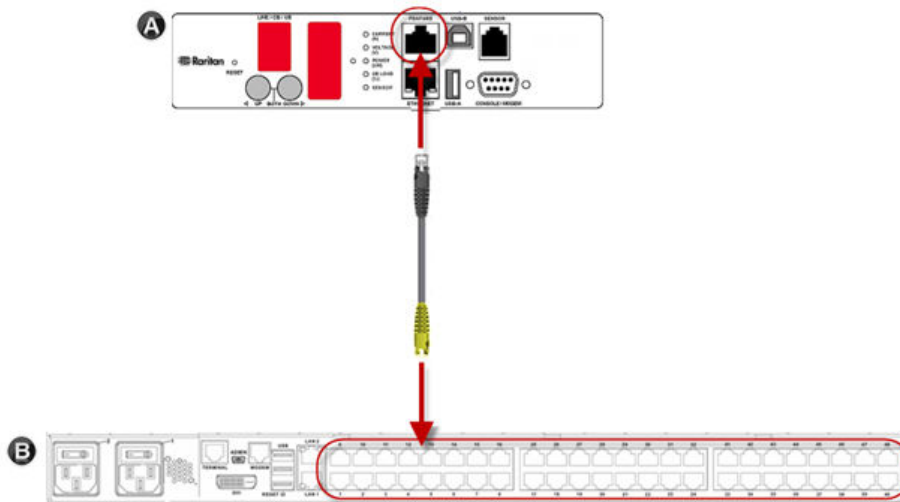
Note: Make sure that the PX PDU's Feature Port is configured to the PowerCIM setting.

Note that the appliances used in the diagram may not match your specific models. However, the connections and ports used are the same across models.

► *To connect the to the Feature port on the PX:*

1. Connect the gray end of the CSCSPCS crossover Cat5 cable into the Feature port on the PX.
2. Connect the yellow end of the CSCSPCS crossover Cat5 cable into a port on the .
3. Power on the PX (if it is not already).

You can now add the PX as a managed power strip to the . See Configure Power Strips from the Remote Console or Configure Power Strips Using CLI..



A	PX appliance
B	

Appendix A Specifications

In This Chapter

SX II Dimensions and Physical Specifications.	48
Supported Remote Connections.	48
Supported Number of Ports and Remote Users per SX II Model.	49
Maximum Number of Users Session.	49
Maximum Number of Support Users Per Port.	49
Port Access Protocol Requirements.	49
Port Pins.	51
Port Ranges.	52
Network Speed Settings.	53
Default User Session Timeouts.	54
SX II Supported Local Port DVI Resolutions.	54
Appliance LED Status Indicators.	54
Target Cable Connection Distances and Rates.	55

SX II Dimensions and Physical Specifications

Form factor	1U, rack mountable
Dimensions	17.3" W x 13.15" D x 1.73'H'; (440mm x 334mm x 44mm)
Weight	9.08 lbs; (4.12 kg)
Power	100/240VAC auto-switching: 50-60 Hz, .35A, 36-72VDC auto-switching
Max power consumption	4-Port SX: 21W 8-port SX: 21W 16-port SX: 22W 32-port SX: 23W 48-port SX: 25W
Temperatures	Operating: 0°C – 50°C. Non-Operating: 0°C – 55°C
Humidity	Operating: 20% – 85%. Non-Operating: 10% – 90%
Altitude	Operates properly at any altitude from 0 to 2,000 meters

Supported Remote Connections

Network

- 10BASE-T
- 100BASE-T
- 1000BASE-T (Gigabit) Ethernet

Protocols

- TCP/IP
- HTTP

- HTTPS
- RADIUS
- LDAP/LDAPS
- SSH
- Telnet
- TACACS+
- UDP
- SNTP

Supported Number of Ports and Remote Users per SX II Model

Model	Number of ports
-04 and -04M	4
-08 and -08M	8
-16 and -16M	16
-32 and -32M	32
-48 and -48M	48

Maximum Number of Users Session

A maximum of 200 users can access a single at the same time.

This applies to the Remote Console access, Direct Port Access and command line interface access via SSH/Telnet.

Maximum Number of Support Users Per Port

A maximum of 10 users can access the same port and the same time.

This applies to the Remote Console access, Direct Port Access and command line interface access via SSH/Telnet.

Port Access Protocol Requirements

Protocol	Port	Communication direction
HTTP	<p>Ports 80, 443 and 5000 must be open in the firewall for the appliance to operate.</p> <p>Port 80</p> <p>This port can be configured as needed. See HTTP and HTTPS Port Settings.</p> <p>By default, all requests received by the via HTTP (port 80) are automatically forwarded to HTTPS for complete security.</p> <p>The responds to Port 80 for user convenience, relieving users from having to explicitly type in the URL field to access the , while still preserving complete security.</p>	Both

Protocol	Port	Communication direction
	<p>Port 443</p> <p>This port can be configured as needed. See HTTP and HTTPS Port Settings.</p> <p>By default, this port is used for multiple purposes, including the web server for the HTML client, the download of client software onto the client's host, and the transfer of data streams to the client.</p> <p>Port 5000</p> <p>This port is used to discover other Dominion devices and for communication between Raritan devices and systems, including CC-SG for devices that CC-SG management is available.</p> <p>By default, this is set to Port 5000, but you may configure it to use any TCP port not currently in use. For details on how to configure this setting, see Network Settings.</p>	
HTTPS SSL only	<p>Port 443</p> <p>TCP port 443 must be open.</p> <p>Port 80 can be closed.</p>	Both
SSH	<p>Port 22</p> <p>TCP port 22 must be open.</p> <p>Port 22 is used for the command line interface (CLI).</p>	Both
Telnet	<p>Port 23</p> <p>TCP port 23 must be open.</p>	Both
TACACS+	<p>Port 49</p> <p>Port 49 must be open.</p>	Outgoing
RADIUS	<p>Port 1812</p> <p>If is configured to remotely authenticate user logins via the RADIUS protocol, port 1812 is used and must be open.</p> <p>However, but the system can also be configured to use any port of your designation. Optional</p> <p>Port 1813</p> <p>If the is configured to remotely authenticate user logins via the RADIUS protocol, and it also employs RADIUS accounting for event logging, port 1813 or an additional port of your designation is used to transfer log notifications.</p>	Outgoing
LDAP	<p>Ports 389 and 636</p> <p>Port 389 or 636 must be open.</p> <p>If the is configured to remotely authenticate user logins via the LDAP/LDAPS protocol, ports 389 or 636 will be used, but the system can also be configured to use any port of your designation. Optional</p>	Outgoing
SNMP	<p>Ports 161 and 162</p> <p>Port 161 is used for inbound/outbound read/write SNMP access.</p> <p>Port 162 must be open. Port 162 is used for outbound traffic for SNMP traps.</p>	Both (Port 161) Outgoing (Port 162)

Protocol	Port	Communication direction
For FTP upgrades	Port 21 Port 21 must be open.	Outgoing
SYSLOG on Configurable UDP Port	Port 514 By default UDP port 514 is used. Configurable to a port of your choice.	Outgoing
SNTP (Time Server) on Configurable UDP	Port 123 The offers the optional capability to synchronize its internal clock to a central time server. This function requires the use of UDP Port 123 (the standard for SNTP), but can also be configured to use any port of your designation. Optional	Both

You may have to open additional ports when NFS logging, using LDAP servers, and so forth.

These ports may vary from installation-to-installation depending on network topologies, virtual Local Area Networks (VLANs), and firewall configurations.

Contact your network administrator for site-specific information and settings.

Port Pins

Local Terminal Port		
pin	Definition	Direction
pin 1	RTS	Output
pin 2	N/A	
pin 3	TXD	Output
pin 4	Ground	
pin 5	Ground	
pin 6	RXD	Input
pin 7	N/A	
pin 8	CTS	Input

DTE Mode on Server Port		
pin	Definition	Direction
pin 1	RTS	Output
pin 2	DTR	Output
pin 3	TXD	Output

DTE Mode on Server Port		
pin 4	Ground	
pin 5	Ground	
pin 6	RXD	Input
pin 7	DSR	Input
pin 8	CTS	Input

DCE Mode on Server Port		
pin	Definition	Direction
pin 1	CTS	Input
pin 2	DSR	Input
pin 3	RXD	Input
pin 4	Ground	
pin 5	Ground	
pin 6	TXD	Output
pin 7	DTR	Output
pin 8	RTS	Output

Port Ranges


The port range for internal port configuration - CSC, HTTP, HTTPS, SSH, Telnet, DPA SSH , DPA Telnet - is 1 to 64510. The configurable port range for socket creation is limited to 1024 to 64510.


External port configuration - LDAP, RADIUS, TACACS+ and SNMP - is not affected by a port range limitation.


Network Speed Settings


network speed setting						
Network switch port setting	Auto	1000/Full	100/Full	100/Half	10/Full	10/Half
Auto	Highest Available Speed	1000/Full	: 100/Full Switch: 100/Half	100/Half	: 10/Full Switch: 10/Half	10/Half
1000/Full	1000/Full	1000/Full	No Communication	No Communication	No Communication	No Communication
100/Full	: 100/Half Switch: 100/Full	: 100/Half Switch: 100/Full	100/Full	: 100/Half Switch: 100/Full	No Communication	No Communication
100/Half	100/Half	100/Half	: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
10/Full	: 10/Half Switch: 10/Full	No Communication	No Communication	No Communication	10/Full	: 10/Half Switch: 10/Full
10/Half	10/Half	No Communication	No Communication	No Communication	: 10/Full Switch: 10/Half	10/Half


Legend:

 Does not function as expected

 Supported

 Functions; not recommended

 NOT supported by Ethernet specification; product will communicate, but collisions will occur

 Per Ethernet specification, these should be “no communication,” however, note that the behavior deviates from expected behavior

Note: For reliable network communication, configure the and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure the and LAN Switch to Autodetect (recommended), or set both to a fixed speed/duplex such as 100MB/s/Full.

Default User Session Timeouts

- interface - 5 minutes (to change this, select Security > Settings and update the "Idle Timeout (minutes)" field)
- SSH - 16 minutes
- Telnet - 2 hours

SX II Supported Local Port DVI Resolutions

Following are the resolutions supported when connecting to a DVI monitor from the local port.

- 1920x1080@60Hz
- 1280x720@60Hz
- 1024x768@60Hz (default)
- 1024x768@75Hz
- 1280x1024@60Hz
- 1280x1024@75Hz
- 1600x1200@60Hz
- 800x480@60Hz
- 1280x768@60Hz
- 1366x768@60Hz
- 1360x768@60Hz
- 1680x1050@60Hz
- 1440x900@60Hz

Appliance LED Status Indicators

LEDs are used to indicate power status, appliance status and target connection status.

There are LEDs located on the front panel and rear panel of the . Front Panel LED Status Indicators

- When boots up, only the Power LED turns on. The power LED turns both red and blue.
- Port Channel LEDs are off the whole time boots up.
- Once is fully powered on, the Power LED remains on.
 - If a single power supply is plugged in, the Power LED is Red.
 - If both power supplies are plugged in, the Power LED is Blue.
- When you physically connect a powered-on target to a port on via a CAT5 cable, the Port channel's LED turns on.

The LED remains on until the target is disconnected.

Note: The target must be powered on in order for the Port channel LED to turn on and the to detect the target.

- When you physically disconnect a target from a port on an , the port channel's LED turns off.
- When you log in to and connect to a target via either HSC, SSH or the Local Console, the port channel's LED blinks.

The LED blinks until you end the your connection to the target.

If you are connected to more than one target at the same time, all LEDs blink in unison.

- When you press the 's Reset button to reset the appliance or when you perform a reboot from the GUI, the Power LED(s) blinks as the appliance powers down and turns off.

While the appliance powers back up, the Power LED(s) continue to blink.

Once the appliance is powered on, the Power LED(s) stop blinking and the LED remains on.

Target Cable Connection Distances and Rates

supports the following connection distances using a CAT5 cable between its Serial port and a target.

Distance	Bits per second
300ft/91m	1,200
300ft/91m	1,800
300ft/91m	2,400
200ft/60m	4,800
100ft/30m	9,600
50ft/15m	19,200
25ft/7.5m	38,400
16ft/5m	57,600
8ft/2.5m	115,200
4ft/1.2m	230,400

Index

Access Clients 13

Appliance LED Status Indicators 54

Port Access Page 27

Port Pins 51

A

Access and Use Remote Console Features 19

Access SX II Using an iOS Device 25

Additional Security Warnings 25

Allow Pop-Ups 20

B

Browser Tips for HSC 45

C

Change Your Password from the Remote Console 26

Command Line Interface High-Level Commands 37

Command Line Interface Partial Searches 36

Command Line Interface Protocols 35

Command Line Interface Shortcuts 36

Command Line Interface Tips 36

Configure for the First Time 15

Connect a Laptop to Using a Cross-Over Cable (Optional) 16

Connect a Rack PDU to and Configure Power Control Options 46

Connect to a Target 30

Connect to Targets Using CLI - Connect, Disconnect, Power On, Power Off and Power Cycle Targets 33

Connecting the to the PX PDU FEATURE Port 47

Connecting the to the PX PDU Serial Port 46

Converting a Binary Certificate to a Base64-Encoded DER Certificate (Optional) 22

Copy and Paste and Copy All 41

CS03 Certification - DSX2-16 and DSX2-48 5

D

Default Login Information 15

Default User Session Timeouts 54

Disconnect from a Target 31

E

Emulator 37

Example 1: Import the Certificate into the Browser 20

Example 2: Add the to Trusted Sites and Import the Certificate 21

F

Features and Benefits 6

H

HTML Serial Console (HSC) Help 37

I

Initial Configuration from the Remote Console 15

Initial Configuration Using Command Line Interface (Optional) 16

Installing a Certificate 20

iOS Support 14

J

Java Validation and Access Warning 24

L

Log In to and HSC 23

Log In to SX II Admin-Only Interface 25

M

Maximum Number of Support Users Per Port 49

Maximum Number of Users Session 49

N

Network Speed Settings 53

P

Package Contents 11

Port Access Protocol Requirements 49

Port Action Menu Options - Connect, Disconnect,
Power On, Power Off and Power Cycle Targets 29

Port Ranges 52

Power Cycle a Target 32, 45

Power Off a Target 32, 44

Power on a Target 44

Power On a Target 31

Power Status 43

S

Security Warnings and Validation Messages 24

Send Text File 42

Set Terminal Emulation on a Target 17

Set the CLI Escape Sequence 18

Specifications 48

Supported Number of Ports and Remote Users per
SX II Model 49

Supported Remote Connections 48

Supported Serial Devices 13

SX II Appliance Diagram 12

SX II Dimensions and Physical Specifications 48

SX II Left Panel 28

SX II Models 12

SX II Supported Local Port DVI Resolutions 54

T

Target Cable Connection Distances and Rates 55

Tools: Start and Stop Logging 43