



# Dominion® SX

## User Guide 3.5.0

---

Copyright © 2014 Raritan, Inc.

DSX-v3.5-0-Z-E

September 2014

255-60-2000-00

---

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 express prior written consent of Raritan, Inc.

© Copyright 2014 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

<b>CS03 Certification - DSXA-16 and DSXA-48</b>	<b>xiii</b>
---	-------------

---

<b>Package Contents</b>	<b>xiv</b>
-------------------------	------------

---

<b>How to - Dominion SX Essentials</b>	<b>xvi</b>
--	------------

---

Case 1. Upgrading SX Firmware via Web Browser.....	xvi
Case 2. Configuring and Using Direct Port Access via SSH.....	xvi
Case 3. Using Exclusive Write Access via RSC.....	xvii
Case 4. Configuring LDAP.....	xvii
Case 5. Creating Power Association Group.....	xviii
Case 6. Performing Factory Reset on SX.....	xix
Case 7. Managing User Profiles on SX.....	xix
Case 8. Accessing Port Access on SX via RSC.....	xix
Case 9. Port Configuration.....	xx
Case 10. CLI / SSH Connection to SX Port.....	xx

<b>Chapter 1 Introduction</b>	<b>22</b>
-------------------------------	-----------

---

Dominion SX Overview.....	22
SX Connections, Ports and Indicators.....	23
4 Port SX.....	24
8 Port SX.....	25
16 Port SX.....	25
32 Port SX.....	26
48 Port SX.....	26
Product Features.....	28
Comprehensive Console Management.....	28
Strong Security and User-Authentication.....	29
Reliable Connectivity.....	29
Simplified User Experience.....	29

**Chapter 2 Installation and Configuration 30**

---

Overview ..... 30  
 Factory Defaults ..... 31  
 LED State ..... 31  
 Power and Connect the SX ..... 32  
 Configure the SX ..... 33  
     Configuring the SX Using a Browser ..... 33  
     Configuring SX Using the Command Line Interface ..... 34

**Chapter 3 Network Settings and Services 36**

---

Configuring the Basic Network Settings ..... 37  
     Configure the Network Settings of SX ..... 38  
     Name the SX ..... 39  
     Change the Discovery Ports ..... 40  
 Configuring the Network Service Settings ..... 40  
     Change Network Service Settings ..... 43  
 Configuring Modem Access ..... 43  
 Configuring IP Forwarding and Static Routes ..... 44  
     Enable IP Forwarding ..... 44  
     Add a New Static Route ..... 45  
     Delete a Static Route ..... 46

**Chapter 4 User Profiles and Groups 47**

---

Managing User Profiles ..... 47  
     Display a List of User Profiles ..... 47  
     Create a User Profile ..... 48  
     Modify a User Profile ..... 50  
     Delete a User Profile ..... 51  
 Managing User Groups ..... 51  
     Display a List of User Groups ..... 51  
     Create a User Group ..... 52  
     Modify a User Group ..... 56  
     Delete a User Group ..... 56

## Chapter 5 Remote Authentication 57

---

Configuring RADIUS .....	57
Configuring LDAP .....	58
Configuring TACACS+ .....	59

## Chapter 6 Port Configuration and Port Access Application 61

---

Port Keywords.....	62
Port Configuration .....	63
Direct Port Access .....	65
Direct Port Access via Username for SSH and Telnet .....	66
Direct Port Access via HTTP .....	66
Anonymous Port Access.....	67
Raritan Serial Console .....	67
Raritan Serial Console Requirements for Java .....	68
Java Runtime Environment (JRE) .....	68
Java Applets and Memory Considerations .....	69
Raritan Serial Console Interface.....	71
Emulator .....	72
Edit.....	80
Tools .....	81
Chat .....	85
Help .....	86
Standalone Raritan Serial Console Installation .....	86
Standalone Raritan Serial Client Requirements .....	87
Setting Windows OS Variables.....	87
Setting Linux OS Variables.....	90
Setting UNIX OS Variables.....	90
Installing Standalone RSC for Windows .....	91
Launching RSC on Windows Systems .....	93
Installing RSC for Sun Solaris and Linux.....	94
Launching RSC on Sun Solaris .....	95

## Chapter 7 Security 96

---

Security Settings .....	96
Login Settings .....	97
Local Authentication .....	97
Login Handling.....	98
Strong Password Settings .....	98
Configure Kerberos.....	99
Certificates .....	100
Generate a Certificate Signing Request.....	101
Install a User Key.....	102
Install a User Certificate .....	103

SSL Client Certificate .....	104
Enable Client Certificate Authentication .....	105
Install a New Trusted Certificate Authority .....	106
Remove a User-Added Certificate Authority .....	106
View a Certificate Authority .....	106
Manage the Client Certificate Revocation List (CRL) .....	106
Add a New Certificate Revocation List to the SX .....	106
Delete a Certificate Revocation List from the SX .....	107
View a Certificate Revocation List .....	107
Banner .....	108
Security Profiles .....	109
About Security Profiles .....	109
Select a Security Profile .....	109
Edit the Custom Profile .....	110
Firewall .....	110
Enable the Firewall .....	111
Add an IPTables Rule .....	111

---

## Chapter 8 Logging 113

Configuring Local Event Logging .....	113
Enable the Event Log File .....	113
Enable System Logging .....	114
Enable Port Syslog .....	114
Enable Port Logging .....	115
Configure Input Port Logging .....	116
Configure Encryption .....	117
Block Port Access On Failure .....	117
Configuring SMTP Logging .....	117
Enable SMTP Logging .....	118
Select a New SMTP Event .....	119
Test SMTP Logging .....	120
Configuring NFS Logging .....	120
Configuring SNMP Logging .....	121
Enable SNMP Logging .....	122
Enable SNMPv3 Logging .....	122
Create a New SNMP Destination .....	123

---

## Chapter 9 Maintenance 124

Managing the Local Event Log .....	124
Display the Local Event Log .....	124
Clear the Event Log .....	125
Send the Event Log .....	125
Displaying a Configuration Report .....	126
Backing Up and Restoring the SX .....	126
Back Up the SX .....	127
Restore the SX .....	128

Upgrading Firmware .....	128
Display the Current Firmware Version.....	129
Upgrade the Firmware.....	129
Display a Firmware Upgrade History.....	131
Performing a Factory Reset on the SX.....	131
Rebooting the SX.....	131

## Chapter 10 Diagnostics 132

---

Network Infrastructure Tools.....	132
Status of Active Network Interfaces.....	132
Network Statistics .....	133
Ping Host .....	134
Trace Route to Host .....	134
Administrator Tools - Process Status .....	135

## Chapter 11 Command Line Interface 136

---

Command Line Interface Overview .....	137
Accessing the SX Using CLI.....	137
SSH Connection to the SX .....	138
SSH Access from a Windows PC.....	138
SSH Access from a UNIX/Linux Workstation .....	138
Login .....	138
Telnet Connection to the SX.....	139
Enabling Telnet.....	139
Accessing Telnet from a Windows PC .....	140
Local Port Connection to the SX.....	140
Port Settings .....	140
Connection.....	141
To Change the Local Port Parameters: .....	141
Navigation of the CLI .....	141
Completion of Commands .....	141
CLI Syntax -Tips and Shortcuts.....	142
Common Commands for all Command Line Interface Levels.....	142
Show Command .....	143
Initial Configuration .....	144
Setting Parameters.....	144
Date and Time Configuration.....	145
Setting Network Parameters.....	145
CLI Prompts .....	146
CLI Commands .....	146
Security Issues .....	152
Configuring Users and Groups .....	153
Command Language Interface Permissions .....	153
Target Connections and the CLI.....	154
Setting Emulation on a Target.....	154
Set Escape Sequence .....	154
Port Sharing Using CLI.....	155

Configuring Authorization and Authentication (AA) Services .....	155
Remote Services .....	155
LDAP Configuration Menu .....	156
RADIUS Command.....	158
TACACS+ Command .....	159
Administering the SX Console Server Configuration Commands .....	159
Configuring Events.....	159
Configuring Log.....	160
Cleareventlog Command.....	160
Eventlogfile Command .....	161
eventsyslog Command.....	161
portsyslog Command.....	162
nfsgetkey Command.....	162
nfssetkey Command.....	163
NFS Encryption Enable Command.....	163
Portlog Command.....	163
Decrypt Encrypted Log on Linux-based NFS Server .....	165
Sendeventlog Command .....	166
Vieweventlog Command.....	166
Configuring a Modem.....	167
Configuring Network .....	170
Ethernetfailover Command.....	171
Interface Command .....	171
IPForwarding Command.....	172
Name Command.....	173
Ports Command.....	173
Route Command.....	173
Routeadd Command .....	174
Routedelete Command.....	174
Getconfig Command.....	175
Runconfig Command.....	175
Configuring NFS .....	175
Configuring Ports .....	177
Ports Configuration Menu .....	177
Ports Config Command .....	177
Ports Keywordadd Command.....	181
Ports Keyworddelete Command.....	182
Configuring Services .....	182
dpa Command .....	183
Encryption Command .....	186
HTTP Command.....	186
HTTPS Command .....	187
Logout Command .....	187
LPA Command .....	188
SSH Command.....	188
Telnet Command .....	189
fixedtcpwindow Command.....	189
Configuring SNMP .....	189
SNMP Add Command .....	190
SNMP Delete Command .....	190
SNMP Command.....	190

Configuring Time.....	191
Clock Command .....	191
NTP Command.....	191
Timezonelist Command.....	192
Configuring Users .....	192
Addgroup Command .....	192
Adduser Command.....	193
Deletegroup Command .....	194
Deleteuser Command.....	194
Editgroup Command.....	194
Edituser Command.....	195
Groups Command .....	195
Users Command.....	196
Connect Commands .....	196
Configuring Power .....	196
Diagnostic Commands.....	197
IPMI Commands .....	198
IPMIDISCOVER.....	198
IPMITOOL.....	199
Listports Command.....	201
Maintenance Commands.....	203
Backup Command .....	203
Cleareventlog Command.....	204
Factoryreset Command .....	204
Firmware Command .....	205
Logoff Command .....	205
Reboot Command.....	206
Restore Command.....	206
Sendeventlog Command .....	207
Upgrade Command .....	208
Upgradehistory Command.....	208
Userlist Command .....	209
Vieweventlog Command.....	209
Security Commands.....	209
Banner Command.....	209
Ftpgetbanner Command.....	210
Certificate Command Menu .....	211
Firewall Command.....	213
IPtables Command .....	214
Kerberos Command .....	216
Loginsettings Commands .....	218
Idletimeout Command .....	218
Inactiveloginexpiry Command .....	218
Invalidloginretries Command .....	219
Localauth Command .....	219
Lockoutperiod Command .....	219
Singleloginperuser Command .....	220
Strongpassword Command .....	220
Unauthorizedportaccess Command .....	221
Portaccess Command .....	222
Securityprofiles Commands.....	222
Profiledata Command.....	222

**Chapter 12 Intelligent Platform Management Interface 224**

---

Discover IPMI Devices .....	224
IPMI Configuration .....	225

**Chapter 13 Power Control 229**

---

Port Power Associations .....	229
Create a Port Power Association.....	229
Delete a Port Power Association .....	230
Power Strip Configuration .....	231
Power Association Groups .....	231
Power Control .....	232
Associations Power Control .....	233
Power Strip Power Control .....	234
Power Strip Status .....	235
CLI Command for Power Control.....	235
CLI Port Power Association.....	235
CLI Power Strip Power Control.....	241
CLI Configure Global Power Strip Delays .....	243
CLI Association Power Control - Port Association .....	244
CLI Association Power Control - Group Association .....	246
CLI Power Strip Status .....	249

**Appendix A Specifications 252**

---

SX Models and Specifications .....	252
Maximum Number of Connections for a Single User .....	255
Maximum Number of CLI Sessions .....	255
Requirements.....	256
Supported Operating Systems, Browsers and Java Versions .....	256
Connectivity .....	257
SX Serial RJ-45 Pinouts .....	258
DB9F Nulling Serial Adapter Pinouts.....	259
DB9M Nulling Serial Adapter Pinouts.....	259
DB25F Nulling Serial Adapter Pinouts.....	260
DB25M Nulling Serial Adapter Pinouts.....	260

SX Terminal Ports .....	261
SX16 and SX32 Terminal Ports .....	262

**Appendix B System Defaults** **264**

---

Initiate Port Access .....	264
Supported Character Length of Various Field Types .....	264

**Appendix C Certificates** **267**

---

Default SX Certificate Authority Settings .....	267
Installing Dominion SX Server Certificate for Netscape Navigator .....	267
Accept a Certificate (Session-Based) .....	267
Install the Dominion SX Server Certificate in Netscape Navigator .....	267
Remove an Accepted Certificate .....	268
Installing a Third-Party Root Certificate .....	270
Install a Third-Party Root Certificate to Internet Explorer .....	271
Install a Third-Party Root Certificate to Netscape Navigator .....	271
Generate a CSR for a Third Party CA to Sign .....	272
Install Client Root Certificate .....	274
Install Client Certificate into Internet Explorer .....	274
Importing Certificates for LDAP .....	274
Retrieve LDAP Certificate via Access from HTTP Interface .....	274
Import Certificates from Windows XP .....	275
Import Certificates from Dominion SX via CLI .....	276

**Appendix D Server Configuration** **278**

---

Microsoft IAS RADIUS Server .....	278
Configure the SX to Use an IAS RADIUS Server .....	278
Create an IAS Policy .....	279
Cisco ACS RADIUS Server .....	281
Cisco ACS 5.x for RADIUS Authentication .....	281

## Contents

TACACS+ Server Configuration .....	282
CiscoSecure ACS .....	282

## **Appendix E Modem Configuration** **285**

---

Client Dial-Up Networking Configuration .....	285
Windows NT Dial-Up Networking Configuration .....	285
Windows 2000 Dial-Up Networking Configuration .....	288
Windows Vista Dial-Up Networking Configuration .....	292
Windows XP Dial-Up Networking Configuration .....	293

## **Appendix F Accessing a PX2 from the SX** **299**

---

Overview .....	299
Connecting the SX to the PX2 Serial Port .....	299
Connecting the SX to the PX2 FEATURE Port .....	300

## **Appendix G Troubleshooting** **302**

---

Page Access .....	302
Firewall .....	303
Login .....	304
Port Access .....	304
Upgrade .....	305
Events Not Captured in Event Log .....	306
Modem .....	306
SSH Connection .....	306
iptables --list Hanging .....	307
Display Issue with Japanese Characters when Using Teraterm 3.1 .....	307
Lines are Overwritten after Column 80 in Linux .....	308
AIX Terminal Settings Not Displaying Correctly .....	308

## **Appendix H Frequently Asked Questions** **309**

---

Chapter 14 FAQs .....	310
-----------------------	-----

## CS03 Certification - DSXA-16 and DSXA-48

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.

In Raritan products that require rack mounting, follow these precautions:

Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the appliances (see **Specifications** (on page 252)).

- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, such as power strips (other than direct connections), to the branch circuit.

## Package Contents

**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.

Check the contents of the carton containing the SX against the packing list that ships with your SX. If any piece is missing or damaged, contact your Raritan sales representative.

The following items ship with all SX models (unless otherwise indicated):

- 1 - Packing list
- 1 - SX with a mounting kit (note that rack-mount kits are optional for some SX models)
- 1 - RJ45 serial loop-back plug
- 1 - AC power cord (only shipped with SX AC models - no power cord is shipped with DC models)
- 1 - SX Quick Setup Guide
- 1 - Warranty card
- 1 - Release notes
- 1 - DB9 Factory Reset Adapter (only shipped with SX models that do not have a reset switch and require an adapter)

# How to - Dominion SX Essentials

---

## Case 1. Upgrading SX Firmware via Web Browser

Upgrade the SX firmware version for enhanced features or service patches.

During the upgrade, SX verifies there is enough space on the device to perform the upgrade. If there is not, the SX restarts and the upgrade does not take place. If the upgrade fails due to lack of space, clear the local logs on the device and try upgrading again. Contact Raritan Technical Support if you still cannot upgrade after clearing the local logs.

► **To upgrade the SX:**

1. Check the Raritan support website for the latest firmware version: (<http://www.raritan.com/support/firmwareupgrades> and look for SX under Dominion Family)
2. Download the new SX firmware stored as UpgradePack from Raritan website to an FTP server, for example, a FileZilla server, assuming that FTP server has an IP address of 192.168.51.204. Extract the zip file to a folder under FTP root directory, for example:  
\\home\downloads\firmware\UpgradePack\_2.5.6\_3.1.0.5.2\Pack1of1.  
Make sure the folder is accessible via an FTP user account.
3. Log in to the SX through a web browser. Choose Maintenance > Firmware Upgrade.
4. Enter the FTP server IP address, FTP username and password, and the FTP folder path where the extracted files are stored (in this example: /UpgradePack\_2.5.6\_3.1.0.5.2\Pack1of1), and click Upgrade.
5. After the firmware upgrade is completed, log in to the SX and check the firmware version by clicking Maintenance > Firmware Version. You can also check firmware upgrade history to make sure: Maintenance > Firmware Upgrade History.

See **Upgrade the Firmware** (on page 129) for details.

---

## Case 2. Configuring and Using Direct Port Access via SSH

► **To allow users to directly SSH into the serial target without using SX GUI:**

1. Determine an IP address or TCP port on SX IP to use for DPA or any port on SX. Since the network administrator has no spare IP address, reuse the SX IP address with a different port.

2. Log back in to the SX and select the port enabled for DPA in Setup > Port Configuration.
3. Edit the DPA SSH TCP Port to which SSH client connects. Click OK.
4. Log in to the SX via a web browser. Click Setup > Services, select TCP port on Direct Port Access Mode, and click OK.
5. Launch an SSH client, such as Plink or PuTTY. Enter the IP address and change the default TCP Port to connect to the enabled port (for example, `plink -ssh -P 2203 192.168.51.9`).

See **Direct Port Access** (on page 65) for details.

---

### Case 3. Using Exclusive Write Access via RSC

► **To ensure that you are the only user who has write access to a serial target:**

1. After logging in to SX via a web browser, the Port Access tab is selected by default.
2. Connect to Port 4 by clicking on the Port 4 link.
3. The Raritan Serial Console (RSC) launches with Write Access enabled unless the port is taken by another user.
4. In the RSC window, click Emulator > Get Write Lock. The icon on the status line displays Write Access (Lock), meaning all users can only view the port connection.

---

*Note: If another has previously obtained Write Access, perform "Get Write Access" first from the Emulator menu of RSC)*

---

5. Log in to the device connected to the port and try interacting with the device using the RSC panel. See Get Write Access for details.
6. To relinquish write lock in the RSC window, choose Emulator > Write Unlock, and the icon on status line displays Write Access again, meaning any other privileged users regain Write Access.

---

### Case 4. Configuring LDAP

► **To configure SX to use LDAP/Active Directory® server for login authentication:**

1. After logging in to SX via a web browser, choose Setup > Remote Authentication.
2. If the LDAP server has a backup server, enter the same parameters (except the IP address) for the secondary LDAP server.

3. Click OK.

See **Configuring LDAP** (on page 58) for details.

---

## Case 5. Creating Power Association Group

See **Power Strip Configuration** (on page 231) for details on how to add power strips to SX management first. If this wasn't already done, see Port Power Associations section to map power strip outlet to a target server connected to an SX serial port, and then see **Power Association Groups** (on page 231) for details on how to group multiple power outlets physically connected to that same target server.

► **To associate the target server with more than one power outlets physically connected to it:**

1. Log in to SX via a web browser and then make sure a power strip has been configured. To add a power strip:
  - a. Choose Setup > Power Strip Configuration. See **Power Strip Configuration** (on page 231) for details.
2. Choose Setup > Port Power Association List and click Add.
3. Use the drop-down menu to select the SX port connected to the dual-powered server device with which you want to associate outlets. Enter a description for it, such as "Internal Web Server Pronto". See **Port Power Associations** (on page 229) for details.
4. Use the drop-down menu to select the power strip and outlet that matches how the unit is connected to the power. Click Add. The information appears in the text box as "[Power Strip Name] \ [outlet 1]".
5. Select the same power strip and another outlet, then click Add. Another line displays in the text box as "[Power Strip Name] \ [outlet 2]". Click OK to commit the changes.
6. Choose Setup > Power Association Group List and click Add. See **Power Association Groups** (on page 231) for details.
7. Enter a group name and description, then select the port ID(s) from the "Available" box. Click Add.
8. Click OK to commit changes.

---

## Case 6. Performing Factory Reset on SX

▶ **To set the SX configuration back to the factory defaults through the GUI:**

1. Log in to SX via a web browser.
2. Choose Maintenance > Factory Reset. Confirm your decision when prompted.
3. Do not power off the SX as it reboots.
4. You are redirected to the login page after the SX is rebooted. When you log in for the first time after a reset, you are advised that you are now in the factory default mode and prompted to change the username and password.

---

*Passwords are case sensitive and can contain up to 64 alphanumeric characters with the exception of " ' < > \ &*

---

See **Performing a Factory Reset on the SX** (on page 131) for details.

---

## Case 7. Managing User Profiles on SX

▶ **To create, update, or delete an SX user:**

1. Log in to SX via a web browser.
2. Choose User Management > User List.
3. To create a user profile, click Add New User.
4. To modify an existing user profile, see **Modify a User Profile** (on page 50) for details.
5. To delete an existing user profile, see **Delete a User Profile** (on page 51) for details.

See **Create a User Profile** (on page 48) for details.

---

## Case 8. Accessing Port Access on SX via RSC

▶ **To access an SX serial target through Raritan Serial Client (RSC):**

1. Log in to the SX via a web browser.
2. Click the Port Access tab, and click the port name you wish to access.

3. Select Yes to proceed through the security warning(s). The Raritan Serial Console (RSC) launches in a separate window. Press the Enter key to "wake up" the session.
  4. Type the target system's native commands in the RSC window/console.
  5. Choose Emulator > Exit. Click Yes on the confirmation dialog to exit.
- See **Raritan Serial Console** (on page 67) for details.

---

## Case 9. Port Configuration

These steps allow you to configure SX serial ports to set up correct serial communications parameters such as baud rate, data bits, stop bit, flow control; the terminal emulation mode to match the serial targets connected to the ports; and name the ports to more easily identify the targets.

▶ **To configure the SX serial ports to set up correct serial communications parameters:**

1. Log in to SX via a web browser.
2. Click Setup > Port Configuration.
3. Check the box associated with the port number you wish to configure, and click Edit.

See **Port Configuration** (on page 63) for details.

---

## Case 10. CLI / SSH Connection to SX Port

▶ **To access the SX and SX ports using text-based command lines:**

1. SSH access from a Windows® PC:
  - a. Launch the SSH client software (such as Plink or PuTTY).
  - b. Enter the IP address of the SX server (for example, 192.168.0.192), and the TCP port if applicable.
  - c. Select SSH using default configuration port 22, and click Open.
  - d. Log in using the default log in credentials admin/raritan. The console displays all ports on the SX with port numbers.
  - e. Enter a port number at the prompt, for example: `admin> 1`

- f. To return to the SX console, enter the escape sequence characters. For example, simultaneously press the control and closed bracket key (]).
  - g. To exit the target serial console session, enter the letter "q" to quit. You are redirected to the SX console, and the port serial console session is now closed.
2. SSH access from a UNIX® Workstation
- a. Enter the following command to log in: `ssh -l admin 192.168.0.192`
  - b. Enter the admin username and raritan as the password. The console displays all the ports on the SX with port numbers.
  - c. Enter a port number at the prompt, for example: `admin> 1`
  - d. To return to the SX console, enter the escape sequence characters. For example, simultaneously press the control and closed bracket key (]).
  - e. To exit the target serial console session, enter the letter "q" to quit. You are redirected to the SX console, and the port serial console session is now closed.

See SSH Connection to the SX for details.

# Chapter 1 Introduction

## In This Chapter

Dominion SX Overview.....	22
SX Connections, Ports and Indicators.....	23
Product Features .....	28

---

## Dominion SX Overview

The SX Series of Serial over IP Console Servers offers convenient and secure remote access and control through LAN/WAN, Internet, or Dial-up modem to all networking devices.

The SX:

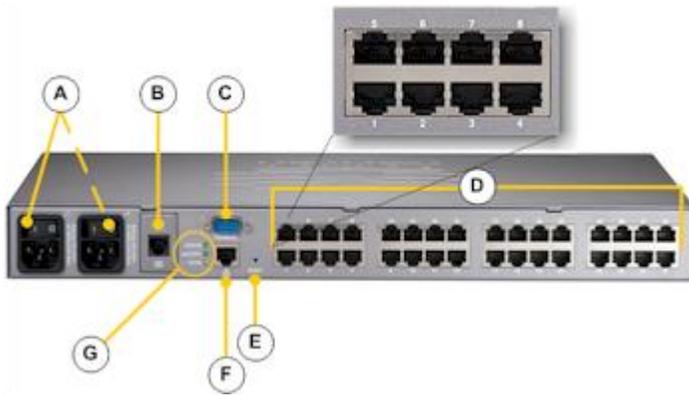
- Provides a non-intrusive solution for managing network elements and does not require any installation of software agents on the target device
- Connects to any networking device (server, firewall, load balancer, and so forth) through the serial port and provides the ability to remotely and securely manage the device using a Web browser

SX is a fully configured stand-alone product in a standard 1U high 19" rack mount chassis.



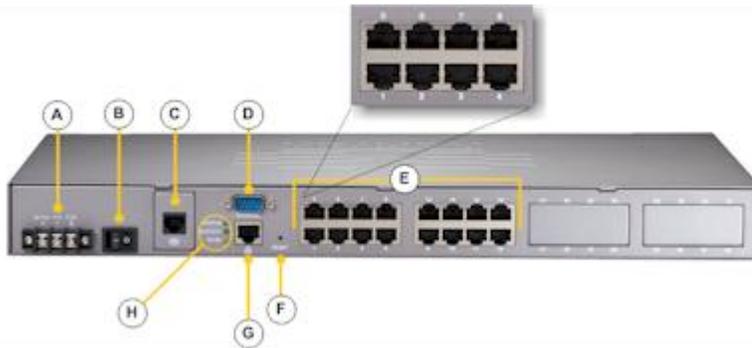
## SX Connections, Ports and Indicators

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



### AC unit diagram key

(A)	AC power outlet(s) and power on/off switch(s)
(B)	Internal modem (if available)
(C)	Terminal port/console port
(D)	Server ports
(E)	Reset button
(F)	Ethernet port
(G)	<p>Unit status indicators</p> <p>In normal operation, the LED blinks whenever there is network or serial activity detected.</p> <p>When booting, the LED blinks three (3) times if the unit is in a factory reset state.</p> <p>The Activity and 10/100 LEDs are tied to the network port. Activity blinks when there is network activity.</p> <p>10/100 displays the link status (10Mbit/s or 100Mbit/s) of the network.</p> <hr/> <p><i>Note: On some SX models, the 10/100 and Activity LED are attached directly to the LAN port, and are not labeled.</i></p>



DC unit diagram key	
(A)	DC power connections
(B)	Power on/off switch
(C)	Internal modem (if available)
(D)	Terminal port/console port
(E)	Server ports
(F)	Reset button
(G)	Ethernet port
(H)	Unit status indicators (see above for details)

### 4 Port SX

4 Port SX Models – Port Numbering

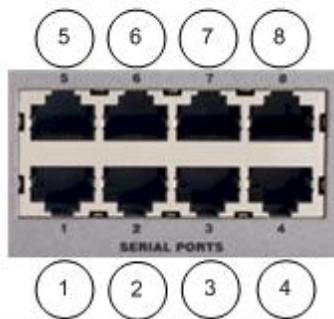


Models	Single-feed AC power	Console port	19" rack-mount kit	Internal modem
DSX4	✓	✓ (2)	✓ (optional)	
DSXB-4-M	✓	✓ (1)	✓ (optional)	✓

---

**8 Port SX**

Models	Single-feed AC power	Dual-feed AC power	Single-feed DC power	Console ports	19" rack-mount kit	Internal modem
DSX8	✓			✓ (2)	✓ (optional)	
DSXA-8		✓		✓ (1)	✓	✓
DSXB-8-M	✓			✓ (1)	✓ (optional)	✓
DSXB-8-DC			✓ (-36-72V)	✓ (2)	✓ (optional)	

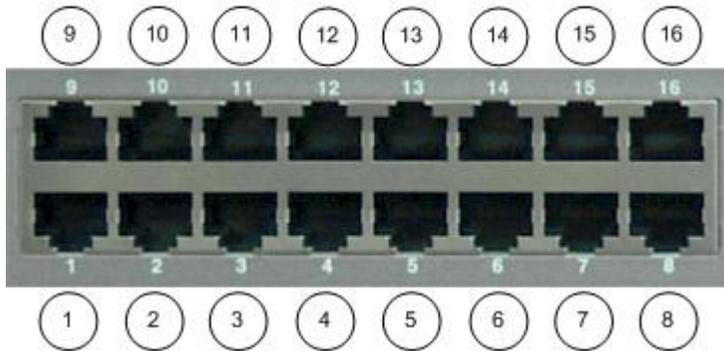
**8 Port SX Models – Port Numbering**



---

**16 Port SX**

Models	Dual-feed AC power	Dual-feed DC power	Dual Ethernet	Console port	Local access port	19" rack-mount kit	Internal modem
DSXA-16	✓			✓ (1)		✓	✓
DSXA-16-DL	✓		✓		✓ (2)	✓	
DSXA-16-DLM	✓		✓		✓ (1)	✓	✓

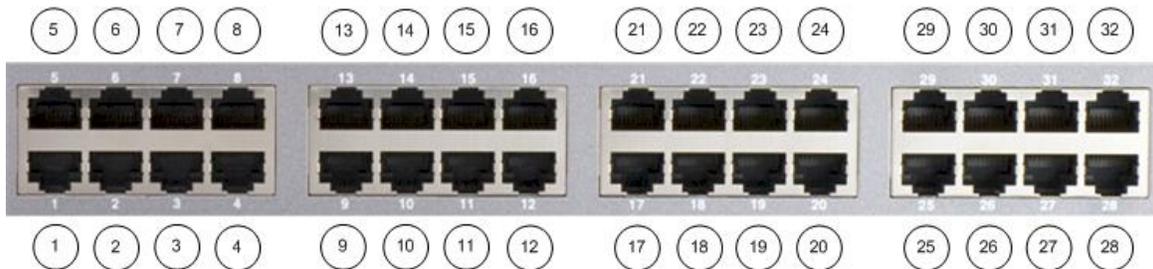
### 16 Port SX Models – Port Numbering



### 32 Port SX

Models	Dual-feed AC power	Dual-feed DC power	Dual Ethernet	Console port	Local access ports	19" rack-mount kit	Internal modem
DSXA-32	✓			✓ (1)		✓	✓
DSXA-32-AC	✓			✓ (2)		✓	
DSXA-32-DL	✓		✓		✓ (2)	✓	
DSXA-32-DLM	✓		✓		✓ (1)	✓	✓
DSXA-32-DC		✓	✓	✓ (1)		✓	✓

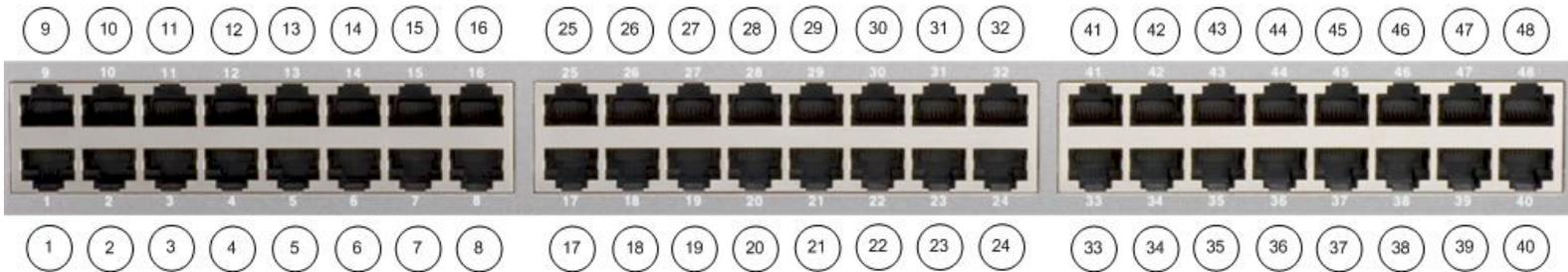
### 32 Port SX Models – Port Numbering



### 48 Port SX

Models	Dual-feed AC power	Dual-feed DC power	Dual Ethernet	Console port	19" rack-mount kit	Internal modem
DSXA-48	✓			✓ (1)	✓	✓
DSXA-48-AC	✓		✓	✓ (2)	✓	
DSXA-48-DC		✓	✓	✓ (1)	✓	✓

48 Port SX Models – Port Numbering



---

## Product Features

---

### Comprehensive Console Management

- Remote Management: Access, monitor, administer, and troubleshoot up to 48 target units (depending on the model) via Secure Socket Shell (SSH), Telnet, Local Port, or web browser with only one IP address
- Direct Port Access via TCP/IP address per port, or one IP address and TCP Port numbers
- Notification: Create notification messages by email alerts
- Collaborative Management and Training: Access ports simultaneously; up to 10 users per port at any time
- SecureChat™: Instant message and other Secure Sockets Layer (SSL) users can securely collaborate on unit management, troubleshooting, and training activities
- Get History: Get up to 256 KB (64KB on units with 64MB SDRAM; 256KB on units with 128MB SDRAM) of recent console history to assist with debugging
- Supports VT100, VT220, VT 320, and ANSI terminal emulation
- Up to a 5,000 line copy-paste buffer
- Local port access
- SYSLOG
- Logging to Network File System (NFS) Server
- Comprehensive SNMP traps
- Port alerts with keyword triggers
- Three Levels of User Access:
  - Administrator: Has read and write access to the console window; can modify the configuration of unit.
  - Operator: Has read and write access to the console window; cannot modify the configuration of unit (except own password).
  - Observer: Has read-only access to the console window; cannot modify the configuration of unit (except own password).

---

**Strong Security and User-Authentication**

- SSHv2 Support
- Encryption Security: 128-bit SSL handshake protocol and RC4 encryption
- User Authentication Security: local database, remote authentication
- Supports RADIUS, TACACS+, LDAP, LDAP(S), Microsoft Active Directory®, and NTP
- Supports user-defined and installable security Certificates

---

**Reliable Connectivity**

- Optional Modem Connectivity: For emergency remote access if the network has failed
- Target Device Connectivity: Simplified RJ45-based CAT 5 cable scheme; serial port adapters are available from Raritan
- Local Access for "crash-cart" applications

See **Connectivity** (on page 257) for a list of necessary SX hardware (adapters and/or cables) for connecting the SX to common Vendor/Model combinations.

---

**Simplified User Experience**

- Telnet
- SSH
- Browser-based Interface: The new GUI provides intuitive access to target devices (click the appropriate button to select the desired target device)
- Upgrades: Built-in firmware upgrade capability through FTP or LPA and integrated with Command Center (CC) and SSH

## Chapter 2 Installation and Configuration

### In This Chapter

Overview .....	30
Factory Defaults .....	31
LED State .....	31
Power and Connect the SX .....	32
Configure the SX .....	33

---

### Overview

There are two ways of completing the initial network installation of the SX:

- Using a serial cable with a VT100/equivalent, such as a PC with HyperTerminal
- Using Ethernet (with an installation computer)

This section describes the steps necessary to configure SX for use on a local area network (LAN).

The following table describes the factory default network settings that come with the SX. After devices are connected to the network, these factory default settings allow you to configure the SX for normal use.

Default Network Settings	
Internet Address (IP)	192.168.0.192
Gateway Address	192.168.0.192
Subnet Mask	255.255.255.0
CSC Port Address	5000
Port Address for CC Discovery	5000
Username	admin (all lowercase)
Password	raritan (all lowercase)

---

*Note: The settings listed in the table above are applicable only if no DHCP server is running on the network.*

*If a DHCP server is running on a local network, the SX is assigned a different IP address than the default by the DHCP server.*

---

---

## Factory Defaults

The SX device is shipped from the factory with the following default settings built in:

Setting	Value
IP address	192.168.0.192
Subnet mask	255.255.255.0
Gateway	192.168.0.192
Username	admin (all lowercase)
Password	raritan (all lowercase)
Device name	SX

---

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

---

---

## LED State

On the front panel of the SX, there are LED indicators on each side.

The green LED is lit at the same time the blue LED is lit.

The blue LED indicator blinks blue in the following three cases:

- Ethernet packets are received or transmitted
- Serial data are received or transmitted
- The watchdog timer is reset to 0.

The LED blinks on a periodic basis as the watchdog timer reaches a certain value, and then is reset to 0

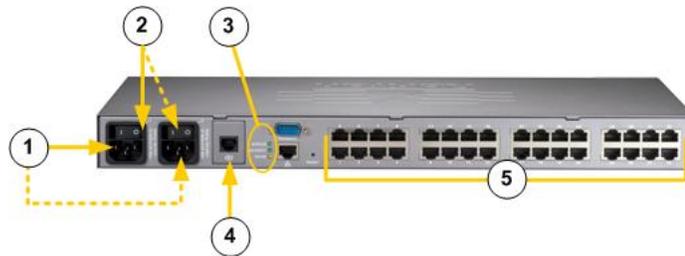
---

## Power and Connect the SX

There are various SX models.

The model shown here contains two power outlets, one LAN interface, and 32 server ports.

Your model may differ, but this does not affect the following installation instructions.



1. After you have installed the SX at the rack, connect the power cord(s) between the power connector on the SX and an external power source(s).  
  
If your device has two power connectors, you can connect the second power connector to a backup power source.
2. Flip the power switch(s) to turn the SX device on.
3. The device performs a hardware and firmware self-test. The software boot sequence starts and is complete when the light goes on and remains on.
4. Connect the modem (if needed).
5. Connect your target servers or other serially managed devices to the server ports on the SX.
  - a. Connect one end of a standard Cat5 Ethernet cable to one of the server ports on the SX.
  - b. Connect the other end to a Raritan Nulling Serial Adapter (p/n ASCSDB9F, ASCSDB9M, ASCSDB25F, ASCSDB25M) as appropriate.
  - c. Connect the adapter to the server port on the target device.

---

**Important: Many Cisco and Sun devices have server ports with non-standard RJ-45 connections. Most can be connected to the SX with a “ serial rollover cable.” This is NOT a standard Ethernet cable or crossover Ethernet cable. If you have misplaced the rollover cable that came with your Cisco or Sun device, you can purchase one from Raritan (Part Number CRLVR-15 or CRLVR-1).**

---

---

## Configure the SX

You can configure the SX using a web browser or a command line interface (CLI).

---

### Configuring the SX Using a Browser

► **To configure the SX using a web browser:**

1. Connect a computer to the LAN interface on the SX using a crossover Ethernet cable.  
If your SX has two LAN interfaces, use LAN1.
2. Open a browser and enter this URL: `http://192.168.0.192`
3. When the Login window appears, enter the default username *admin* and password *raritan*. Use all lowercase letters.
4. You are prompted to change the default password. Do so now, and be sure to remember this password for future login.
5. Choose Setup > Network.
6. In the Network Basic Settings panel, select an IP configuration method (DHCP is enabled by default)
7. Give SX an IP address, subnet mask, and gateway address on your LAN.
8. You can give the device a name to help identify it. Up to 64 characters are allowed, but special characters and spaces are not supported.
9. Add a domain. This is required to send SMTP messages.

---

*Note: If DHCP is selected and the client computer used to configure SX via crossover cable is running a DHCP server, the SX will not be accessed at 192.168.0.192, but instead at any IP address the configuring machine assigns.*

---

10. The SX reboots.
11. Once it is rebooted, enter new IP address in a browser and log in again using your new password.
12. Choose Setup > Date/Time.
  - a. Select your time zone from the drop-down menu in the UTC Offset field.
  - b. Enter the date and time manually, or enter the IP addresses of up to two Network Time Protocol (NTP) servers.
  - c. When you are finished, click OK. The SX's clock is now set.
13. Choose Setup > Port Configuration. You can now configure each console port that has a target device connected to it:

- a. Click the checkbox next to a port with a target device connected to it. If more than one target device will have the exact same settings, you can select multiple ports.
- b. Click Edit to display the settings for the port(s) and enter the information. See the user guide for details.
- c. When finished, click OK and repeat for any other ports.

---

### Configuring SX Using the Command Line Interface

► **To configure the SX using the CLI:**

1. Connect a computer to the Terminal port on the SX.  
This port is a DB9 male port on all models except those that have 2 power connectors and 2 LAN interfaces. These models have both RJ-45 connectors and DB9 male port, such as SX model - DSXA-16-DL.
2. Open a terminal emulation program and connect to the SX.  
Make sure the communications parameters are set to 9600 bps, no parity, 8 data bits, and 1 stop bit.
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. Do so now, and be sure to remember this password for future login.
5. At the `admin >` prompt, enter `config` and at the next prompt enter `network`.
6. Give the SX an IP address, subnet mask, and gateway address on your LAN.
  - a. At the `admin > config > network >` prompt, enter `interface enable true if lan1 ip <ip address> mask <subnet mask> gw <gateway ip address>`
7. You are prompted to reboot the SX. Enter `yes` to reboot.
8. Log in again using your new password.
9. Give the device a name to help identify it and enter your domain, which is required to send SMTP messages.
  - a. Enter `name unitname <DSX name> domain <domain name>`  
Up to 64 characters are supported for the name. Spaces and special characters not supported.
10. You are prompted to reboot the SX. Enter `yes` to start the reboot.
11. When the reboot is complete, log in again.

12. At the `admin >` prompt, enter `config` and at the next prompt enter `time`.
13. At the `admin > config > time >` prompt, set the date and time on the SX.
  - a. Enter `timezonelist` and find the number code that corresponds to your time zone.
  - b. Enter `clock tz <timezone code> datetime <"time string">`

where `<timezone code>` is the time zone code and `<"time string">` is the current date and time in "YYYY-MM-DD HH:MM:SS" format (quotes included, use 24-hour time).

Example: `clock tz 9 datetime "2007-03-15 09:22:33"`
14. Enter `top` to return to the top level prompt.
15. Next, enter `config` and then enter `ports` at the next prompt.
16. You can now configure each console port that has a target device connected to it.

- a. Enter `config port <port number>` followed by these additional parameters:

```
[port <number|range|*>] [name string] [bps
value] [parity <none|even|odd>] [flowcontrol
<none|hw|sw>] [detect <true|false>] [escapemode
<none|control>] [escapechar char] [emulation
type] [exitstring <cmd[#delay;]>] [dpaip
ipaddress] [telnet port] [ssh port]
[alwaysactive <true|false>] [suppress
<none|all>] [sendbreak duration]
```

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.

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

## Chapter 3 Network Settings and Services

### In This Chapter

Configuring the Basic Network Settings .....	37
Configuring the Network Service Settings.....	40
Configuring Modem Access.....	43
Configuring IP Forwarding and Static Routes .....	44

## Configuring the Basic Network Settings

Network basic settings include:

- Enabling/disabling Ethernet failover, and enabling/disabling LAN Interface 1 and 2 - see **Configure the Network Settings of SX** (on page 38)
- Specifying the SX unit name - see **Name the SX** (on page 39)
- Configuring the discovery ports - see **Change the Discovery Ports** (on page 40)

Setup > Network

Network Basic Settings	Ports
<input checked="" type="checkbox"/> Enable Ethernet Failover Interval (seconds): 20	CSC Port: 5000
<input checked="" type="checkbox"/> Enable LAN Interface 1: IP Auto Configuration: None IP Address: 192.168.61.210 Subnet Mask: 255.255.255.0 Gateway IP Address: 192.168.61.126 Mode: Auto	Discovery Port: 5000
<input type="checkbox"/> Enable LAN Interface 2: IP Auto Configuration: None IP Address: 192.168.0.192 Subnet Mask: 255.255.255.0 Gateway IP Address: 192.168.0.192 Mode: Auto	
Domain: 	
Unit Name: wwSX-COLDBOOT-TEST	

---

### Configure the Network Settings of SX

SX dual LAN models can be configured for failover or for dual LAN mode.

When configured for failover, the IP address you enter is shared between Ethernet ports. When configured for dual LAN mode, different IP addresses are assigned to each Ethernet port and failover is not supported.

If you apply dual LAN mode and you use Command Center Secure Gateway to interact with SX, CC-SG must be assigned one of the IP addresses.

► **To configure the network settings:**

1. Choose Setup > Network. The Network Basic Settings and Ports page opens.

---

*Note: If you have a dual LAN model, the Enable Ethernet Failover checkbox is selected by default. Uncheck it as needed.*

---

2. If Enable Ethernet Failover is selected, enter the failover interval in seconds in the "Interval (seconds)" field.
3. Configure the LAN interface 1:
  - a. Check the Enable LAN Interface 1 checkbox to enable the feature.
  - b. Select either None or DHCP from the drop-down menu to determine a method for IP Auto Configuration. The default is DHCP.
  - c. Type an IP address for the SX in the IP Address field.
  - d. Type the subnet mask in the Subnet Mask field.
  - e. Type the IP address of the gateway router in the Gateway IP Address field.
  - f. Select the speed from the drop-down menu in the Mode field. Your choices are Auto (default) or 100 Mbps.
4. Configure the LAN interface 2 (if needed):
  - a. Check the Enable LAN Interface 2 checkbox to enable the feature.
  - b. Select either None or DHCP from the drop-down menu to determine a method for IP Auto Configuration. The default is DHCP.
  - c. Type an IP address for the SX in the IP Address field.
  - d. Type the subnet mask in the Subnet Mask field.

- e. Type the IP address of the gateway router in the Gateway IP Address field.
  - f. Select the speed from the drop-down menu in the Mode field. Your choices are Auto (default) or 100 Mbps.
5. Type your domain name in the Domain field.
  6. Click OK.

Setup > Network

### Network Basic Settings

Enable Ethernet Failover  
Interval (seconds):  
20

Enable LAN Interface 1:  
IP Auto Configuration:  
None  
IP Address:  
192.168.61.210  
Subnet Mask:  
255.255.255.0  
Gateway IP Address:  
192.168.61.126  
Mode:  
Auto

Enable LAN Interface 2:  
IP Auto Configuration:  
None  
IP Address:  
192.168.0.192  
Subnet Mask:  
255.255.255.0  
Gateway IP Address:  
192.168.0.192  
Mode:  
Auto

Domain:

---

### Name the SX

► **To give the SX a name to help identify it:**

1. Choose Setup > Network. The Network Basic Settings and Ports page opens.
2. Type a name in the Unit Name field.
3. Click OK.

---

### Change the Discovery Ports

► **To change the discovery ports:**

1. Choose Setup > Network. The Network Basic Settings and Ports page opens.

The SX has two discovery ports:

- TCP 5000 Common Socket Connection (CSC) discovery
- UDP 5000 Command Center (CC) discovery

2. If either of these ports is used by another application, change the discovery port number in the SX in the appropriate field and click OK.

---

*Note: The port range for internal port configuration (CSC, HTTP, HTTPS, SSH, Telnet, DPA SSH, DPA Telnet) is 1 ~ 64510, while the configurable port range for socket creation is limited to 1024 ~ 64510. External port configuration (LDAP, RADIUS, TACACS+, SNMP) is not affected by this port range limitation, but allowed with full range of configuration.*

---



---

### Configuring the Network Service Settings

Following are the default settings for the various network access services:

Service	Default Setting
HTTP	Enabled. The default port is 80. This can be changed.  HTTPS redirect is enabled by default. If HTTPS is also enabled, all HTTP requests are automatically redirected to the HTTPS port (see below).
HTTPS	Enabled. The default port is 443. This can be changed.
Encryption	Encryption is set to SSL, but this can be changed to TLS.
Telnet	Disabled for security reasons. This can be enabled and the port configured.  23 is the default Telnet port.
SSH	Disabled by default. This can be enabled and the port configured.  The configurable option labeled Fixed TCP Window is enabled by default when SSH access is enabled, making SSH connection work under

Service	Default Setting
	Windows Vista® operating system. Available authorization methods are: <ul style="list-style-type: none"> <li>• Both certificate and password</li> <li>• Password</li> <li>• Certificate</li> </ul> 22 is the default Telnet port.
Local Port Access	Enabled. The baud rate is set to 9600 bps, but this can be changed.
Direct Port Access Mode	Set to Normal by default, but this can be changed to IP or TCP port.
Allow DPA via the username for SSH/Telnet	Configure direct port access for SSH and Telnet based on username. Disabled by default.

Setup > Services

### Network Service Settings

Enable HTTP

Enable HTTP to HTTPS Redirect

HTTP Port:  
80

Enable HTTPS

HTTPS Port:  
443

Encryption:  
SSL

Enable TELNET Access

Telnet Port:  
23

Enable SSH Access

SSH Port:  
22

Auth Method  
Both Certificate and Pas

Enable Local Port Access

Bits Per Second:  
115200

Direct Port Access Mode:  
TCP Port

Allow DPA via the username for SSH/Telnet.

Fixed TCP Window

OK Cancel

---

## Change Network Service Settings

► **To change network service settings:**

1. Choose Setup > Services. The Network Service Settings page opens.
2. Make any necessary changes to the appropriate fields.
3. Fixed TCP Window is checked by default, enabling SSH connection to work under the Windows Vista® operating system.

---

*Note: Some operating systems may require TCP window scaling for successful SSH connections, in which case the 'Fixed TCP Window' option needs to be disabled.*

*Note: Customers experiencing slow SSH connectivity in SX 3.1.5 or select the SX 3.1.6 after upgrading to SX 3.1.7 should enable the ssh enable true setting to avoid this issue in the future.*

---

4. Click OK.

---

## Configuring Modem Access

► **To set up SX access via a modem:**

1. Choose Setup > Modem. The Modem Settings page opens.

Setup > Modem

---

### Modem Settings

Enable Modem

**Modem Access Modes:**

All ▼

**PPP Server IP:**

10.0.0.1

**PPP Client IP:**

10.0.0.2

Enable Modem Dial Back

OK

Cancel

2. Select the Enable Modem check box to enable modem access.
3. For the Modem Access Mode, do one of the following:

- a. Select All to allow modem access to all modems. Looks for a PPP signal and falls back to allow console access if the PPP signal is not detected. In this mode, Modem Dial Back cannot be enabled.
  - b. Select PPP Only to allow only PPP connections. Allows GUI, SSH and Telnet access (if enabled).
  - c. Select Console Only to allow only console connections. Allows only CLI access through a terminal emulation programs such as Hypertterminal.
4. If you selected All or PPP Only as the modem access mode:
    - a. Type the IP addresses of the Point-to-Point (PPP) server in the PPP Server IP field. The default is 10.0.0.1
    - b. Type the IP address of the PPP client in the PPP Client IP field. The default is 10.0.0.2.
  5. If you selected PPP Only as the modem access mode:
    - a. If you want to enable modem dialback, select the Enable Modem Dial Back check box.
  6. Click OK. Modem access is enabled. Reboot the modem so the changes to take effect.

---

## Configuring IP Forwarding and Static Routes

You can enable IP forwarding. You can also create static routes if your SX has two LAN ports or is configured for modem access.

---

### Enable IP Forwarding

► **To enable IP forwarding:**

1. Choose Setup > Static Routes. The Static Routes page opens.
2. Go to the IP Forwarding panel and click the Enable IP Forwarding checkbox.



Enable IP Forwarding

3. Click OK. IP forwarding is enabled.

## Add a New Static Route

### ► To add a new Static Route:

1. Choose Setup > Static Routes. The Static Routes page opens.

Static Route List

<input type="checkbox"/>	Interface	Destination	Mask	Gateway	MTU	Window	IRTT	Flags
<input type="checkbox"/>	LAN 1	192.56.76.0	255.255.255.0	0.0.0.0	0	0	0	0
<input type="checkbox"/>	LAN 1	0.0.0.0	0.0.0.0	192.168.60.126	0	0	0	0

2. Go to the Static Routes List and click Add New Route.

**Route**

**Interface:**

**Destination:**

**Mask:**

**Gateway:**

**MSS:**

**Window:**

**IRTT:**

**Flags:**

3. For an SX with one LAN interface, LAN appears automatically in the Interface field. On an SX with two LAN interfaces, select the one you want from the drop-down menu in the Interface field.
  - LAN1 = eth0
  - LAN2 = eth1
4. Type the IP address, subnet mask, and gateway of the destination host in the Destination, Mask, and Gateway fields.

5. Type the TCP maximum segment size (MSS) in bytes in the MSS field.
6. Type the TCP windows size for connections over this route in bytes in the Window field.
7. Type the initial round trip time (IRTT) for TCP connections over this route in milliseconds (1-12000) in the IRTT field.
8. Select your route type from the Flags drop-down menu.
  - Host means this route is for a host machine.
  - Net means this route is for a subnet.
9. Click OK.

---

### Delete a Static Route

► **To delete a static route:**

1. Choose Setup > Static Routes. The Static Routes page opens, containing an Enable IP Forwarding panel and a Static Routes List.
2. Go the Static Routes List and select the checkbox next to the route you want to delete.
3. Click Delete. You are prompted to confirm the deletion.
4. Click OK. The route is deleted.

# Chapter 4 User Profiles and Groups

## In This Chapter

Managing User Profiles .....47  
Managing User Groups .....51

---

### Managing User Profiles

User profiles serve two purposes:

- To provide users with a username and password to log into the SX.
- To associate the user with a user group. The user group determines which system functions and ports the user can access.

The SX is shipped with one user profile built in: the admin user. This profile is associated with the Admin user group and has full system and port permissions. This profile cannot be modified or deleted.

Up to 140 users are supported by the SX. You can create individual user profiles for each person who is logging into the SX, or you can create a limited number of profiles and allow more than one person to use each profile.

---

#### Display a List of User Profiles

1. To display a list of existing user profiles, choose User Management > User List. The User List page opens.

User List

<input type="checkbox"/>	Username	Full Name	Dialback	Group	Active
<input type="checkbox"/>	Alexander	Alexander		Designers	Yes
<input type="checkbox"/>	Andre	Andre		Managers	Yes
<input type="checkbox"/>	Charlie	Charles Kord		Designers	Yes
<input type="checkbox"/>	Elaine	Elaine		Admin	Yes
<input type="checkbox"/>	Erma	Erma Kall		Admin	Yes
<input type="checkbox"/>	Lauren	Lauren		Managers	Yes
<input type="checkbox"/>	Maureen	Maureen Rand		Admin	Yes
<input type="checkbox"/>	Stan	Stan		Admin	Yes
<input type="checkbox"/>	Vic	Victor		Admin	Yes
	admin	Administrator		Admin	Yes

2. The User List page shows every user profile created to date, and for each one, lists:
  - Username
  - Full name
  - Dialback number (if one has been defined)

- User group
3. The User List page also indicates whether the user profile is active or inactive.

---

### Create a User Profile

► **To create a new user profile:**

1. Choose User Management > User List. The User List page opens (as shown in **Display a List of User Profiles** (on page 47)).
2. Click Add New User. The New User page opens.

**New User**

**Username:**

**Full Name:**

**Dialback:**

**Information:**

**Password:**

**Confirm Password:**

**User Group:**  
Admin

Active

3. Type a login name in the Username field. This is the name the user enters to log into the SX. This field is required.
  - You can enter any number of characters up to a maximum of 255.
  - You can enter any printable character except " ' < > \ &
  - The user name is case sensitive.

4. Type the user's full name in the Full Name field. This field is required.
5. Type the user's telephone number in the Dialback field. This field is optional.
6. Type any comments about the user profile in the Information field. This field is to help you identify the profile and is optional.
7. Type the password in the Password field, and then type it again in the Confirm Password field. This field is required.
  - You can enter any number of characters up to a maximum of 64.
  - You can enter any character except " ' < > \ &
  - The password is case sensitive.

---

*Note: If the strong password feature is enabled, there are other password requirements. See **Port Configuration and Port Access Application** (on page 61) for details.*

---

8. Select a user group from the drop-down menu in the User Group field. By default, the Admin group is entered.

---

*Tip: If the user group you want has not yet been created, you can create it and then return to the user profile and select it. For now, keep the default.*

---

9. Decide whether or not to activate this profile immediately. By default, the Active checkbox is selected. To deactivate this account, deselect this checkbox. You can return at any time and activate the user when necessary.
10. Click OK. The user profile is created and should appear in the User List page.

### SSH Connections for Users

If needed, configure a SSH (Secure Shell) via client certificate for a user. The user must first be created before the client certificate can be added.

#### ► To add a SSH client certificate to the user:

1. Create the user. See **Create a User Profile** (on page 48).
2. From the User page, click on the name of the user you want to add a SSH client certificate to. The User's page opens.
3. Select the Add SSH Key radio button.
4. Enter the SSH key data in the SSH Key Data box. This data is the rsa\_id.pub key generated for your client.
5. Click Apply.

- When you SSH with this user, the key data should be used for authentication and you should not have to enter a password.

SSH Keys

Stored SSH Keys : 0

Delete SSH Key

SSH Key Index:

Add SSH Key

SSH Key Data:

► **To delete an SSH key:**

- Click on the Delete SSH Key radio button.
- In the SSH Key Index, enter the SSH key's index.
- Click Apply.

---

**Modify a User Profile**

► **To modify an existing user profile:**

- Choose User Management > User List. The User List page opens (as shown in **Display a List of User Profiles** (on page 47)).
- Click the Username of the profile you want to edit. The Edit User page opens. It looks exactly like the New User page (as shown in **Create a User Profile** (on page 48)).
- You can change any of the fields except the Username field.

- For security reasons, the password is not displayed. To change the profile's password, type a new password in the Password and Confirm Password fields. If you leave these fields as is, the password is unchanged.

Passwords are case sensitive and can contain up to 64 alphanumeric characters with the exception of " ' < > \ &

- Click OK when finished. The user profile is modified.

---

### Delete a User Profile

► **To delete an existing user profile:**

- Choose User Management > User List. The User List page opens (as shown in **Display a List of User Profiles** (on page 47)).
- Click the checkbox to the left of the user profile you want to delete. You can select more than one.
- Click Delete. You are prompted to confirm the deletion.
- Click OK. The selected user profiles are deleted.

---

## Managing User Groups

User groups serve two purposes:

- To determine which system functions the users associated with a group are permitted to perform
- To determine which ports the users associated with a group are permitted to access

The SX is shipped with one user group built in: the Admin user group. Users associated with this group can perform all system functions and access all ports. This group cannot be modified or deleted.

You can create as many other user groups as necessary.

---

### Display a List of User Groups

To display a list of existing user groups, choose User Management > User Group List. The Group List page opens.

Group List

	Group	Class
	Admin	Administrator
<input type="checkbox"/>	Designers	Observer
<input type="checkbox"/>	Managers	Operator
<input type="checkbox"/>	Support	Operator
<input type="checkbox"/>	Writers	Operator

The Group List page shows every user group created to date, and for each one gives the group's name and class.

---

### Create a User Group

▶ **To create a new user group:**

1. Choose User Management > User Group List. The Group List page opens (as shown in ***Display a List of User Groups*** (on page 51)).

2. Click Add New User Group. The New Group page opens.

**New Group**

**Group Name:**

**Class:**  
Operator

**Port Sharing**

**Port Access:**

<input type="checkbox"/> <b>Select All</b>	<input type="checkbox"/> <b>02: Henschman 24 PCS12-2</b>
<input type="checkbox"/> <b>01: Triana</b>	<input type="checkbox"/> <b>04: ThePerfectMan</b>
<input type="checkbox"/> <b>03: Henschman 21</b>	<input type="checkbox"/> <b>06: Port6</b>
<input type="checkbox"/> <b>05: Port5</b>	<input type="checkbox"/> <b>08: Port8</b>
<input type="checkbox"/> <b>07: Port7</b>	<input type="checkbox"/> <b>10: Port10</b>
<input type="checkbox"/> <b>09: Port9</b>	<input type="checkbox"/> <b>12: Port12</b>
<input type="checkbox"/> <b>11: Port11</b>	<input type="checkbox"/> <b>14: Port14</b>
<input type="checkbox"/> <b>13: Port13</b>	<input type="checkbox"/> <b>16: Port16</b>
<input type="checkbox"/> <b>15: Port15</b>	

- |  |  |
|--|--|
| <input type="checkbox"/> 17: Port17    | <input type="checkbox"/> 18: Port18    |
| <input type="checkbox"/> 19: Port19    | <input type="checkbox"/> 20: Port20    |
| <input type="checkbox"/> 21: Port21    | <input type="checkbox"/> 22: Port22    |
| <input type="checkbox"/> 23: Port23    | <input type="checkbox"/> 24: Port24    |
| <input type="checkbox"/> 25: Port25    | <input type="checkbox"/> 26: Port26    |
| <input type="checkbox"/> 27: Port27    | <input type="checkbox"/> 28: Port28    |
| <input type="checkbox"/> 29: Port29    | <input type="checkbox"/> 30: Port30    |
| <input type="checkbox"/> 31: Loop Back | <input type="checkbox"/> 32: Loop Back |

**Power Access:**

- Select All
- 01: Triana
- 02: Henschman 24 PCS12-20
- 03: Henschman 21
- 04: ThePerfectMan
- 05: Port5
- 06: Port6
- 07: Port7
- 08: Port8
- 09: Port9
- 10: Port10
- 11: Port11
- 12: Port12
- 13: Port13
- 14: Port14

15: Port15  
 16: Port16  
 17: Port17  
 18: Port18  
 19: Port19  
 20: Port20  
 21: Port21  
 22: Port22  
 23: Port23  
 24: Port24  
 25: Port25  
 26: Port26  
 27: Port27  
 28: Port28  
 29: Port29  
 30: Port30  
 31: Loop Back  
 32: Loop Back

3. Type a group name in the Group Name field.
  - You can enter any number of characters up to a maximum of 255.
  - You can enter all letters and numbers, as well as the underscore character (\_).
  - The user name is case sensitive.
4. Select the class from the drop-down menu in the Class field. Your choices are:
  - Operator - This is the default. Users associated with the Operator class have read/write access to the console window, and cannot change any system configuration parameters except their own password.
  - Observer - Users associated with the Observer class have read-only access to the console window, and cannot change any system configuration parameters except their own password.
5. Port Sharing: By checking this option, users in the group are allowed to access a port that already has users connected to it, if the port access mode is set to Share. (See **Login Settings** (see "**Login Handling**" on page 98) for information about port access mode.)

6. Select the ports that the users associated with this group are permitted to access. You can select all ports or you can select any combination of individual ports.
7. Select the ports for which users associated with the group are allowed to access the power commands. Only administrators can access the power strips via CLI directly.
8. Click OK. The user group is created and should appear in the User List page.

---

### Modify a User Group

► **To modify an existing user group:**

1. Choose User Management > User Group List. The Group List page opens (as shown in **Display a List of User Groups** (on page 51)).
2. Click the Group Name of the group you want to edit. The Edit Group page opens. It looks exactly like the New Group page (as shown in **Create a User Group** (on page 52)).
3. You can change any of the fields except the Group Name field.
4. Click OK when finished. The user group is modified.

---

### Delete a User Group

► **To delete an existing User Group:**

1. Choose User Management > User Group List. The Group List page opens (as shown in **Display a List of User Groups** (on page 51) section).
2. Select the checkbox to the left of the user group you want to delete. You can select more than one.
3. Select Delete. You are prompted to confirm the deletion. Click OK. The selected user group is deleted.

# Chapter 5 Remote Authentication

## In This Chapter

Configuring RADIUS.....	57
Configuring LDAP .....	58
Configuring TACACS+ .....	59

---

## Configuring RADIUS

You can use Remote Dial-In User Service (RADIUS) to authenticate SX users instead of local authentication. To configure RADIUS:

1. Choose Setup > Remote Authentication. The Remote Authentication page opens, displaying a RADIUS panel.

**Radius**

**Primary Radius**

**IP Address:**

**Port:**

**Secret:**

**Secondary Radius**

**IP Address:**

**Port:**

**Secret:**

2. In the RADIUS panel, click the RADIUS button to enable RADIUS authentication.
3. Under Primary Radius, type the following information:
  - IP address of the RADIUS server
  - Port on which the RADIUS server is listening (default is 1812)
  - Shared secret
4. If you have a backup RADIUS server, enter the same information in the Secondary Radius fields.

5. Click OK. RADIUS authentication is enabled.

---

## Configuring LDAP

You can use the Lightweight Directory Access Protocol (LDAP) to authenticate SX users instead of local authentication. To configure LDAP:

1. Choose Setup > Remote Authentication. The Remote Authentication page opens, displaying an LDAP panel.

<input checked="" type="radio"/> LDAP	<input type="checkbox"/> Secondary LDAP
<b>LDAPS Certificate Settings</b>	
<b>Primary LDAP</b>	
<b>IP Address:</b>	<b>IP Address:</b>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
<b>Port:</b>	<b>Port:</b>
<input type="text" value="389"/>	<input type="text" value="389"/>
<b>Secret:</b>	<b>Secret:</b>
<input type="text"/>	<input type="text"/>
<b>Base DN:</b>	<b>Base DN:</b>
<input type="text"/>	<input type="text"/>
<b>Query:</b>	<b>Query:</b>
<input type="text"/>	<input type="text"/>
<b>Search:</b>	<b>Search:</b>
<input type="text"/>	<input type="text"/>
<b>Dialback Query String:</b>	<b>Dialback Query String:</b>
<input type="text"/>	<input type="text"/>

2. In the LDAP panel, click the LDAP button to enable LDAP authentication.
3. Under Primary LDAP, type the IP address of the LDAP server and the port it is listening on (default is 389) in the IP Address and Port fields.
4. Type the root password to access the directory server/manager in the Secret field. The name for this field depends on the Directory Server. For example, Microsoft Windows Active Directory® refers to the field as Password, while the SUN iPlanet directory server uses Secret.
5. Type the 'root' point to bind to the server in the Base DN field. This is the same as Directory Manager DN (for example, BaseDn: cn=Directory Manager).
6. Type a string in the Query field. Make sure the same string is added as an attribute in the Search field. For example, if the authorization query string is SX, an attribute named SX must be added under the given domain specified by the Search field. On top of that, a user group must have been created in SX to map with the one in Windows Active Directory for these configurations to work correctly.

7. Type the domain name where the search starts in the Search field. The Search field is the sub-tree of the Base DN to direct the search to the path of the user information such as UID and speed up search time. In other words, it is the domain name. This is where the search starts for the user name. The user name is created in this domain (for example, Search: dc=raritan, dc=com) to process LDAP authentication queries from SX.
8. If you are using a modem to connect to the LDAP server, type a dialback string in the Dialback Query String field.
9. If you have a backup LDAP server, enter the same information in the Secondary LDAP fields.
10. Click OK. LDAP authentication is enabled.

---

## Configuring TACACS+

You can use the Terminal Access Controller Access-Control System Plus (TACACS+) to authenticate SX users instead of using local authentication. To configure TACACS+:

1. Choose Setup > Remote Authentication. The Remote Authentication page opens, displaying a TACACS+ panel.

**TACACS+**

**Primary TACACS+**

**IP Address:**

**Port:**

**Secret:**

**Secondary TACACS+**

**IP Address:**

**Port:**

**Secret:**

2. In the TACACS+ panel, click the TACACS+ button to enable TACACS+ authentication.
3. Under Primary TACACS+, type the IP address of the TACACS+ server and the port on which it is listening (default is 49) in the IP Address and Port fields.

4. Type the root password to access the directory server/manager in the Secret field. The name for this field depends on the Directory Server. For example, Microsoft Windows Active Directory® refers to the field as Password, while the SUN iPlanet directory server refers to it as Secret.
5. If you have a backup TACACS+ server, enter the same information in the Secondary TACACS+ fields.
6. Click OK. TACACS+ authentication is enabled.

# Chapter 6 Port Configuration and Port Access Application

## In This Chapter

Port Keywords .....	62
Port Configuration.....	63
Direct Port Access .....	65
Direct Port Access via Username for SSH and Telnet .....	66
Direct Port Access via HTTP .....	66
Anonymous Port Access .....	67
Raritan Serial Console.....	67
Raritan Serial Console Requirements for Java .....	68
Raritan Serial Console Interface .....	71
Standalone Raritan Serial Client Requirements.....	87
Installing Standalone RSC for Windows.....	91
Launching RSC on Windows Systems.....	93
Installing RSC for Sun Solaris and Linux .....	94
Launching RSC on Sun Solaris.....	95

---

## Port Keywords

You can create port keywords and associate them with:

- Events
- Local/remote syslog messages
- SNMP traps

Port keywords work as a filter. If a keyword is detected, a corresponding message is logged in a local/NFS port log. A corresponding event is sent via SMTP (if configured) and corresponding trap is sent via SNMP (if configured).

Port keywords are useful for notifying administrators if a particular event occurs on a port, but they do not affect NFS log sizes.

---

*Note: The SMTP notification (event.amp.keyword) is selected from the Event configuration page.*

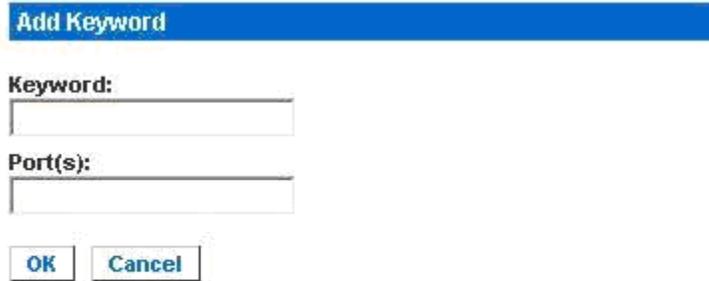
---

---

*Note: For keywords to trigger when no users are connected to the port, "Always Active" in port configuration should be set to True. See **Port Configuration** (on page 63) for details.*

---

1. Choose Setup > Port Keywords. The Port Keywords page opens.



**Add Keyword**

Keyword:

Port(s):

### Keyword List

2. Type a keyword in the Keyword field.
3. Type the Port(s) you want to associate with that keyword.
4. Click OK.

## Port Configuration

### ► To configure one or more ports:

1. Choose Setup > Port Configuration. The Port Configuration page opens.

Port Configuration

#	No	Name	Application	Baud Rate	Parity Bits	X on / X off	HW Flow
<input type="checkbox"/>	1	Port1	RaritanConsole	9600	None/8	Enabled	Disabled
<input type="checkbox"/>	2	Port2	RaritanConsole	9600	None/8	Disabled	Disabled
<input type="checkbox"/>	3	Port3	RaritanConsole	9600	None/8	Disabled	Disabled
<input type="checkbox"/>	4	Port4	RaritanConsole	9600	None/8	Disabled	Disabled

2. Select the port(s) you want to configure. You can select one port or several ports, providing that all selected port configurations are identical.
  - To select specific ports, click the checkboxes to the left of the port numbers and then click Edit.
  - To select all ports, click Select All.

The Edit Port page opens.

3. Make sure the port values match the target system's serial port configuration for the first three values.
  - Select the value of Bits Per Second from the Bits Per Second drop-down menu.
  - Select the Parity Bits from the Parity Bits drop-down menu.
  - Select the Flow Control from the Flow Control drop-down menu.
4. In the Detect field, indicate whether you want the SX to detect or not detect the physical connection to the target. The default is Do Not Detect. Change this by selecting Detect Physical Connection to the Target from the drop-down menu in the Detect field.
5. Type a command in the Exit Command field, for example, logout. This is the command that is sent to your system when a user with write permission disconnects from the port. The main function of this command is to ensure that the user's session on the target machine is closed; however, it is not imperative to have an Exit command configured on a port.
6. Select the Escape Mode. The default is None. The escape sequence affects only the CLI. When entering the escape mode, the user is given a menu of commands that can be performed (for example, gethistory, power commands, and so forth), a command to return to the port session, and a command to exit the port connection.

Change as follows:

- Select control from the drop-down menu in the Escape Mode field.
- Type the character in the Escape Character field. The default for the SX is ] (closed bracket).

---

*Note: See **Configuring Ports** (on page 177) for details on port configuration commands.*

---

7. Select the terminal emulation type from the drop-down menu in the Emulation field. The choices are:
  - VT100
  - VT220
  - VT320
  - ANSI
8. Set Encoding if you want the RSC for this port to always use a specific character encoding. It overrides the global RSC setting for this port to whatever value you set. The choices are: DEFAULT,US-ASCII,ISO8859-1, ISO8859-15,UTF-8, Shift-JIS, EUC-JP, EUC-CN, EUC-KR.
9. If you need to configure the length of the send break signal for targets that require a short or longer sendbreak duration, enter the send break time in the Send Break Duration field. The send break is configurable from 100ms - 1000ms in 100ms increments.
10. If you plan to use Direct Port Access (DPA), you must enter either an IP address or one/both of the following TCP ports, depending on your choice of the DPA service mode:
  - The port number, such as 7700, in the DPA SSH TCP Port field
  - The port number, such as 8800, in the DPA Telnet TCP Port field.
11. In the Always Active field, indicate if you want to log activities coming into a port even if no user is connected. The default option is to not maintain port access without a connected user, which means: ignore data coming into a port when no user is connected. Change by selecting Maintain port access continuously from the drop-down menu in the Always Active field. This option is for NFS port data logs.

---

*Note: When no users are logged into a port session, port traffic, by default, is discarded .*

---

12. Select none or all from the drop-down menu of Messages suppressed field to indicate if any message should be displayed during a DPA connection, such as "Authentication successful." Otherwise, it goes directly to the port without displaying any message. The default is none.

---

*Note: Anonymous access should be enabled for DPA to succeed.*

---

13. Select from the Multiple Writers drop-down if you want multiple clients to be able to write to the port at the same time. The default behavior is that only one user may have write access to the port at a single time.
14. Click OK.

---

## Direct Port Access

► **To configure direct port access:**

1. Choose Setup > Services. The Network Service Settings page opens.
2. In the Direct Port Access Mode field, the default is Normal, which means CLI DPA access is disabled. To enable DPA, select either IP or TCP Port from the drop-down menu.
3. Click OK to save this information. The page displays the following message: "Reboot for the changes to take effect."
4. You may reboot now if you have already set up the ports for DPA or are otherwise prepared for the DPA mode to become effective.
5. Choose Setup > Port Configuration. The Port Configuration page opens (as shown in **Port Configuration** (on page 63)).
6. Select the ports to configure for direct port access:
  - To select specific ports, click the checkboxes to the left of the port number. You can select more than one. When you have finished, click Edit.
  - To select all the ports, click Select All.

The Edit Port Configuration page opens (as shown in **Port Configuration** (on page 63)). The DPA fields are at the bottom of the page.

7. Type the DPA IP address of the SX and the DPA ports used for SSH and Telnet in the appropriate fields.
8. Click OK.
9. Reboot the SX. This is necessary for the direct port access settings to take effect.

---

## Direct Port Access via Username for SSH and Telnet

You are able to configure direct port access for SSH and Telnet based on username.

► **To enable direct port access via username for SSH and Telnet:**

1. Choose Setup > Services. The Network Service Settings page opens.
2. Select the "Allow DPA via the username for SSH/Telnet" checkbox.

Direct Port Access Mode:

IP

Allow DPA via the username for SSH/Telnet.

3. Click OK to save this information. The page displays the following message: "Reboot for the changes to take effect."
4. You may reboot now if you have already set up the ports for DPA or are otherwise prepared for the DPA mode to become effective.

With the DPA for username setting, it automatically applies to all ports without needing any configuration.

5. To access a port with this username based DPA, use the following ssh command to connect to the SX: `ssh -l name[:portname/number]` where name is the username, portname is the port name and number is the port number.

---

## Direct Port Access via HTTP

You can connect directly to a port on the SX without having to log in to a GUI interface by using HTTP.

► **To access the a SX port using HTTP:**

- Use the following address:

`http://<sxIPAddress>/dpa.php?username=<SXUserName>&password=<SXPassword>&port=<PortNumber>`

---

## Anonymous Port Access

Anonymous port access allows users to access DPA configured ports without entering a password.

► **To enable the feature:**

1. Choose Security > Login Settings. The Login Settings page opens (as shown in **Login Settings** (on page 97)).
2. Make sure the Anonymous Port Access checkbox at the bottom of the page is selected.
3. Click the User Management tab, and then click User Group List. The Group List appears (as shown in **Display a List of User Groups** (on page 51)).

---

*Note: See **User Profiles and Groups** (on page 47) for additional information about user groups.*

---

4. The Anonymous Group automatically appears in the User Group List.
5. The default group belongs to Operator class and has no port permission assigned.
6. Select the ports for which you want anonymous port access in the Port Access field.
7. Click OK.

---

## Raritan Serial Console

Use the following steps to launch the Raritan Serial Console (RSC).

1. Click the Port Access tab.

**Port Access**

▲ No	Name	Status
1	Port1-RedHatLinux7	Up
2	Port2-RedHatLinux	Up
3	Port3	Up
4	Port4	Up
5	Port5	Up
6	Port6	Up
7	Port7-HP8000 Switch	Up
8	Port8	Up

2. Click the Name of the port you want to access for the RSC, for example, Port1 or Port2. Firefox users are prompted to enter the personal client certification key.

---

*Note: A Security message appears only if you use HTTPS to connect to the RSC.*

---

3. Click Yes. A Warning - Security pop up appears.
4. Click Yes to access the Raritan Serial Client from the Port page.

---

*Note: If you click Always, security pop up is displayed when the SX is accessed in the future.*

---

The Raritan Serial Console window appears. See **Raritan Serial Client Interface** (see "**Raritan Serial Console Interface**" on page 71).

---

## Raritan Serial Console Requirements for Java

The Raritan Serial Console (RSC) requires a PC of minimum 1.0 GHz CPU speed with 512 MB RAM. Java™ must be installed to access targets (managed devices) before you can use the RSC.

---

### Java Runtime Environment (JRE)

The RSC functions with JRE™ version 1.4.2\_05 or later (except for JRE version 1.5.0\_02). However, for optimum performance, Raritan recommends using JRE 1.5.0 (except for version 1.5.0\_02).

Depending on your operating system and browser, it is possible that you must adjust JRE configurations to prevent problems with the system's memory.

---

*Note: Raritan does not support JRE version 1.5.0\_02 for use with the RSC.*

---

JRE provides configuration instructions with the JRE download. Determine the JRE version on your system by going to the Java™ Web page at:

**<http://www.java.com/en/download/help/testvm.xml>**  
**(<http://www.java.com/en/download/help/testvm.xml> to**  
**<http://www.java.com/en/download/help/testvm.xml>)**

---

**IMPORTANT: When launching RSC from a browser, Raritan highly recommends that Java Applet Caching be disabled and that you perform the following steps to make sure that Java does not create problems for the system's memory.**

---

## Java Applets and Memory Considerations

Usually, a browse- based RSC does not need to make any changes to the Runtime parameters for Java™ Applets. Following these steps if you notice any "Out of Memory" errors happening when executing RSC via a web browser:

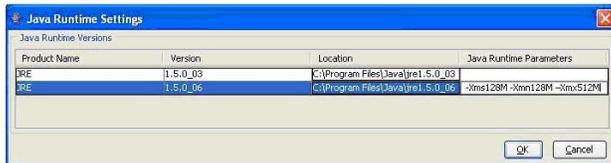
- Change the Runtime settings for Java Applets.
- Use the following links to find out how to use Runtime settings in the Java Control Panel.

**<http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html>**  
 (**<http://java.sun.com/j2se/1.5.0/docs/guide/deployment/deployment-guide/jcp.html>**)

**[http://java.sun.com/j2se/1.4.2/docs/guide/plugin/developer\\_guide/control\\_panel.html](http://java.sun.com/j2se/1.4.2/docs/guide/plugin/developer_guide/control_panel.html)**  
 (**[http://java.sun.com/j2se/1.4.2/docs/guide/plugin/developer\\_guide/control\\_panel.html](http://java.sun.com/j2se/1.4.2/docs/guide/plugin/developer_guide/control_panel.html)**)

To increase the heap settings so that more RSC applets can be launched to access multiple SX targets:

1. Launch the Java Control Panel, located in the:
  - Advanced Tab in JRE™ 1.4.x
  - Java Tab in JRE 1.5
2. Locate Java Runtime Settings.



3. Insert the values of the Java Runtime Parameters using the syntax in the following table, which contains the non-standard options.

Values - Syntax	Description	Default/Comments
-Xms<Size> in bytes	Sets the initial size of the Java heap	2097152 (2MB) <ul style="list-style-type: none"> <li>▪ The -server flag increases the default size to 32M.</li> <li>▪ The values must be a multiple of, and greater than, 1024 bytes (1KB).</li> <li>▪ Append the letter "m" or "M" to indicate megabytes and "k" or "K" to indicate kilobytes.</li> </ul>

Values - Syntax	Description	Default/Comments
-Xmn<Size> in bytes	Sets the initial Java heap size for the Eden generation	640K <ul style="list-style-type: none"> <li>▪ The -server flag increases the default size to 2M.</li> <li>▪ Append the letter “m” or “M” to indicate megabytes and “k” or “K” to indicate kilobytes.</li> </ul>
-Xmx<Size> in bytes	Sets the maximum size to which the Java heap can grow	64M <ul style="list-style-type: none"> <li>▪ The -server flag increases the default size to 128M.</li> <li>▪ The maximum heap limit is approximately 2 GB (2048MB).</li> <li>▪ Append the letter “m” or “M” to indicate megabytes and “k” or “K” to indicate kilobytes..</li> </ul>

Command Example:

```
-Xms128M -Xmn128M -Xmx512M
```

See the following links for additional information and for all the non-standard options:

**<http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/java.html>**  
**(<http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/java.html>)**

**<http://java.sun.com/docs/hotspot/VMOptions.html>**  
**(<http://java.sun.com/docs/hotspot/vmoptions.html>)**

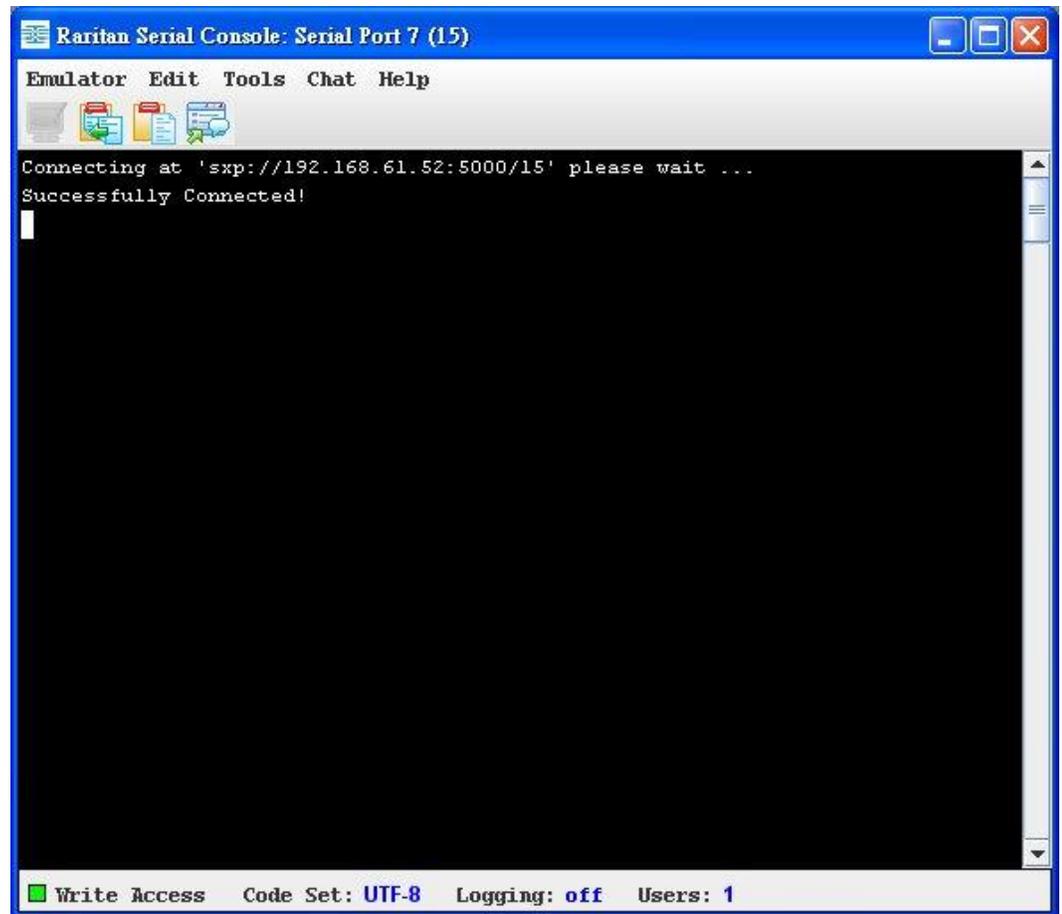
---

## Raritan Serial Console Interface

---

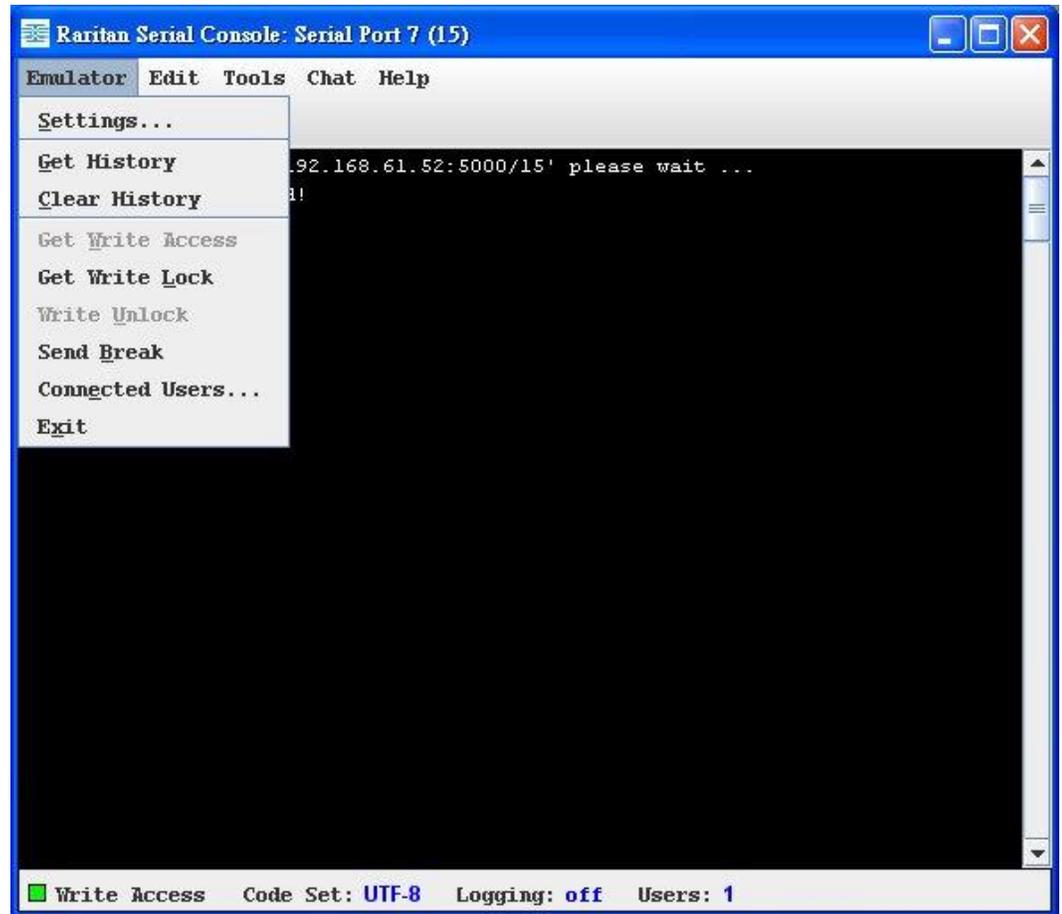
**Important:** The Raritan Serial Console page usually opens in a separate window behind the Port page. With some versions of Java™ on the Windows® operating system, the page opens in front of the Port page.

---



## Emulator

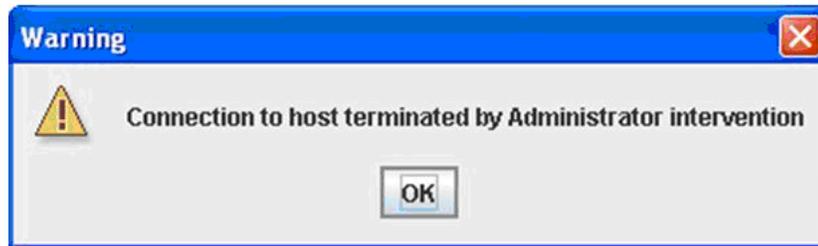
1. Click the Emulator drop-down menu to display a list of topics.



---

**IMPORTANT:** RSC sessions are affected by the Idle Timeout, which is set, by default, to 10 minutes for security purposes. If you have not changed the Idle Timeout setting from the default, your RSC session could be closed automatically if your RSC configuration time exceeds the Idle Timeout period. See *Security* (on page 96) for details on changing the Idle Timeout setting.

---



1. Change the default Idle Timeout setting and then launch the RSC.

---

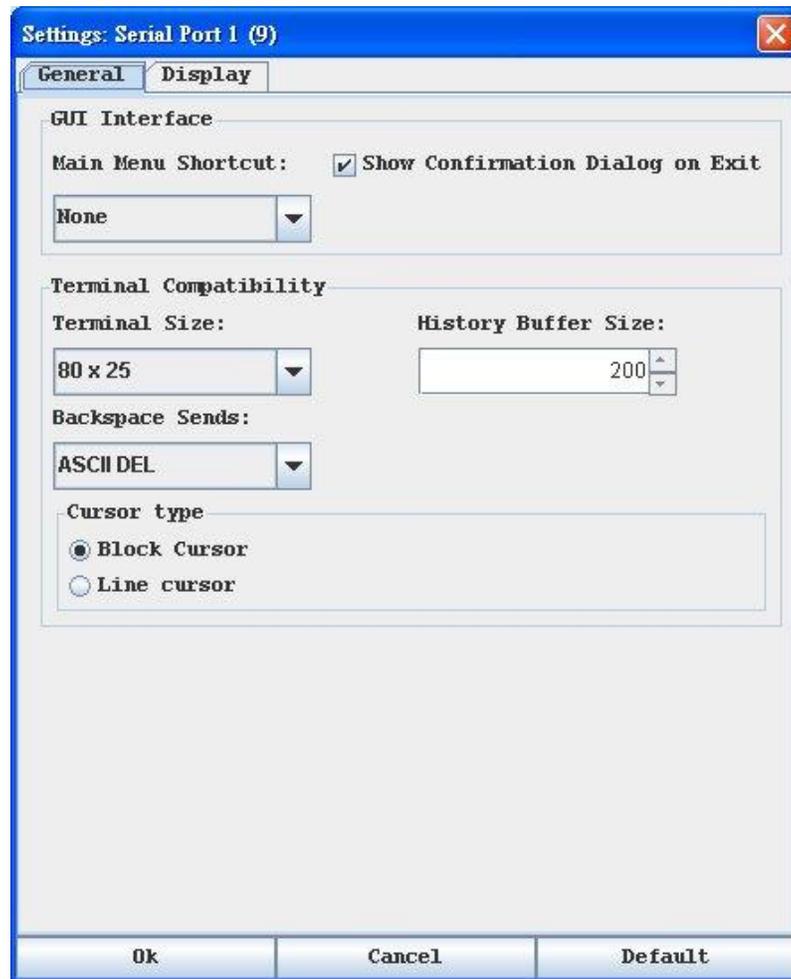
*Note: If the RSC Idle timeout expires, the SX Idle timeout period begins.*

---

Settings

*Note: An Administrator can set Terminal emulation settings using Setup > Port Configuration.*

1. Choose Emulator > Settings. The Settings screen displays the General tab with the default settings.

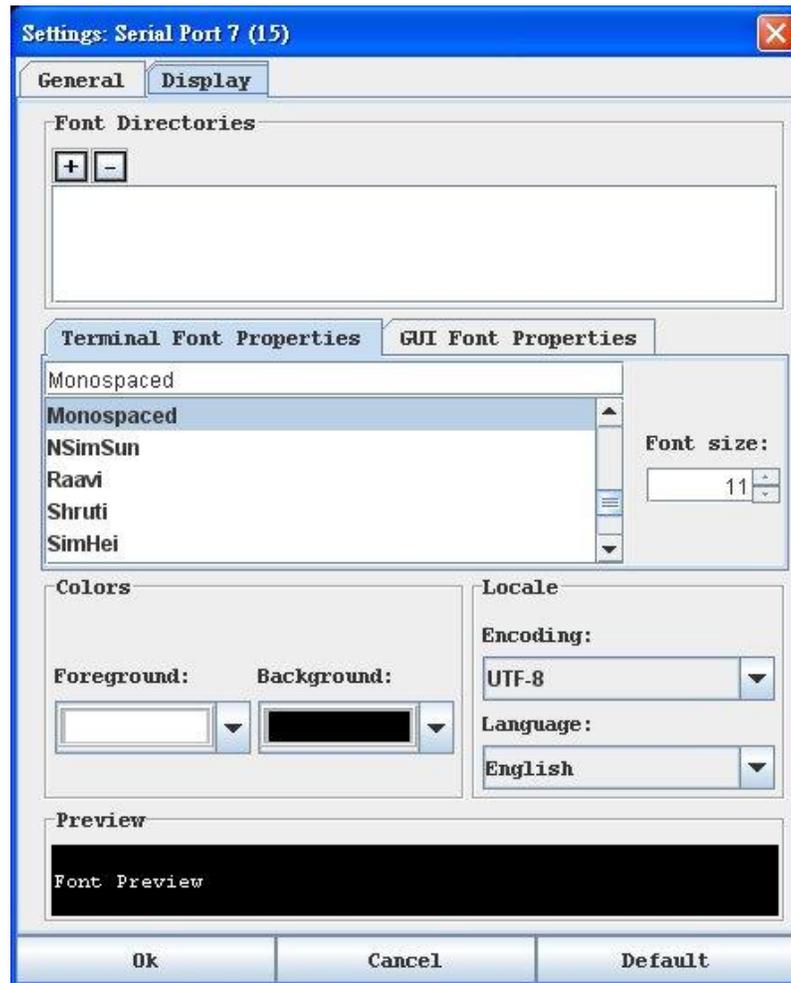


2. The Main Menu Shortcut default is None; accept this, or choose one of the following from the Main Menu Shortcut drop-down menu:
  - F10
  - Alt
3. The Show Confirmation Dialog on Exit checkbox is selected by default, but you can deselect it based on preference.
4. The Terminal Size default is selected, or you can choose a different size from the drop-down menu.

5. The Backspace Sends default is ASCII DEL, or you can choose Control-H from the Backspace Sends drop-down menu.
6. The History Buffer Size default is 200, or you can use the arrows to change the buffer size.
7. The Cursor type default is Block Cursor, or you can select the Line Cursor radio button.
8. Click OK.

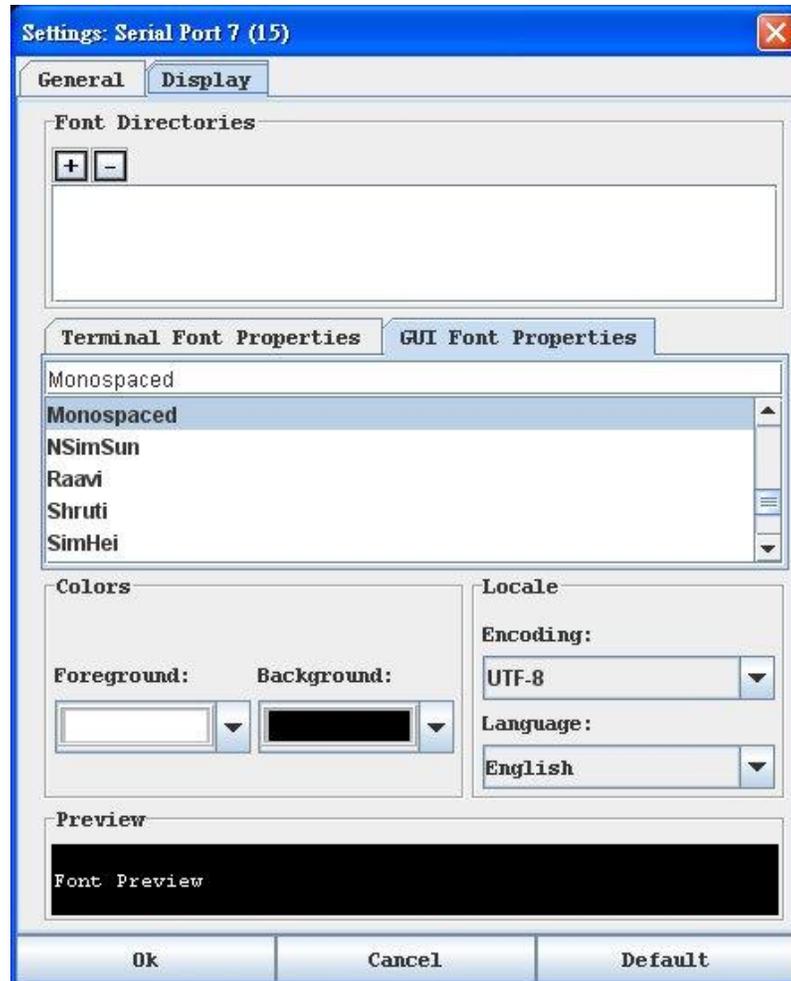
Display Settings

1. Choose Emulator > Settings and click the Display tab.



2. Click Default to accept the Default settings, and then click Ok to close the Display Settings window. To change the settings, follow these steps:
  - a. The Terminal Font Properties default is Arial, or you can choose a font from the Terminal Font Properties scrolling list.

- b. The Antialias Font checkbox is selected by default, or you can deselect the checkbox.
- c. To change the font size, select the Lock Font Size checkbox and then use the arrows to choose a font size in the Font size field.
- d. Click the GUI Font Properties tab
- e. The default font property is Moonscape, or you can choose a font from the GUI Font Properties scrolling list.



---

*Note: For Simplified Chinese characters, Raritan Serial Console supports EUC-CN encoding system.*

---

3. Choose the following from their respective drop-down menus:
  - Foreground Color
  - Background Color
4. Choose one of the following from the Encoding drop-down menu:

- US-ASCII
  - ISO-8859-1
  - ISO-8859-15
5. Choose one of the following from the Language drop-down menu:
    - English
    - Japanese
    - Korean
    - Chinese
  6. Click Ok to close the Display Settings window. If you changed the Language setting, the RSC changes to that language when the Display Settings window is closed.

---

*Note: In case of unrecognized characters or blurry screens that might appear when RSC is launched, due to localization support, try changing the font to Courier New.*

---

#### 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 256 KB (64KB only on models with 64MB SDRAM; 256KB available on 128MB SDRAM Models) 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: Verify the memory on your unit from the Maintenance > Configuration menu. 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 Administrators and Operators can 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 Raritan Serial Console 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 RSC 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 Administrator privileges can send a break.
- Users who are Observers cannot send a break.

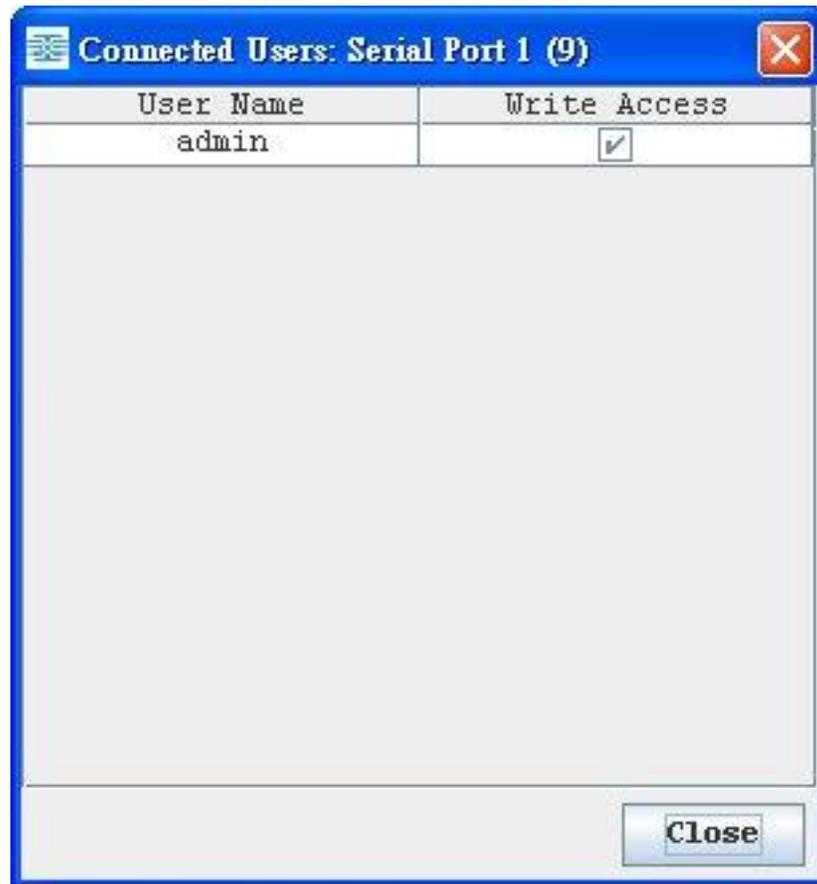
To send an intentional “break” to a Sun Solaris server:

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.

## 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.



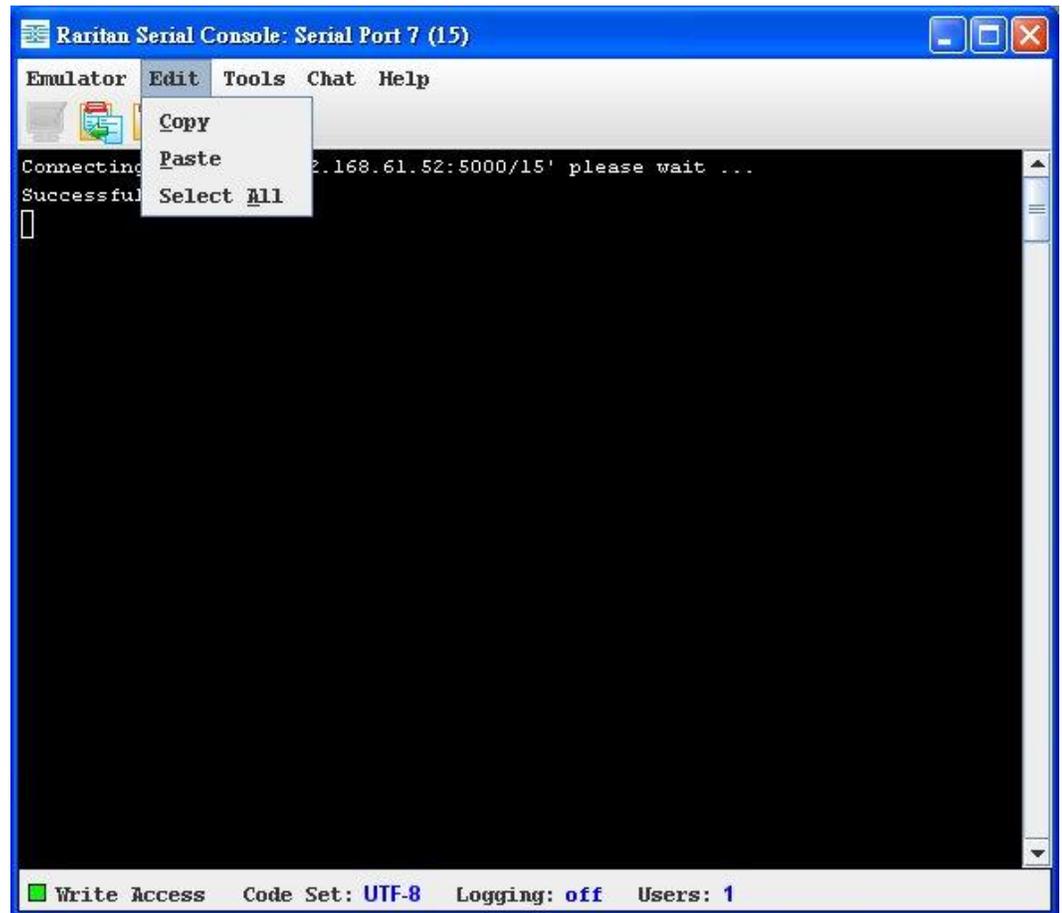
2. A check mark appears in the Write Access column after the name of the User who has Write Access to the console.
3. Click Close to close the Connected Users window.

## Exit

1. Choose Emulator > Exit to close the Raritan Serial Console. The Exit Confirmation dialog appears.
2. Click Yes.

## Edit

Use the Copy, Paste, and Select All text commands to relocate and/or re-use important text.



► **To copy and paste all text:**

1. Choose Edit > Select All.
2. Choose Edit > Copy.
3. Position the cursor at the location where you want to paste the text.
4. Click once to make that location active.
5. Choose Edit > Paste.

---

*Note: The copy-paste limit of text in Raritan Serial Console is 9999 lines.*

---

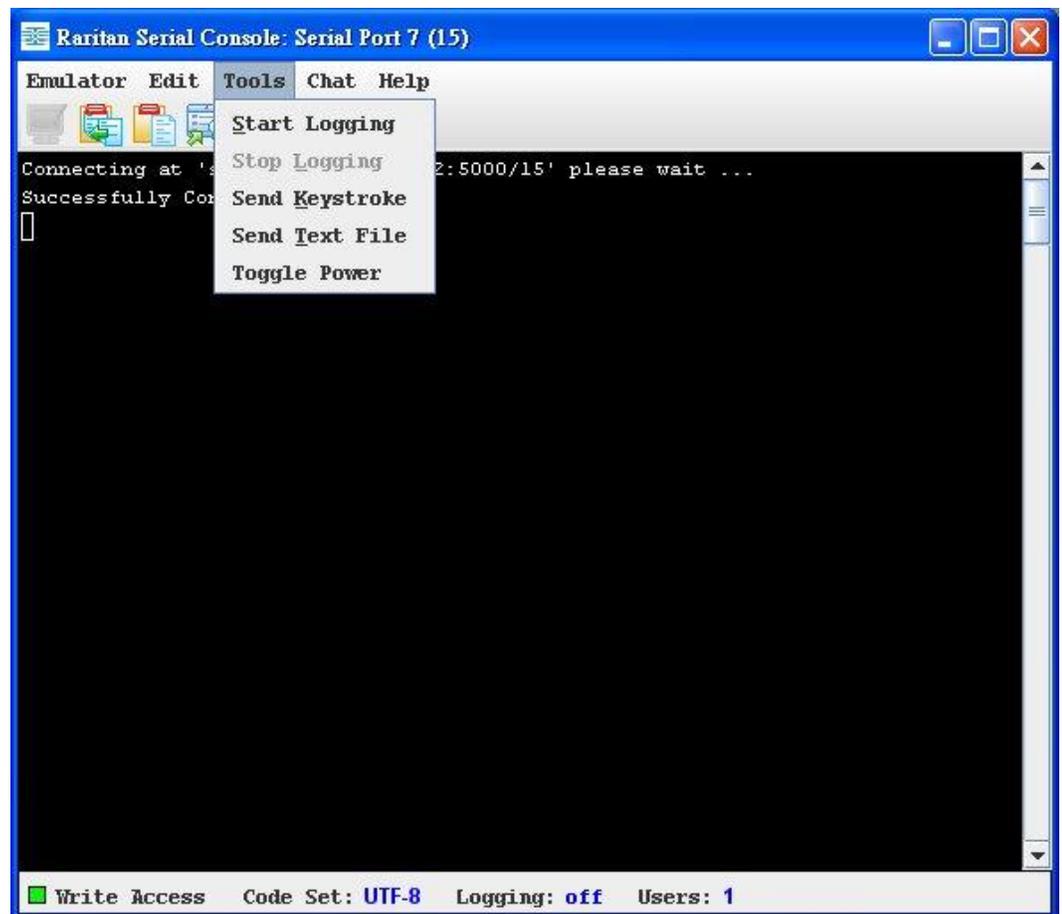
Keyboard shortcuts to highlight, copy, and paste all or partial lines of text:

- Click and drag your mouse over the text you wish to copy.
- Use Ctrl+C to copy text.
- Position the cursor where you want to paste the text and click in that location to make it active.
- Use Ctrl+V to paste text.

---

## Tools

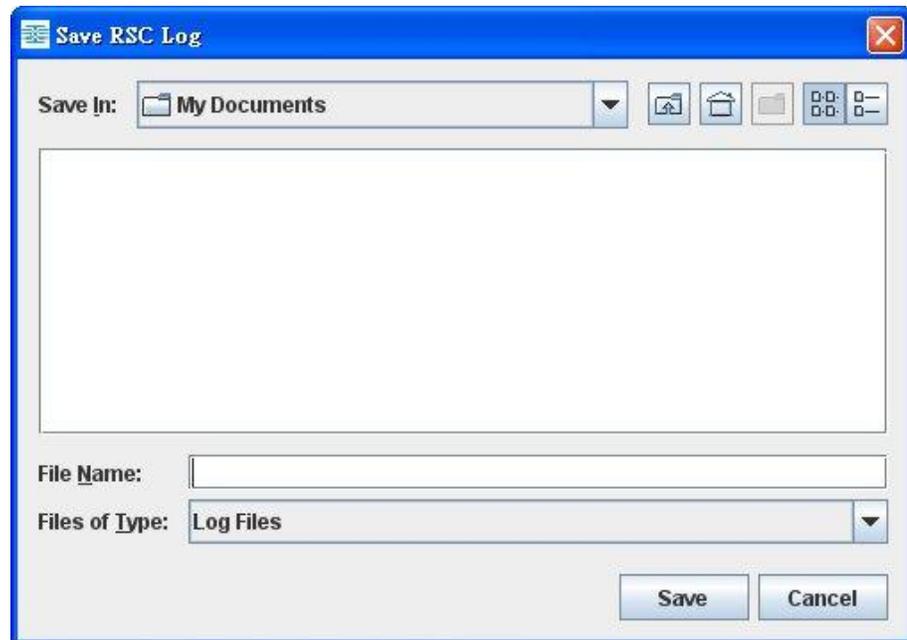
Click the Tools drop-down menu to display a list of topics.



### Start Logging

The Start Logging function allows you to collect raw console data from the target device and save it to a file on your computer. When you start RSC, the Logging indicator on the status bar indicates whether logging is on or off.

1. Choose Tools > Start Logging.
2. Choose an existing file or provide a new file name in the Save RSC Log dialog.
  - When an existing file is selected for logging, data gets appended to the contents.
  - If you provide a new file name, a new file is created.



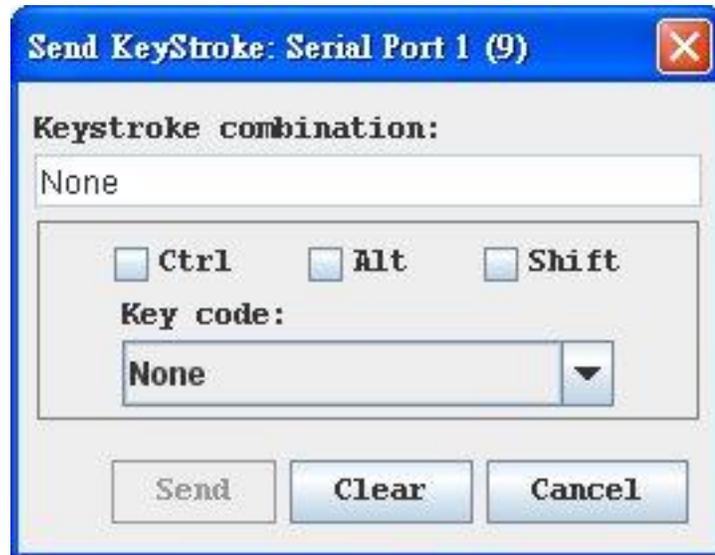
3. Click Save after selecting or creating a file.

**Stop Logging**

Choose Tools > Stop Logging. The logging stops.

**Send Keystroke**

1. Choose Tools > Send Keystroke. A Send Keystroke dialog appears:



2. Enter the keystroke combinations that you want and select a Key Code name from the drop-down menu.
3. Send the keystroke combinations.

**Send Text File**

1. Choose Tools > Send Text File. A Send Text File screen appears.
2. Open the directory of the Text file.
3. Click on or enter the File Name of the Text file.
4. Click Open.
  - When you click Open, it sends whatever file you selected directly to the port.
  - If there is a loopback plug inserted, you will see the file displayed.
  - If there is currently no target connected, then nothing will be visible on the screen.

### Toggle Power

The Toggle Power function lets you power on or off the device that is connected to the associated outlet on a Power Distribution Unit (PDU). For example, if a router is connected to one of the outlets on the PDU, you can toggle the router's power on or off.

You must configure the association of outlets to the target port of the device before you can use the Toggle Power feature. Assign a power port to the serial target from the Device Settings > Port Configuration tab of the device. If you have not done this, the system displays a message stating that the target is not associated with a power outlet.

---

*Note: If RSC is launched through CC-SG (version 4.x onwards) by users without the permission to toggle power, the option Toggle Power will appear as disabled.*

---

1. Select Toggle Power to turn the device (router) on or off. A prompt appears displaying the current status of the outlet(s). You can turn the device on or off depending on its current status.
2. If you select No, the system returns you to the RSC screen.
3. If you select Yes, the system sends the power command to either turn on or off the outlets associated to the target port of the device.

If you receive a:

- Hardware error message: this means that the PDU command failed.

Software error message: this means that another user is controlling the power outlet and the power control command cannot be sent.

---

## Chat

When using browser access over SSL, an interactive chat feature called Chat allows you and other users on the same port to communicate. The maximum length of a chat message is 300 characters.

---

*Note: When a chat is initiated, a chat window appears on the monitors of all SSL users logged on to the port. If a user is logged into a port multiple times, multiple chat messages do not appear to that user.*

---

► **To open chat:**

- Choose Chat > Chat.



► **To clear text in a chat text box:**

- Click Clear to delete the typed text.

---

## Help

Help Topics include online assistance for operating the Raritan Serial Console and release information about Raritan Serial Console.

### Help Topics

▶ **To access help topics:**

- Choose Help > Help Topics. A list of help topics are displayed.

### About Raritan Serial Console

The About Raritan Serial Console dialog displays the copyright and version information (name and revision number) of the console terminal emulation software. When contacting Raritan for technical support or when performing a software upgrade, you may be asked for this information.

▶ **To access 'About' information:**

- Choose Help > About Raritan Serial Console. An About Raritan Serial Console message appears.

---

## Standalone Raritan Serial Console Installation

---

*Note: You can download the Standalone Raritan Serial Client from the Raritan support Web site: <http://www.raritan.com/support>  
<http://www.raritan.com/support>*

---

The standalone Raritan Serial Client (RSC) is used to make direct connections to the target without going through the SX application. The user specifies the SX address and the port number (target) and then is connected.

The steps in this section install the standalone Raritan Serial Client (RSC).

---

## Standalone Raritan Serial Client Requirements

The following requirements must be met to support the Raritan Serial Console:

- The RSC functions with JRE™ version 1.4.2\_05 or later (except for JRE version 1.5.0\_02) . However, for optimum performance, Raritan recommends using JRE 1.5.0 (except version 1.5.0\_02).
- Your system may require configuration adjustments depending on the operating system and browser. The JRE provides configuration instructions with the JRE download. See <http://www.java.com/en/download/help/testvm.xml> (<http://www.java.com/en/download/help/testvm.xml> to <http://www.java.com/en/download/help/testvm.xml>) to determine the JRE version currently installed on your system.

If you do not have a compatible version of the JRE, go to <http://www.java.com> (<http://www.java.com>) and click the Download Now button.

---

*Note: Raritan does not support JRE version 1.5.0\_02 for use with the RSC.*

---

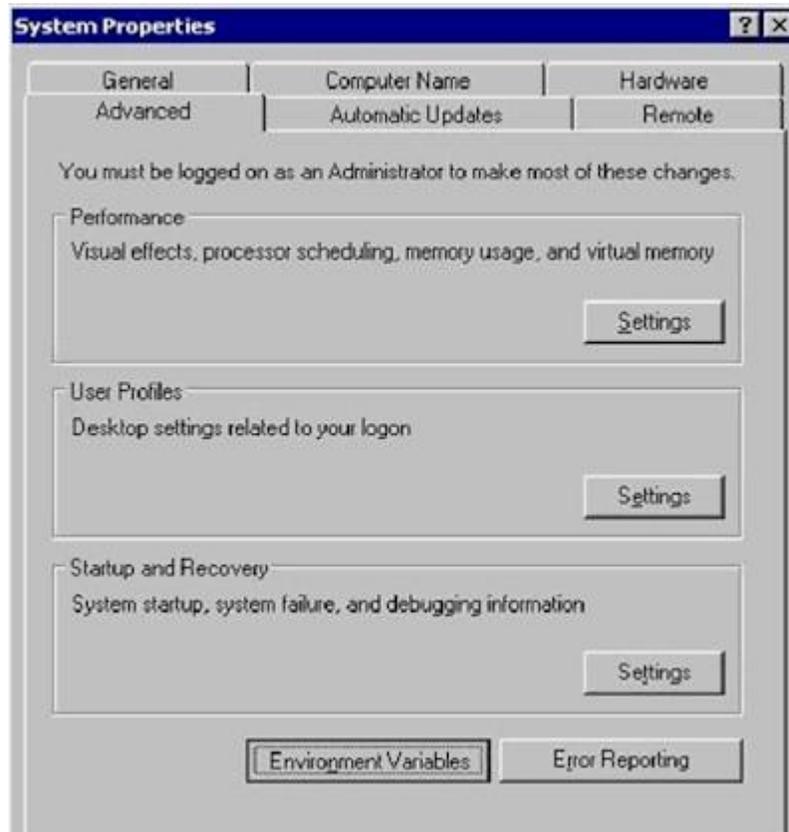
- Minimum 1 GHz PC with 512 MB RAM.
- Ensure that Java™ can be started from the command line. To do this, you must configure environment variables. Make a note of the exact path where Java was installed (the path information is used later).

---

### Setting Windows OS Variables

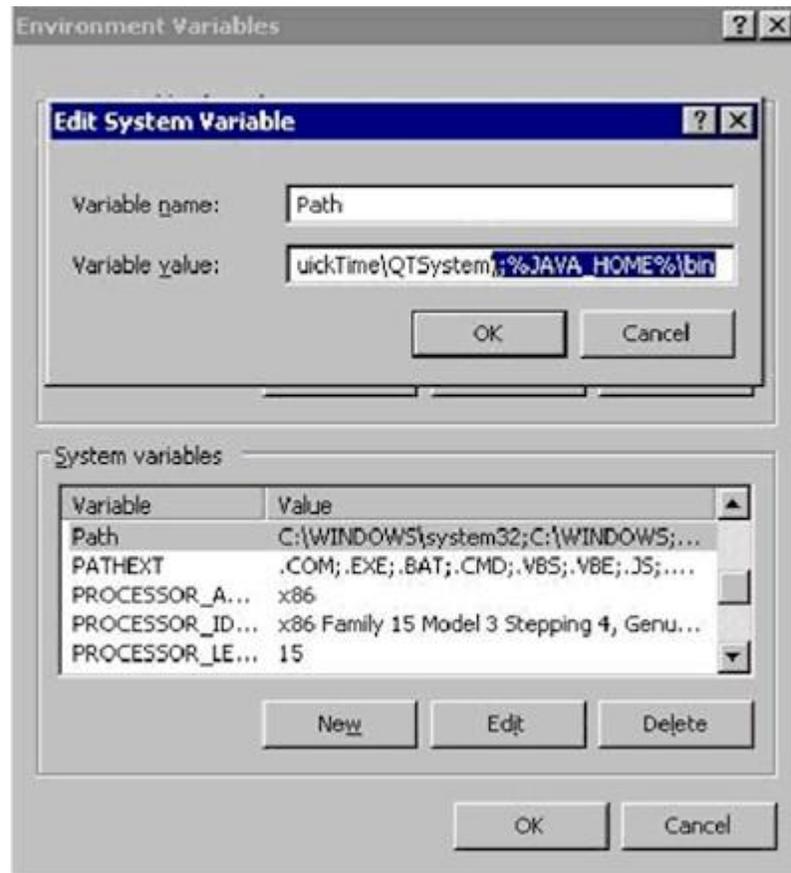
1. Choose Start > Control Panel > System.

2. Click the Advanced tab and then click Environment Variables.



3. In the System variables section, click New.
4. In the New System Variable dialog, add JAVA\_HOME to the Variable name block and the path you wrote down earlier in the Variable value block.
5. Click OK.
6. Select the PATH variable and click Edit.
7. Add %JAVA\_HOME%\bin to the end of the current Variable value. Ensure a semicolon (;) separates the new value from the last value in the string.

8. Click OK.



9. Select the CLASSPATH variable and click Edit.

10. Ensure the CLASSPATH Variable value is configured properly; that is, its value must have a period (.) in it. If, for any reason, there is no CLASSPATH variable defined, create one.



---

### Setting Linux OS Variables

To set Java™ for a specific user, open and edit the `.profile` file located in the `/home/Username` folder.

To set Java for all users, open the `.profile` file in your `/etc` folder:

1. Find the line where you set your path:

```
export
PATH=$PATH:/home/username/somefolder
```

2. Before that line you must set your `JAVA_HOME` and then modify your `PATH` to include it by adding the following lines:

```
export
JAVA_HOME=/home/username/j2sdk1.6/
export PATH=$PATH:$JAVA_HOME/bin
```

3. Save the file.

---

### Setting UNIX OS Variables

To check the latest JRE™ version on Sun Solaris™:

1. Launch a terminal window on the Sun Solaris desktop.
2. Type `java-version` in the command line and press Enter. The currently-installed version of Java™ Runtime Environment (JRE) appears.
  - If your path variable is not set to where the Java binaries have been installed, you may not be able to see the JRE version.
  - Assuming JRE 1.6 is installed in `/usr/local/java`: you must set your `PATH` variable.
  - To set a path for the bash shell:

```
export
PATH=$PATH:/usr/local/java/j2re1.6/bin
```
  - To set path for `tcsh` or `csh`:

```
set
PATH = ($PATH /usr/local/java/j2re1.6/bin)
```
  - These commands can either be typed at the terminal each time you log in, or add them to your `.bashrc` for bash shell or `.cshrc` for `csh` and `tcsh` so that each time you log in, the path is already set. See your shell documentation if you encounter problems.
3. If the JRE is version 1.6 or later, proceed with the RSC installation. If the JRE is an older version than 1.6, go to the Sun website at (<http://java.sun.com/products/>) to download the latest Runtime Environment.

---

## Installing Standalone RSC for Windows

You must have administrative privileges to install RSC.

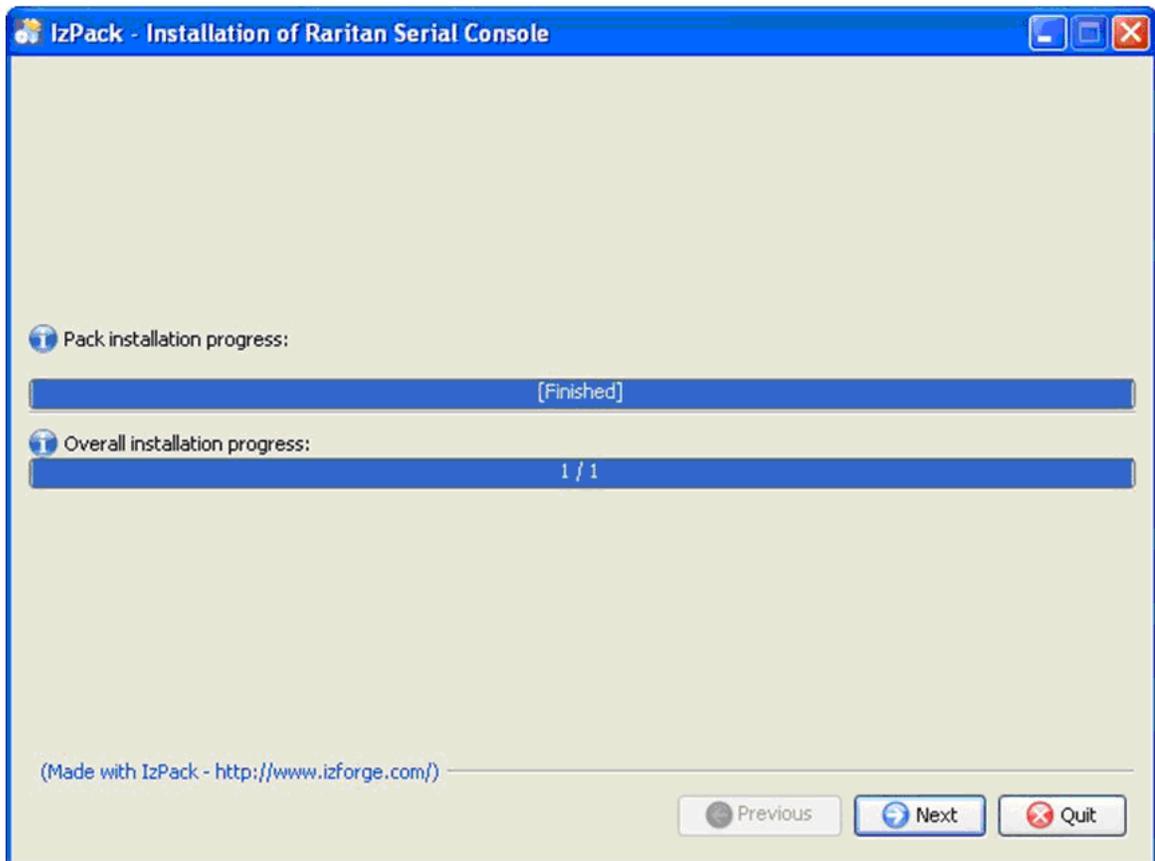
1. Log in to a Windows® machine.
2. Download, or copy from a known location, the RSC-installer.jar installation file.
3. Double-click on the executable file to start the installer program. The splash page opens.
4. Click Next. The installation path page opens.
5. Change the path, if desired.
6. Click Next. The installation progress page opens.

---

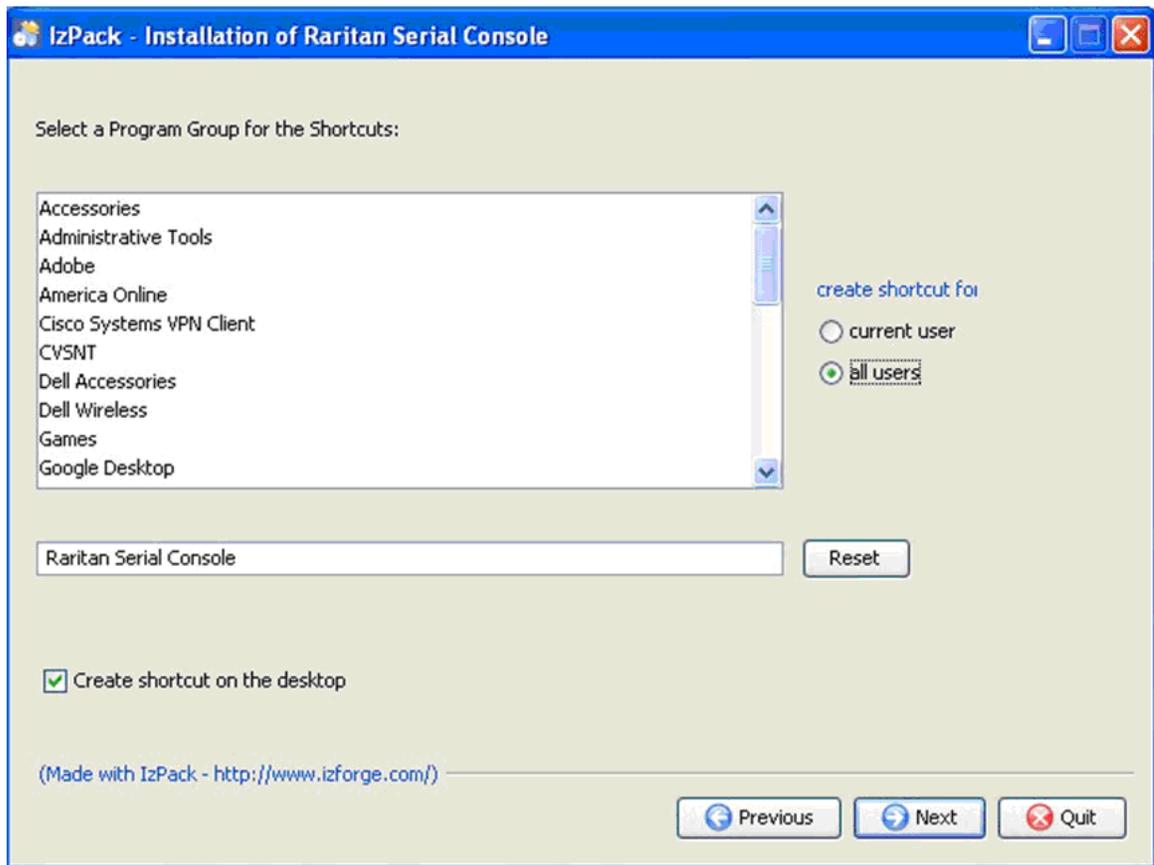
*Note: The standalone version of RSC is available from the Raritan Support website:*

**[http://www.raritan.com/support/sup\\_upgrades.aspx](http://www.raritan.com/support/sup_upgrades.aspx)**  
**([http://www.raritan.com/support/sup\\_upgrades.aspx](http://www.raritan.com/support/sup_upgrades.aspx))**

---



7. Click Next. The Windows shortcut page opens.



8. Select the Program Group for the Shortcut.

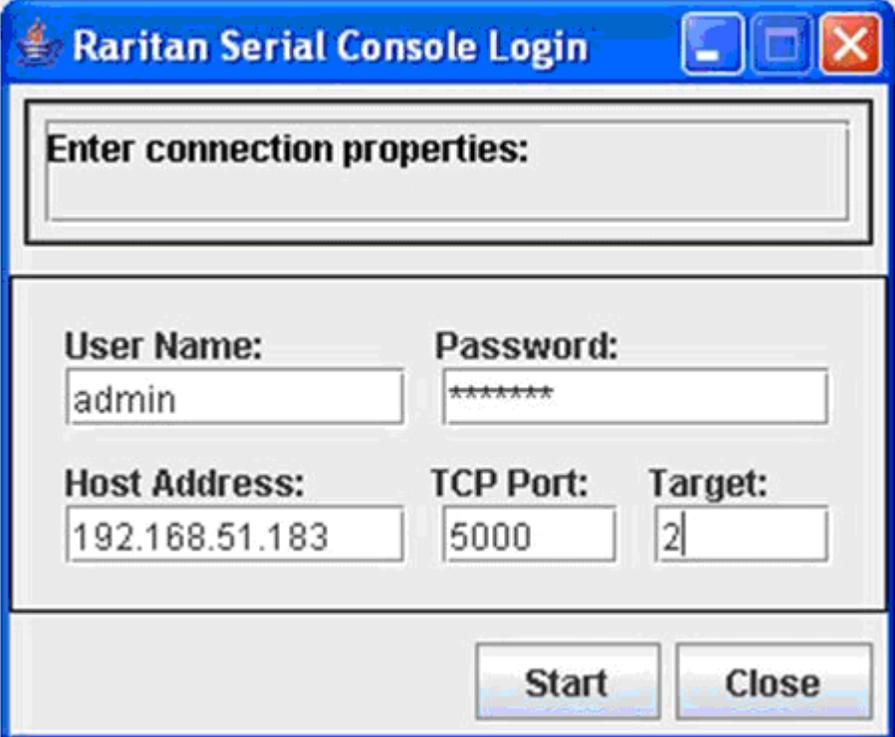
9. Click Next. The installation finished page opens.

10. Click Done.

---

## Launching RSC on Windows Systems

1. Double-click the shortcut or use Start Programs to launch the standalone RSC. The Raritan Serial Console Login connection properties dialog appears.



**Raritan Serial Console Login**

Enter connection properties:

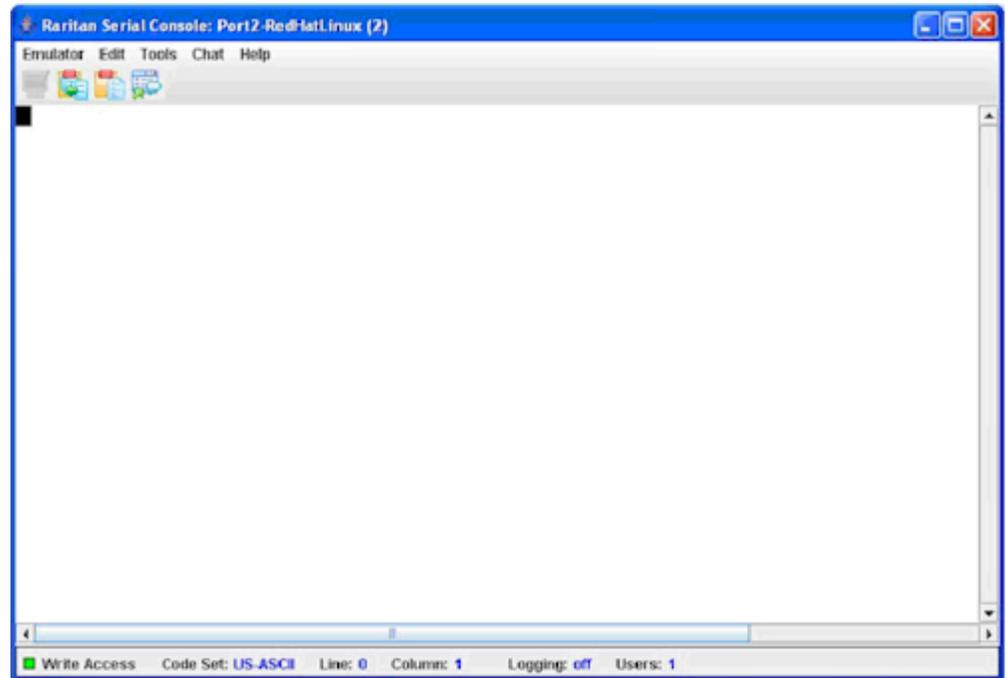
**User Name:**  **Password:**

**Host Address:**  **TCP Port:**  **Target:**

**Start** **Close**

2. Enter the Dominion SX IP address, account information, and the desired target (port).

3. Click Start. The RSC opens with a connection to the port.



---

*Note: In case of unrecognized characters or blurry screens in RSC window due to localization support, try changing the font to Courier New. Choose Emulator > Settings > Display, and select Courier New for Terminal Font Properties or GUI Font Properties.*

---

## Installing RSC for Sun Solaris and Linux

You must have administrative privileges to install RSC.

1. Log in to your Sun Solaris™ machine.
2. Download, or copy from a known location, the RSC-installer.jar installation file.
3. Open a terminal window and change to the directory where the installer is saved.
4. Type `java -jar RSC-installer.jar` and press Enter to run the installer.
5. Click Next after the initial page loads. The Set Installation Path page opens.
  - a. Select the directory where you want to install RSC and click Next.
  - b. Click Browse to navigate to a non-default directory.
  - c. Click Next when the installation is complete.

- d. Click Next again. The installation is complete. The final page indicates where you can find an uninstaller program and provides the option to generate an automatic installation script.
6. Click Done to close the Installation dialog.

---

## Launching RSC on Sun Solaris

1. Open a terminal window and change to the directory where you installed the RSC.
2. Type `./start.sh` and press the Enter key to launch RSC.
3. Double-click on the desired device to establish a connection.
4. Type your username and password.
5. Click OK to log in.

# Chapter 7 Security

## In This Chapter

Security Settings.....	96
Login Settings.....	97
Configure Kerberos .....	99
Certificates.....	100
SSL Client Certificate .....	104
Banner .....	108
Security Profiles.....	109
Firewall .....	110

---

## Security Settings

Choose the Security tab to view security-related tools. The Security Settings page opens.

A blue rectangular header with the text "Security Settings" in white, bold font.

Login Settings

Kerberos

Certificate

SSL Client Certificates

Banner

Security Profiles

Firewall

## Login Settings

- Choose Security > Login Settings. This panel includes Local Authentication, Login Handling, and Strong Password Settings.

Local Authentication	Strong Password Settings
<input checked="" type="checkbox"/> Enable Local Authentication	<input type="checkbox"/> Strong Passwords Required for All Users
Inactive Login Expiry (days): <input type="text" value="330"/>	Minimum Password Length: <input type="text" value="8"/>
Invalid Login Retries: <input type="text" value="3"/>	Maximum Password Length: <input type="text" value="15"/>
Lockout Period on Invalid Login (minutes): <input type="text" value="5"/>	Password Reuse Restriction: <input type="text" value="5"/>
	Password Expiration Period: <input type="text" value="60"/>
	<b>Strong Password Requirements:</b> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Passwords must contain at least one lower case letter</li> <li><input checked="" type="checkbox"/> Passwords must contain at least one upper case letter</li> <li><input checked="" type="checkbox"/> Passwords must contain at least one number</li> <li><input checked="" type="checkbox"/> Passwords must contain at least one special character</li> </ul>
Login Handling	
User Idle Timeout (minutes): <input type="text" value="10"/>	
<input type="checkbox"/> Single Login per User	
<input checked="" type="checkbox"/> Anonymous Port Access	
Port Access Mode: <input type="text" value="Share"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### Local Authentication

- Go to the Local Authentication panel and select the Enable Local Authentication checkbox.
- The system displays these defaults in the following fields:
  - Inactive Login Expiry (days): 330
  - Invalid Login Retries: 3
  - Lockout Period on Invalid Login (minutes): 5

3. Accept the system defaults or type your own.

---

### Login Handling

1. Go to the Login Handling panel and enter a value in the User Idle Timeout (minutes) field. This is the length of inactive time, after which the user is timed out. Default time is 10 (minutes).

---

*Note: If no port connections are established from CC-SG to SX within the configured time of User Idle Timeout, service sessions from both devices are disconnected.*

---

2. To enable single login only, select the Single Login per User checkbox. Only one user can log in at a time using the same profile.
3. Select the Anonymous Port Access checkbox to turn this feature on. An Anonymous User Group is created by default and it cannot be deleted, even by the Administrator. It is visible in the Group List if Anonymous Port Access is selected, but invisible in Group List if Anonymous Port Access is deselected.

---

*Note: See **Port Configuration and Port Access Application** (on page 61) for additional information about anonymous port access.*

---

4. Select Share in the Port Access Mode drop-down menu if port access should be shared, allowing users to connect to the port while another user is using it. The default value is Share. Change this to Private if you want to keep other users from connecting to a port while a user is using it.

---

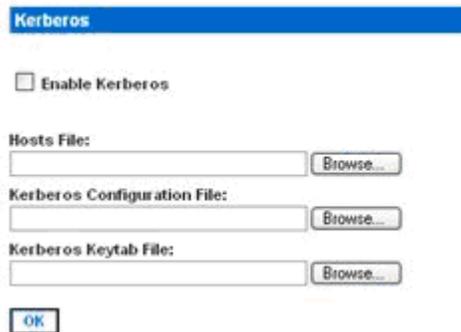
### Strong Password Settings

To enable strong passwords, go to the Strong Password panel and select the requirements for a strong password. This includes maximum and minimum length and special character requirements.

Passwords are case sensitive and can contain up to 64 alphanumeric characters with the exception of " ' < > \ &

---

## Configure Kerberos



The screenshot shows a dialog box titled "Kerberos" with a blue header bar. Below the header, there is a checkbox labeled "Enable Kerberos". Underneath, there are three text input fields, each followed by a "Browse..." button. The labels for these fields are "Hosts File:", "Kerberos Configuration File:", and "Kerberos Keytab File:". At the bottom left of the dialog, there is an "OK" button.

1. Click Enable Kerberos.
2. Type the name of the file you want for your Hosts File in the Hosts File field or click on the Browse drop-down menu and select your file.
3. Type the name of the file you want for your Kerberos Configuration File in the Kerberos Configuration File field or click on the Browse drop-down menu and select your file.
4. Type the name of the file you want for your Kerberos Keytab File in the Kerberos Keytab File field or click on the Browse drop-down menu and select your file.
5. Click OK.

---

## Certificates

The Certificate feature allows you to generate a Certificate Signing Request (CSR), install a user key on the SX, and install a user certificate on the SX.

If you are using Firefox®, you must install a Java® client authentication certificate. To do this, open the Java Control Panel and select Security > Certificates. Select Client Authentication from the certificate types and import the .p12 certificate.

This certificate does not need to be installed if you connect to a port with another certificate.

---

*Note: By default, SSL certificates are good for one year after they are installed. Install a new certificate, as needed, after it expires. A warning letting you know the certificate is expired is displayed when you access the SX after the expiration date. You are still able to fully communicate with the SX even after an SSL certificate expires.*

---

---

## Generate a Certificate Signing Request

► **To generate a Certificate Signing Request (CSR):**

1. Choose Security > Certificate. The Certificate page opens.

**Certificate**

Activate Default Certificate

Activate User Certificate

Generate Default Certificate

Generate Certificate Signing Request

**Bits:**

**Name:**

**Country:**

**State:**

**Locality:**

**Organization:**

**Unit:**

**Email:**

2. Click the Generate a Certificate Signing Request radio button.
3. Click on the drop-down menu in the Bits field. Keep the 1024 default or change it to 512.
4. Type the following in the corresponding fields:
  - Name
  - Country
  - State
  - Locality
  - Unit
  - Email address

5. To view the default certificate or the CSR, click the appropriate radio buttons.
6. Click OK. The CSR is generated.

---

### Install a User Key

► **To install a user key on the SX:**

1. Choose Security > Certificate. The Certificate page opens.

**Install User Key**

**IP Address:**

**Login:**

**Password:**

**Remote Path:**

**Remote File:**

2. Select the Install User Key radio button.
3. Type the following in the corresponding fields:
  - IP address of the host with the key
  - Login on host
  - Password on host
  - Remote Path containing the key
  - Remote File containing the key
4. Click OK.

---

*Note: If the SX is not used to generate the certificate signing request and an external certificate is used instead, encryption needs to be removed from the private key before installing it on the SX. If this is the case, to remove the encryption from the key, a command such as `openssl rsa -in server.key -out server2.key` and `server2.key` should be used. Encrypted private keys are used to prevent the web server from being started by unauthorized users. Since SX does not allow users to access the web server directly, encrypted private keys are not required and does not compromise security.*

*Note: When the SX is used to generate the certificate signing request, the private key is not required since SX keeps the private key exclusive.*

---

---

## Install a User Certificate

► **To install a user certificate on the SX:**

1. Choose Security > Certificate. The Certificate page opens.

**Install User Certificate**

**IP Address:**

**Login:**

**Password:**

**Remote Path:**

**Remote File:**

1. Select the Install User Certificate radio button.
2. Type the following information in the corresponding fields:
  - The IP address of the host with the certificate
  - Login on the host
  - Password on the host
  - Remote Path containing the certificate
  - Remote File containing the certificate
3. Click OK.

---

## SSL Client Certificate

SSL Security certificates are used in browser access to ensure that the device to which you are attached is the device that is authorized to be connected. See **Appendix C: Certificates** (see "**Certificates**" on page 267) for details on SSL Certificates. This section describes only how to configure the certificates, but you can find additional SSL Certificate information at:

**<http://www.microsoft.com/technet/prodtechnol/ie/reskit/6/part2/c06ie6rk.mspx?mfr=true>**

**(<http://www.microsoft.com/technet/prodtechnol/ie/reskit/6/part2/c06ie6rk.mspx?mfr=true>)**

Enable SSL Client Certificates

Install Certificate Authority

IP Address:

Login:

Password:

Remote Path:

Remote File:

CA Name:

Remove Certificate Authority

CA Name:

View Certificate Authority

CA Name:

Add Certificate Revocation List

IP Address:

Login:

Password:

Remote Path:

Remote File:

Url:

CRL Name:

Delete Certificate Revocation List

CRL Name:

View Certificate Revocation List

CRL Name:

---

### Enable Client Certificate Authentication

► **To enable Client Certificate Authentication:**

1. Select the Enable SSL Client Certification checkbox.
2. Click OK to enable the Client Certificate authentication.

---

### Install a New Trusted Certificate Authority

To install a new trusted Certificate Authority (CA) to the SX, the CA certificate must be on an accessible FTP server.

1. Select the Install Certificate Authority checkbox.
2. Fill in the data needed to retrieve the certificate from the FTP server.
3. Click OK to retrieve and install the CA certificate to the SX.

---

### Remove a User-Added Certificate Authority

► **To remove a user-added CA from the SX:**

1. Select the Remove Certificate Authority checkbox.
2. In the CA Name field, type the name that was specified when the CA certificate was added.
3. Click OK to remove the certificate.

---

### View a Certificate Authority

► **To view a CA:**

1. Select the View Certificate Authority checkbox.
2. In the CA Name field, type the name of the CA you want to view.
3. Click OK to retrieve the list of CAs.

---

### Manage the Client Certificate Revocation List (CRL)

The SX comes with VeriSign and Thawte CA certificates and CRLs preinstalled. If a user adds a custom CA to the SX, a corresponding CRL should be added to keep track of revoked certificates. For the CRL to be automatically retrieved when it expires, it should be retrievable from a web server to which the SX can connect.

---

### Add a New Certificate Revocation List to the SX

To add a new CRL to the SX, the CRL list must be on an accessible FTP server.

1. Select the Add Certificate Revocation List checkbox.
2. Fill in the fields to access the FTP Server.
  - The CRL Name field should match the name that was used to add the CA.
  - The URL field should be the numeric dot notation of the IP address of the HTTP server.

3. Click OK to add the CRL.

---

### **Delete a Certificate Revocation List from the SX**

▶ **To delete a CRL from the SX:**

1. Select the Delete Certificate Revocation List checkbox.
2. In the CRL Name field, type the name of the CA to which this CRL belongs.
3. Click OK to delete the CRL.

---

### **View a Certificate Revocation List**

▶ **To view a CRL:**

1. Select the View Certificate Revocation List checkbox.
2. Click OK to retrieve the list of CRLs.

---

## Banner

SX optionally supports a customizable welcome banner with a maximum 5000 words, 8 words per row, that appears after log in. The banner identifies where the user has logged into. SX also allows you to add a consent banner that forces the user to accept stated conditions prior to advancing into operation of the console server.

---

*Note: When you are logged in to the SX via GUI, a banner using a fixed width typeface and a common dimension like 80x25 appears. Even if the source banner is very large, the banner displayed on the GUI does not increase the overall page size, as it is contained within a self-scrolled text area.*

---

**Banner**

Display Restricted Service Banner

Require Acceptance of Restricted Service Banner

**Restricted Service Banner Message:**

Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activities are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.

**Restricted Service Banner File:**

1. Select one of the following checkboxes.
  - Display Restricted Service Banner
  - Require Acceptance of Restricted Service Banner
2. Click one of the following radio buttons:
  - Restricted Service Banner Message
  - Restricted Service Banner File
3. If you selected Restricted Service Banner File, click on the Browse drop-down menu

4. Locate and select the file that contains the Restricted Service Banner message you want to display on the SX login dialog.
5. Click OK.

---

## Security Profiles

The SX provides three security profiles for your use. The profiles simplify the task of assigning permissions to users and groups by defining basic permissions that automatically apply to all users.

---

### About Security Profiles

The three security profiles are:

- Standard - Custom defaults
- Secure - All functions in Custom are checked
- Custom - Can be configured by a user

If you enable the Standard or Secure profiles, you cannot enable/disable manually any of the features they include. You must disable the profile to make those changes.

If a profile is disabled, the features in the profile keep the states they had when the profile was enabled. For example, if the default TLS Required feature is deselected and you enable the Secure profile, this feature becomes selected. When you disable the Secure profile, the TLS Required feature remains selected.

---

### Select a Security Profile

► **To select a security profile:**

1. Choose Security > Security Profiles. The Security Profiles page opens.

**Security Profiles**

Enable Security Profile

**Profile:**

Custom

[Edit Custom Profile](#)

2. Click the Enable Security Profile checkbox.
3. Select the profile from the drop-down menu in the Profile field.

4. Click OK.

---

### Edit the Custom Profile

► **To edit the Custom profile:**

1. Choose Security > Security Profiles. The Security Profiles page opens.
2. Click the Edit Custom Profile link. The Edit Custom Security Profile page opens.

#### Edit Custom Security Profile

**Name:**

Custom

- Telnet Access**
- Strong Password Required**
- Single Login Per User**
- Timeout Required**
- TLS Required**
- Redirect HTTP to HTTPS**

**OK**

**Cancel**

3. Check one or more of the following checkboxes.
  - Telnet Access
  - Strong Password Required
  - Single Login Per User
  - Timeout Required
  - TLS Required
  - Redirect HTTP to HTTPS
4. Click OK.

---

## Firewall

The SX provides a firewall function to provide protection for the IP network and to control access between the internal router and LAN 1, LAN 2, and the dial modem interfaces.

---

## Enable the Firewall

► **To enable the firewall:**

1. Choose Security > Firewall. The Firewall page opens, displaying the existing IPTables rules.

Firewall	Add / Delete IPTables Rule
<input type="checkbox"/> Enable Firewall <input type="button" value="OK"/> <input type="button" value="Cancel"/>	IPTables Command: <input style="width: 100%; height: 20px;" type="text"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>

### IPTables Rules

```
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
ACCEPT    0    -- localhost.localdomain anywhere

Chain FORWARD (policy ACCEPT)
target    prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
```

2. Select the Enable Firewall checkbox.
3. Click OK.

---

*Note: When you enable IP forwarding for Dual LAN units, use IPTables rules to create policies for traffic being forwarded between LAN interfaces*

---

## Add an IPTables Rule

► **To add an IPTables rule:**

1. Choose Security > Firewall. The Firewall page opens, displaying the default IPTables rules.
2. Go to the Add/Delete IPTables Rule field and enter a rule.
3. Click Apply, and then click Save. The rule is displayed on the screen.
4. Delete some or all of the default rules if you choose to.
5. Add new rules if you choose to.

---

*Note: Rules are added using the IPTables command to the kernel. These rules take effect immediately but persist permanently only after clicking the Save button. If there is a mistake in the rules and as a result, the unit becomes inaccessible, while the Save action allows you to recover from the mistake. Reboot the system. If you do not Save the rules, you lose them in the reboot.*

---

# Chapter 8 Logging

## In This Chapter

Configuring Local Event Logging .....	113
Configuring SMTP Logging .....	117
Configuring NFS Logging .....	120
Configuring SNMP Logging .....	121

---

## Configuring Local Event Logging

To configure the local log settings, choose Setup > Log. The Log Settings page opens. It contains a number of individual logging panels.

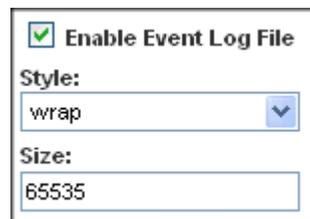
---

### Enable the Event Log File

This feature enables event log messages to be stored locally on the SX unit.

► **To enable the Event Log File:**

1. Go to the Event Log panel and select the Enable Event Log File checkbox. To turn this feature off, deselect this checkbox.



The screenshot shows a configuration panel with the following elements:

- A checked checkbox labeled "Enable Event Log File".
- A "Style:" label above a dropdown menu currently showing "wrap".
- A "Size:" label above a text input field containing the value "65535".

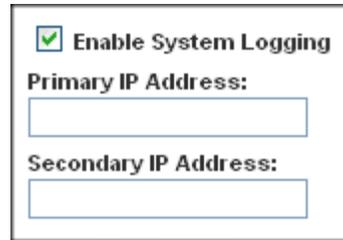
2. Select the log file style in the Style field. This determines how the file reacts when the maximum file size is reached. Your choices are:
  - Wrap: This causes the log file to circle around to the beginning when the end of the file is reached.
  - Flat: This causes logging to stop when the end of the file is reached.
3. Enter the maximum size of the file in the Size field. The default is 65535 bytes.
4. Click OK.

---

### Enable System Logging

This feature sends event log messages to a remote Syslog server. The messages from the SX unit are sent to the LOCAL0 channel of the Syslog server for more efficient parsing. To set this feature up:

1. Go to the System Logging panel and click the Enable System Logging checkbox. (To turn this feature off, clear this checkbox.)



**Enable System Logging**  
**Primary IP Address:**  
  
**Secondary IP Address:**

2. Type the IP address of the remote Syslog server in the Primary IP Address field.
3. If you have a backup Syslog server, types its IP address in the Secondary IP Address field.
4. Click OK.

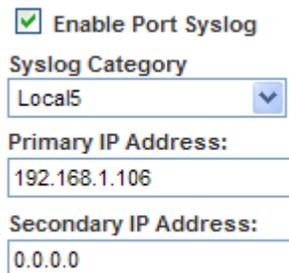
---

### Enable Port Syslog

This feature enables port data to be logged to a syslog server. Output from all ports is logged to the same file in syslog. Please use NFS Port Logging if you prefer separate files for each port's data.

► **To enable Port Syslog:**

1. Go to the System Logging panel and select the Enable Port Syslog checkbox. To turn this feature off, deselect this checkbox.



**Enable Port Syslog**  
**Syslog Category**  
Local5 ▼  
**Primary IP Address:**  
192.168.1.106  
**Secondary IP Address:**  
0.0.0.0

2. Select a channel from the drop-down menu of Syslog Category, and the messages from the SX unit are sent to the selected channel (for example, Local5) of the Syslog server.

---

*Note: If no specific IPs are entered for the port data destination servers, port logs are sent to the Syslog server configured in the System Logging section. If the Syslog category is set to Local0, then system events and port logs are sent to all servers configured in the System Logging section and Port Syslog section.*

---

3. Type the IP address of the remote Syslog server in the Primary IP Address field.
4. If you have a backup Syslog server, type its IP address in the Secondary IP Address field.
5. Click OK.

---

### Enable Port Logging

Configure NFS port logging after you have enabled NFS Logging (see Configuring NFS Logging for details).

This feature enables port data to be logged to a Network File System (NFS) server, allowing you to save and access the log files over a network.

NFS supports file sharing, which means you can store the files on the network that you want other people to access, while keeping your secure files on the SX unit. NFS stores the port sessions as viewed by the user, as well as adding messages when a user connects to or disconnects from a port.

#### ► To set up port logging:

1. Go to the Port Logging panel and select the Enable NFS Port Logging checkbox. To turn this feature off, deselect this checkbox.

Enable NFS Port Logging

**File Prefix:**

domSX-NFS

**Size (bytes):**

65535

**Timestamp (Interval):**

20

**NFS Update Frequency (seconds):**

20

**Out Directory:**

output

2. Type the prefix to the port data file's name on the NFS server in the File Prefix field.

3. Type the maximum file size allowed in the Size field. Once this size is reached, a new file is created to store the port log data. If you enter a value of 0, the SX creates a new file.
4. Type the time interval (in seconds) between two timestamp messages in the log file in the Timestamp (Interval) field. If you enter a value of 0, this disables timestamps in the log file. The maximum value is 99999. This field is optional, but if a timestamp is configured, the syslog has timestamps interspersed with the same timestamp interval.
5. Type the time interval (in seconds) between two updates of the port log file in the NFS Update Frequency (seconds) field. Data is buffered until the internal buffer is full or this timestamp occurs. Then the data is written to the file. This prevents severe network traffic on port activity where every character would trigger a write to the NFS server.
6. Type the subdirectory on the configured NFS server to write the output port data to in the Out Directory field. This is the default log file and contains the port sessions as visible to the user.
7. Click OK.

The following is an example of an output file.

```
Sep 3 11:31:20 sx8 DomSX: DominionSX Port 1 : Port1 : edition of this book, which has naturally been very pleasant for me.  
Sep 3 11:31:20 sx8 DomSX: DominionSX Port 1 : Port1 : However, every now and then someone will have complaints, and for  
Sep 3 11:31:20 sx8 DomSX: DominionSX Port 1 : Port1 : -- DominionSX UP -- Tue Sep 03-2008 15:30:28  
Sep 3 12:03:17 sx8 DomSX: DominionSX Port 2 : Port2 : -- DominionSX UP -- Tue Sep 03-2008 16:02:23  
Sep 3 12:03:17 sx8 DomSX: DominionSX Port 3 : Port3 : -- DominionSX UP -- Tue Sep 03-2008 16:02:23  
Sep 3 12:03:17 sx8 DomSX: DominionSX Port 4 : Port4 : -- DominionSX UP -- Tue Sep 03-2008 16:02:23  
  
sx8 DomSX: DominionSX Port 1 : Port1 :  
<HostIP> DomSX: <hostname> Port <portnumber> : <Portname>: <port data>
```

---

### Configure Input Port Logging

► **To configure input port logging:**

1. Go to the Input Port Logging panel and select the Enable Input Port Logging checkbox. To turn this feature off, deselect this checkbox.

**Enable Input Port Logging**

**In Directory:**

input

2. Type a directory for input in the In Directory field.
3. Click OK.

---

### Configure Encryption

▶ **To configure encryption:**

1. Go to the Encryption panel and select the Encryption checkbox. To turn this feature off, deselect this checkbox.

**Encryption**

**NFS Encryption Key (RC4):**

ba5d990e3afa0f2f0def0254

2. Accept the default encryption key or type a new one in the NFS Encryption Key (RC4) field.
3. Click OK.

---

### Block Port Access On Failure

This feature specifies NFS mount behavior. This feature appears as checked by default, and NFS behaves as a soft mount. When it is a soft mount, NFS is re-mounted if an operation goes wrong on the file system. If the re-mount succeeds, logging continues; otherwise, further logging events are inhibited.

**Block Port Access On Failure**

---

## Configuring SMTP Logging

To configure SMTP logging, choose Setup > Events. The SMTP Logging screen appears, containing SMTP Settings panel and a New SMTP Event panel.

---

## Enable SMTP Logging

► **To enable SMTP logging:**

1. Go to the SMTP Settings panel and select the Enable SMTP Server checkbox.



**SMTP Settings**

Enable SMTP Server

SMTP Server IP Address:

Username:

Password:

Source address:

2. Type the IP address of the SMTP server in the SMTP Server IP Address field.
3. Type the username and password in the Username and Password fields. These are required to access the SMTP server.
4. Type your source address in the Source Address field.
5. Click OK.

---

## Select a New SMTP Event

► **To select a new SMTP event:**

1. Go to the New SMTP Event panel and select a new event from the Event drop-down list.

**New SMTP Event**  
**Event:**  
   
**Destination:**

Available events include:

- event.amp.notice.port.connection
- event.amp.notice.user.logoff
- event.amp.notice.backup
- event.amp.notice.restore
- event.amp.notice.config.directaccesslockout
- event.amp.notice.reboot
- event.amp.notice.boot
- event.amp.notice.config.datacom
- event.amp.notice.config
- event.amp.notice.upgrade
- event.amp.keyword
- event.amp.strongpassword
- event.amp.banner
- event.amp.firewall
- event.amp.iptablesaved
- event.amp.security.clientauth
- event.amp.security.clientcert.ca
- event.amp.security.clientcert.crl.expired
- event.amp.security.clientcert.crl.updated

2. In the Destination field, type the email address to which you want to send the event.

3. Click OK.

---

### Test SMTP Logging

It is important that the SMTP server information be accurate so that the SX unit can send messages using that SMTP server.

To verify that the information is correct and working:

1. Send a test email by selecting an event such as:  
*event.amp.notice.port connection*
2. Connect to a port and see if the message is received by the intended email target. If there are problems, contact your SMTP administrator to make sure your SMTP server IP address and authorization information are correct.

---

### Configuring NFS Logging

Network File System (NFS) logging allows you to log all port activity to an NFS shared directory. All user activity and user port logins and logouts are logged. There are two log files:

- Input: Records all input (keystrokes) from users.
- Output: Contains all the messages that come from the server into the console server. This includes all user input that is echoed back from the managed device/server.

You must also enable port logging. For more information on port logging, see Enable Port Logging.

---

*Note: The NFS server must have the exported directory with write permission for the port logging to work.*

---

To configure NFS Logging:

1. Choose Setup > NFS. The NFS Settings page opens.

2. Select the Enable NFS checkbox to enable NFS logging.
3. Type the IP address of the NFS server in the Primary IP field, and then enter the path to the log file in the Primary Directory field.
4. If you have a backup NFS server, enter the same information for this server in the Secondary IP field and Secondary Directory fields. If the primary server fails, port logging is redirected to the secondary server.
5. Click OK.

---

## Configuring SNMP Logging

The SX supports Simple Network Management Protocol (SNMP) traps and logging.

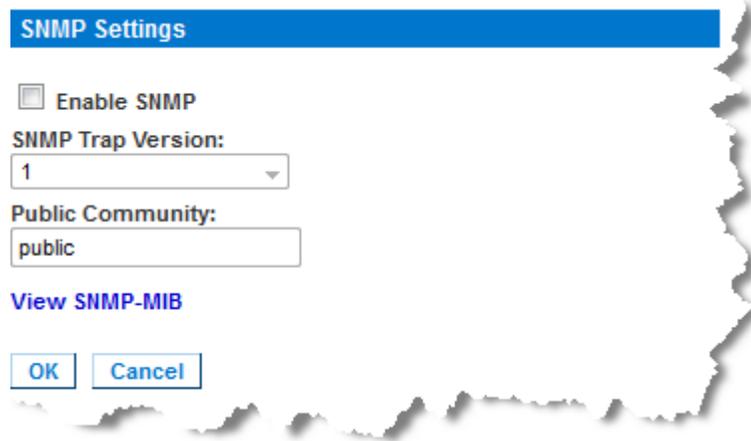
Information on SNMP traps that the SX sends can be found in the MIB file, which can be viewed from the SNMP page. After the "-- Start the Traps" header in the document, all of the traps are listed, as well as the data elements that are sent in each trap. Each data element is defined in the MIB file before this section of the document.

---

### Enable SNMP Logging

► **To enable SNMP logging:**

1. Choose Setup > SNMP. The SNMP page opens.
2. Go to the SNMP Setting panel and select the Enable SNMP checkbox.
3. Select the SNMP Trap Version - either 1 or 2c.



4. Type an SNMP public community in the Public Community field. The default is Public. The public community determines which SNMP management stations receive SNMP alerts.
5. If needed, click View SNMP-MIB to view the MIB.
6. Click OK.

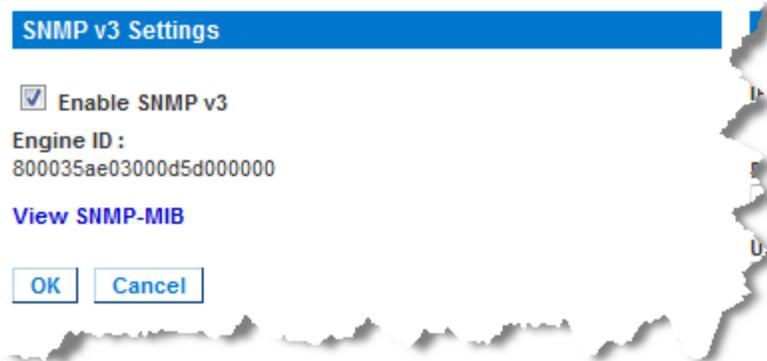
---

### Enable SNMPv3 Logging

► **To enable SNMPv3 logging:**

1. Choose Setup > SNMPv3. The SNMP page opens.

- Go to the SNMP Setting panel and select the Enable SNMP v3 checkbox.



- If needed, click View SNMP-MIB to view the MIB.
- Click OK.

---

### Create a New SNMP Destination

SNMP destinations determine which SNMP management stations receive SNMP traps.

► **To create a new SNMP destination:**

- Go the SNMP Destination panel and type the IP address of the new destination in the IP Address field.

- By default, the new destination uses the standard SNMP port of 162. Change this to another port by entering a different port number in the Port field. Click OK.

---

*Note: To display the SNMP Management Information Base (MIB), click the View SNMP-MIB link in the SNMP Settings Panel (as shown in **Enable SNMP Logging** (see **Enable SNMPv3 Logging** on page 122)).*

---

# Chapter 9 Maintenance

## In This Chapter

- Managing the Local Event Log ..... 124
- Displaying a Configuration Report ..... 126
- Backing Up and Restoring the SX ..... 126
- Upgrading Firmware ..... 128
- Performing a Factory Reset on the SX ..... 131
- Rebooting the SX ..... 131

---

### Managing the Local Event Log

The SX allows you to display the contents of the event log, clear the log, and send the log to a remote FTP server.

#### Display the Local Event Log

To display the contents of the local event log, choose Maintenance > View Event Log. The following figure shows a typical event log.

Date/Time	Event
Dec 18 19:13:44	TheMonarch DomSX: [RDMDEBUG] Command()
Dec 18 19:13:44	TheMonarch DomSX: [RDMDEBUG] Running command id: 1
Dec 18 19:13:44	TheMonarch DomSX: [RDMDEBUG] -272651163 send() result 4
Dec 18 19:13:44	TheMonarch DomSX: [RDMDEBUG] -272651063 send() result 126
Dec 18 19:13:59	TheMonarch DomSX: [RDMDEBUG] begin
Dec 18 19:13:59	TheMonarch DomSX: [RDMPRINT] length = 848
Dec 18 19:13:59	TheMonarch DomSX: [RDMDEBUG] -272635850 UDP Sending CSC_Info
Dec 18 19:13:59	TheMonarch DomSX: [RDMPRINT] TheMonarch
Dec 18 19:14:29	TheMonarch DomSX: [RDMDEBUG] begin
Dec 18 19:14:29	TheMonarch DomSX: [RDMPRINT] length = 848
Dec 18 19:14:29	TheMonarch DomSX: [RDMDEBUG] -272605820 UDP Sending CSC_Info
Dec 18 19:14:29	TheMonarch DomSX: [RDMPRINT] TheMonarch
Dec 18 19:14:45	TheMonarch DomSX: [RDMDEBUG] -272590434 rcv() result 4
Dec 18 19:14:45	TheMonarch DomSX: [RDMDEBUG] RDM -----
Dec 18 19:14:45	TheMonarch DomSX: [RDMDEBUG] -272590425 rcv() result 127
Dec 18 19:14:45	TheMonarch DomSX: [RDMDEBUG] -272590393 rcv() result 1
Dec 18 19:14:45	TheMonarch DomSX: [RDMDEBUG] <input type="text"/> *
Dec 18 19:14:45	TheMonarch DomSX: [RDMDEBUG]
Dec 18 19:14:45	TheMonarch DomSX: [RDMDEBUG] Command()
Dec 18 19:14:45	TheMonarch DomSX: [RDMDEBUG] Running command id: 1

---

*Note: If the number of events in the log exceeds the size of one page, click the Next link that appears under “Event Log” at the top of the screen to display the next page.*

---

For each event, the log gives the date and time the event was logged and a brief description. The following are typical events:

Feb 5 12:55:23 DominionSX DomSX: DominionSX notice  
SXRebootCompleted

Feb 5 12:55:25 DominionSX DomSX: DominionSX notice  
SXSystemReady

Feb 1 16:30:35 DominionSX DomSX: DominionSX notice  
SXSettingSaved User Elaine changed  
configuration for Logging

---

### Clear the Event Log

► **To clear the event log:**

1. Choose Maintenance > Clear Event Log. You are prompted to confirm the clear action.
2. Click Yes. The log is cleared of all contents. (If you change your mind, click No.)

---

### Send the Event Log

► **To send the contents of the event log to a remote FTP server:**

1. Choose Maintenance > Send Event Log. The Send Event Log page opens.

**Send Event Log**

**IP Address:**

**Login:**

**Password:**

**Remote Path:**

**Remote File:**

2. Enter the IP address of the FTP server in the IP address field.
3. Enter a login name and password on the FTP server in the Login and Password fields. This is necessary to access the FTP server.
4. Enter the path to the location where the event log is stored in the Remote Path field.
5. Enter the name of the file to store the event log in the Remote File field.
6. Click Send.

---

## Displaying a Configuration Report

The Configuration Report provides detailed information about the SX unit. To display the report, choose Maintenance > Configuration Report. The report shows:

- Version and firmware information
- Port settings
- User and group settings
- HTTP, HTTPS, SSH, and Telnet settings
- RADIUS, LDAP, TACACS+, and Kerberos settings
- Local authentication settings
- Other settings

---

## Backing Up and Restoring the SX

When you back up the SX, the system makes a copy of the SX configuration (without network settings) and writes the copy to an FTP server. The file can be recovered using a Restore operation, if necessary.

---

## Back Up the SX

► **To back up the SX unit:**

1. Choose Maintenance > Backup. The Backup page opens.

**Backup**  
**IP Address:**  
  
**Login:**  
  
**Password:**  
  
**Remote Path:**  
  
**Remote File:**

2. Type the IP address of the target FTP server where the backup is written in the IP Address field.
3. Type the login name of the account on the system where the backup is stored in the Login field.
4. Type the password of the account on the system where the backup is stored in the Password field.
5. Type the path to the backup file in the Remote Path field.
6. Type the name of the file in which the backup is saved in the Remote File field.
7. Click OK.

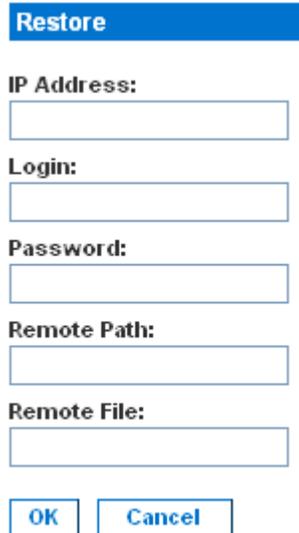
---

### Restore the SX

Restoring the SX retrieves a copy of the SX configuration from the FTP server where it has been backed up and writes the file to the SX.

► **To perform a restore operation:**

1. Choose Maintenance > Restore. The Restore page opens.



**Restore**

**IP Address:**

**Login:**

**Password:**

**Remote Path:**

**Remote File:**

2. Type the IP address of the source FTP server system from which the restore data is retrieved in the IP Address field.
3. Type the login name of the account on the system where the restore data is stored in the Login field.
4. Type the password of the account on the system where the restore data is stored in the Password field.
5. Type the path to the restore file in the Remote Path field.
6. Type the name of the file in which the restore is saved in the Remote File field.
7. Click OK.

---

### Upgrading Firmware

You can display the version of the firmware currently running on the SX, upgrade the firmware to a later version, and display a history of firmware upgrades.

---

*Note: The SX can only be upgraded, while downgrade is not possible.*

---

---

### Display the Current Firmware Version

To display the current version of firmware running on an SX unit, choose Maintenance > Firmware Version. The Firmware Version page opens, displaying the Firmware Version, RSC, Kernel, and PMOI.

Firmware Version	
<b>Firmware Version:</b>	3.1.7.5.2
<b>RSC:</b>	3.0.0.5.37
<b>Kernel:</b>	2.4.13
<b>PMOI:</b>	2.0.1

---

### Upgrade the Firmware

During the upgrade, SX verifies there is enough space on the device to perform the upgrade. If there is not, the SX restarts and the upgrade does not take place. If the upgrade fails due to lack of space, clear the local logs on the device and try upgrading again. Contact Raritan Technical Support if you still cannot upgrade after clearing the local logs.

Before you perform a firmware upgrade, you must:

1. Download the upgrades file(s), which are in WinZip format onto a folder on the local FTP server.
2. Obtain the IP address of the FTP server.
3. Obtain the file path to the upgrade file(s). This is the path to the extracted upgrade files, for example, cert\_pact.tgz, on the FTP server.
4. Obtain a user account (optional) if “anonymous” access to the FTP server is not supported.

The Firmware Upgrade feature allows you to upgrade the SX unit's firmware to a newer version. These upgrades preserve user-defined settings. You do not need to re-configure the unit after the upgrade is complete.

---

**Important: During an upgrade procedure, do not attempt to access any unit features or functions, including, but not limited to, Reset and Exit. Interrupting the upgrade procedure can cause memory corruption and render the unit non-functional. Such an action may void your warranty or service contract, and in such a case unit repair/replacement costs are solely the responsibility of the user.**

---

---

*Note: Many upgrades can be performed "anonymously" from the FTP server.*

---

► **To perform the upgrade:**

1. Choose Maintenance > Firmware Upgrade. The Firmware Upgrade page opens.

**Firmware Upgrade**

**IP Address:**

**Login:**

**Password:**

**File Path:**

2. Type the IP Address of the FTP server in the IP Address field.
3. Type your login name in the Login field.
4. Type your password in the Password field.
5. Type the path to the firmware file in the File Path field (for example, /home/downloads/firmware/UpgradePack\_2.5.6\_3.1.0.5.2/Pack1of1).
6. Click Upgrade.

The upgrade lasts about 20 minutes. After about half the time, the SX unit will restart. The upgrade will continue for another 20 minutes or so after the restart.

Once the upgrade is initiated, the upgrade status message indicates the progress of the upgrade. The files are copied and the unit is reset. You receive the following message:

Upgrade is Complete, The unit is now resetting.

The blue light on your SX will turn off, flash once while it is extracting more files, turn off, then turn on and remain on. You are logged out. It should now be running the new firmware.

---

*Note: If the upgrade fails, the system will display an error message detailing the failure.*

---

---

### Display a Firmware Upgrade History

To display the firmware upgrade history for an SX unit, choose Maintenance > Firmware Upgrade History. The Firmware Upgrade History page opens, displaying the version of each past firmware upgrade and the date and time the upgrade was performed.

Name
3.1.0.1.2 Tue Feb 20 16:15:19 2007
3.1.0.1.5 Thu Mar 15 15:14:32 2007

---

### Performing a Factory Reset on the SX

Performing a factory Reset returns the SX unit to its default factory settings. Be very careful when doing this, because it will erase all the data and settings on the SX unit and return it to the state in which it was originally shipped.

To perform a factory reset, choose Maintenance > Factory Reset. You are prompted to confirm the reset. Click Yes to proceed. If you change your mind, click No.

---

*Note: In case you are not aware of the administrative password to log in the SX GUI to perform a factory reset, you may want to try resetting from the SX hardware. To do so, insert a pin into the RESET hole on the back panel of the SX unit and hold for about 15 seconds. The SX is then reset to factory defaults.*

---

---

### Rebooting the SX

Performing a reboot powers the SX off and then back on. Be careful when doing this, because it will log all current users off the system.

To perform a reboot, choose Maintenance > Reboot. You are prompted to confirm the reboot. Click Yes to proceed. If you change your mind, click No.

# Chapter 10 Diagnostics

## In This Chapter

Network Infrastructure Tools .....	132
Administrator Tools - Process Status .....	135

---

### Network Infrastructure Tools

Network infrastructure tools allow you to view the status of the active network interfaces and important network statistics. You can also perform ping and trace route operations.

---

#### Status of Active Network Interfaces

1. Choose Diagnostics > Status of Active Network Interfaces. The system displays status information about the active network interfaces.

##### Status of Active Network Interfaces

Refresh

#### Result:

```
eth0      Link encap:Ethernet  HWaddr 00:0D:5D:00:E2:4D
          inet addr:192.168.51.183  Bcast:192.168.51.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2525902 errors:0 dropped:0 overruns:0 frame:0
          TX packets:168545 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:227412923 (216.8 Mb)  TX bytes:47829101 (45.6 Mb)
          Interrupt:19 Base address:0x1000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:331334 errors:0 dropped:0 overruns:0 frame:0
          TX packets:331334 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:67001364 (63.8 Mb)  TX bytes:67001364 (63.8 Mb)
```

2. Click Refresh to update the information.

## Network Statistics

1. Choose Diagnostics > Network Statistics. The Network Statistics page opens.

**Network Statistics**

**Options:**

--all ▼

**Refresh**

**Result:**

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	*:5000	*:*	LISTEN
tcp	0	0	*:www	*:*	LISTEN
tcp	0	0	*:ssh	*:*	LISTEN
tcp	0	0	*:telnet0	*:*	LISTEN
tcp	0	0	*:443	*:*	LISTEN
tcp	0	0	192.168.50.132:443	192.168.58.88:2298	TIME_WAIT
tcp	0	0	localhost:5000	localhost:1363	ESTABLISHED
tcp	0	0	192.168.50.132:443	192.168.58.88:2299	TIME_WAIT
tcp	0	0	192.168.50.132:443	192.168.58.88:2296	TIME_WAIT
tcp	0	0	192.168.50.132:443	192.168.58.88:2297	TIME_WAIT
tcp	0	0	192.168.50.132:443	192.168.58.88:2302	ESTABLISHED
tcp	0	0	localhost:1363	localhost:5000	ESTABLISHED
tcp	0	0	192.168.50.132:443	192.168.58.88:2292	TIME_WAIT
tcp	0	0	192.168.50.132:443	192.168.58.88:2300	TIME_WAIT
tcp	0	0	192.168.50.132:443	192.168.58.88:2293	TIME_WAIT
tcp	0	0	192.168.50.132:443	192.168.58.88:2301	ESTABLISHED
udp	0	0	*:5000	*:*	

Active UNIX domain sockets (servers and established)

Proto	RefCnt	Flags	Type	State	I-Node	Path
unix	2	[ ACC ]	STREAM	LISTENING	48	/dev/log
unix	2	[ ACC ]	STREAM	LISTENING	122	/tmp/internal_rdmf
unix	2	[ ACC ]	STREAM	LISTENING	130	/tmp/filterSock
unix	2	[ ACC ]	STREAM	LISTENING	173	/tmp/.150
unix	3	[ ]	STREAM	CONNECTED	17371	/dev/log
unix	3	[ ]	STREAM	CONNECTED	17370	
unix	3	[ ]	STREAM	CONNECTED	59	/dev/log
unix	3	[ ]	STREAM	CONNECTED	47	

2. By default, all statistics are shown. To show specific statistics, select an entry from the drop-down menu in the Options field. Your choices are:
  - Route

- Interfaces
  - Groups
  - Statistics
  - Program
3. Click Refresh to update the information.

---

### Ping Host

1. Choose Diagnostic > Ping Host. The Ping Host page opens.



**Ping Host**

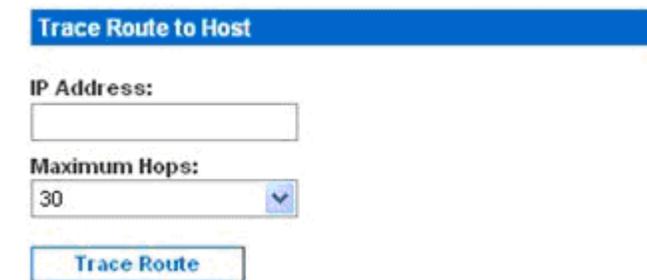
**IP Address:**

**Ping**

2. Type the IP address of the host to be pinged in the IP Address field.
3. Click Ping. The page displays the results of the ping.

---

### Trace Route to Host



**Trace Route to Host**

**IP Address:**

**Maximum Hops:**

**Trace Route**

1. Choose Diagnostics > Trace Route to Host. The Trace Route to Host page opens.
2. Type the IP address of the host in the IP Address field.
3. Select the maximum amount of hops from the drop-down menu in the Maximum Hops field.
4. Click Trace Route. The page displays the results of the Trace Route.

## Administrator Tools - Process Status

1. Choose Diagnostics > Process Status. The Process Status page opens.



**Process Status**

Refresh

**Result:**

PID	Uid	Stat	Command
1	root	S	[swapper]
2	root	S	[keventd]
3	root	S	[ksoftirqd_CPU0]
4	root	S	[kswapd]
5	root	S	[bdflush]
6	root	S	[kupdated]
7	root	S	init
18	root	S	[jffs2_gcd_mtd1]
62	root	S	[eth0]
70	root	S	/sbin/klogd
72	root	S	/sbin/syslogd
74	root	S	/ata/kernel/logwatch
75	root	S	/bin/sh /sbin/run_dom.sh
80	root	S	/ata/kernel/dom
83	root	S	/tmp/seriald modem
84	root	S	/usr/sbin/inetd
87	root	S	/usr/bin/sconsole --
92	root	S	sshd -p 22 -p 3001 -p 3002 -p 3003 -p 3004 -p 3005 -p 3006
99	root	S	/ata/kernel/dom
101	root	S	/ata/kernel/dom

2. Click Refresh to update the information.

# Chapter 11 Command Line Interface

## In This Chapter

Command Line Interface Overview .....	137
Accessing the SX Using CLI.....	137
SSH Connection to the SX .....	138
Telnet Connection to the SX .....	139
Local Port Connection to the SX .....	140
Navigation of the CLI .....	141
Initial Configuration.....	144
CLI Prompts.....	146
CLI Commands.....	146
Target Connections and the CLI .....	154
Configuring Authorization and Authentication (AA) Services .....	155
Administering the SX Console Server Configuration Commands.....	159
Configuring Events .....	159
Configuring Log .....	160
Configuring a Modem .....	167
Configuring Network .....	170
Configuring NFS .....	175
Configuring Ports.....	177
Configuring Services .....	182
Configuring SNMP.....	189
Configuring Time .....	191
Configuring Users .....	192
Connect Commands.....	196
Configuring Power .....	196
Diagnostic Commands .....	197
IPMI Commands.....	198
Maintenance Commands.....	203
Security Commands .....	209

---

## Command Line Interface Overview

The SX Serial Console supports all serial devices, including:

- Servers, including Windows Server 2003® when using the Emergency Management Console (EMS-) Special Administration Console, or SAC with BIOS redirection in the server BIOS
- Routers
- Layer 2 switches
- Firewalls
- Power strips
- Other user equipment

The SX allows an Administrator or User to access, control, and manage multiple serial devices. You can use the Command Line Interface (CLI) to configure the SX or to connect to target devices. The RS-232 interface may operate at all standard rates from 1200 bps to 115200 bps.

The following common commands can be used from all levels of the CLI to the preceding figure:

- top
- history
- logout
- quit
- show
- help

---

## Accessing the SX Using CLI

Access the SX using one of these methods:

- TELNET via IP connection
- HTTP and HTTPS via IP connection
- SSH (Secure Shell) via IP connection
- Local Port-via RS-232 serial interface

Many SSH/TELNET clients are available and can be obtained from the following locations:

- PuTTY - <http://www.chiark.greenend.org.uk/~sgtatham/putty/>  
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- SSH Client from ssh.com - [www.ssh.com](http://www.ssh.com) <http://www.ssh.com>
- Applet SSH Client - [www.netspace.org/ssh](http://www.netspace.org/ssh)  
<http://www.netspace.org/ssh>
- OpenSSH Client - [www.openssh.org](http://www.openssh.org) <http://www.openssh.org>

---

## SSH Connection to the SX

Use any SSH client that supports SSHv2 to connect to the SX. You must enable SSH access from Network Service Settings page (See **Change Network Service Settings** (on page 43)).

---

*Note: For security reasons, SSH V1 connections are not supported by the SX.*

---

---

### SSH Access from a Windows PC

► **To open an SSH session from a Windows® PC:**

1. Launch the SSH client software.
2. Enter the IP address of the SX server. For example, 192.168.0.192.
3. Choose SSH, which uses the default configuration port 22.
4. Click Open.
5. The `login as:` prompt appears.

---

### SSH Access from a UNIX/Linux Workstation

► **To open an SSH session from a UNIX®/Linux® workstation and log in as the user admin, enter the following command:**

```
ssh -l admin 192.168.30.222
```

The Password prompt appears.

---

### Login

► **To log in, enter the user name admin as shown:**

```
Login: admin
```

The password prompt appears. Enter the default password raritan.

```
Password: raritan
```

The welcome message appears. You are now logged in as an Administrator.

```
login as: admin
Password:
Authentication successful.
-----
Welcome to the DominionSX.  [Model: SX32]
UnitName:TheMonarch        FirmwareVersion:3.1.5.5.1      Serial:WAOF300029
IP Address:192.168.60.114   UserIdleTimeout:0min
-----

Port Port          Port Port          Port Port
No.  Name            No.  Name            No.  Name
1 - Triana [U]      2 - Henchman 24 P [U]  3 - Henchman 21 [U]
4 - [P] ThePerfec [U,B] 5 - Port5 [U]         6 - Port6 [U]
7 - Port7 [U]       8 - Port8 [U]         9 - Port9 [U]
10 - Port10 [U]     11 - Port11 [U]       12 - Port12 [U]
13 - Port13 [U]     14 - Port14 [U]       15 - Port15 [U]
16 - Port16 [U]     17 - Port17 [U]       18 - Port18 [U]
19 - Port19 [U]     20 - Port20 [U]       21 - Port21 [U]
22 - Port22 [U]     23 - Port23 [U]       24 - Port24 [U]
25 - Port25 [U]     26 - Port26 [U]       27 - Port27 [U]
28 - Port28 [U]     29 - Port29 [U]       30 - Port30 [U]
31 - Loop Back [U]  32 - Loop Back [U]
Current Time: Thu Apr 17 06:42:30 2008

admin > █
```

After reviewing *Navigation of the CLI* (on page 141), perform the initial configuration tasks.

---

## Telnet Connection to the SX

Due to the lack of security, user name, password and all traffic is in clear-text on the wire. Telnet access is disabled by default.

---

### Enabling Telnet

To use Telnet to access the SX, first access the SX from the CLI or a browser.

CLI

1. Use the following command:  
Admin Port > Config > Services > telnet enable  
true

The system returns the following message:

The system will need to be rebooted for changes to take effect.

---

*Note: By default, the telnet port is set to 23. You may change it by issuing the following command:*

```
Admin Port > Config > Services > telnet enable  
true port <preferred port number>
```

---

2. Reboot the system.

Browser (GUI)

Enable Telnet access in the Setup > Services menu.

Accessing the SX Unit

Once Telnet access is enabled, use it to access the SX unit and set up the remaining parameters.

---

### Accessing Telnet from a Windows PC

► **To open a Telnet session from a Windows® PC:**

1. Choose Startup > Run.
2. Type *Telnet* in the Open text box.
3. Click OK. The Telnet page opens.
4. At the prompt enter the following command: `Microsoft Telnet> open <IP address>` where <IP address> is the SX IP address.
5. Press the Enter key. The following message appears: `Connecting To <IP address>...` The login as prompt appears.

---

### Local Port Connection to the SX

If your SX's terminal port uses an RJ45 jack, a special cable (CRLVR) is used with an ASCSDB9F connector on the client machine. The CRLVR may also be used if RJ45-RJ45 connection to local port is established - that is, if you connect the local port of an SX as a serial target to another SX.

---

#### Port Settings

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

- Data bits = 8
- Parity = None
- Stop bits = 1
- Flow Control = None

---

## Connection

### ► To make a local port connection:

1. Open a HyperTerminal application or equivalent.
2. Ensure the HyperTerminal is configured to communicate with the port that is connected to the SX unit.
3. Disable Flow control.
4. Press the Enter key and the following prompt appears: `user name`

See **Login** (on page 138) for details.

---

### To Change the Local Port Parameters:

The local port is enabled by default and is enabled on both serial ports for units with two local ports at 9600 bps.

### ► To change the local port parameters:

As an example, to change the baud rate from the default 9600 bps to 115200 bps, type:

```
Admin Port > Config > Services > lpa enable true  
bps 115200
```

### ► To disable local port access:

```
Admin Port > Config > Services > lpa enable false
```

---

## Navigation of the CLI

Before using the CLI, it is important to understand CLI navigation and syntax. There are also some keystroke combinations that simplify CLI use.

---

### Completion of Commands

The CLI supports the completion of partially-entered commands. After entering the first few characters of an entry, press the Tab key. If the characters form a unique match, the CLI will complete the entry.

- If no match is found, the CLI displays the valid entries for that level.
- If multiple matches are found, the CLI displays all valid entries.

Enter additional text to make the entry unique and press the Tab key to complete the entry.

---

## CLI Syntax -Tips and Shortcuts

### Tips

- Commands are listed in alphabetical order.
- Commands are not case sensitive.
- Parameter names are single word without underscore.
- Commands without arguments default to show current settings for the command.
- Typing a question mark ( ? ) after a command produces help for that command.
- A pipe symbol ( | ) indicates a choice within an optional or required set of keywords or arguments.

### 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 to execute the command.
- Press Tab to complete a command. For example, `Admin Port >` `Conf.` The system then displays the `Admin Port > Config >` prompt.

---

## Common Commands for all Command Line Interface Levels

CLI Commands lists the commands that are available at all CLI levels. These commands also help navigate through the CLI.

Commands	Description
top	Return to the top level of the CLI hierarchy, or the “username” prompt
history	Display the last 200 commands the user entered into the SX CLI
show	Show the settings for the given parameter or show all configurations by default
help	Display an overview of the CLI syntax
quit	Places the user back one level
logout	Logs out the user session

---

## Show Command

The show command displays various configuration settings and is available at all levels.

The syntax of the show command is:

```
show [ clock | version | network | route | firewall |
      ipforwarding | modem | dpa |
      anon | port | idletimeout | users | groups |
      lpa | ssh | telnet | http | https |
      encryption | clientcert | ntp | keywords |
      smtp | snmp | eventlogfile | syslog | nfs | portlog
      |
      ldap | radius | tacacs | kerberos | security_profile
      |
      strongpassword | inactiveloginexpiry |
      invalidloginretries |
      lockoutperiodoninvalidlogin | localauth |
      singleloginperuser |
      powerstrip | powerdelay | association | powergroup ]
[all]
```

### Command Example

The following command shows the general settings of the SX unit:

```
Admin Port > show
```

```
SX4 [64Mb]   Serial: WACEA00008
```

```
Current time: 2006-09-20 23:08:42
```

```
-----
```

### Date /Time Settings:

```
    Date : 2006-09-20 23:08:42
```

```
    Timezone : 13
```

### Version Information :

```
Firmware Version : 3.0.0.1.15
```

```
Kernel Version : 2.4.12
```

PMON Version: 2.0.1

RSC Version: 1.0.0.1.16

Supporting software:

OpenSSH\_4.3p2, OpenSSL 0.9.7i 14 Oct 2005

HTTP Server version: Apache/2.2.0

HTTP Server built: Mar 29 2006 16:06:30

TELNET Linux NetKit 0.17

---

*Note: SX security is not impacted if the version of Apache 2.2 installed on the remote host is older than 2.2.9.*

---

---

## Initial Configuration

SX units come from the factory with default factory settings. When you first turn on and connect to the unit, you must set the following basic parameters so the unit can be accessed securely from the network:

1. Reset the administrator password.

All SX units are shipped with the same default password; therefore, to avoid security breaches it is imperative that you change the admin password from "raritan" to one customized for the administrators who will manage the SX.

Passwords are case sensitive and can contain up to 64 alphanumeric characters with the exception of " ' < > \ &

2. Assign the IP address, subnet mask, and gateway IP address to allow remote access.
3. Set the time and date.

After the preceding parameters are set, the rest of the system configuration can be performed.

---

### Setting Parameters

To set parameters, you must be logged on with administrative privileges. At the top level, you will see the "Username" > prompt, which for the initial configuration is "admin". Enter the top command to return to the top menu level.

---

*Note: If you have logged on with a different user name, that user name will appear instead of admin.*

---

---

## Date and Time Configuration

---

*Note: It is important to set the date and time correctly to ensure that log entries and events contain the correct timestamp.*

---

Return to the top menu level by entering the top command. Use the following command to view the current date and time settings:

```
Admin Port > Config > Time > clock
```

The system displays the current settings. For example:

```
Date /Time Settings:
    Date : 2006-09-20 23:20:24
    Timezone : 13
```

Use the following steps to set the user date and time.

1. Admin Port > Config > Time > timezonelist
2. Admin Port > Config > Time > clock tz 21 datetime "2006-09-23 13:22:33"

---

## Setting Network Parameters

---

Network parameters are configured using the interface command.

```
Admin Port > Config > Network > dhcp false interface
enable true if lan1 ip 192.16.151.12 mask 255.255.255
gw 192.168.51.12
```

When the command is accepted, the unit automatically reboots and drops the connection. You must reconnect to the unit using the new IP address and the username admin and password newp/w entered in the resetting factory default password section.

---

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

---

The SX now has the basic configuration and can be accessed remotely via SSH, GUI or locally using the local serial port. Next, you must configure the users and groups, services, security, and serial ports to which the serial targets are attached to the SX.

## CLI Prompts

The Command Line Interface prompt indicates the current command level. The root portion of the prompt is the login name. For a direct admin serial port connection with a terminal emulation application, Admin Port is the root portion of a command.

```
admin >
```

For Telnet/SSH, admin is the root portion of the command:

```
admin > config > network >
```

0

## CLI Commands

Command	Definition
config	Switches to config menu
authentication	Switches to authentication menu
ldap	Switches to ldap menu
primaryldap	Primary LDAP Server settings
secondaryldap	Secondary LDAP Server Settings
ldaps	Switches to ldaps menu
getservercert	FTP Retrieval of LDAP certificate file
removecert	Remove LDAPS Certificate
viewcert	View LDAPS Certificate
radius	Switches to radius menu
primaryradius	Primary RADIUS Server Settings
secondaryradius	Secondary RADIUS Server Settings
tacacsplus	Switches to tacacsplusmenu
primarytacacs	Primary TACACS+ Server Settings
secondarytacacs	Secondary TACACS+ Server Settings
events	Switches to events menu
add	Add an SMTP Event
delete	Delete SMTP event
smtp	SMTP Server Configuration
log	Switches to log menu

Command	Definition
cleareventlog	Clear Contents of the local log
eventlogfile	Local log configuration for logging of events
eventsyslog	Syslog configuration for logging of events
nfsgetkey	Get the NFS Encryption key used for encrypting port log
nfssetkey	Set the encryption key to be used for encrypting port log
portlog	Configure logging of port data
portsyslog	Portlog Syslog Server configuration
sendeventlog	Send local logfile to remote FTP server
vieweventlog	View local syslog
modem	Switches to modem menu
dialback	Set/Get modem dialback parameters
dialin	Set/Get modem dialin parameters
network	Switches to network menu
ethernetfailover	Set/Get ethernet parameters
interface	Set/Get ethernet parameters
ipforwarding	IP Forwarding configuration
name	Network name configuration
ports	Network port configuration
route	Show kernel routing table
routeadd	Add route to kernel routing table
routedelate	Delete route of kernel routing table
nfs	Switches to nfs menu
nfs	NFS Server configuration
port	Switches to port menu
config	Port configuration command
keywordadd	Add keyword notification for port
keyworddelete	Delete keyword notification for port
services	Switches to services menu
dpa	Per-port Direct Port Access type
encryption	Encryption configuration

Command	Definition
fixedtcpwindow	TCP Window Tuning Parameter
http	HTTP configuration
https	HTTPS configuration
lpa	Local Port configuration
ssh	SSH configuration
telnet	Telnet configuration
snmp	Switches to snmp menu
add	Add SNMP destination
addv3	Add SNMP destination
delete	Delete SNMP destination
deletev3	Delete SNMP v3 destination
snmp	SNMP Server configuration
snmpv3	SNMP Server configuration
time	Switches to time menu
clock	Set/Get time parameters
ntp	Set/Get ntp parameters
timezonelist	Timezone List
users	Switches to users menu
addgroup	Add new group to system
addsshkey	Add SSH keys to a user
adduser	Add a new user
deletegroup	Delete a group
deletesshkey	Delete SSH keys for a user
deleteuser	Delete a user
editgroup	Edit existing group in system
edituser	Edit an existing user
groups	Show details of groups
users	Show details of users
viewsshkey	View SSH keys for a user
connect	Connect to a port
diagnostics	Switches to diagnostics menu

Command	Definition
ifconfig	Show detailed network configuration
netstat	Print network connections
ping	Ping a remote system
ps	report system process status
tracert	Print the route to a remote system
uptime	Print system uptime information
getconfig	Retrieve remote configure script
ipmi	Switches to ipmi menu
ipmidiscover	discover all the IPMI enabled devices
ipmitool	send command to remote ipmi device
listports	List accessible ports
logout	Logout of the current CLI session
maintenance	Switch to System Maintenance commands menu
backup	Backup system
clearventlog	Erase contents of local event log file
factoryreset	Reset the system to factory default state
firmware	Get current firmware version
logoff	Force logoff (terminate) a user or port session
reboot	Restart the SX
restore	Restore system
sendeventlog	Send local logfile to remote FTP server
upgrade	Upgrade system
upgradehistory	Retrieve upgrade history
upgradestatus	Display current file being upgraded. This is applicable when upgrade is in progress.
userlist	List active user sessions
vieweventlog	View local event log file
password	Set the current user's password. Eg., password Hello123\$
power	Switch to Power Control menu
associate	Associate a Power Strip outlet to a SX Port

Command	Definition
association	View Currently configured associations
cycle	Power cycle specified ID
off	Power off specified ID
on	Power on specified ID
outlet	Edit Outlet information
powerdelay	Configure global Power Strip delays
powergroup	Switch to Power Group Menu
powerstatus	Get Power Strip status
powerstrip	Edit Power Strip information
setpowerport	Configure an SX Port to contain a Power Strip device
unassociate	Remove a power outlet association from a SX Port
unsetpowerport	Configure an SX Port to remove a Power Strip device
runconfig	Run Configuration Script
security	Switch to security menu
banner	Switches to banner menu
banner	Banner display and audit configuration settings
ftpgetbanner	Get customized banner.txt using FTP
certificate	Switches to certificate menu
client	Switches to client menu
add	Install a User Certificate
addcrl	Install a CA's CRL
clientcert	Activate Client Side Certificate Verification
delete	Remove Client CA Certificate
deletecrl	Remove Client CA's CRL
viewcacert	View Client CA Certificate
viewcrl	View Client CA CRL Certificate
server	Switches to server menu
activatedefaultcert	Activate Default System SSL Certificate
activateusercert	Activate User SSL Certificate

Command	Definition
generatecsr	View Default System Cert
generatedefaultcert	Generate Default System SSL Certificate
installusercert	Install a User Certificate
installuserkey	Install a User Certificate Key
viewcsr	View The Certificate Signing Request
viewdefaultcert	View Default System Cert
firewall	Switches to firewall menu
firewall	Enable/Disable firewall
iptables	administration tool for IPv4 packet filtering and NAT
iptables-save	save IP Tables to make firewall rules persistent
Kerberos	Switches to Kerberos menu
gethostnamefile	Get /etc/hosts in case of DNS failure file
getkrbconfig	Get kerberos 5 configuration file
kadmin	Kerberos admin client
kerberos	Kerberos based Network Authentication
kinit	get kerberos ticket
klist	list kerberos ticket
loginsettings	Switches to loginsettings menu
idletimeout	Set system wide idletimeout
inactiveloginexpiry	Configure local login expiry time
invalidloginretries	Configure local login max number of retries
localauth	Configure local authentication
lockoutperiod	lockout period on invalid login attempt
portaccess	Allow/Restrict concurrent users per port
singleloginperuser	Restrict to a single login session per user
strongpassword	Configure strong password rules
unauthorizedportaccess	Unauthorized (Anonymous) port access
securityprofiles	Switches to securityprofiles menu
profiledata	View or modify a Security Profile
securityprofiles	Enable and select a Security Profile

Command	Definition
userlist	List active user sessions

---

### Security Issues

Elements to consider when addressing security for console servers:

- Encrypting the data traffic sent between the operator console and the SX unit.
- Providing authentication and authorization for users.
- Logging data relevant to the operation for later viewing and auditing purposes. In some cases, this data is required for compliance with governmental or company regulations.
- Security profile.

SX supports each of these elements; however, they must be configured prior to general use.

Encryption of traffic between the operator console and the SX unit is determined by the access methodology being used. SSH and encrypted browser access (HTTPS) are enabled by default. SSH and HTTPS, by definition, support 128-bit encryption of the traffic between the two ends of the link. To accept unencrypted connections, you must manually enable the HTTP and Telnet services.

### Welcome Banner Configuration

The SX optionally supports a customizable (maximum 6000 words) welcome banner that is displayed after login. When you log in to a SX via a GUI, a banner with a fixed width typeface and a common dimension like 80x25 appears. If the banner is very large, that is, over 9000 lines, the banner displayed on GUI will not increase overall page size because it is contained within a self-scrolled text area.

The banner identifies the location to which the user has logged in. You can also add a consent banner that forces the user to accept stated conditions prior to advancing into operation of the console server.

### Defining SSL Security Certificates

SSL Security certificates are used in browser access to ensure that the unit you are attaching to is the unit that is authorized to be connected. This section describes only how to configure the certificates on the console server. See **Appendix C: Certificates** (see "**Certificates**" on page 267) for details on SSL Certificates.

### Enabling Firewall Protection

SX provides a firewall function to provide protection for the IP network and to control access between the internal router, LAN (or LAN1 and LAN2 if dual-LAN units) and the dial modem interfaces.

### Enabling Security Profiles

SX provides the ability to define security profiles which simplify the assigning of permissions to users and groups. There are three types of profiles. Two are predefined: standard and secure. The third allows for the definition of custom profiles; this allows assignment of all permissions by assigning one security profile. Multiple custom security profiles may be defined.

### Configuring Logging and Alerts

As part of the security capabilities of the SX, facilities are provided to log data and to provide alerts based on activities between the users, SX, and the target device. These facilities provide an audit trail that allows authorities to review what has happened in the system, determine who implemented what action, and when.

Among these facilities are event logging and SNMP traps. Events may be logged locally using Syslog. Local events are maintained in a 256K per port buffer and can be stored, reviewed, cleared, or sent periodically to an FTP server.

---

### Configuring Users and Groups

Users and groups are related. SX allows the administrator to define groups with common permissions and attributes. They can then add users to the groups and each user takes the attributes and permissions of that group. By enabling groups, the permissions for each user do not have to be configured individually, reducing the time to configure users one by one.

---

### Command Language Interface Permissions

Administrators can execute all commands.

Operators and Observers can execute only the following commands:

- connect (the port list appears after returning from connect command)
- ? (functions as help)
- logout
- password
- history

---

## Target Connections and the CLI

The purpose of the SX is to let authorized users establish connections to various targeted devices using the connect command. Before connecting to a target, the terminal emulation and escape sequence must be configured. When a target is disconnected, the appropriate disconnect message appears. The SX also provides the ability to share ports among users.

---

### Setting Emulation on a Target

► **To set emulation on the target:**

- Ensure that the encoding in use on the host matches the encoding configured for the target device, that is, if the character-set setting on a Sun™ Solaris™ server is set to ISO8859-1, the target device should also be set to ISO8859-1.

---

*Note: ISO9660 format is the standard supported by Raritan. However, other CD-ROM extensions may also work.*

---

- Ensure that the terminal emulation on the target host connected to the SX 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, that is, if the terminal type setting on a HP-UX® server is set to VT100, the Access Client should also be set to VT100.

The setting for terminal emulation on the SX is a property associated with the port settings for a particular target device. Ensure that the settings for terminal emulation in the client software such as Telnet or SSH client are capable of supporting the target device.

---

### Set Escape Sequence

To set the Escape sequence, ensure that the default Escape sequence set on the SX server does not conflict with a key sequence required by either the Access Client or the host operating system. The Escape key sequence is user-configurable. Console sub-mode should be displayed when the default escape key sequence ^] (programmable) is pressed.

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

---

### Port Sharing Using CLI

Access Client users can share ports with other authenticated and authorized users, regardless of whether they are Access Client users or SSH/Telnet users. Port sharing is used for training or for troubleshooting applications.

- Users are notified in real time if they have Write access or Read Only access at any point during the port-sharing session.
- Users can request Write permission to a port.

---

## Configuring Authorization and Authentication (AA) Services

SX supports both local and remote authentication and authorization (AA) services. Local databases for AA are maintained in an encrypted format to prevent unauthorized access.

---

### Remote Services

For remote services, SX supports LDAP, Active Directory®, TACACS+ and Kerberos. The SX server supports an additional level of security services that further enhance protection of the console server. These services are:

- Idle timeout for inactive users
- User defined certificates
- Security profiles

Command	Description
ldaps	getservercert removecert viewcert
primaryldap	
secondaryldap	
radius	primaryradius secondaryradius
tacacsplus	primarytacacs secondarytacacs

---

*Note: When configuring the LDAP server, the query string format on the server should contain the name of a group configured on the SX.*

*When configuring the Radius server, the Filter-ID format for the users on the server should have the following format  
"rاران:G{GroupOnSX}:D{DialbackNumber}".*

*When configuring the TACACS+ server, the user-group format for the user on the server should contain the name of a group configured on the SX.*

*If you use older formats of "op:1:2:4" or "a:\*" , the system will allow you to log in and will restrict port accessibility according to user types and their limitations. The SX will not have any database information about groups at this time and will therefore display the following message in the banner after login.*

*Error: Cannot get group information*

*The port display will show all ports because the client will not know which port limitations exist.*

---

### LDAP Configuration Menu

The LDAP configuration menu offers commands to set up LDAP and LDAPS.

LDAP is entered by typing *ldap* at the following prompt:

```
admin > Config > Authentication > ldap
```

LDAP Command	Description
ldaps	Switches to the ldaps menu which includes the following commands: getservercert - FTP Retrieval of ldap certificate removecert - Remove LDAPS Certificate viewcert - View LDAPS Certificate
primaryldap	Used to configure the primary ldap settings.
secondaryldap	Used to configure the secondary ldap settings.

LDAP Command Examples

```
admin > Config > Authentication > ldap
```

```
admin > Config > Authentication > ldap > ldaps
```

```
admin > Config > Authentication > ldap > ldaps >  
viewcert
```

---

## RADIUS Command

The RADIUS menu provides access to commands used to configure access to a RADIUS server.

### Syntax

```
primaryradius <>
```

### RADIUS Command Example

```
admin > Config > Authentication > radius >
primaryradius
```

Following is information using the Raritan-Vendor-Specific attribute, which is defined in the custom dictionary file.

The dictionary file must be created at following location  
/usr/share/freeradius/

### Dictionary File Configuration

```
# -*- text -*-
#
# dictionary.raritan
#
# Version: $Id$
#
VENDOR          Raritan          8267
#
#      Standard attribute
#
BEGIN-VENDOR    Raritan
ATTRIBUTE      Raritan-Vendor-Specific  26
                string
END-VENDOR     Raritan
```

Update Radius users to use the new attribute in the `users` file, which is usually located at `/etc/raddb/`.

```
Raritan-Vendor-Specific = "G{Administrator}"
```

---

*Note: If both filter ID and vendor specific attribute are present, the vendor specific attribute will take preference.*

---

---

### TACACS+ Command

The TACACS+ menu offers commands used to configure access to a TACACS+.

Syntax

```
primarytacacs <>
```

TACACS+ Command Example

```
admin > Config > Authentication > radius >
primarytacacs
```

---

## Administering the SX Console Server Configuration Commands

---

*Note: CLI commands are the same for SSH, Telnet, and Local Port access sessions.*

---

The configuration menu provides commands to help configure the SX:

- authentication
- events
- log
- modem
- network
- nfs
- ports
- services
- snmp
- time
- users

---

## Configuring Events

The Events menu provides access to commands used to configure SMTP events and servers.

Command	Description
add	Add an SMTP event.
delete	Delete an SMTP event.

Command	Description
smtp	Configure the SMTP server settings.

Events Menu Command Examples

```
admin > Config > events
```

```
admin > Config > events > add
```

```
admin > Config > events > smtp
```

---

## Configuring Log

Configuration log commands allow you to manage the logging features of the SX server:

- `cleareventlog`
- `eventlogfile`
- `eventsyslog`
- `nfsggetkey`
- `nfsssetkey`
- `portlog`
- `sendeventlog`
- `vieweventlog`

---

### Cleareventlog Command

The `cleareventlog` command clears the contents of the local event log.

Syntax

```
cleareventlog
```

Cleareventlog Command Example

```
admin > Config > Log > cleareventlog
```

---

## Eventlogfile Command

The eventlogfile command controls and configures the logging of events to the local log.

Syntax

```
eventlogfile [enable <true|false>] [size value]
[style <wrap|flat>]
```

eventlogfile Command	Description
enable <true false>	Enable or disable the system event log logging.
size value	<p>Maximum size of local log file (in bytes).</p> <p>If the event log file size exceeds the available flash memory on your SX model, the event is not saved.</p> <p>To avoid this, Raritan recommends you set the file size to greater than 1024 but less than 10000000.</p> <hr/> <p><i>Note: Each SX has a different amount of available flash memory.</i></p>
style <wrap flat>	<p>Specifies what action to take when the maximum size is reached:</p> <ul style="list-style-type: none"> <li>▪ wrap will cause the log to circle around when end is reached.</li> <li>▪ flat will cause logging to stop when the end is reached.</li> </ul>

Eventlogfile Command Example

```
admin > Config > Log > eventlogfile enable true size
256000 style wrap
```

---

## eventsyslog Command

The eventsyslog command controls system event logging.

The syntax of the eventsyslog command is:

```
eventsyslog [enable <true|false>] [primip ipaddress] [secip ipaddress]
```

The eventsyslog command options are described in the following table.

Command	Description
enable <true false>	Enable or disable the system event log logging.

Command	Description
primip ipaddress	Primary FTP server address
secip ipaddress	Secondary FTP server address

**Eventsyslog Command Example**

```
admin > Config > Log > eventsyslog enable true primip 192.168.134.11
secip 192.168.245.11
```

---

**portsyslog Command**

The portsyslog command controls system event logging.

**Syntax**

```
portsyslog [enable <true|false>] [primaryip
ipaddress] [secondaryip ipaddress] [category
category]
```

portsyslog Command	Description
enable <true false>	Enable or disable logging of port data to remote a NFS server and also to the Syslog server.
primaryip ipaddress	Primary Portlog Syslog server address
secondaryip ipaddress	Secondary Portlog Syslog server address
category category	Portlog Syslog message category 0 ~ 7 corresponds to Local0 ~ Local7

**portsyslog Command Example**

```
admin > Config > Log > portsyslog enable true
primaryip 192.168.134.11 secondaryip 192.168.245.11
category 5
```

---

**nfsggetkey Command**

The nfsggetkey command gets an NFS encryption key to be used for encrypting port log data. Use the key value as input to the nfsgsetkey command.

**Syntax**

```
nfsggetkey [type <rc4|aes128>]
```

nfsggetkey Command	Description
type <rc4 aes128>	Type of encryption key used for

<b>nfsgetkey Command</b>	<b>Description</b>
	encryption (rc4 or aes128)

nfsgetkey Command Example

```
admin > Config > Log > nfsgetkey type aes128
```

---

### **nfssetkey Command**

The nfssetkey command sets the type of encryption and the key. Because NFS is insecure, it can be easily accessed and the data misused. With SX, you can encrypt the data stored on the NFS server. Consequently, if the data were to be accessed inappropriately, it would be of no use to anyone without the encryption key.

The key can be set and obtained only from the SX.

Syntax

```
nfssetkey [type <rc4|aes128>] [key string]
```

<b>nfssetkey Command</b>	<b>Description</b>
type <rc4 aes128>	Type of encryption type to be used
key string	Provide key string to be used for encryption

---

*Note: aes128 is not supported in 3.0.*

nfssetkey Command Example

```
admin > Config > Log > nfssetkey type aes128 key
D2F05B5ED6144138CAB920CD
```

---

### **NFS Encryption Enable Command**

To enable port logging and encryption of data:

```
admin > Config > Log > portlog enable true encrypt
true
```

---

### **Portlog Command**

The portlog command enables and configures the logging of port data.

Syntax

```
portlog [enable <true|false>] [prefix name] [size
value] [timestamp interval] [update interval]
[inputlog <true|false>] [indir name] [outdir name]
[encrypt <true|false>] [block <true|false>]
```

<b>portlog Command</b>	<b>Description</b>
enable <true false>	Enable/Disable logging of port data to remote NFS server.
prefix name	Prefix for log file name.
size value	Maximum Size (in bytes) for the log file.
timestamp interval	Time interval (in seconds) between two timestamps in the log file. A value of 0 will disable timestamp logging. The default value is 20. The max value is 99999.
update interval	Time interval (in seconds) between two updates to the remote log file The default interval is 20. The max value is 99999.
inputlog <true false>	Enable/Disable logging of user input data on the port. Input implies data sent to the target; that is, keystrokes entered by the user).
indir name	Filename for storing input log
outdir name	Filename for storing output log. Output implies data sent from target to the SX port.
encrypt <true false>	Enable/Disable Encryption of log data sent to the remote NFS Server.
block on failure <true false>	Indicate whether the NFS Server is a soft mount (when set to false) or a hard mount (when set to true).

**Portlog Command Example**

```
portlog enable true prefix DomSX1size 1000000
timestamp 1 update 20 inputlog false indir
/nfs_SX_DomIn outdir SX_Dom_Out encrypt true
```

The following command displays the default portlog values:

```
admin > Config > Log > portlog
Portlog Settings :
    Enable : false
    File Prefix: domSX-NFS
    File Size : 65535
    UpdateFrequency : 20
    TimestampFrequency : 20
    Input Log Enable : false
    Input Log Directory: input
    Output Log Directory: output
    Encrypted : false
    Block on Failure : true
```

---

**Decrypt Encrypted Log on Linux-based NFS Server**

To decrypt nfs encryption on Linux® platform, follow these steps:

1. Retrieve the current nfs encryption key:  

```
admin > Config > Log > nfsgetkey type rc4
```
2. Cut and paste the response of this command into a file, for example, dsx-encrypt.key.
3. Retrieve decryption application and either place it on the Linux machine or compile its source.
4. Save the encryption key file (dsx-encrypt.key) in the same directory where the decryption application is stored.
5. Copy the encrypted portlog file to the same directory.
6. Decrypt the file using the command:  

```
./decrypt -f <portlogfile> -e <keyfilename> -o <outputfile>
```
7. The decrypted file should be saved in <outputfile>.

---

### Sendeventlog Command

The sendeventlog command sends the local logfile to a remote FTP server.

Syntax

```
sendeventlog [ip ipaddress] [login login] [password password] [path pathname] [file filename]
```

sendeventlog Command	Description
ip ipaddress	FTP server IP address
login login	FTP Server login name
password password	FTP Server password
path pathname	FTP server path, for example, /ftphome
file filename	Filename on FTP server to save log. For example, sxlogfile

sendeventlog Command Example

```
sendeventlog ip 72.236.162.187 login acy password pasraritansword path sxlogfile file log_32
```

---

### Vieweventlog Command

The vieweventlog command displays the local log file.

Syntax

```
vieweventfile
```

vieweventlog Command Example

```
admin > Config > Log > vieweventlog
```

## Configuring a Modem

The Modem menu offers commands used to configure modem access. Callback (dialback) occurs when the originator of a call is immediately called back in a second call as a response to the first dial-in. Both Dial-in and Dialback must be enabled, and the dialback number for a user must be configured in the authentication service used on the unit (local, RADIUS, LDAP, or TACACS+).

Once you have configured the modem, the SX needs to be rebooted in order for the changes to take effect (you will receive a message prompting you to do this once you have made and applied your changes).

The modem can be configured to allow a PPP connection, a direct modem connection via Hyperterm, or both.

- All - Allows modem access to all modems. Looks for a PPP signal and falls back to allow console access if the PPP signal is not detected. In this mode, Modem Dial Back cannot be enabled.
- PPP Only - Allows only PPP connections. Allows GUI, SSH and Telnet access (if enabled). Dialback is only allowed when utilizing a PPP-Only configuration since allowing direct modem access would circumvent this security protection.
- Console Only - Allows only console connections. Only CLI access is allowed through a terminal emulation programs such as Hypertreminal.

If All or PPP Only are used:

- The IP addresses of the Point-to-Point (PPP) server must be entered. The default is 10.0.0.1
- The IP address of the PPP client must be entered. The default is 10.0.0.2.

If PPP Only is used:

- If you want to enable modem dialback, select the Enable Modem Dial Back check box.

Command	Description
dialback	Enable/Disable the modem dial-back. Modem must be enabled for this to work.
dialin	Enable/Disable Modem and PPP settings. [enable <true false>] [serverip ipaddress] [clientip ipaddress]
accessmodes	[accessmodes <All PPPOnly ConsoleOnly]

#### Modem Menu Command Examples

```
admin > Config > modem > dialin enable true serverip  
10.0.13.211
```

```
clientip 10.0.13.212 accessmodes PPPOnly
```

```
admin > Config > modem > dialback enable true
```

```
admin > Config > Modem > show modem
```

#### Modem Settings

```
Dialin Enabled: false
```

```
Access Mode: All
```

```
Server Address: 10.0.13.211
```

```
Client Address: 10.0.13.212
```

#### Dialback with local user

Before a modem connection can be established, the local user for dial-in authentication should be configured. A new user can be added or an existing one can be reconfigured with a correct dialback. An example configured user (dialback number is 129) should have the following settings:

PPP dial back works for 3 digit extensions and 7 and 11 digit numbers. If you are using 7 and 11 digit numbers, you must use commas to separate the 9 used for dialing an outside line and the 1 that precedes an area code from the rest of the number. For example, 9,1,5555551212.

#### User Settings:

```
Login : Modem
```

```
Name : Dialback
```

```
Info: SX
```

```
Dialback: 129
```

```
Group :Admin
```

```
Active : 1
```

When this configuration is set, the modem connection can be established. The user may use various types of modem dial-up clients to accomplish a successful modem connection to the SX.

#### Dialback with remote Radius user (Cistron Radius v1.6.7)

Dialin and Dialback should be enabled on the SX used for modem communication. Primary (or/and Secondary) RADIUS Server Settings should be configured correctly and enabled on the SX:

```
admin > Config > Authentication > RADIUS >
primaryradius
```

```
RADIUS Server Settings
```

```
-----
Primary Server
```

```
Enabled - true
IP Address - 10.0.0.188
Port - 1812
Secret - qazlwsx
```

On the Remote Radius Server, the user's configuration should contain the following line:

```
Filter-Id = "raritan:G{<local user group>}:D{<number
for dialback>}"
```

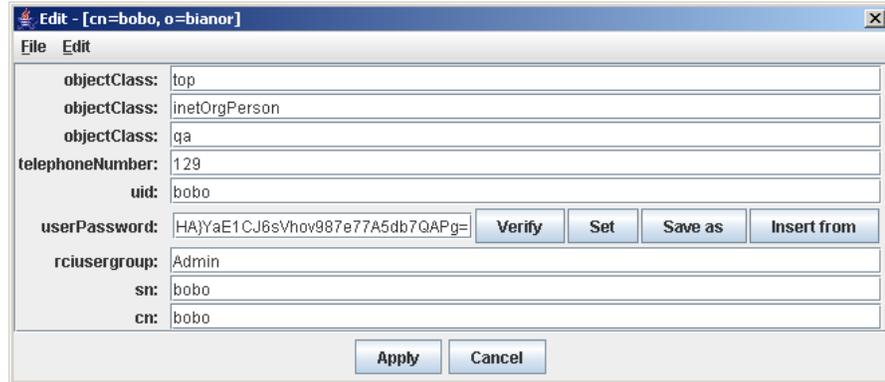
Dialback with remote LDAP user (OpenLdap v.2 & v.3)

Dial-in and Dialback should be enabled on the SX used for modem communication. Primary (or/and Secondary) LDAP Server Settings should be configured correctly and enabled on the SX:

```
LDAP Server Settings
```

```
-----
Primary Server
```

```
Enabled - true
IP Address - 10.0.0.188
Port - 389
Secret - root
Base DN - cn=root,o=bianor
Base Search - o=bianor
Auth Query String -rciusergroup
Dialback Query String - telephoneNumber
```



The Remote LDAP Server user's configuration should be:

Dialback with remote TACACS user (Tacacs+ v.4.0.3a)

Dial-in and Dialback should be enabled on the SX used for modem communication. Primary (or/and Secondary) TACACS Server Settings should be configured correctly and enabled on the SXs:

Primary Server

```

Enabled - true
IP Address - 10.0.0.188
Port - 49
Secret - alabala
    
```

On the Remote Tacacs Server user's configuration should own the following line:

```
user-dialback='129'
```

---

## Configuring Network

The Network menu commands allow you to configure the SX network adapter.

Commands	Description
ethernetfailover	Enable/Disable network failover
interface	The SX network interface configuration
ipforwarding	IP forwarding configuration
name	Network name configuration
ports	Network port configuration
route	Show kernel routing table

Commands	Description
routeadd	Add route to kernel routing table
routedelate	Delete route of kernel routing table

*Note: All operations that normally trigger a reboot or prompt the user for feedbacks are now added a new parameter named force. This force parameter prevents reboot, prompting or both from taking place until all configurations are completed. The commands that now have a force parameter are: ethernetfilover (see "Ethernetfailover Command" on page 171), interface (see "Interface Command" on page 171), name (see "Name Command" on page 173), ports (see "Ports Command" on page 173), factoryreset (see "Factoryreset Command" on page 204) and reboot (see "Reboot Command" on page 206).*

### Ethernetfailover Command

The ethernetfailover command is used to enable and disable the ability to failover from one LAN to another.

#### Syntax

```
ethernetfailover [enable <true|false>] [interval
value] [force <true|false>]
```

### Interface Command

The interface command is used to configure the SX network interface. When the command is accepted, the unit automatically reboots and drops the connection. You must then reconnect using the new IP address and the username admin and password newp/w in the resetting factory default password section.

#### Syntax

```
interface [enable <true|false>] [if <lan1 | lan2>]
[dhcp <true|false>] [ip ipaddress] [mask subnetmask]
[gw ipaddress] [mode <auto | 100fdx>] [force
<true|false>]
```

interface Command	Description
enable <true false>	Enable/Disable Interface
dhcp	Enable DHCP as ip configuration
if <lan1   lan2>	Select LAN interface you are configuring
ip ipaddress	IP Address of the SX assigned for access from the IP network
mask subnetmask	Subnet Mask obtained from the IP

interface Command	Description
	administrator
gw ipaddress	Gateway IP Address obtained from the IP administrator.
mode <auto   100fdx>	Set Ethernet Mode to auto detect or force 100Mbps full duplex (100fdx)
force <true false>	The force parameter is used so that sequences of commands can be inserted without need for user interaction.

#### interface Command Example

The following command enables the interface number 1, sets the IP address, mask, and gateway addresses, and sets the mode to auto detect.

```
Admin Port > Config > Network > interface enable true
if lan1 ip 192.16.151.12 mask 255.255.255 gw
192.168.51.12 mode auto
```

```
Admin Port > Config > Network > interface if lan1 ip
10.0.13.98 force true
```

---

#### IPForwarding Command

The ipforwarding command is used to configure the ability to forward between two networks.

##### Syntax

```
ipforwarding [enable <true|false>]
```

#### ipforwarding Command Example

The following command enables the IP Forwarding:

```
admin > Config > Network > ipforwarding enable true
```

---

### Name Command

The name command is used to configure the unit and host name.

#### Syntax

```
name [unitname name] [domain name] [force  
<true|false>]
```

#### name Command Example

The following command sets the unit name:

```
Admin Port > Config > Network > name unitname <unit  
name> domain <host name> force trues
```

---

### Ports Command

The ports command is used to configure the network ports.

#### Syntax

```
ports [discoveryport value] [csc value] [force  
<true|false>]
```

- discoveryport - udp discovery port used with Command Center - Secure Gateway
- csc - CSC Protocol tcp port used with Command Center - Secure Gateway

#### ports Command Example

The following command configures the network ports:

```
Admin > Config > Network > ports discoveryport 5000  
csc 5000
```

---

### Route Command

The route command is used to view the kernel routing table.

#### Syntax

```
route <>
```

#### route Command Example

The following command displays the routing table:

```
Admin Port > Config > Network > route
```

---

### **Routeadd Command**

The routeadd command is used to add a route to the kernel routing table.

Syntax

```
routeadd [if <eth0 | eth1>] [flags <net|host>] [dest  
ipaddress] [mask mask] [gw ipaddress] [mss value]  
[window value] [irtt value]
```

If Interface [eth0 | eth1], LAN1 is mapped to eth0, LAN2 is mapped to eth1

- flags net - Route for a subnet host/host machine
- dest - Destination host IP Address or subnet
- mask - Netmask
- gw - Gateway IP Address
- mss - Set the TCP Maximum Segment Size (MSS) in bytes
- window - Set the TCP window size for connections over this route in bytes
- irtt - Set the initial round trip time (irtt) for TCP connections over this route in milliseconds (1-12000)

routeadd Command Example

The following command adds a route to the routing table:

```
admin > Config > Network > routeadd if eth0 flags net  
dest 192.56.76.0 mask 255.255.255.0
```

---

### **Routedelete Command**

The routedelete command is used to remove a route from the kernel routing table.

Syntax

```
routedelete <>
```

routedelete Command Example

The following command remove a route from the routing table:

```
admin > Config > Network > routedelete
```

---

### Getconfig Command

The `getconfig` command retrieves the script from an FTP server. This command appears only in the administrator's help menu.

You can write a script using the same sequence and commands used in a normal CLI session, also known as a recorded session. The script can be used to set up commonalities among multiple SX units, including remote authentication servers, users, and security settings. The script can also be used by technicians who know little about the SX to set up machines after the administrator has written the script.

#### getconfig Command Example

The following command retrieves remote configure script from an FTP server.

```
admin > getconfig [ip ipaddress] [login login]
[password password] [path pathname]
```

`ip` IP Address of FTP Server

`login` FTP Server login name

`password` FTP Server password

`path` FTP server path.for config file Eg.,  
/ftphome/config.txt

---

### Runconfig Command

The `runconfig` command attempts to run the configuration script downloaded by the `getconfig` command. This command appears only in the administrator's help menu.

#### runconfig Command Example

```
admin > runconfig
```

---

## Configuring NFS

The `nfs` command enables all keystrokes echoed from the target device to be logged to a remote NFS server located within the network. The logs can be reviewed at a later time.

```
admin > Config > NFS > nfs
```

#### Syntax

```
nfs [enable <true|false>] [primaryip primaryip]
[secondaryip secondaryip] [primarydir primarydir]
[secondarydir secondarydir]
```

nfs Command	Description
enable <true false>	Enable or disable NFS logging.
primaryip primaryip	IP address of the primary NFS server.
secondaryip secondaryip	IP address of the secondary NFS server.
primarydir primarydir	Primary Server mount directory
secondarydir secondarydir	Secondary Server mount directory

#### nfs Command Example

The following command displays the current NFS settings:

```
admin > Config > NFS > nfs
```

```
NFS Settings :
```

```
    Enable : 0
```

```
    Primary IP : 0.0.0.0
```

```
    Primary Directory: /export/domSX/
```

```
    Secondary IP : 0.0.0.0
```

```
    Secondary Directory: /export/domSXLog/
```

Use the following command to enable remote NFS logging and configure the NFS Server:

```
admin > Config > NFS > nfs enable true primaryip  
72.236.162.172 secondaryip 72.236.161.173 primarydir  
/nfs/domlogging1 secondarydir /nfs/domlogging2
```

## Configuring Ports

### Ports Configuration Menu

Target serial ports are configured from the CLI using the ports menu. In addition to the description of the physical nature of the ports, other services may also be defined, including:

- The escape sequence used to disconnect from the port to access the emulator to send breaks or control multi user functions such as Ctrl + a.
- The exit string sent to the target when an idle timeout occurs. By sending the exit string, the port is disconnected from the SX and the next user logging in to the port will have to log in to the target as well. (Cisco router example: logout)
- The addresses used for direct port addressing. Direct port addressing can use an individual IP address per port or a unique TCP Port address per port. Direct Port Addressing is supported by both Telnet and SSH. See **Direct Port Access** (on page 65) for details.

### Ports Config Command

Syntax

```
config [port <number|range|*>] [name string] [bps
value] [parity <none|even|odd>] [flowcontrol
<none|hw|sw>] [detect <true|false>] [escapemode
<none|control>] [escapechar char] [emulation type]
[sendbreak <duration>] [exitstring <cmd[#delay;]>]
[dpaip ipaddress] [telnet port] [ssh port]
[alwaysactive <true|false>] [suppress
<none|all>][encoding type] [ multiwrite <true|false>]
[chardelay delay] [linedelay delay]
```

ports config Command	Description
port <number range *>	Single port or range of ports (1-n or 1,3,4 or * for all ports)
name string	Port Name
bps value	Port speed (bitrate) in bits-per-second (1200 1800 2400 4800 9600 19200 38400 57600 115200)
parity <none even odd>	Port parity type
flowcontrol <none hw sw>	Port flowcontrol type hw = hardware flow control

ports config Command	Description
	sw =X on/X off)
detect <true false>	Enable/Disable detection of port connection
escapemode <none control>	Use Ctrl-key (escapemode=control) or single key (escapemode=none) as escape sequence; for example, Ctrl-] => escapemode=control, escapechar=]
escapechar char	Escape character
emulation type	Target Emulation type: VT100 VT220 VT320 ANSI
sendbreak duration	Duration of the sendbreak signal. (100 200 300 400 500 600 700 800 900 1000)
exitstring <cmd[#delay;]>	Execute exit string when port session closes, for example, config port 1 exitstring logout (execute logout on exit) config port 1 exitstring #0 (disable exit string for the port)
dpaip ipaddress	IP Address assigned for direct port access
telnet port	TCP Port assigned for direct port access via Telnet
ssh port	TCP Port assigned for direct port access via ssh
alwaysactive	Determine whether data coming into a port is logged, for example, config port 1 alwaysactive true (always log activities coming into a port even if no user is connected) config port 1 alwaysactive false (ignore data coming into a port when no user is connected)
suppress	Determine whether none or all messages should be displayed during a DPA connection, such as "Authentication successful"
encoding	Target Encoding type (DEFAULT US-ASCII ISO-8859-1 ISO-8859-15 UTF-8 Shift-JIS EUC-JP EUC-CN EUC-KR)
multiwrite	Port set in Multiple Writer Mode.
chardelay delay	Delay inserted between writing characters (0-9999ms)
linedelay delay	Delay inserted between writing lines (0-9999ms)

**ports config Command Example**

```
admin > ports >config port 1 name ld1 bps 115200
parity odd flowcontrol hw detect true escapemode none
emulation VT100
```

The following command displays the current settings for port 1:

```
admin > Config > Port > config port 1
```

Port number 1:

```
Name: Port1
BPS: 9600
Parity: 0
Flow control: 0
RSC Terminal Emulation: VT100
Disconnect: Disabled
Application: RaritanConsole
Exit String:
Escape: Control-]
DPA:
    IP: 0.0.0.0
    Telnet Port: 0
    SSH Port: 0
Always Active: False
Messages suppressed: none
```

The following example configures DPA port settings when the you choose DPA mode IP. The IP Address is assigned for direct port access using the following command:

```
admin > Config > Port > config port 1 dpaip 10.0.13.1
```

```
admin > Config > Services > dpa mode IP (upper case for IP!)
```

After this option is enabled, the SX unit is restarted. DPA changes will not be available until after the SX is rebooted.

```
ssh -l sx_user 10.0.13.1
```

Password:

```
Authentication successful.
```

```
Port 1: Configuration Saved.
```

After entering the password, you have direct access to port 1, using the newly assigned IP specifically for port 1.

The following example configures DPA port settings for a group of ports (make sure a free range of IPs are available for dpa IP mode usage):

```
admin > Config > Port > config port 1-32 dpaip  
10.0.13.200
```

or

```
admin > Config > Port > config port * dpaip  
10.0.13.200
```

In both cases above, port 1 will have an IP assigned as 10.0.13.200, while port 2 will have 10.0.13.201, port 3 10.0.13.203, and so on.

The following example configures DPA port settings when you choose DPA mode TCPPort. You must set the SSH or Telnet port value assigned for direct port access:

```
admin > Config > Port > config port 1 ssh 7000 telnet  
8000
```

```
admin > Config > Services > dpa mode TCPPort
```

After this option is enabled, the SX is restarted. DPA changes will not be available until after the SX is rebooted.

```
try ssh -l sx_user -p 7000 10.0.13.13 or telnet -l  
sx_user 10.0.13.13 8000
```

```
Password:
```

```
Authentication successful.
```

```
Port 1: Configuration Saved.
```

After entering the password, you have direct access to port 1, using the newly assigned TCPPorts(either ssh or telnet), specifically for port 1.

The following example configures DPA port settings for a group of ports (make sure no TCPPorts have been assigned, and a free range of TCPPorts are available for dpa TCPPort mode usage):

```
admin > Config > Port > config port 1-32 ssh 7000  
telnet 8000
```

or

```
admin > Config > Port > config port * ssh 7000 telnet
8000
```

In both cases above, port 1 will have ssh port 7000 and telnet port 8000 assigned for direct port access, port 2 will have ssh port 7001 and telnet port 8001, and so on.

Other DPA TCPPort options:

```
config <port *> <ssh tcpport>
config <port portnumber> <ssh tcpport>
config <port port_range> <ssh tcpport>
config <port *> <telnet tcpport>
config <port portnumber> <telnet tcpport>
config <port port_range> <telnet base_tcpport>
```

To configure all ports using a block of contiguous port numbers, use the <port \*> command. If port\_range is specified, a block of contiguous port numbers are used. The given value of base\_tcpport is used as starting value. For individual port configuration, the <port portnumber> command can be used.

---

*Note: Large char and line delays on a port (2 seconds +) should only be used in interactive sessions. If a large file is cut/pasted into the terminal when a large delay is present, it is possible for some of the data to get dropped instead of written to the port.*

---

### Ports Keywordadd Command

Keywords can be configured per port. After a keyword is configured for a port, if the event is selected for notification, an SMTP notification is sent upon detecting this keyword in the data coming from the target connected to the port.

Syntax

```
keywordadd [port <number|range|*>] [keyword value]
```

keywordadd Command Example

```
admin > configuration > ports > keywordadd port 1
keyword ll
```

---

### Ports Keyworddelete Command

The keyworddelete command removes an existing keyword.

Syntax

```
keyworddelete [keyword value]
```

keyworddelete Command Example

```
admin > configuration > ports > keyworddelete keyword  
11
```

---

## Configuring Services

These commands provide the ability to configure the SX server services:

- DPA
- Encryption
- HTTP
- HTTPS
- Logout
- LPA
- SSH
- Telnet
- fixedtcpwindow

---

### dpa Command

The permitted TCP Port Range is 1024-64510. When run without the mode parameter, the system displays the current dpa type.

The general syntax of the dpa command is:

```
dpa [mode <Normal|IP|TCPPort>]
```

The syntax for accessing a port directly using tcp port# is:

```
ssh -l sx_user -p tcp_port_N sx_ip_addr
sx_user@sx_ip_addr's password: <prompted by ssh>
```

```
telnet -l sx_user sx_ip_addr tcp_port_N
Password: <prompted by telnet>
```

The syntax for accessing a port directly using the ip address assigned per port is:

```
ssh -l sx_user dpa_ip_addr
sx_user@dpa_ip_addr's password: <prompted by ssh>
```

```
telnet -l sx_user dpa_ip_addr
Password: <prompted by telnet>
```

The dpa command options are described in the following table.

dpa Command	Description
mode <Normal IP TCPPort>	Per-port Direct Port Access type mode Normal - a default value that means DPA access cannot be established IP - access target port directly by unique IP Address via ssh/telnet/http/https TCPPort - access target port directly by unique TCP port via ssh/telnet

---

*Note: There is currently no way to set the unit back to the default DPA IP of 0.0.0.0.*

---

#### dpa Command Example

The following example chooses the DPA IP mode IP:

```
admin > Config > Services > dpa mode IP
```

---

*Note: When any changes are made over DPA mode and ports DPA configuration, the SX needs to be rebooted to apply new settings. DPA changes will not be available until after the SX is rebooted.*

---

After a successful DPA connection, try the following:

```
ssh -l sx_user 10.0.13.1
```

```
Password:
```

```
Authentication successful.
```

```
Starting DPA for port 1
```

```
Authentication successful.
```

```
Escape Sequence is: Control-]
```

You can now go directly to port 1 using the newly assigned IP.

To disable DPA (set by default, this option could be used after you have explicitly enabled DPA before):

```
admin > Config > Services > dpa mode Normal
```

Enabling unauthorizedportaccess to a set of ports assigned to 'Anonymous' group.

Unauthorized port access is available only for configured DPA methods. Use the following command:

```
admin > Security > LoginSettings >
unauthorizedportaccess enable true
```

When unauthorizedportaccess is enabled, it automatically enables Anonymous group and the user is able to configure it according to his requirement:

```
admin > Security > LoginSettings >
unauthorizedportaccess
```

```
Unauthorized Port Access Settings:
```

```
Enable: 1
```

```
Group Settings:
```

```
Name: Anonymous
```

```
Class: Operator
```

```
Ports:
```

To configure Anonymous group settings choose `config > user` and execute the following command:

```
admin > Config > User > editgroup name Anonymous
class op ports 1,2,3,4,5
```

```
Editing group...
```

```
Group Anonymous: Configuration Saved
```

The 'Anonymous' group is successfully configured.

DPA Anonymous access

The DPA is already configured (see the DPA configuration settings section).

DPA Mode is IP, IP 10.0.13.240 is assigned to port 1.

When accessing the serial port with Anonymous port access, user name should be "anonymous" and empty password <blank> as shown below. Anonymous access is granted if both username and password fields are empty (<blank>).

---

*Note: If "anonymous" with a lower case a is entered, the application will allow access without prompting for a password.*

---

```
ssh -l anonymous 10.0.13.240
```

```
Password:
```

```
Authentication successful.
```

```
Starting DPA for port 1
```

```
Authentication successful.
```

```
Escape Sequence is: Control-]
```

If suppress option is "all", no authentication credentials are shown and you jump directly to the target prompt.

```
configuration > ports > config port 1 suppress all
```

```
ssh -l anonymous 10.0.13.240
```

If option suppress is "none", authentication credentials are shown (username: password:).

```
configuration > ports > config port 1 suppress none
```

```
ssh -l anonymous 10.0.13.240
```

```
Password:
```

```
Authentication successful.
```

```
Starting DPA for port 1
```

```
Authentication successful.
```

```
Escape Sequence is: Control-]
```

You are now master for the port.

---

### Encryption Command

The encryption command sets the type of encryption for HTTPS.

---

*Note: The factory default value of this protocol is SSL.*

---

Syntax

```
encryption [prot <TLS|SSL>]
```

encryption Command	Description
prot <TLS SSL>	Select TLS or SSL encryption

encryption Command Example

The following example sets SSL encryption for HTTPS:

```
admin > Config > Services > encryption prot SSL
```

---

### HTTP Command

The http command is used to control http access and redirection and to define the port.

Syntax

```
http [enable <true|false>] [port value] [redirect <true|false>]
```

http Command	Description
enable <true false>	Enable/Disable HTTP access
port value	HTTP server default listen port (tcp)
redirect <true false>	Enable/Disable redirection from HTTP to HTTPS

#### http Command Example

The example below enables http access and redirection to https and sets the default port to 2.

```
admin > Config > Services > http enable true port 2
redirect true
```

---

#### HTTPS Command

The https command is used to control https access and define the port.

##### Syntax

```
https [enable <true|false>] [port value]
```

https Command	Description
enable <true false>	Enable/Disable HTTP access
port value	HTTP server default listen port (tcp)

#### https Command Example

```
admin > Config > Services > https
```

##### Https Settings:

```
Enabled : true
```

```
Port : 443
```

---

#### Logout Command

The logout command is used to log out of the current CLI session.

You can log out at any command level.

---

### LPA Command

The lpa command is used to display and set local port access configuration. SX units have one or two local ports, depending on the model. See **Appendix A** (see "**SX Serial RJ-45 Pinouts**" on page 258) for pinouts on DB9-M and RJ45-F ports.

Syntax

```
lpa [enable <true|false>] [bps value]
```

lpa Command	Description
none	The lpa command with no parameters specified displays the current LPA configuration.
enable <true false>	enable Enable/Disable Local Port access
[bps value]	Local Port speed (bit rate) in bit/s. Possible values are: (9600 19200 38400 57600 115200)

lpa Command Example

The following command enables local port access and sets the baud rate.

```
admin > Config > Services > lpa enable true 115200
```

---

### SSH Command

Syntax

```
ssh [enable <true|false>] [port value]
```

ssh Command	Description
enable <true false>	Enable or disable SSH access.
port value	SSH server tcp listen port

ssh Command Example

```
admin > Config > Services > ssh enable true port 4
```

The system displays this message after entering the preceding command.

The system must be rebooted for changes to take effect.

---

*Note: Customers experiencing slow SSH connectivity in SX 3.1.5 or SX 3.1.6 after upgrading to SX 3.1.7 should invoke the `ssh enable true` command to avoid this issue in the future.*

---

---

## Telnet Command

Syntax

```
telnet [enable <true|false>] [port value]
```

telnet Command	Description
enable <true false>	Enable or disable Telnet access.
port value	Telnet server tcp listen port

telnet Command Example

The command below enables telnet access on port 23.

```
admin > Config > Services > telnet enable true port
23
```

---

## fixedtcpwindow Command

The fixed TCP Window is enabled by default. The Fixed TCP window command is used to disable automatic TCP window scaling. This is necessary for some Windows Vista® clients to be able to properly connect to the SX. If you notice connection issues to the SX, you may need to disable this.

Syntax

```
fixedtcpwindow [enable <true|false>]
```

```
enable <true|false>    enable fixed tcp windows, or
disable(allow TCP
```

```
window scaling)
```

fixedtcpwindow Command Example

```
admin > Config > Services > fixedtcpwindow enable true
```

---

## Configuring SNMP

The SX server supports sending SNMP alerts to a predefined SNMP server. The Raritan SNMP MIB is found in the FAQs in the support section of the Raritan web site. The following commands configure the SNMP features:

- add
- delete
- snmp

---

### SNMP Add Command

The add command adds trap recipients. A recipient is an IP address with an optional space-separated port number. Traps may be sent to multiple ports with the same IP address.

Syntax

```
add [dest ipaddress] [port value]
```

add Command	Description
dest ipaddress	SNMP destination IP address
port value	SNMP destination port

SNMP add Command Example

```
admin > Config > SNMP > add dest 72.236.162.33 port 78
```

---

### SNMP Delete Command

The SNMP delete command deletes trap recipients. A recipient is an IP address with an optional space-separated port number. When removing a recipient with a port number, include the port number in the delete command. Traps may be sent to multiple ports with the same IP address.

Syntax

```
delete [dest ipaddress]
```

delete Command	Description
dest ipaddress	SNMP destination ip address to be deleted

SNMP delete Command Example

```
admin > Config > SNMP > delete dest 72.236.162.33
```

---

### SNMP Command

The SNMP command controls SNMP traps and specifies the community name used to send traps.

Syntax

```
snmp [enable <true|false>] [public community-string]
```

snmp Command	Description
enable <true false>	Enable/Disable SNMP

public community-string	Community string
-------------------------	------------------

snmp Command Example

```
admin > Config > SNMP > snmp enable true public
XyZZy1
```

---

## Configuring Time

Time-related configuration mode commands:

- clock
- ntp
- timezonelist

---

### Clock Command

The clock command allows you to set the time and date for the server.

Syntax

```
clock [tz timezone] [datetime datetime-string]
```

clock Command	Description
tz timezone	The timezone index is a number corresponding to the desired time zone.
datetime datetime-string	The date and time string for the console server unit. Enter in the following format: "YYYY-MM-DD HH:MM:SS"
timezonelist	Using this option displays a list of time zones and index values. Use the index values with the [tz] option.

clock Command Example

The following command sets the SX date and time to 12-Jul-06, 09:22:33 AM, in time zone 21.

```
admin > Config > Time > clock tz 21 datetime "2006-07-12 09:22:33"
```

---

### NTP Command

The ntp command lets you determine if a Network Time Protocol (NTP) server should be used to synchronize the SX clock to a reference.

Syntax

```
ntp [enable <true | false>] [primip primip] [secip secip]
```

ntp Command	Description
enable	Enable or disable the use of NTP.
primip primip	The primary NTP server to use first.
secip secip	The NTP server to use if the primary is not available.

ntp Command Example

The following command enables NTP.

```
admin > Config > Time > ntp enable true primip
132.163.4.101
```

---

### Timezonelist Command

The timezonelist command returns a list of timezones and associated index values. The index values are then used as part of the clock command.

Syntax

```
timezonelist
```

---

## Configuring Users

The following commands allow you to manage users:

- addgroup
- adduser
- deletegroup
- deleteuser
- editgroup
- edituser
- groups
- users

---

### Addgroup Command

The addgroup command creates a group with common permissions.

Syntax

```
addgroup [name groupname] [class <op|ob>] [ports
<number|range|*>] [power <number|range|*>] [sharing
<true|false>]
```

<b>addgroup Command</b>	<b>Description</b>
name groupname	Group name
class <op ob>	Group user class <op>erator or <ob>server
ports <number range *>	Port(s) assigned to the group. Single port or range of ports (1-n or 1,3,4 or * for all ports)
power <number range *>	Power strip assigned to the group. Single power strip or range of power strips.
sharing <true false>	Indicate whether users in the group are allowed to access a port that already has users connected to it if the port access mode is set to Share.

#### addgroup Command Example

```
admin > Config > User > addgroup name unixgroup class
op ports 1,2,3 power 1,2,3
```

---

#### Adduser Command

The adduser command is used to manage information about a specified user.

#### Syntax

```
adduser [user loginname] [fullname user's-fullname]
[group name] [dialback phonenumber] [password
password] [info user-information] [active
<true|false>]
```

<b>adduser Command</b>	<b>Description</b>
user loginname	Login Name (Required)
fullname user's-fullname	User's full name (required)
group name	Group to associate with user (required)
dialback phonenumber	Dialback phone number for this user (optional)
password password	User's password (required)
info user-information	Miscellaneous user information
active <true false>	Activate/Deactivate user account

#### adduser Command Example

The following command shows how to add a user:

```
admin > Config > User > adduser user jjones fullname
John-Jones group unix dialback 12146908003 password
123abc info AP-Systems active true
```

---

**Deletegroup Command**

The deletegroup command deletes an existing group.

Syntax

```
deletegroup [name groupname]
```

<b>deletegroup Command</b>	<b>Description</b>
name groupname	Group name

deletegroup Command Example

```
admin > Config > User > deletegroup name unixgroup
```

---

**Deleteuser Command**

The deleteuser command is used to remove a specified user.

Syntax

```
adduser [user loginname]
```

<b>deleteuser Command</b>	<b>Description</b>
user loginname	Login Name (Required)

deleteuser Command Example

```
admin > Config > User > deleteuser user jjones
```

---

**Editgroup Command**

The editgroup command edits an existing group.

Syntax

```
editgroup [name groupname] [class <op|ob>] [ports <number|range|*>] [power <number|range|*>] [sharing <true|false>]
```

<b>editgroup Command</b>	<b>Description</b>
name groupname	Group name
class <op ob>	Group user class <op>erator or <ob>server
ports <number range *>	Port(s) assigned to the group. Single port or range of ports (1-n or 1,3,4 or * for all ports)
power <number range *>	Single power strip or range of power strips

editgroup Command	Description
	assigned to the group.
sharing <true false>	Indicate whether port access is shared while the port is being utilized.

**editgroup Command Example**

```
admin > Config > User > editgroup name unixgroup
class op ports 1,4 power 1,4
```

**Edituser Command**

The edituser command is used to manage information about a specified user.

**Syntax**

```
edituser [user loginname] [fullname user's-fullname]
[group name] [dialback phonenumber] [password
password] [info user-information] [active
<true|false>]
```

edituser Command	Description
user loginname	Login Name (Required)
fullname user's-fullname	User's full name
group name	Group to associate with user
dialback phonenumber	Dialback phone number for this user
password password	User's password
info user-information	Miscellaneous user information
active <true false>	Activate/Deactivate user account

**edituser Command Example**

The following command shows how to change a user's password:

```
admin > Config > User > edituser user admin password
newp/w
```

**Groups Command**

The groups command shows the details of existing groups.

**Syntax**

```
groups
```

**groups Command Example**

```
admin > Config > User > groups
```

---

### Users Command

The users command shows the details of existing users.

Syntax

```
users
```

users Command Example

```
admin > Config > User > users
```

---

### Connect Commands

The connect commands allow you to access ports and their histories.

Command	Description
connect	Connect to a port. The port sub-menu, reached using escape key sequence.
clearhistory	Clear history buffer for this port.
close, quit, q	Close this target connection.
gethistory	Display the history buffer for this port.
getwrite	Get write access for the port.
return	Return to the target session.
sendbreak	Send a break to the connected target.
writelock	Lock write access to this port.
writeunlock	Unlock write access to this port.
powerstatus	Query Power status of this port.
powertoggle	Toggle Power On/Off of this port.
uptime	Prints the current system uptime information.

---

### Configuring Power

The following power commands allow you to manage power strips attached to the SX.

Command	Description
associate	Associate a Power Strip outlet to a SX Port.
association	View Currently configured associations.
cycle	Power cycle specified ID. <hr/> <i>Note: If you are connecting a PX to the SX, it is recommended you set the power cycle time to 5 seconds.</i> <hr/>
off	Power off specified ID.
on	Power on specified ID.
outlet	Edit outlet information.
powerdelay	Configure global Power Strip delays.
powergroup	Switch to Power Group Menu.
powerstatus	Get Power Strip status.
powerstrip	Edit Power Strip information.
setpowerport	Configure an SX Port to contain a power strip.
unassociate	Remove a power outlet association from an SX Port.
unsetpowerport	Configure an SX Port to remove a power strip.

See **CLI Command for Power Control** (on page 235) for details about power command scenarios.

---

## Diagnostic Commands

The diagnostic commands allow you to gather information for troubleshooting.

Command	Description
ifconfig	Show detailed network configuration
netstat	Print network connections
ping	Ping a remote system
ps	Report system process status
traceroute	Trace the network route to a host [-dnrv] [-m maxttl] [-p port#] [-q nqueries] [-s srcaddr] [-t tos] [-w wait] host [data size]
uptime	Print the current system uptime information

## IPMI Commands

IPMIDiscover and IPMITool commands allow you to work with IPMI-supported devices.

### IPMIDISCOVER

The ipmidiscover tool is user to discover Intelligent Platform Management Interface (IPMI) servers in the network.

- The IP address range can be set using startIP and endIP.
- Only users belonging to the Administrator group are able to configure the support of IPMI. The supported IPMI version 2.0.

Syntax

```
ipmidiscover [OPTIONS] startIP endIP
```

All discovered targets supporting IPMI version 2.0 is listed, allowing the user to select one and execute the IPMI operations.

ipmidiscover Command	Description
[OPTIONS]	Two options are supported: -t timeout [seconds] to complete the discovery -i interval [seconds] between each ping
startIP	Beginning IP address
endIP	Ending IP address

ipmidiscover Command Example

```
admin> IPMI > ipmidiscover -t 20 10.0.22.1 10.0.22.10
```

Discovering IPMI Devices :

```
IPMI IP: 10.0.22.2
```

```
IPMI IP: 10.0.22.7
```

It is possible for the IP address range to span different subnets.

## IPMITOOL

This command lets you manage the IPMI functions of a remote system, including printing FRU information, LAN configuration, sensor readings, and remote chassis power control. The ipmitool command controls IPMI-enabled devices. The user name to access the IPMI device is ADMIN, password ADMIN.

### Syntax

```
ipmitool [-c|-h|-v|-V] -I lanplus -H <hostname> [-p <port>] [-U <username>] [-L <privlvl>] [-a|-E|-P|-f <password>] [-o <oemtype>] [-C <ciphersuite>]
```

ipmitool Command	Description
-c	Present output in CSV (comma separated variable) format. This is not available with all commands.
-h	Get basic usage help from the command line.
-v	Increase verbose output level. This option may be specified multiple times to increase the level of debug output. If given three times you will get hexdumps of all incoming and outgoing packets.
-V	Display version information.
-I <interface>	Selects IPMI interface to use. Supported interfaces that are compiled in are visible in the usage help output.
-H <address>	Remote server address, can be IP address or hostname. This option is required for lan and lanplus interfaces.
[-p <port>]	Remote server UDP port to connect to. Default is 623.
[-U <username>]	Remote server username, default is NULL user.
[-L <privlvl>]	Force session privilege level. Can be CALLBACK, USER, OPERATOR, ADMIN. Default is ADMIN.
[-a -E -P -f <password>]	-a Prompt for the remote server password. -E The remote server password is specified by the environment variable IPMI_PASSWORD. -P <password> Remote server password is specified on the command line. If supported it is obscured in the process list. -f <password_file> Specifies a file containing the remote server password. If this option is absent, or if password_file is empty, the password will default to NULL.

ipmitool Command	Description
[-o <oemtype>]	Select OEM type to support. This usually involves minor hacks in place in the code to work around quirks in various BMCs from various manufacturers. Use -o list to see a list of current supported OEM types.
[-C <ciphersuite>]	The remote server authentication, integrity, and encryption algorithms to use for IPMIv2 lanplus connections. See table 22-19 in the IPMIv2 specification. The default is 3 which specifies RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity, and AES-CBC-128 encryption algorithms.
<command>	<p>raw - Send a RAW IPMI request and print response</p> <p>i2c - Send an I2C Master Write-Read command and print response</p> <p>lan - Configure LAN Channels</p> <p>chassis - Get chassis status and set power state</p> <p>power - Shortcut to chassis power commands</p> <p>event - Send pre-defined events to MC</p> <p>mc - Management Controller status and global enables</p> <p>sdr - Print Sensor Data Repository entries and readings</p> <p>sensor - Print detailed sensor information</p> <p>fru - Print built-in FRU and scan SDR for FRU locators</p> <p>sel - Print System Event Log (SEL)</p> <p>pef - Configure Platform Event Filtering (PEF)</p> <p>sol - Configure and connect IPMIv2.0 Serial-over-LAN</p> <p>tsol - Configure and connect with Tyan IPMIv1.5 Serial-over-LAN</p> <p>isol - Configure IPMIv1.5 Serial-over-LAN</p> <p>user - Configure Management Controller users</p> <p>channel - Configure Management Controller channels</p> <p>session - Print session information</p>

ipmitool Command	Description
	firewall - Configure firmware firewall (IPMIv2.0)
	sunoem - OEM Commands for Sun servers
	picmg - Run a PICMG/ATCA extended cmd
	fwum - Update IPMC using Kontron OEM Firmware Update Manager
	shell - Launch interactive IPMI shell
	exec - Run list of commands from file
	set - Set runtime variable for shell and exec

#### ipmitool Command Example

The following command allows the user to get the chassis status and set the power state.

```
admin> IPMI > ipmitool -I lan -H 10.0.22.7 -U ADMIN
chassis status
```

Password:

```
System Power           : on
Power Overload         : false
Power Interlock        : inactive
Main Power Fault       : false
Power Control Fault    : false
Power Restore Policy   : always-off
Last Power Event       : command
Chassis Intrusion      : active
Front-Panel Lockout    : inactive
Drive Fault            : false
Cooling/Fan Fault      : false
```

See <http://ipmitool.sourceforge.net/manpage.html> for additional information.

---

#### Listports Command

Command	Description										
listports	List accessible ports. admin > listports  <table border="1"> <thead> <tr> <th>Port no.</th> <th>Port name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Port1 [U]</td> </tr> <tr> <td>2</td> <td>Port2 [U]</td> </tr> <tr> <td>3</td> <td>Port3 [U]</td> </tr> <tr> <td>4</td> <td>Port4 [U]</td> </tr> </tbody> </table>	Port no.	Port name	1	Port1 [U]	2	Port2 [U]	3	Port3 [U]	4	Port4 [U]
Port no.	Port name										
1	Port1 [U]										
2	Port2 [U]										
3	Port3 [U]										
4	Port4 [U]										
column	Can be 1,2,3. Indicates the number of columns to display the port list in.										

Port names up to 23 characters are displayed when two columns are needed to display the available ports. When three columns are needed to list the ports, the port names are limited to 13 characters in order to ensure the entire port list fits on a standard 80x25 screen.

Longer port names are truncated to 22 characters, with a \$ sign at the end. The letter after the port name describes the state of each port. This includes:

- D, B - Down, Busy
- U, B - Up, Busy
- D - Down
- U - Up

---

## Maintenance Commands

The maintenance commands allow you to perform maintenance-related tasks on the SX firmware:

- backup
- cleareventlog
- factoryreset
- firmware
- logoff
- reboot
- restore
- sendeventlog
- upgrade
- upgradehistory
- upgradestatus
- userlist
- vieweventlog

---

*Note: All operations that normally trigger a reboot or prompt the user for feedbacks are now added a new parameter named force. This force parameter prevents reboot, prompting or both from taking place until all configurations are completed. The commands that now have a force parameter are: ethernetfailover (see "Ethernetfailover Command" on page 171), interface (see "Interface Command" on page 171), name (see "Name Command" on page 173), ports (see "Ports Command" on page 173), factoryreset (see "Factoryreset Command" on page 204) and reboot (see "Reboot Command" on page 206).*

---

### Backup Command

The backup command makes a copy of the SX configuration and writes the backup onto an ftp server. The current SX configuration is saved to the computer with the IP set in the command parameters in an encrypted format. All device settings except network settings are stored in the file, wh can be recovered if a Restore operation becomes necessary.

Syntax

```
backup [ip ipaddress] [login login] [password
password] [path pathname] [file filename]
```

backup Command	Description
[ip ipaddress]	IP address of the target system where the

	backup is written.
<login login>	Username of the account on the system where the backup is stored.
<password password>	Password of the account on the system where the backup is stored.
[path pathname]	Specifies the path to the backup file.
[file filename]	Specifies the name of the file in which the backup is saved.

#### backup Command Example

In this example, the console server data is sent to a system at the IP address 192.168.51.220. The guest account and password are used. The data is saved at the top level of the guest account as a file named backupfile.

```
admin > system > backup ip 10.0.0.188 login sx
password qazlwsx path /home/backup file bac
```

---

#### Clear eventlog Command

The clear eventlog command clears the contents of the local event log.

##### Syntax

```
Clear eventlog
```

##### clear eventlog Command Example

```
admin > Config > Log > clear eventlog
```

---

#### Factoryreset Command

The factoryreset command returns the SX console server to its default factory settings.

---

**Important: If you choose to revert to the factory settings, you will erase all your custom settings and will lose your connection to the SX because, upon rebooting, the IP address of the unit is reset to the factory default IP address of 192.168.0.192. If the network is running a DHCP server, the unit is reset to a different IP address, because DHCP is enabled by default when the unit is reverted to factory settings.**

---

**Syntax**

```
factoryreset
```

**factoryreset Command Example**

```
admin > Maintenance > factoryreset
```

**Network Settings:**

```
Name: DominionSX
Domain : raritan.com
CSC Port: 5000
Discover Port: 5000
DHCP Client: true
IP: 192.168.0.192
Net Mask : 255.255.255.0
Gateway : 192.168.0.192
Failover : true
```

```
Do you wish to commit these settings (no/yes)
(default: no)
```

---

**Firmware Command**

The firmware command provides the versions of the firmware.

**Syntax**

```
firmware
```

**firmware Command Example**

```
admin > Maintenance > firmware
```

**Version Information :**

```
Firmware Version : 3.0.0.1.15
Kernel Version : 2.4.12
PMON Version: 2.0.1
RSC Version: 1.0.0.1.16
```

---

**Logoff Command**

Command	Description
logoff	Force logoff (terminate) a user or port session.

---

### Reboot Command

The reboot command restarts the SX console server. This command is only available to users with administrative privileges. All user sessions are terminated without warning, and no confirmation is required. It is highly recommended that you ask all users to log off before you reboot the unit. The userlist command can be used to display a list of connected users and sessions.

**Syntax**

```
reboot
```

**reboot Command Example**

```
admin > Maintenance > reboot
```

The system responds with the following messages:

```
Rebooting the system will log off all users.
```

```
Do you want to proceed with the reboot? (no/yes)
(default: no) yes
```

---

### Restore Command

The restore command retrieves a copy of the SX system from a system and writes the file to the SX server.

**Syntax**

```
restore [ip ipaddress] [login login] [password
password] [path pathname] [file filename]
```

restore Command	Description
[ip ipaddress]	IP address of the target system from which the restore data is retrieved
<login login>	Username of the account on the system where the restore data is stored
<password password>	Password for the above account
[path pathname]	Specifies the path to the backup file to be restored to a similar system with the same port density
[file filename]	Specifies the name of the file in which the backup data was saved

**restore Command Example**

In this example, the console server data is being retrieved from a system at IP address 192.168.51.220. The guest account and password are used. The data is pulled from the top level of the guest account in a file named backupfile.

```
admin > system > restore ip 192.168.51.220 login
guest password guestpassword path /home/bac file
backupfile1
```

**Sendeventlog Command**

The sendeventlog command sends the local logfile to a remote FTP server.

**Syntax**

```
sendeventlog [ip ipaddress] [login login] [password
password] [path pathname] [file filename]
```

<b>sendeventlog Command</b>	<b>Description</b>
ip ipaddress	FTP server IP address
login login	FTP Server login name
password password	FTP Server password
path pathname	FTP server path. For example, /ftphome
file filename	Filename on FTP server to save log. For example, sxlogfile

**sendeventlog Command Example**

```
admin > Config > Log > sendeventlog ip 72.236.162.187
login acy password pasraritansword path sxlogfile
file log 32
```

---

## Upgrade Command

---

*Note: To perform an upgrade, there must be a configured remote ftp server.*

---

The upgrade command upgrades one version of the system to another version, for example v2.5 to v3.0.

During the upgrade, SX verifies there is enough space on the device to perform the upgrade. If there is not, the SX restarts and the upgrade does not take place. If the upgrade fails due to lack of space, clear the local logs on the device and try upgrading again. Contact Raritan Technical Support if you still cannot upgrade after clearing the local logs.

### Syntax

```
upgrade [ip ipaddress] [login login] [password password] [path pathname]
```

upgrade Command	Description
ip ipaddress	IP Address of FTP Server
login login	FTP Server login name
password password	FTP Server password
path pathname	FTP server path. For example, /ftphome/UpgradePack/Pack1of1

### upgrade Command Example

```
admin > Maintenance > upgrade ip 10.0.0.188 login sx
password qaz1wsx path
/var/ftp/UpgradePack_2.5.6_3.0.0.1.15/Pack1of1
```

---

## Upgradehistory Command

The upgradehistory command provides information about the last time you upgraded the system.

### Syntax

```
upgradehistory
```

### upgradehistory Command Example

```
admin > Maintenance > upgradehistory
```

Overall Upgrade History:

```
3.0.0.1.15          Wed Sep 13 19:07:38 2006
```

---

**Userlist Command**

The userlist command displays a list of all users who are logged in, their source IP Addresses and any ports to which they are connected.

Syntax

```
userlist
```

---

**Vieweventlog Command**

The vieweventlog command displays the local log file.

Syntax

```
Vieweventfile
```

vieweventlog Command Example

```
admin > Config > Log > vieweventlog
```

---

**Security Commands**

SX controls the ability to hack into the system by using random logins. These security command menus provide access to the commands needed to configure the SX security features:

- banner
- certificate
- firewall
- kerberos
- loginsettings
- securityprofiles

---

**Banner Command**

The banner command controls the display of a security banner immediately after login.

Syntax

```
banner [display <true|false>] [audit <true|false>]
```

banner Command	Description
display <true false>	Enable/Disable banner display
audit <true false>	Enable/Disable audit for the banner, when banner display is enabled

banner Command Example

```
admin > Security > banner > banner display true audit  
false
```

---

**Ftpgetbanner Command**

The ftpgetbanner command directs the SX to go to this site to retrieve the welcome banner. The welcome banner and the audit statement are maintained on an external FTP site.

Syntax

```
ftpgetbanner [ip ipaddress] [login login] [password  
password] [path pathname]
```

<b>ftpgetbanner Command</b>	<b>Description</b>
ip ipaddress	FTP server IP address
login login	FTP Server login name
password password	FTP Server password
path pathname	FTP server path for the banner file banner.txt. for example,/ftphome/banner.txt

ftpgetbanner Command Example

```
admin > Security > Banner> ftpgetbanner ip  
72.236.162.171 login raritan password acy path  
/ftphome/banner.txt
```

---

## Certificate Command Menu

The certificate command menu provides the client and server commands to create and manage security certificates.

---

*Note: If the SX is not used to generate the certificate signing request and an external certificate is used instead, encryption needs to be removed from the private key before installing it on the SX. If this is the case, to remove the encryption from the key, a command such as `openssl rsa -in server.key -out server2.key` and `server2.key` should be used. Encrypted private keys are used to prevent the web server from being started by unauthorized users. Since SX does not allow users to access the web server directly, encrypted private keys are not required and does not compromise security.*

*Note: When the SX is used to generate the certificate signing request, the private key is not required since SX keeps the private key exclusive.*

---

Syntax

`certificate <>`

---

*Note: For a description of how to enable LDAP over SSL with a third-party certification authority, see <http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>. The document requires the exchange of certificate of authority created by the MS Server.*

---

<b>certificate Command</b>	<b>Description</b>
add	Install a User Certificate
addcrl	Install a CA's CRL
clientcert	Activate Client Side Certificate Verification
delete	Remove Client CA Certificate
deletecrl	Remove Client CA's CRL
viewcacert	View Client CA Certificate
viewcrl	View Client CA CRL Certificate

Certificate Client Command Example

Enable SSL Client Certificates:

```
admin > Security > certificate > clientcert enable
true
```

Install Certificate Authority:

```
admin > Security > certificate > add ip 10.0.0.189
login root password passwordword path /home/cert/
SXCert file cacert.pem ca ca_test
```

Add Certificate Renovation List:

```
admin > Security > certificate > addcrl ip 10.0.0.189
login root password pass path /home/cert/SXCert file
demoCA.crl ca crl_test
```

Delete Certificate Renovation List:

```
admin > Security > certificate > deletecrl ca
crl_test
```

<b>certificate Command</b>	<b>Description</b>
activatedefaultcert	Activate Default System SSL Certificate
activateusercert	Activate User SSL Certificate
generatecsr	View Default System Cert
generatedefaultcert	Generate Default System SSL Certificate
installusercert	Install a User Certificate
installuserkey	Install a User Certificate Key
viewcsr	View The Certificate Signing Request
viewdefaultcert	View default system certificate

**Server Command Example****Install User Certificate:**

```
admin > Security > certificate > installusercert ip
10.0.0.189 login root password pass path /home/SXCert
file sx.pem
```

**Install User Key:**

```
admin > Security > certificate > installuserkey ip
10.0.0.189 login root password pass path /home/
SXCert file sx.pem
```

**Activate User Certificate:**

```
admin > Security > certificate > activateusercert
```

**Generate Certificate Signing Request:**

```
admin > Security > certificate > generatecsr bits
1024 name test_csr country BG state Ko locality Seoul
org Bnr unit SX email sx@bir.net
```

---

**Firewall Command**

The firewall command provides control for the turning on or off the firewall.

**Syntax**

```
firewall [enable <true|false>]
```

firewall Command	Description
enable <true false>	Enable/Disable firewall with true or false

**firewall Command Example**

```
admin > Security > Firewall > firewall enable true
```

---

*Note: Use the following when working with the Firewall.*

---

```
Chain FORWARD (policy ACCEPT)
```

```
target      prot opt source          destination
```

When you enable IP forwarding for Dual LAN units, use IPTables rules to create policies for traffic being forwarded between LAN interfaces.

### Iptables Command

The iptables command is an administration tool for IPv4 packet filtering and Network Address Translation (NAT). The iptables command provides an interface to the linux iptables. The command parameters and options are the same as the linux system command.

iptables Command	Description
-A input	Append one or more rules to specified chain.
--dport	Destination port.
--flush	Clear the iptables.
-j target	Jump based on the following target keywords: ACCEPT - Packet is passed through (i.e. for INPUT chain, processed by local stack, for OUTPUT, sent) DROP -Packet is dropped and no further processing is performed LOG - QUEUE - Passes datagram to user space (if supported by kernel) RETURN - Terminates processing by this chain and resumes the calling chain (or executes the chain policy if there is no calling chain)
-list	View the current iptables.
--log-prefix DOM_IPACL	
-m state	Load a match extension module.
-p	The protocol of the traffic.
-s	Source address.
-save	Save the IP Tables.
--state NEW <enter rule to trigger here>	
-t filter	

### iptables Command Examples

Iptables can be configured in a plethora of ways that is outside the scope of this document. The examples below show some simple configuration options created with iptables.

The following example enables a log for iptables:

```
admin > firewall > iptables -A INPUT -t filter -j LOG
--log-prefix DOM_IPACL -m state --state NEW -s <IP>
```

#### Adding a default local rule

The default local rule is included as part of the standard SX implementation.

#### Restricting Access from an IP Address

To restrict access to the SX from a specific IP address (192.168.1.100):

```
admin > Security > firewall > iptables -A INPUT -t
filter -j DROP
-s 192.168.1.100
```

#### Logging a message when IP Address connects

To send a syslog message when an IP Address connects to the SX:

```
admin > Security > firewall > iptables -A INPUT -t
filter -j LOG
--log-prefix DOM_IPACL -m state --state NEW -s
192.168.1.100
```

#### Allowing Access from an IP Range

To allow access to the SX from a specific IP range (192.168.0.1-192.168.0.255).

```
admin > Security > firewall > iptables -A INPUT -t
filter
-j ACCEPT -s 192.168.0.0/255.255.255.0
```

#### Disable all ICMP traffic

To disable ICMP protocol traffic, and have the SX not respond to pings.

```
admin > Security > firewall > iptables -A INPUT -p
icmp -j DROP
```

#### Prevent Access to the Telnet port from an IP Address

To disable access to the telnet port for a particular ip address

```
admin > Security > firewall > iptables -A INPUT -p
tcp --dport 23
-j DROP -s 192.168.0.100
```

#### View the current iptables

To view the current iptables rule:

```
admin > Security > firewall > iptables --list
```

or

```
admin > Security > firewall > iptables -xvnl
```

Clear the iptables rules

To clear the iptables rules.

```
admin > Security > firewall > iptables --flush
```

Save the configured settings

To save the iptables rules into the local database.

```
admin > Security > firewall > iptables-save
```

---

*Note: No spaces between iptables and save.*

---

Execute this command once you have configured all the settings.

---

### Kerberos Command

The Kerberos command menu offers access to the commands used to configure the Kerberos network authentication protocol:

Kerberos Command	Description
gethostnamefile	Get /etc/hosts in case of DNS failure file.
getkrbconfig	Get Kerberos 5 configuration file.
kadmin	Kerberos admin client.
kerberos	Kerberos-based Network Authentication.
kinit	get kerberos ticket.
klist	list kerberos ticket.

Kerberos and SX

The SX can use Kerberos authentication with the following steps and as a result, Kerberos-based network mutual authentication, and symmetric, also called private/secret, key cryptography can be achieved in the CLI and GUI of the SX for remote user authentication.

See the MIT Kerberos website for information about Kerberos, KDC, kadmin, client machine setup, and the FAQs related to these topics.

1. Set your krb5.conf stanzas and ftp it using getkrbconfig [configuration settings available in: <http://www.faqs.org/faqs/kerberos-faq/general/section-38.html>]
2. Get a ticket using kinit.

3. Use `kadmin` to add the keys to `/etc/krb5.keytab` for `HTTP/FQDN@REALM` and `host/FQDN@REALM`. These keys are consistent across boots.
4. Remote authentication and authorization can be set up along with Kerberos authentication. HTTP and telnet access will prompt you to enter username and password. Currently Kerberos does not automatically map to local or remote usernames.
5. Enable Kerberos.
6. After a reboot, the SX is ready for secure telnet and HTTP protocol remote access.

Diagnostic Tips:

- Use the `name` command in the network menu to set the FQDN for the SX.
- Disable HTTP redirect from the services menu.
- Synchronize the time of the client machine, SX, KDC and `kadmin` machines using time menu and `ntp` option.
- The above 3 machines should be pingable by FQDN. Get the hosts file using `gethostnamefile` from the Kerberos menu.
- Use `klist` to check the ticket expiration. Most of the `kadmin` error messages are associated with ticket expiration
- `Kadmin`: List principal and add missing principal if it doesn't already exist in the KDC database.
- Browser rule: Do not include the REALM part when the browser prompts for principal.
- Telnet access: Use `-x -l` and `-k` option appropriately. Telnet will initially print that authentication

Key and Definitions:

1. For KDC, `kadmin`, the application server, and client machine, see MIT Kerberos FAQ [<http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>]
2. FQDN: Fully Qualified Domain Name

---

*Note: Information about setting up KDC `kadmin` is not in the scope of this document. Use the references mentioned in this section for this information.*

---

Kerberos Command Example

1. `admin > Security > Kerberos > getkrbconfig ip 192.168.52.197 login vijay password vijayv path /home/vijay/krb5.conf`  
Success
2. `kadmin: addprinc host/dsx-182.domain.com@REALM`  
`kadmin: addprinc HTTP/dsx-182.raritan.com@RARITAN.COM`

---

### Loginsettings Commands

The loginsettings command menu offers commands used to configure the systemwide login settings:

Command	Description
idletimeout	Set systemwide idletimeout.
inactiveloginexpiry	Configure local login expiry time.
invalidloginretries	Configure local login max number of retries.
localauth	Configure local authentication.
lockoutperiod	Lockout period on invalid login attempt.
singleloginperuser	Restrict to a single login session per user.
strongpassword	Configure strong password rules.
unauthorizedportaccess	Unauthorized (Anonymous) port access.
portaccess	Configure port access shared by user group.
profiledata	Modify or view a security profile.

---

### Idletimeout Command

The idletimeout command sets or changes the amount of idle time allowed before the system disconnects the user.

Syntax

```
idletimeout [time value]
```

idletimeout Command Example

```
admin > Security > LoginSettings > idletimeout time
99
```

---

### Inactiveloginexpiry Command

The inactiveloginexpiry command sets the number of days before an account will expire due to inactivity.

Syntax

```
inactiveloginexpiry [days value]
```

inactiveloginexpiry Command	Description
days <value>	Number of days before

<b>inactiveloginexpiry Command</b>	<b>Description</b>
	account will expire for local users on inactivity

**Command Example**

```
admin > Security > LoginSettings >
inactiveloginexpiry days 5
```

**Invalidloginretries Command**

The `invalidloginretries` command specifies the number of failed invalid login attempts before the account is deactivated.

**Syntax**

```
invalidloginretries [number value]
```

<b>invalidloginretries Command</b>	<b>Description</b>
number value	Number of failed login retries allowed before account is deactivated

**invalidloginretries Command Example**

```
admin > Security > LoginSettings >
invalidloginretries number 5
```

**Localauth Command**

The `localauth` command is used to configure local authentication.

**Syntax**

```
localauth [enable <true|false>]
```

**localauth Command Example**

```
admin > Security > LoginSettings > localauth enable
false
```

**Lockoutperiod Command**

The `lockoutperiod` command defines the lockout period on invalid login attempts.

**Syntax**

```
lockoutperiod [time time]
```

<b>lockoutperiod Command</b>	<b>Description</b>
time time	Period of time (in minutes) for which the user cannot login after account deactivation.

lockoutperiod Command Example

```
admin > Security > LoginSettings > lockoutperiod time
120
```

---

**Singleloginperuser Command**

The singleloginperuser command enables or disables multiple logins per user.

Syntax

```
singleloginperuser [enable <true|false>]
```

singleloginperuser Command	Description
enable <true false>	Enable/Disable multiple login sessions per user.

singleloginperuser Command Example

```
admin > Security > LoginSettings > singleloginperuser
enable true
```

---

**Strongpassword Command**

The SX server supports both standard and strong passwords.

- Standard passwords have no rules associated with them; they can be in any format and will not expire
- Strong passwords increase the effectiveness of the password by setting rules around content, length, and expiration dates
- Strong passwords allow the administrator to pick the rules they want to implement from the following table

Passwords are case sensitive and can contain up to 64 alphanumeric characters with the exception of " ' < > \ &

Syntax

```
strongpassword [enable <true|false>] [minlength
value] [maxlength value] [expiry time] [history
value] [uppercase <true|false>] [lowercase
<true|false>] [numeric <true|false>] [other
<true|false>]
```

strongpassword Command	Description
enable <true false>	Enable/Disable strong password rules for local users.
minlength	Minimum password length.
maxlength	Maximum password length.

<b>strongpassword Command</b>	<b>Description</b>
expiry	Number of days before password will expire for local users.
history	Number of passwords to store in password history.
uppercase <true false>	If true, force uppercase characters in password.
lowercase <true false>	If true, force lowercase characters in password.
numeric <true false>	If true, force numeric characters in password.
other <true false>	If true, force other characters in password.

#### strongpassword Command Example

The following example sets the Strong Password rules in effect:

- Strong password is enabled.
- The minimum length of the password when you create user is 6 symbols.
- The maximum length of the password is 30.
- The password will expire in 30 days.
- Number of password changes to be kept in history is 3 times.
- There should be at least one and more uppercase/numeric/other symbols in the password.
- There could be 0 or more lowercase symbols in the password.

```
admin > Security > LoginSettings > strongpassword
enable true minlength 6 maxlength 30 expiry 30
history 3 uppercase true numeric true other true
```

---

#### Unauthorizedportaccess Command

Syntax

```
unauthorizedportaccess [enable <true|false>]
```

<b>unauthorizedportaccess Command</b>	<b>Description</b>
enable <true false>	Enable/Disable unauthorized access to a set of ports assigned to 'Anonymous' group

#### unauthorizedportaccess Command Example

```
admin > Security > LoginSettings >
unauthorizedportaccess enable false
```

---

### Portaccess Command

Syntax

```
portaccess <share|private>
```

portaccess Command	Description
portaccess <share private>	Indicate whether port access should be private or shared.

portaccess Command Example

```
admin > Security > LoginSettings > portaccess share
```

```
admin > Security > LoginSettings > portaccess private
```

---

### Securityprofiles Commands

The securityprofiles command menu provides access to the commands used to configure and control security profiles.

securityprofiles Command	Description
profiledata	View or modify a Security Profile.
securityprofiles	Enable and select a Security Profile.

---

### Profiledata Command

The profiledata command allows you to modify or view a security profile. SX provides the ability to define security profiles that simplify assigning permissions to users and groups. There are three types of profiles:

- Two are predefined and are standard and secure.
- The third allows definition of custom profiles to allow assignment of all permissions by assigning one security profile. Multiple custom security profiles may be defined.

Syntax

```
profiledata [name <Standard|Secure|Custom>] [telnet <true|false>] [strongpass <true|false>] [timeout <true|false>] [single <true|false>] [redirect <true|false>] [tls_required <true|false>]
```

profiledata Command	Description
[name <Standard Secure Custom>]	Specifies the type of security profile.
[telnet <true false>]	Enable/Disable telnet.
[strongpass <true false>]	Enable/Disable strong password.
[timeout <true false>]	Enable/Disable idle timeout.
[single <true false>]	Enable/Disable single login per user.
[redirect <true false>]	Enable/Disable redirection from HTTP to HTTPS.
[tls_required <true false>]	Enable/Disable forcing of Transport Layer Security (TLS) on HTTPS.

#### Profiledata Command Example

The following example defines the custom security profile with telnet disabled, strong passwords required, idle timeout enabled, multiple logins allowed, HTTP to HTTPS redirection disabled, and the forcing of Transport Layer Security (TLS) on HTTPS.

```
admin > Security > SecurityProfiles > profiledata
name Custom telnet false strongpass true timeout true
single false redirect false tls_required true
```

# Chapter 12 Intelligent Platform Management Interface

## In This Chapter

Discover IPMI Devices .....	224
IPMI Configuration .....	225

---

### Discover IPMI Devices

► **To discover IPMI servers on the network:**

1. Choose IPMI > Discover IPMI Devices. The Discover IPMI Devices page opens.



**Discover IPMI Devices**

**Options:**

**Start IP Address:**

**End IP Address:**

2. Leave the Options field blank or enter -t timeout [seconds].
3. Type starting and ending IP addresses in the corresponding fields. SX will discover all IPMI devices within this range of IP addresses.
4. Click the IPMI Discover button.

**Example**

The following is an example of the output when nothing has been entered in the Options field:

Result:

```

    Discovering IPMI Devices ...
--- ipmidiscover statistics ---
448 requests transmitted, 0 responses received in
time, 100.0% packet loss

```

---

## IPMI Configuration

IPMI configuration allows you to manage the IPMI functions of a remote system, including printing FRU information, LAN configuration, sensor readings, and remote chassis power control.

1. Choose IPMI > IPMI Configuration. The IPMI Configuration page opens.

The screenshot shows the IPMI Configuration page. At the top, there is a blue header bar with the text "IPMI Configuration". Below the header, there are five input fields, each with a label to its left: "IP Address:", "Username:", "Password:", "Options:", and "Command:". Each label is in bold. Below the input fields, there are three buttons: "OK", "Clear", and "Help", each in a blue box with white text.

2. Click the Help button to get IPMI configuration information, which appears on the IPMI Configuration page.

Help:

ipmitool version 1.8.7

usage: ipmitool [options...]

-h	This help
-V	Show version information
-v	Verbose (can use multiple times)
-c format	Display output in comma separated
-l intf	Interface to use
-H hostname	Remote host name for LAN interface
-p port	Remote RMCP port [default=623]
-U username	Remote session username
-f file	Read remote session password from file
-S sdr	Use local file for remote SDR cache
-a	Prompt for remote password
-e char	Set SOL escape character
-C ciphersuite interface	Cipher suite to be used by lanplus
-k key	Use Kg key for IPMIv2 authentication
-L level [default=ADMINISTRATOR]	Remote session privilege level
-A authtype	Force use of auth type NONE, PASSWORD, MD2, MD5 or OEM
-P password	Remote session password
-E environment variable	Read password from IPMI_PASSWORD
-m address	Set local IPMB address
-b channel request	Set destination channel for bridged request
-l lun	Set destination lun for raw commands
-t address	Bridge request to remote target address
-o oemtype OEM types)	Setup for OEM (use 'list' to see available OEM types)
-O seloem	Use file for OEM SEL event descriptions

Interfaces:

open	Linux OpenIPMI Interface [default]
imb	Intel IMB Interface

## lan IPMI v1.5 LAN Interface

## Commands:

raw	Send a RAW IPMI request and print response
i2c	Send an I2C Master Write-Read command and print response
lan	Configure LAN Channels
chassis	Get chassis status and set power state
power	Shortcut to chassis power commands
event	Send pre-defined events to MC
mc	Management Controller status and global enables
sdr	Print Sensor Data Repository entries and readings
sensor	Print detailed sensor information
fru	Print built-in FRU and scan SDR for FRU locators
sel	Print System Event Log (SEL)
pef	Configure Platform Event Filtering (PEF)
sol	Configure and connect IPMIv2.0 Serial-over-LAN
tsol	Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
isol	Configure IPMIv1.5 Serial-over-LAN
user	Configure Management Controller users
channel	Configure Management Controller channels
session	Print session information
firewall	Configure firmware firewall (IPMIv2.0)
sunoem	OEM Commands for Sun servers
picmg	Run a PICMG/ATCA extended cmd
fwum	Update IPMC using Kontron OEM Firmware Update Manager
shell	Launch interactive IPMI shell
exec	Run list of commands from file
set	Set runtime variable for shell and exec

3. Type the IP address in the IP Address field.
4. Type your username in the Username field.

5. Type your password in the Password field.
6. Type an option in the Option field.
7. Type a command in the Command field.
8. Click the IPMI Discover button. The system displays the results of your command.

# Chapter 13 Power Control

## In This Chapter

Port Power Associations.....	229
Power Strip Configuration.....	231
Power Association Groups .....	231
Power Control.....	232
Associations Power Control.....	233
Power Strip Power Control .....	234
Power Strip Status .....	235
CLI Command for Power Control .....	235

---

## Port Power Associations

---

**Important: A maximum of 31 powerstrips can be run with the SX.**

---

You can associate one or more outlets on a powerstrip connected to the SX to specific SX ports.

---

### Create a Port Power Association

► **To create a port power association:**

1. Choose Setup > Port Power Association List.

2. Click Add. The Port Power Association page opens.

### Port Power Associations

**Port:**

**Description:**

**Associated Outlets:**

Power Strip:       Outlet:

3. Select the port from the drop-down menu in the Port field.
4. Select the power strip name from the drop-down menu in the Power Strip field.
5. Select the outlet to associate with the port from the drop-down menu in the Outlet field.
6. Click Add.

---

*Note: It is not recommended to access the port associated with a power strip via RSC or CLI. Accessing the power strip directly will display a raw character stream of commands between SX and the power strip and you are write-locked from any control.*

---

### Delete a Port Power Association

► **To delete a port power association:**

1. Choose Setup > Port Power Association List.

2. Click Add. The Port Power Association page opens.
3. Select the association in the Outlet Association list.
4. Click Delete.

---

## Power Strip Configuration

Important: A maximum of 31 powerstrips can be run with the SX.

► **To configure a power strip:**

1. Choose Setup > Power Strip Configuration.
2. Click Add. The Power Strip Configuration page opens.

**Name:**

**Description:**

**Number of Outlets:**  
 ▼

**Port:**

3. Type a name and description in the Name and Description fields.
4. Select the number of outlets from the drop-down menu in the Number of Outlets field.
5. Type the port number in the Port field.
6. Click OK.

---

## Power Association Groups

► **To create a power associations group:**

1. Choose Setup > Power Association Groups List.

2. Click Add. The Power Association Groups page opens.

**Group Name:**

**Description:**

Available: Selected:

3. Type a name and description in the Group Name and Description fields.
4. Select the number of outlets from the drop-down menu in the Number of Outlets field.
5. Click OK.

---

## Power Control

Click the Power Control tab to display the power control-related tools.

### Power Control

[Associations Power Control](#)

[Power Strip Power Control](#)

[Power Strip Status](#)

---

## Associations Power Control

Choose Power Control > Associations Power Control to access the tool to manage power control associations.

Group and Port Power Associations			
	Name	Type	Outlet Status
<input type="checkbox"/>	Purl2	Purl	ON/OFF

*Note: When executing power on/off operation, about ~5 seconds are added to the configured sequential interval, resulting in an operational delay time (minimum amount of time to operate). If power cycle is selected, all associated outlets are powered off sequentially, and then powered on sequentially. The cycle delay time reacted here determines the minimum length of time needed to turn back on the outlets after they're shut down, which is user-specified by administrator. The delay time to experience would be operational delay + user-specified delay.*

*Note: If you are connecting a PX to the SX, it is recommended you set the power cycle time to 5 seconds.*

*Note: If you disconnect the Dominion PX after creating an association in SX, the association would appear empty until you re-plug-in the PX into the same port.*

---

## Power Strip Power Control

Choose Power Control > Power Strip Power Control to access the Outlet Control page, where you can manage power strips.

The screenshot shows the 'Outlet Control' interface. It features a table with 20 rows, each representing an outlet. The table has three columns: a checkbox, the outlet name (Outlet 1 through Outlet 20), and the current state (ON or OFF). A 'Select All' button is located to the right of the table. Below the table are three buttons: 'On', 'Off', and 'Cycle'.

	Outlet	State
<input type="checkbox"/>	Outlet 1	OFF
<input checked="" type="checkbox"/>	Outlet 2	OFF
<input type="checkbox"/>	Outlet 3	OFF
<input type="checkbox"/>	Outlet 4	ON
<input checked="" type="checkbox"/>	Outlet 5	OFF
<input type="checkbox"/>	Outlet 6	OFF
<input type="checkbox"/>	Outlet 7	ON
<input type="checkbox"/>	Outlet 8	OFF
<input checked="" type="checkbox"/>	Outlet 9	OFF
<input type="checkbox"/>	Outlet 10	OFF
<input type="checkbox"/>	Outlet 11	OFF
<input type="checkbox"/>	Outlet 12	OFF
<input type="checkbox"/>	Outlet 13	OFF
<input type="checkbox"/>	Outlet 14	OFF
<input type="checkbox"/>	Outlet 15	OFF
<input type="checkbox"/>	Outlet 16	OFF
<input type="checkbox"/>	Outlet 17	OFF
<input type="checkbox"/>	Outlet 18	OFF
<input type="checkbox"/>	Outlet 19	OFF
<input type="checkbox"/>	Outlet 20	ON

Buttons: On, Off, Cycle

Select All

## Power Strip Status

Choose Power Control > Power Strip Status to check power strip status.

### DPX Status:

```
Power strip:
Outlet Breaker Status: 1
True RMS Current: 0.0
Maxium Detected Current: 0.4
True RMS Voltage : 113.0
Internal Temperature : 45.0
Average Power : 0
Apparent Power : 0
Outlets: 20
    1. Outlet 1 : Off
    2. Outlet 2 : Off
    3. Outlet 3 : Off
    4. Outlet 4 : On
    5. Outlet 5 : Off
    6. Outlet 6 : Off
    7. Outlet 7 : On
    8. Outlet 8 : Off
    9. Outlet 9 : Off
   10. Outlet 10 : Off
   11. Outlet 11 : Off
   12. Outlet 12 : Off
   13. Outlet 13 : Off
   14. Outlet 14 : Off
   15. Outlet 15 : Off
   16. Outlet 16 : Off
```

## CLI Command for Power Control

### CLI Port Power Association

Description: Power Control menu - Associate a power strip outlet to an SX port

Scenario #1	Port power association - add outlet
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) is physically connected to SX named PowerStr1. User is in power menu.
Action	Type command. Press Enter.
CLI Input	associate port 1 powerstrip PowerStr1 outlet 1

<b>Scenario #2 Port power association - associate 6 outlets to one port</b>	
Pre-condition	<p>Administrator user is logged in via CLI.</p> <p>Power strip (DPX) is physically connected and configured to DSX named PowerStr1.</p> <p>User is in power menu.</p>
Action	<p>Type command - associate [port port] [powerstrip powerstrip] [outlet outlet] to associate Outlet1 to Port1</p> <p>Press Enter.</p> <p>Repeat steps 3 and 4 for Outlet 2, 3, 4, 5 and 6.</p>
CLI Input	associate port 1 powerstrip PowerStr1 outlet 1-6
<b>Scenario #3 Port power association - associate 6 outlets to one port spread across two PDUs</b>	
Pre-condition	<p>Administrator user is logged in via CLI.</p> <p>Two Power strip (DPX) are physically connected and configured to the SX, respectively named PowerStr1 and PowerStr2.</p> <p>User is in power menu.</p>
Action	<p>Type command - associate [port port] [powerstrip powerstrip] [outlet outlet] to associate Outlet1 of PowerStr1 to Port1</p> <p>Press Enter.</p> <p>Repeat steps 1 and 2 for Outlet 2 and 3.</p> <p>Type command - associate [port port] [powerstrip powerstrip] [outlet outlet] to associate Outlet1 of PowerStr2 to Port1</p> <p>Press Enter.</p> <p>Repeat steps 4 and 5 for Outlet 2 and 3.</p>
CLI Input	associate port 1 powerstrip PowerStr1 outlet 1,2,3 associate port 1 powerstrip PowerStr2 outlet 1,2,3
<b>Scenario #4 Port power association - associate one outlet to two ports</b>	
Pre-condition	<p>Administrator user is logged in via CLI.</p> <p>Power strip (DPX) is physically connected and configured to the SX named PowerStr1.</p> <p>User is in power menu.</p>

<b>Scenario #4 Port power association - associate one outlet to two ports</b>	
Action	Enter command Press Enter
CLI Input	associate port 1 powerstrip PowerStr1 outlet 1 associate port 2 powerstrip PowerStr1 outlet 1
<b>Scenario #5 Port power association - associate all available outlets to ports</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) is physically connected and configured to the SX named PowerStr1. User is in power menu
Action	Enter command. Press Enter. Repeat steps 1 and 2 for all available Outlets with up to 6 outlets associated to a single port.
CLI Input	associate port 1 powerstrip PowerStr1 outlet 1
<b>Scenario #6 Port power association - associate outlets to one port from different power strips</b>	
Pre-condition	Administrator user is logged in via CLI. Two Power strip (DPX) are physically connected and configured to the SX respectively named PowerStr1 and PowerStr2. User is in power menu.
Action	Enter command to associate Port1 to Outlet1 from PowerStr1. Press Enter. Enter command to associate Port1 to Outlet1 from PowerStr2. Press Enter.
CLI Input	associate port 1 powerstrip PowerStr1 outlet 1 associate port 1 powerstrip PowerStr2 outlet 1
<b>Scenario #7 Port power association - associate outlets from 6 different power strips to one port</b>	
Pre-condition	Administrator user is logged in via CLI.

<b>Scenario #7 Port power association - associate outlets from 6 different power strips to one port</b>	
	6 Power strip (DPX) are physically connected and configured to SX. User is in power menu.
Action	Enter Command to associate Port1 to Outlet1 of PowerStr1. Press Enter. Repeat steps 1 and 2 to associate Port1 with Outlet1 from each of the other PDUs.
CLI Input	associate port 1 powerstrip PowerStr1 outlet 1 associate port 1 powerstrip PowerStr2 outlet 1 associate port 1 powerstrip PowerStr3 outlet 1 associate port 1 powerstrip PowerStr4 outlet 1 associate port 1 powerstrip PowerStr5 outlet 1 associate port 1 powerstrip PowerStr6 outlet 1

<b>Scenario #8 Port power association - edit outlet names</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) is physically connected and configured to SX named PowerStr1. User is in power menu.
Action	Enter Command to edit outlet1 name of PowerStr1. Press Enter.
CLI Input	outlet name PowerStr1 outlet 1 newname TestName

Remove Port Power Association

Description: Power Control Menu - Remove a power outlet association from an SX port.

<b>Scenario #1 Remove port power association</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) is physically connected and configured to SX named PowerStr1. User is in power menu.
Action	Enter command.

<b>Scenario #1 Remove port power association</b>	
	Press Enter.
CLI Input	Command: unassociate port 1 powerstrip PowerStr1 outlet 1
<b>Scenario #2 Delete multiple outlets association</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) is physically connected and configured to the SX named PowerStr1. User is in power menu.
Action	Enter command. Press Enter.
CLI Input	Command: unassociate port 1 powerstrip PowerStr1 outlet 1,4,7

CLI Power Strip Configuration  
Description: Power Control Menu

<b>Scenario #1 Configure an SX port to contain a power strip device (the port is previously connected to a power strip)</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) is physically connected to Port1 of SX. Administrator is in power menu.
Action	Enter command. Press Enter.
CLI Input	setpowerport name PowerStr1 type DPCS12 port 1
<b>Scenario #2 Power strip configuration after factory reset</b>	
Pre-condition	Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. SX user has already configured the port as a power strip.
Action	Log in to SX unit with administrator privileges via CLI. Go to Maintenance menu Perform Factory Reset
CLI Input	Command: factoryreset

CLI Power Association Group

Description: Power &gt; PowerGroups menu

<b>Scenario #1 Create new power group</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in Power > PowerGroups menu.
Action	Enter Command. Press Enter.
CLI Input	Command: addpowergroup name "Test Group" description "Test group"
<b>Scenario #2 Add a port to a power group</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in Power > PowerGroups menu.
Action	Enter Command. Press Enter.
CLI Input	Command: addpowergroupport name "test Group" port port 2
<b>Scenario #3 Add multiple ports to a power group</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in Power > PowerGroups menu.
Action	Enter Command. Press Enter.
CLI Input	Command: addpowergroupport name "test Group" port port 2-4,10
<b>Scenario #4 Remove group member</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX.

<b>Scenario #4 Remove group member</b>	
	Administrator is in Power > PowerGroups menu.
Action	Enter Command. Press Enter.
CLI Input	Command: deletepowergroupport name "Test Group" port 2
<b>Scenario #5 Delete power group</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in Power > PowerGroups menu.
Action	Enter Command. Press Enter.
CLI Input	Command: deletepowergroup name "Test Group"

---

### CLI Power Strip Power Control

Description: Power Control Menu

<b>Scenario #1 Switch on/off a single Outlet</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in power menu.
Action	Enter Command. Press Enter.
CLI Input	on powerstrip PowerStr1 outlet 1 off powerstrip PowerStr1 outlet 1
<b>Scenario #2 Switch on/off all Outlets</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in power menu.
Action	Enter Command.

<b>Scenario #2 Switch on/off all Outlets</b>	
	Press Enter.
CLI Input	on powerstrip PowerStr1 outlet * off powerstrip PowerStr1 outlet *
<b>Scenario #3 Switch on/off group of outlets</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in power menu.
Action	Enter Command. Press Enter.
CLI Input	on powerstrip PowerStr1 outlet 1,3,7 off powerstrip PowerStr1 outlet 1,3,7
<b>Scenario #4 Power recycle group of outlets</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in power menu.
Action	Enter Command. Press Enter.
CLI Input	cycle powerstrip PowerStr1 outlet 1,3,7
<b>Scenario #5 Sequence interval for switch off operation</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in power menu.
Action	Enter command to set sequence interval. Press Enter. Enter command to switch off group of outlets. Press Enter.
CLI Input	powerdelay sequence 2 off powerstrip PowerStr1 outlet 1,3,7

<b>Scenario #6 Sequence interval for switch on operation</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in power menu.
Action	Enter command to set sequence interval. Press Enter. Enter command to switch on group of outlets. Press Enter.
CLI Input	powerdelay sequence 2 off powerstrip PowerStr1 outlet 1,3,7
<b>Scenario #7 Power Recycle Interval</b>	
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in power menu.
Action	Enter command to set sequence and power recycle interval. Press Enter. Enter command to power recycle group of outlets. Press Enter.
CLI Input	powerdelay sequence 2 cycle 5 cycle powerstrip PowerStr1 outlet 1,3,7

---

### CLI Configure Global Power Strip Delays

Syntax: `powerdelay [sequence sequence] [cycle cycle]`

- `sequence` - Sequence Delay is the delay between executing power commands.

The sequence delay effects the time between power operations on different outlets when using a single power command to power on/off/cycle multiple outlets at once.

- `cycle` - Cycle Delay is the delay in power cycle between off and on.

The cycle delay effects the time between the power off and on of an outlet when cycling power.

A `powerdelay` setting of 0 executes the commands as fast as possible.

Example: `powerdelay sequence 2 cycle 5`

---

*Note: The `powerdelay` setting of 0 may not function on PX1 devices. This command does function on Baytech® and PX2 PDUs.*

---

### CLI Association Power Control - Port Association

Description: Power Control Menu

<b>Scenario #1 Association Power Control - Recycle Port Association (Target is associated to One Outlet)</b>	
Pre-condition	<p>Administrator user is logged in via CLI.</p> <p>Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX.</p> <p>Port Power Association named Target2 is already created and available in the list.</p> <p>Outle1 of PowerStr1 is associated to Target2.</p> <p>Administrator is in Power Control &gt; Associations Power Control menu.</p>
Action	<p>Select Port Association named Target2</p> <p>Click on Power Recycle Interval and enter value:</p> <p>Press Recycle button.</p>
CLI Input	Power Recycle Interval value: 1 sec.
<b>Scenario #2 Association Power Control - Recycle Port Association (Target is associated to Two Outlets from one power strip)</b>	
Pre-condition	<p>Administrator user is logged in via CLI.</p> <p>Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX.</p> <p>Port Power Association named Target2 is already created and available in the list.</p> <p>Outle1 of PowerStr1 is associated to Target2.</p> <p>Administrator is in Power Control &gt; Associations Power Control menu.</p>
Action	<p>Select Port Association named Target2</p> <p>Click on Power Recycle Interval and enter value:</p>

<b>Scenario #2 Association Power Control - Recycle Port Association (Target is associated to Two Outlets from one power strip)</b>	
	Press Recycle button.
CLI Input	Power Recycle Interval value: 1 sec.
<b>Scenario #3 Association Power Control - Recycle Port Association (Target is associated to Two Outlets from two different power strips)</b>	
Pre-condition	<p>Administrator user is logged in via CLI.</p> <p>Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX.</p> <p>Port Power Association named Target2 is already created and available in the list.</p> <p>Outle1 of PowerStr1 is associated to Target2.</p> <p>Administrator is in Power Control &gt; Associations Power Control menu.</p>
Action	<p>Select Port Association named Target2</p> <p>Click on Power Recycle Interval and enter value</p> <p>Press Recycle button.</p>
CLI Input	Power Recycle Interval value: 1 sec.
<b>Scenario #4 Association Power Control - Recycle Port Association (outlets in the association are with different statuses)</b>	
Pre-condition	<p>Administrator user is logged in via GUI.</p> <p>Two power strips (DPX) named PowerStr1 and PowerStr2 are physically connected to SX Ports.</p> <p>Port Power Association named Target2 is already created and available in the list.</p> <p>Outle1 of PowerStr1 and Outlet2 of PowerStr2 are associated to Target2.</p> <p>Outlet1 and Outlet2 are with different statuses.</p> <p>Administrator is in Power Control &gt; Associations Power Control menu.</p>
Action	<p>Select Port Association named Target2</p> <p>Click on Power Recycle Interval and enter value:</p> <p>Press Recycle button.</p>
CLI Input	Power Recycle Interval value: 1 sec.

**CLI Association Power Control - Group Association**

Description: Power Control Menu

<b>Scenario #1 Turn ON Group Association</b>	
Pre-condition	Administrator user is logged in via CLI. Administrator is in power menu. Group Association named Group1 (shown in Fg.1) is already created.
Action	Enter Command. Press Enter.
CLI Input	Command: on nodegroup Group1
<b>Scenario #2 Turn ON Group Association (outlets in association are with different statuses)</b>	
Pre-condition	Administrator user is logged in via CLI. Administrator is in power menu. Group Association named Group1 (shown in Fg.1) is already created. Outlets in Group1 are with different statuses.
Action	Enter Command. Press Enter.
CLI Input	Command: on nodegroup Group1
<b>Scenario #3 Turn OFF Group Association</b>	
Pre-condition	Administrator user is logged in via CLI. Administrator is in power menu. Group Association named Group1 (shown in Fg.1) is already created.
Action	Enter Command. Press Enter.
CLI Input	Command: off nodegroup Group1
<b>Scenario #4 Turn OFF Group Association (outlets in association are with different statuses)</b>	
Pre-condition	Administrator user is logged in via CLI.

<b>Scenario #4 Turn OFF Group Association (outlets in association are with different statuses)</b>	
	Administrator is in power menu. Group Association named Group1 (shown in Fig.1) is already created. Outlets in Group1 are with different statuses.
Action	Enter Command. Press Enter.
CLI Input	Command: off nodegroup Group1
<b>Scenario #5 Recycle Group Association</b>	
Pre-condition	Administrator user is logged in via CLI. Administrator is in power menu. Group Association named Group1 (shown in Fig.1) is already created.
Action	Enter Command. Press Enter.
CLI Input	powerdelay sequence 2 cycle 5 cycle nodegroup Group1
<b>Scenario #6 Recycle Group Association (outlets in association are with different statuses)</b>	
Pre-condition	Administrator user is logged in via CLI. Administrator is in power menu. Group Association named Group1 (shown in Fig.1) is already created. Outlets in Group1 are with different statuses.
Action	Enter Command. Press Enter.
CLI Input	powerdelay sequence 2 cycle 5 cycle nodegroup Group1
<b>Scenario #7 Turn ON Group and Port Association simultaneously</b>	
Pre-condition	Administrator user is logged in via CLI. Administrator is in power menu. Group Association named Group1 (shown in Fig.1) is already created. Port3 is already associated with

<b>Scenario #7 Turn ON Group and Port Association simultaneously</b>	
	outlet8 of PowerStr1 which has been created and available in the list.
Action	Enter Command. Press Enter.
CLI Input	powerdelay sequence 2 cycle 5 on port 3 nodegroup Group1
<b>Scenario #8 Turn OFF Group and Port Association simultaneously</b>	
Pre-condition	Administrator user is logged in via CLI. Administrator is in power menu. Group Association named Group1 (shown in Fig.1) is already created. Port3 is already associated with outlet8 of PowerStr1 which has been created and available in the list.
Action	Enter Command. Press Enter.
CLI Input	powerdelay sequence 2 cycle 5 off port 3 nodegroup Group1
<b>Scenario #10 Recycle Group and Port Association simultaneously</b>	
Pre-condition	Administrator user is logged in via CLI. Administrator is in power menu. Group Association named Group1 (shown in Fig.1) is already created. Port3 is already associated with outlet8 of PowerStr1 which has been created and available in the list.
Action	Enter Command. Press Enter.
CLI Input	powerdelay sequence 2 cycle 5 cycle port 3 nodegroup Group1.

**CLI Power Strip Status**

Description: Power Control Menu

<b>Scenario #1</b>	<b>Power Strip Status</b>
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX. Administrator is in Power menu.
Action	Enter Command. Press Enter.
CLI Input	Command: powerstrip name PowerStr1
Result	Status of PDU should correctly display the following parameters: Power Consumption Average Power Apparent Power True RMS Voltage True RMS Current Maximum Current Status of the outlet breaker Internal Temperature
<b>Scenario #2</b>	<b>Status of Power Strip that is actually turn off or disconnected</b>
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is disconnected from Port1 or turned off. Administrator is in Power menu.
Action	Enter Command. Press Enter.
CLI Input	Command: powerstrip name PowerStr1
<b>Scenario #3</b>	<b>Power Strip Status - Outlet status</b>
Pre-condition	Administrator user is logged in via CLI. Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX.

<b>Scenario #3 Power Strip Status - Outlet status</b>	
Action	<p>Check the current status of outlets - outlet1 is turn on</p> <p>Turn off outlet1.</p> <p>Go to Power menu and check the status of outlet1.</p>
CLI Input	<pre>powerstrip name PowerStr1 off powerstrip PowerStr1 outlet 1 powerstrip name PowerStr1</pre>
<b>Scenario #4 Power Strip Status - Outlet status when port association is removed</b>	
Pre-condition	<p>Administrator user is logged in via CLI.</p> <p>Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX.</p> <p>Outlet1 and Outlet2 are associated with Port1.</p> <p>Outlet1 and Outlet2 are with status "ON".</p> <p>Administrator is in Power menu.</p>
Action	<p>Check the current status of outlets - outlet1 is turn on</p> <p>Remove Outlet1 and Outlet2 from outlet association to Port1.</p> <p>Go to Power menu and check the status of outlet1.</p>
CLI Input	<pre>powerstrip name PowerStr1 unassociated port 1 powerstrip PowerStr1 outlet 1,2 powerstrip name PowerStr1</pre>
<b>Scenario #5 Power Strip Status - Outlet status when group association is removed</b>	
Pre-condition	<p>Administrator user is logged in via CLI.</p> <p>Power strip (DPX) named PowerStr1 is physically connected to Port1 of SX.</p> <p>Group association named Group1 is created.</p> <p>Outlet1 and Outlet2 are with status "ON".</p> <p>Administrator is in Power menu.</p>
Action	<p>Check the current status of outlets - outlet1 is turn on</p> <p>Remove Group1.</p> <p>Go to Power menu and check the status of outlet1.</p>

<b>Scenario #5</b>	<b>Power Strip Status - Outlet status when group association is removed</b>
CLI Input	powerstrip name PowerStr1 deletepowergroup name Group1 powerstrip name PowerStr1

# Appendix A Specifications

## In This Chapter

SX Models and Specifications .....	252
Maximum Number of Connections for a Single User .....	255
Maximum Number of CLI Sessions .....	255
Requirements .....	256
Supported Operating Systems, Browsers and Java Versions .....	256
Connectivity .....	257
SX Serial RJ-45 Pinouts .....	258
SX Terminal Ports .....	261
SX16 and SX32 Terminal Ports .....	262

---

## SX Models and Specifications

The following table lists the SX models by the number of ports (4 - 48) in the unit.

Model	Ports	Built-In Modem	# of Local Ports	# of Ethernet Ports	Power Supply
DSX4	4	No	2	1	Single AC
DSXB-4-M	4	Yes	1	1	Single AC
DSX8	8	No	1	1	Single AC
DSXA-8	8	Yes	1	1	Dual AC
DSXB-8-M	8	Yes	1	1	Single AC
DSXA-16	16	Yes	1	1	Dual AC
DSXA-16-DL	16	No	2	2	Dual AC
DSXA-16-DLM	16	Yes	1	2	Dual AC
DSXA-32	32	Yes	1	1	Dual AC
DSXA-32-AC	32	No	2	1	Dual AC
DSXA-32-DL	32	No	2	2	Dual AC
DSXA-32-	32	Yes	1	2	Dual AC

Model	Ports	Built-In Modem	# of Local Ports	# of Ethernet Ports	Power Supply
DLM					
DSXA-48	48	Yes	1	2	Dual AC
DSXA-48-AC	48	No	2	2	Dual AC

The following table lists the SX models, their dimensions, and weights.

MODEL	DIMENSIONS (W) x (D) x (H)	WEIGHT
DSX4	11.41" x 10.7" x 1.75"; 290 x 270 x 44 mm	4.61 lbs; 2.08 kg
DSXB-4-M	11.41" x 10.7" x 1.75"; 290 x 270 x 44 mm	4.61 lbs; 2.08 kg
DSX8	11.41" x 10.7" x 1.75"; 290 x 270 x 44 mm	4.81 lbs; 2.17 kg
DSXA-8	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.00 lbs; 3.60 kg
DSXB-8-M	11.41" x 10.7" x 1.75"; 290 x 270 x 44 mm	4.81 lbs; 2.17 kg
DSXA-16	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.28 lbs; 3.756 kg
DSXA-16-DL	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.58 lbs; 3.86 kg
DSXA-16-DLM	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.58 lbs; 3.86 kg
DSXA-32	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.40 lbs; 3.78 kg
DSXA-32-AC	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.40 lbs; 3.78 kg
DSXA-32-DL	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.78 lbs; 3.95 kg
DSXA-32-DLM	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.78 lbs; 3.95 kg
DSXA-48	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.97lbs; 4.04 kg
DSXA-48-AC	17.32" x 11.41" x 1.75"; 440 x 290 x 44 mm	8.97lbs; 4.04 kg

The following table lists the information of Cables/Adapters/Brackets. The SX is able to support long distance cables. The actual distance you may achieve is dependent on many factors including baud rate, cable quality, environmental radiation, and the target serial device's specifications, quality and tolerances. You may achieve higher or lower lengths based on these factors. Raritan recommends that you test in your environment to validate the desired distance.

Part Number	Description
ASCSD9F	RJ-45(F) to DB9(F) serial adapter
ASCSD9M	RJ-45(F) to DB9(M) serial adapter
ASCSD25F	RJ-45(F) to DB25(F) serial adapter
ASCSD25M	RJ-45(F) to DB25(M) serial adapter
ASCSD9F-DCE	Serial Adapter for DB9 DCE Port to SX
CRLVR-15	15' (4.5m) serial rollover Cat5 cable - for most Cisco and Sun serial RJ-45 ports ( <b>Note:</b> This is NOT a standard or a crossover Ethernet cable.)
CSCSPCS-10	10' (3m) Cat5e cable to connect the SX to a Raritan remote power control unit
CRLVR-1	1' (0.3m) serial rollover Cat5 adapter cable (RJ45 Male to RJ45 Female) - for most Cisco and Sun serial RJ-45 ports
CRLVR-1-5PK	Package of 5 CRLVR-1 (1'; 0.3m) serial rollover Cat5 adapter cables (RJ45 Male to RJ45 Female) - for most Cisco and Sun serial RJ-45 ports
CSCSPCS-1	1' (0.3m) Cat5e adapter cable (RJ45 Male to RJ45 Female) to connect the SX to a Raritan remote power control unit
CSCSPCS-1-5PK	Package of 5 CSCSPCS-1 (1'; 0.3m) adapter cables (RJ45 Male to RJ45 Female) to connect the SX to a Raritan remote power control unit
RUST-LM304	19" (482.6mm) standard rack mount brackets for DSX4, DSXB-4-M, DSX8, and DSXB-8-M

Only RoHS and WEEE compliant units are available in the EU and other selected areas. RoHS and WEEE compliant units can be provided elsewhere upon request.

#### **CRLVR-15:**

1. A Cat5 cable in YELLOW color with a length of 15 feet.
2. RJ-45 male terminators, wired with the following pin-out:

Pin	Pin
1	8
2	7
3	6
4	5
5	4
6	3
7	2
8	1

---

### Maximum Number of Connections for a Single User

The following maximum number of connections for a single user apply to the SX;

- All SX models support a maximum of twelve (12) simultaneous RSC port sessions per user per host. A maximum of six (6) SSH port sessions per user are supported.
- In order to use 48 port connections, a single user must connect from four (4) different hosts (for example, 4 hosts/12 RSC sessions per user per host).
- If you are running RSC and SSH sessions simultaneously, use one of the following scenarios:
  - 6 RSC connections plus 2 SSH sessions with a single user for same host, or
  - 10 RSC sessions/1 SSH session, or
  - 2 RSC/5 SSH sessions

---

### Maximum Number of CLI Sessions

In order to avoid expending the SX device's memory, 64Mb machines are limited to 12 CLI sessions at a time, and 128Mb machines are limited to 32 CLI sessions at a time.

---

## Requirements

The following table lists the requirements for the SX.

Requirements	Description
Form factor	1U, rack mountable (brackets included on DSX16, DSX32, DSXA-8 and DSX48)
Power	110/240VAC auto-switching: 50-60 Hz
Max. power consumption	4-Port SX: 5.75W 8-port SX: 6W 16-port SX: 8W 32-port SX: 9.375W 48-port SX: 12.5W
<b>Environmental requirements</b>	
Operating temperature	32° to 104° F (0° to 40° C)
Humidity	20% - 85% RH non-condensing
Altitude	Operates properly at any altitude from 0 to 10,000 feet
Approvals	CE, FCC Part 15 Class A, US and Canadian UL, VCCI-A
<b>Remote Connection</b>	
Network	One (1) or two (2) 10/100 Ethernet Base-T; RJ-45 connection
Protocols	TCP/IP, PPP, PAP, HTTP, HTTPS, SSL, SSH, TACACS+, LDAP(S), RADIUS, SNMP, Kerberos
Warranty	Two Years with Advanced Replacement*

\*To qualify for advanced replacement under the standard warranty, you must register the product at [http://Raritan.com/standard\\_warranty](http://Raritan.com/standard_warranty) ([p://Raritan.com/standard\\_warranty](p://Raritan.com/standard_warranty)). Specifications are subject to change without notice.

---

## Supported Operating Systems, Browsers and Java Versions

Operating Systems	Browsers	Java™ versions
Windows 7® Home Premium SP1 64-bit	<ul style="list-style-type: none"> <li>▪ Internet Explorer® 10, 11</li> <li>▪ Firefox® 31</li> <li>▪ Chrome® 35</li> </ul>	<ul style="list-style-type: none"> <li>▪ 1.7.0_55, 1.7.0_60,</li> <li>▪ 1.7.0_65, and</li> <li>1.7.0_67</li> </ul>
Windows 7 Ultimate SP1 64-bit	<ul style="list-style-type: none"> <li>▪ Internet Explorer 8, 9, 11</li> <li>▪ Firefox 28</li> <li>▪ Chrome 31</li> </ul>	<ul style="list-style-type: none"> <li>▪ 1.7.0_55</li> </ul>
Windows 7 Ultimate 32-bit	<ul style="list-style-type: none"> <li>▪ Internet Explorer 8</li> <li>▪ Firefox 25</li> <li>▪ Chrome 31</li> </ul>	<ul style="list-style-type: none"> <li>▪ 1.7.0_55</li> </ul>
Windows 8® 64-bit	<ul style="list-style-type: none"> <li>▪ Internet Explorer 10, 11</li> <li>▪ Firefox 25</li> <li>▪ Chrome 31</li> </ul>	<ul style="list-style-type: none"> <li>▪ 1.7.0_60</li> </ul>
Windows Server 2012® Standard 64-bit	<ul style="list-style-type: none"> <li>▪ Internet Explorer 10</li> <li>▪ Firefox 27</li> <li>▪ Chrome 31</li> </ul>	<ul style="list-style-type: none"> <li>▪ 1.7.0_55, 1.7.0_60</li> <li>and</li> <li>▪ 1.7.0_65</li> </ul>
Windows XP® Professional x64 Edition with SP 2	<ul style="list-style-type: none"> <li>▪ Internet Explorer 8</li> <li>▪ Firefox 28</li> <li>▪ Chrome 31</li> </ul>	<ul style="list-style-type: none"> <li>▪ 1.7.0_45</li> </ul>
openSUSE® 13.1	<ul style="list-style-type: none"> <li>▪ Firefox 25</li> </ul>	<ul style="list-style-type: none"> <li>▪ 1.7.0_55</li> </ul>
Fedora® 18	<ul style="list-style-type: none"> <li>▪ Firefox 28</li> </ul>	<ul style="list-style-type: none"> <li>▪ 1.7.0_65</li> </ul>
Mac® OS X Mountain Lion® 10.7.5	<ul style="list-style-type: none"> <li>▪ Firefox 30</li> <li>▪ Safari 6.1.2</li> </ul>	<ul style="list-style-type: none"> <li>▪ 1.6.0_65</li> </ul>
Mac OS X Mavericks® 10.9.4	<ul style="list-style-type: none"> <li>▪ Firefox 30</li> <li>▪ Safari 7.0.5</li> </ul>	1.7.0_67
Solaris® 10 64-bit	<ul style="list-style-type: none"> <li>▪ Firefox 28</li> <li>▪ Safari 7.0.5</li> </ul>	1.7.0_55 and 1.7.0_67

---

## Connectivity

The following table lists the necessary SX hardware (adapters and/or cables) for connecting the SX to common Vendor/Model combinations.

Vendor	Device	Console Connector	Serial Connection
Checkpoint™	Firewall	DB9M	ASCSD9F adapter

Vendor	Device	Console Connector	Serial Connection
Cisco®	PIX Firewall		and a CAT 5 cable
Cisco	Catalyst	RJ-45	CRLVR-15 rollover cable; or CRLVR-1 adapter cable and a CAT5 cable  CRLVR-1 cable for connecting a terminal port (RJ-45 Connector type) of SX-48 models that have this connector to another SX.
Cisco	Router	DB25F	ASCSD25M adapter and a CAT 5 cable
Hewlett Packard®	UNIX® Server	DB9M	ASCSD9M adapter and a CAT 5 cable
Silicon Graphics®	Origin		
Sun®	SPARCStation	DB25F	ASCSD25M adapter and a CAT 5 cable
Sun	Netra T1	RJ-45	CRLVR-15 cable; or CRLVR-1 adapter and a CAT5 cable
Sun	Cobalt	DB9M	ASCSD9M adapter and a CAT 5 cable
Various	Windows NT®		
Raritan	RPCU	RJ-45	CSCSPCS-10 cable or CSCSPCS-1 adapter cable

Contact your reseller or Raritan Support for further information on cables and adapters.

---

## SX Serial RJ-45 Pinouts

To provide maximum port density and to enable simple UTP (Category 5) cabling, SX provides its serial connections via compact RJ-45 ports. However, no widely adopted industry-standard exists for sending serial data over RJ-45 connections.

The following tables list the RJ-45 pinouts for the RJ-45 connector, located on the back of the SX.

RJ-45 PIN	SIGNAL
1	RTS
2	DTR
3	TxD
4	GND
5	Signal GND
6	RxD
7	DSR
8	CTS

See <http://www.raritan.com/support> for the latest information about the SX serial pinouts (RJ-45).

---

#### DB9F Nulling Serial Adapter Pinouts

RJ-45 (female)	DB9 (female)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

---

#### DB9M Nulling Serial Adapter Pinouts

RJ-45 (female)	DB9 (male)
1	8
2	1, 6
3	2
4	SHELL
5	5

RJ-45 (female)	DB9 (male)
6	3
7	4
8	7

---

**DB25F Nulling Serial Adapter Pinouts**

RJ-45 (female)	DB25 (female)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

---

**DB25M Nulling Serial Adapter Pinouts**

RJ-45 (female)	DB25 (male)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

## SX Terminal Ports

All SX models, except the DSX16 and DSX32, have the same pinouts on the two DB9M serial ports. This applies to models with two serial ports. All dual-LAN (dual-power) models have one RJ-45 serial port. The DSX16 and DSX32 models have only one external DB9M serial port (labeled TERMINAL). All dual-LAN (dual-power) models have one RJ-45 serial port. The DSX16 and DSX32 models have only one external DB9M serial port (labeled TERMINAL).

Both ports support a VT100 terminal or equivalent (that is, a PC running VT100 emulation software such as HyperTerminal® or Linux® Minicom). Local port access must be enabled and set to the same speed as the managed device for it to work. Local port access can be enabled or disabled from the GUI and the CLI using the lpa command through SSH or Telnet, if it is enabled. The telnet server on the SX is disabled by default.

Models with two terminal ports support an external modem only on the port with the RI signal. On models with only one serial port, a modem is built in. The externally accessible serial port does not include the RI signal, so it supports only devices such as a VT100 terminal or equivalent.

The following table identifies the first DB9M serial port pinouts.

DB9M PIN	SIGNAL
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI

The second DB9M serial port supports only two pins as identified in the following table (Pin 4 and pin 7 are fixed too high).

DB9M PIN	SIGNAL
1	
2	RxD
3	TxD

DB9M PIN	SIGNAL
4	DTR (H)
5	GND
6	
7	RTS (H)
8	
9	

---

### SX16 and SX32 Terminal Ports

A modem should not be connected to the terminal ports on DSX16 and DSX32 because the Ring Indicator (RI) signal is not present. These models have a built-in modem that can be enabled or disabled. The modem is disabled by default.

DB9M PIN	Color	SIGNAL
1	Brown	GND
2	Red	RxD
3	Orange	TxD
4	--	--
5	Green	GND
6	No Connection	
7	Purple	RTS
8	Gray	CTS
9	Blue	BUSY-Reserved for Factory Reset Plug

Additional information about the SX16 and SX32 Terminal Ports:

- Pins 1 and 9 are used to factory reset units shipped after August 2004.
- Units shipped prior to August 2004 have the DB9M port labeled RESERVED (not TERMINAL/RESERVED), since this port was used to factory reset the unit, with a Factory reset adapter shipped with each SX. Pins 1 and 6 were used for factory reset. The reset adapters for these early units are different from the current units, which have local port functionality.
- DSX16 and DSX32 units shipped from the factory with the SX 2.2 (or higher) release support the local port capability.
- SX versions through 2.5 have the local port disabled by factory default.
- In SX 3.1 or higher, the local port is enabled by default.

# Appendix B System Defaults

## In This Chapter

Initiate Port Access .....	264
Supported Character Length of Various Field Types .....	264

---

### Initiate Port Access

Use the following information for initiating port access:

Initiate port access using	Ports Kept open or Closed	Directions
HTTP	Ports 80, 443 and 5000 must be kept open in the firewall for the unit to operate. Port 5000 can be configured.	Both
HTTPS SSL(S) only	TCP port 443 needs to be open; port 80 can be closed	Both
SSH	TCP port 22 needs to be open	Both
Telnet	TCP port 23 needs to be open	Both
RADIUS	TCP port 1812 needs to be open	Outgoing
LDAP	Port 389 needs to be open	Outgoing
SNMP	Port 162 needs to be open	Outgoing
TACACS+	Port 49 needs to be open	Outgoing
<b>Notes</b>		
For FTP Upgrades	Port 21 needs to be open	Outgoing
For syslog	UDP port 514 needs to be open	Outgoing

You may have to open additional ports when NFS logging, 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.

---

### Supported Character Length of Various Field Types

The following table lists the supported character length of various field types:

Field Type	Character Length
username	255
user full name	255
user information	64
user password	64
group name	255
Remote Auth Secret	128
LDAP BaseDN	128
LDAP Query	128
LDAP Search	128
LDAP Dialback Query	128
Remote Auth Port	1-65535
Network Failover Interval	0-65535
Network Domain Name	255
Network Unit Name	64
CSC port	1-64510
CSC Discovery Port	1-64510
HTTP/HTTPS Port	1-64510
Telnet /SSH Port	1-64510
Port Name	64
Port Exit Command	100
Port DPA SSH Port	1024-64510
Port DPA Telnet Port	1024-64510
Port Keyword	40
Power Sequence Delay	2-60
Power Cycle Delay	5-60
Power Strip Name	64
Power Strip Description	255
Power Association Group Name	255
Power Association Group Description	255
PortLog Prefix	64
PortLog Timestamp	0-99999

Appendix B: System Defaults

Field Type	Character Length
PortLog NFS Update	0-99999
PortLog In/Out Directory	64
SMTP Username	255
SMTP Password	128
SMTP Source address	64
Event Destination	64
NFS Directory	128
SNMP Community	64
SNMP Dest Port	1-65535
Login Inactive Expiration	0-65535
Login Retries	0-65535
Login Lockout Period	0-65535
Strong Password Min Length	8 - 15
Strong Password Max Length	15 - 64
Idle Timeout Period	0-65535

# Appendix C Certificates

## In This Chapter

Default SX Certificate Authority Settings .....	267
Installing Dominion SX Server Certificate for Netscape Navigator .....	267
Installing a Third-Party Root Certificate.....	270
Importing Certificates for LDAP .....	274

---

### Default SX Certificate Authority Settings

The Server Certificate generated in the SX must be installed in the browser in order for the browser to trust the Server Certificate.

Each time you access an SSL-enabled SX, you see a New Site Certificate window. You can accept this on a per-session basis or you can eliminate this window's appearance by accepting a session certificate permanently. The following steps will show how to install the SX's certificate into the browser's certificate store.

These steps must be performed for each SX to be accessed for each client browser that accesses the SX.

---

### Installing Dominion SX Server Certificate for Netscape Navigator

By installing the SX Server certificate in Netscape®, you can prevent the Security Alert pop-up from appearing whenever you access the SX. This step will have to be performed for each SX you wish to access from each client's browser.

---

#### Accept a Certificate (Session-Based)

Upon initial connection to a SX, a certificate warning pop-up appears. By default, this certificate is signed by the local SX's CA as described above and you will have to accept this certificate to continue. To eliminate the appearance of the warning pop-up for this SX permanently, you must install the server certificate in your browser. This procedure is described in the section that follows.

---

#### Install the Dominion SX Server Certificate in Netscape Navigator

1. Launch Netscape Navigator® and connect to the IP address of the SX. The "Web Site Certified by an Unknown Authority" page appears.

2. Select Accept this certificate permanently and click OK.
3. Select OK on the Security Warning window
4. The Raritan default certificate is now accepted on this computer.

---

### **Remove an Accepted Certificate**

Removing a previously accepted certificate from a SX uses the same process whether removing a Raritan default certificate or removing a user-installed third-party certificate.

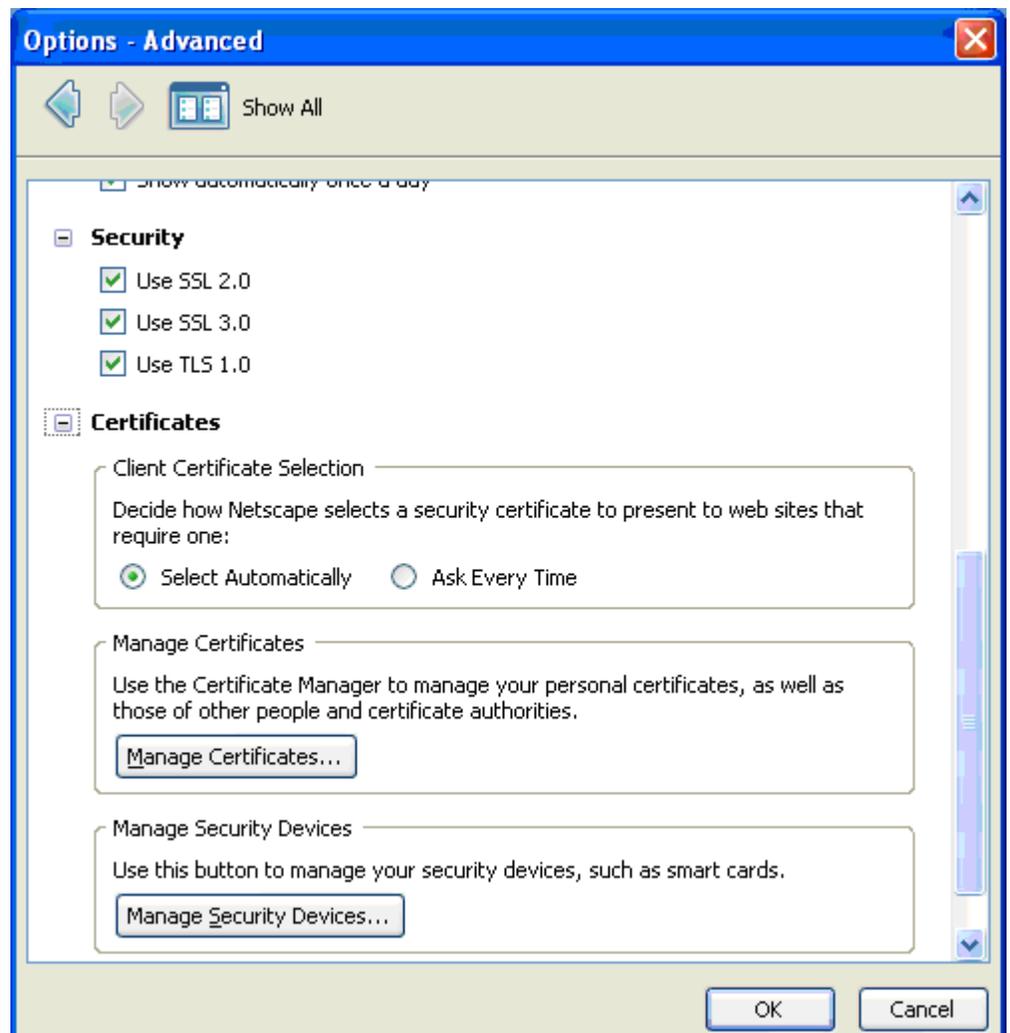
---

*Note: The SX does not use encrypted private keys. When removing encryption from the key, the SX uses a command such as `openssl rsa -in server.key -out server2.key` or `server2.key`.*

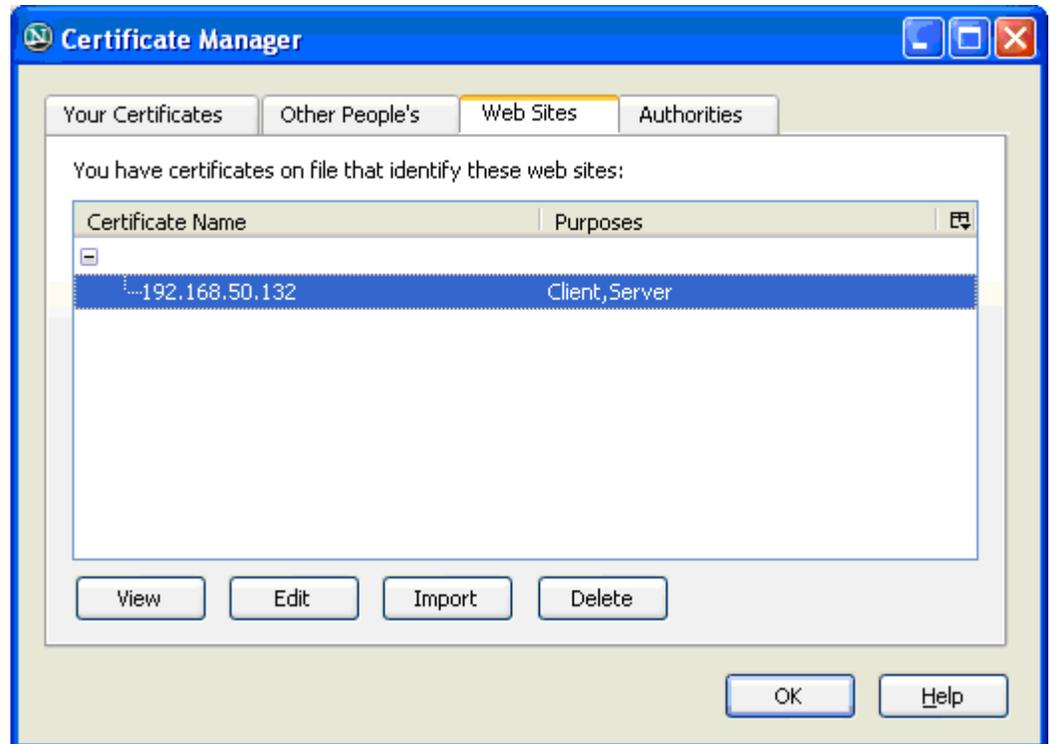
---

1. Choose Tools > Options.
2. Select Advanced panel and double-click the Certificates category.

3. In the Manage Certificates section, click the Manage Certificates... button to view the Certificate Manager.



4. Select the Web Sites tab, select the certificate name that is the common name of the IP address of the SX, and click Delete.



5. Click OK on the Delete Web Site Certificates window to confirm the deletion of the certificate.
6. On the left side of this page, locate Certificates, and click Web Sites.
7. Click OK on the Options Advanced Window.

---

## Installing a Third-Party Root Certificate

If you have installed a third-party certificate on the SX, you can get its corresponding root certificate from the Certificate Authority that provided you with a certificate. These instructions can be used for any of the CAs; this example uses Thawte.

The CA that provided you with a certificate will have a root certificate available for download. Root certificates are available on the CA web site; click on the links to download. Some of the popular CAs and their sites:

Thawte Digital Certificate Services

**<http://www.thawte.com/> <http://www.thawte.com/>**

VeriSign Incorporated

**<http://www.verisign.com/> <http://www.verisign.com/>**

---

*Note: Some CAs will provide the root certificate code in text format rather than providing a downloadable root certificate. If this occurs, select the root certificate code, copy it, and follow the steps outlined in the section Install the Raritan Root Certificate, then follow the steps outlined below.*

---

---

### **Install a Third-Party Root Certificate to Internet Explorer**

To install a third party certificate to Internet Explorer®, download the CA certificate and install it following the steps above in Install the SX Server Certificate In Internet Explorer.

---

### **Install a Third-Party Root Certificate to Netscape Navigator**

1. On the CA Web site, click on the root certificate link and the New Certificate Authority window appears. Click Next, and then click Next again.
2. The Certificate Fingerprint will appear, providing information about the CA and the root certificate you are downloading. It will look similar to the following window. Record the Signed by information and click Next.
3. Select the Accept this Certificate Authority for Certifying network sites checkbox. The second and third boxes are optional.
4. Click Next, and then click Next again. When prompted to type a name for the Certificate Authority, type the Signed by name that you recorded in Step 6.
5. Click Finish. The root certificate for this Certificate Authority is now installed for this computer.
6. If the root certificate has already been installed, the following error will appear and you must follow the steps below to remove the currently installed certificate.
7. Click the Security button in Netscape® or click on the lock icon in the lower left of the window to access the Security Information window.
8. Locate the Certificates section in the left panel and click Signers to display a list of root certificates currently installed.
9. Find the name of the CA whose certificate you are installing. There may be more than one listing for your CA. Select the listing with the same name as the certificate you are trying to install.
10. Click Delete and then click OK.
11. Return to the CA's Web site and try to download the root certificate again and follow steps 1 through 5 again.

---

### Generate a CSR for a Third Party CA to Sign

To have a third party CA certificate (for example, Verisign) installed on the SX rather than the internal CA on the SX signing the certificate, a Certificate Signing Request (CSR) must be generated by the SX to be signed. The third party CA will take this CSR and generate a Certificate. This certificate must be installed on the SX along with the CA's public key in order for this certificate to be enabled. This Certificate and key must then be installed onto the SX.

All GUI fields except the "Country" field accept spaces in their names without the need to put them in single quotes.

1. Choose Security > Certificate.
2. Click the Generate Certificate Signing Request radio button.

**Generate Certificate Signing Request**

**Bits:**  
1024

**Name:**  
mySX\_certificate

**Country:**  
BG

**State:**  
Sofia

**Locality:**  
Sofia

**Organization:**  
'Bianor Services'

**Unit:**  
DSX

**Email:**  
sx@bianor.com

3. Fill in parameters underneath the radio button (bits, name, and so forth), and click OK. Note that the email address is mandatory.

---

*Note: Spaces between words can be used in all fields without needing to use single quotes except the Country field.*

---

4. Click OK to generate a CSR.
5. Send the generated CSR to a third party CA to get it signed.
6. CA returns a Signed Certificate built from the CSR.

7. Install the certificate to SX.

 **Install User Certificate**

**IP Address:**  
10.0.0.189

**Login:**  
ani

**Password:**  
\*\*\*\*\*

**Remote Path:**  
/home/ani/ServerCert

**Remote File:**  
server.pem

8. Reboot the SX.

If the CSR is generated by an external source:

1. Generate a CSR for the SX by an external computer.
2. Send this CSR to the third party CA to get it signed.
3. CA returns a Signed Certificate built from the CSR.
4. Install the certificate to the SX.
5. Upload the private key received for this CSR to the SX.

 **Install User Key**

**IP Address:**  
10.0.0.189

**Login:**  
ani

**Password:**  
\*\*\*\*\*

**Remote Path:**  
/home/ani/ServerCert

**Remote File:**  
server.key

6. Reboot the SX.

---

### **Install Client Root Certificate**

In order for Client Certificates to be recognized as valid by the SX, the Root Certificate of the CA that signed the Client Certificates must be installed on the SX with the following steps:

1. Retrieve the CA's Root certificate used to sign the client certificates and place it on an accessible FTP server
2. Choose Security > SSL Client Certificates.
3. Select Install Certificate Authority.
4. Fill in the FTP parameters to retrieve the CA Root certificate.
5. Click OK.
6. Make sure the Enable SSL Client Certificate checkbox is selected.
7. Restart the SX for the settings to take place.

---

### **Install Client Certificate into Internet Explorer**

Installing client certificate into Internet Explorer® mostly follows the steps described in the following link:

<http://www.microsoft.com/technet/prodtechnol/ie/reskit/6/part2/c06ie6rk.msp?mfr=true>

---

## **Importing Certificates for LDAP**

The SX will properly add only binary encoded certificates to the local certdb. In order to import LDAP certificates, the certificates should be retrieved from the LDAP's server and placed on an FTP server from which the SX can retrieve them.

---

### **Retrieve LDAP Certificate via Access from HTTP Interface**

The following steps must be taken in order to insert the Retrieved Server certificate to SX from the GUI. The LDAPS Server certificate should be available on a valid FTP Server to which you know the authentication information.

1. Log into the SX as admin.
2. Click the Set tab.
3. Click the Remote Authentication button.
4. Click the LDAPS Certificate Settings link.
5. Fill in IP, username, password, and path to the LDAPS Certificate.

6. If the certificate is ASCII encoded, select ASCII. If it is a binary certificate file, select binary.
7. Enter a unique name for this certificate to be stored on the SX.
8. Click OK and the SX should retrieve the specified certificate file with supplied credentials.

---

### **Import Certificates from Windows XP**

Follow these steps to load the SX certdb with sufficient certificates to allow for LDAP connectivity:

1. Launch Internet Explorer®.
2. Type `https://<ldap server ip_addr>:636`.  
Click View Certificate in the name mismatch dialog box.
3. Click the Certification Path tab.
4. Select VeriSign/RSA Secure Server CA.
5. Click View Certificate in the name mismatch dialog box.
6. Click the Details tab.
7. Click Copy To File.
8. Click Next in the certificate import wizard box.
9. Select DER encoded Binary and click Next.
10. Complete the wizard to save ROOT\_BIN.cer in the FTP root.
11. Close all windows.

---

### Import Certificates from Dominion SX via CLI

A user with Administrator privileges can do the following to import certificates for LDAP.

Type the configuration command and issue the following commands:

```
Config > Authentication > LDAP > LDAPS >getservercert
ip <FTP Server ip_addr> login <FTP username> password
<FTP password> path / file ROOT_BIN.cer encode binary
name root_bin
```

The command will then display the certificate retrieved, and prompt you to insert the certificate if it can be retrieved as a valid certificate (as shown below).

Certificate:

Data:

Version: 1 (0x0)

Serial Number:

02:ad:66:7e:4e:45:fe:5e:57:6f:3c:98:19:5e:dd:c0

Signature Algorithm: PKCS #1 MD2 With RSA Encryption

Issuer: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US

Validity:

Not Before: Wed Nov 09 00:00:00 1994

Not After: Thu Jan 07 23:59:59 2010

Subject: OU=Secure Server Certification Authority, O="RSA Data Security, Inc.", C=US

Subject Public Key Info:

Public Key Algorithm: PKCS #1 RSA Encryption

RSA Public Key:

Modulus:

92:ce:7a:c1:ae:83:3e:5a:aa:89:83:57:ac:25:01:76:

0c:ad:ae:8e:2c:37:ce:eb:35:78:64:54:03:e5:84:40:

51:c9:bf:8f:08:e2:8a:82:08:d2:16:86:37:55:e9:b1:

21:02:ad:76:68:81:9a:05:a2:4b:c9:4b:25:66:22:56:

6c:88:07:8f:f7:81:59:6d:84:07:65:70:13:71:76:3e:

9b:77:4c:e3:50:89:56:98:48:b9:1d:a7:29:1a:13:2e:

4a:11:59:9c:1e:15:d5:49:54:2c:73:3a:69:82:b1:97:

39:9c:6d:70:67:48:e5:dd:2d:d6:c8:1e:7b

Exponent: 65537 (0x10001)

Fingerprint (MD5):

D4:1D:8C:D9:8F:00:B2:04:E9:80:09:98:EC:F8:42:7E

Fingerprint (SHA1):

DA:39:A3:EE:5E:6B:4B:0D:32:55:BF:EF:95:60:18:90:AF:D8:07:09

Signature Algorithm: PKCS #1 MD2 With RSA Encryption

Signature:

65:dd:7e:e1:b2:ec:b0:e2:3a:e0:ec:71:46:9a:19:11:

b8:d3:c7:a0:b4:03:40:26:02:3e:09:9c:e1:12:b3:d1:

5a:f6:37:a5:b7:61:03:b6:5b:16:69:3b:c6:44:08:0c:

88:53:0c:6b:97:49:c7:3e:35:dc:6c:b9:bb:aa:df:5c:

bb:3a:2f:93:60:b6:a9:4b:4d:f2:20:f7:cd:5f:7f:64:

7b:8e:dc:00:5c:d7:fa:77:ca:39:16:59:6f:0e:ea:d3:

b5:83:7f:4d:4d:42:56:76:b4:c9:5f:04:f8:38:f8:eb:

d2:5f:75:5f:cd:7b:fc:e5:8e:80:7c:fc:50

Certificate Trust Flags:

SSL Flags:

Valid CA

Trusted CA

Trusted Client CA

Email Flags:

Object Signing Flags:

Do you wish to add this certificate to the system database? (no/yes)

(default: no) yes

Adding certificate root\_bin to database...

# Appendix D Server Configuration

## In This Chapter

Microsoft IAS RADIUS Server .....	278
Cisco ACS RADIUS Server .....	281
TACACS+ Server Configuration .....	282
CiscoSecure ACS .....	282

---

## Microsoft IAS RADIUS Server

The Internet Authentication Service (IAS) is a Microsoft implementation of the Remote Authentication Dial-In User Service (RADIUS) protocol. The procedures in this section describe how to configure the SX to use an IAS server.

---

### Configure the SX to Use an IAS RADIUS Server

The tasks to set up the SX to use an IAS RADIUS server are:

- Configure a Primary Radius Server (and optional secondary Radius server).
- Configure a Radius port.
- Configure a secret (shared secret) that is matched in the IAS client configuration within IAS.

The following example shows a simple setup based on a new IAS installation.

---

*Note: If the IAS setup already exists, these instructions may not apply exactly as shown.*

---

### Enable IAS on the Server

1. On the IAS server, go to the Control Panel and launch Add or Remove Programs.
2. Click Add/Remove Windows Components.
3. Highlight Networking Services then click the Details... button.
4. Select the Internet Authentication Service checkbox and then click OK.
5. Click Next> and continue with the wizard steps.

### IAS Active Directory Access

If using a Domain Controller, set IAS to access the Active Directory® using the following steps:

1. Launch IAS (choose Start > All Programs > Administrative Tools > Internet Authentication Service).
2. Right-click on Internet Authentication Service (Local) and select Register Server in Active Directory.

---

*Note: See the following Microsoft URL for information about Active Directory: <http://support.microsoft.com/default.aspx?scid=kb;en-us;321051>*

---

### Add SX to the client list

1. From the Internet Authentication Service, right-click on RADIUS Clients and select New RADIUS Client.
2. Type a friendly name and the IP address of the SX.
3. Select the RADIUS Standard in the Client-Vendor drop-down menu, and type a Shared Secret that matches the SX configuration.

---

### Create an IAS Policy

This section describes the steps to create a policy to allow Radius users to access the SX. The example in this section requires two conditions: the client source IP address of the SX and that the UserID is a member of the SX User Group:

- NAS-IP-Address = Type the IP address of SX
- Windows-Group = SX User Group

---

*Note: If you have multiple SX units or different models of Dominion product family (DKX, DKSX or KX101), then using an appropriate condition to match (NAS-IP-Address) rule will help apply the correct policy for the appropriate Dominion unit.*

---

1. From Internet Authentication Service, right-click on Remote Access Policies and select New Remote Access Policy.
2. The New Remote Policy Wizard starts. Click Next>.
3. Select the Set up a custom policy radio button and type a Policy name.
4. The Policy Conditions dialog appears. Click the Add... button.
5. Select the NAS-IP-Address name and click the Add... button. Type the IP address of the SX.
6. Type a second condition using the name Windows-Group and the value SX User Group. Click Next>.

7. Select the Grant remote access permission radio button.
8. Click Next>. The Profile dialog appears.
9. Click the Edit Profile... button.
10. Choose the Authentication tab. Deselect all other checkboxes select the Unencrypted authentication (PAP, SPAP) checkbox.

---

*Note: This version of SX does not support Challenge Authentication Protocol (CHAP).*

---

11. Click the Advanced tab. Remove Framed-Protocol.

---

*Note: Each policy has conditions that must be met. If the conditions are not met, then IAS goes to the next policy and examines the conditions.*

---

12. Click the Add... button. The RADIUS attributes list appears.
13. Select Filter-Id Name and click the Add button. Click Add in the Attribute values section. Type the attribute value: Raritan:G{Admin}.
14. Click OK.
15. The value in G{} is the name of a group locally on the SX, in this case the default Admin group.
  - The value can be Raritan:G{Admin}:D{1234567890} if you are using the dial back feature, where 1234567890 is the phone number for dial back.
  - The value Raritan:G{Admin} must match with the local group on the SX.
  - The SX comes from the factory with the default Admin group.
  - Additional user groups can be created on the SX by using the User Management>User Group option.
  - Appropriate port access and user class (Operator or Observer) can be defined. The group name should be specified in the Filter-Id attribute value accordingly in order to authorize the RADIUS user to access the SX.

16. Move the new policy so it appears as the first (top) policy in the Policy List.

---

*Note: If required, create a policy to allow dialup access to all users that are members of a group (Windows® may already have a default Policy in place to permit access by any user with Dial In enabled, so this new policy would be optional. If you want to use a new Policy, ensure that it appears above the default policy).*

---

17. Ensure that the service is started.

18. Ensure that the Active Directory®/Local account for the user has Dial In access enabled in their user profile. If the Windows 2000® Domain server is in Native Mode and IAS is registered with the Active Directory, you can set the User Profile > Dial In setting to use Remote Access Policies.

---

## Cisco ACS RADIUS Server

The Cisco Access Control Server (ACS) is another authentication solution supported by the SX. For the SX to support RADIUS, both the SX and the user information must be added into the RADIUS configuration.

---

### Cisco ACS 5.x for RADIUS Authentication

If you are using a Cisco ACS 5.x server, after you have configured the SX for RADIUS authentication, complete the following steps on the Cisco ACS 5.x server.

*Note: The following steps include the Cisco menus and menu items used to access each page. Please refer to your Cisco documentation for the most up to date information on each step and more details on performing them.*

---

- Add the SX as a AAA Client (**Required**) - Network Resources > Network Device Group > Network Device and AAA Clients
- Add/edit users (**Required**) - Network Resources > Users and Identity Stores > Internal Identity Stores > Users
- Configure Default Network access to enable CHAP Protocol (**Optional**) - Policies > Access Services > Default Network Access
- Create authorization policy rules to control access (**Required**) - Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
  - Dictionary Type: RADIUS-IETF
  - RADIUS Attribute: Filter-ID
  - Attribute Type: String
  - Attribute Value: Raritan:G{Serial\_Admin} (where Serial\_Admin is group name created locally on SX). Case sensitive.
- Configure Session Conditions (Date and Time) (**Required**) - Policy Elements > Session Conditions > Date and Time
- Configure/create the Network Access Authorization Policy (**Required**) - Access Policies > Access Services > Default Network Access>Authorization

## TACACS+ Server Configuration

The SX has the capability to use Terminal Access Controller Access-Control System Plus (TACACS+) for authentication services.

The SX requires a new service to be added and two argument-value pairs to be returned by the server. The new service is called dominionsx. The valid authorization parameter is user-group. If this user is to have a modem dialback, the valid dialback parameter is user-dialback.

- user-group: Specifies the user group name that matches with local group on SX. Group name specified for this attribute on TACACS+ Must exactly (case sensitive) match with group name on SX or else authentication for TACACS+ user on SX will fail.
- user-dialback: Specifies the user's modem dialback number. If the SX has dialback enabled, this phone number will be used to call back the user.

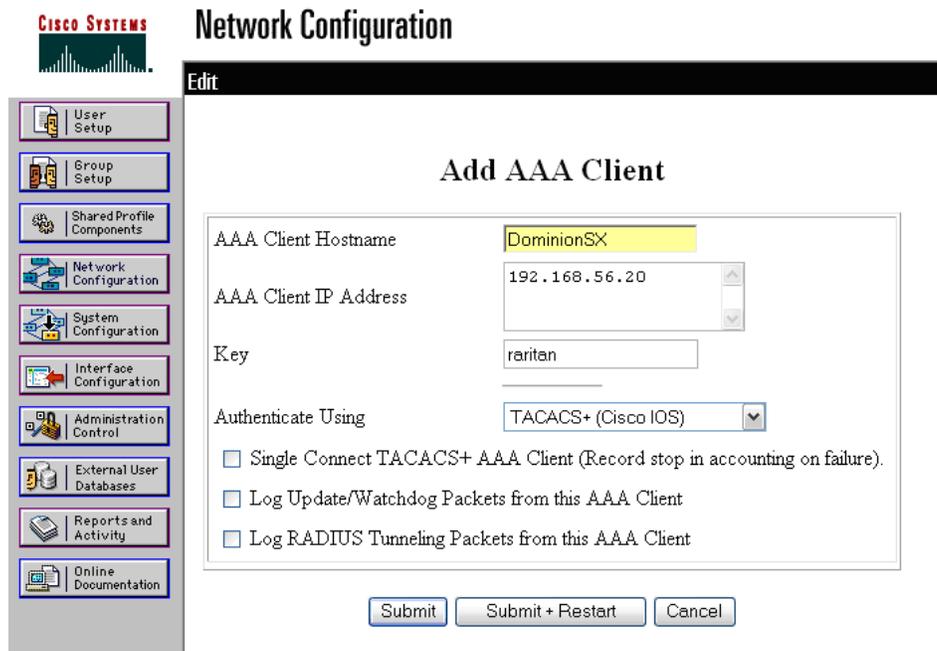
## CiscoSecure ACS

These instructions are written for CiscoSecure ACS version 3.2.

*Note: See the following URL:*

[http://cisco.com/en/US/products/sw/secursw/ps2086/products\\_user\\_guide\\_e\\_chapter09186a008007cd49.html#12231](http://cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_e_chapter09186a008007cd49.html#12231)

1. Add SX as a client on Cisco ACS TACACS+.



2. Select Interface Configuration.

**CISCO SYSTEMS** Interface Configuration

Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration**
- Administration Control
- External User Databases
- Reports and Activity
- Online Documentation

[User Data Configuration](#)  
[TACACS+ \(Cisco IOS\)](#)  
[RADIUS \(IETF\)](#)  
[Advanced Options](#)

[Back to Help](#)

3. Select TACACS+ (Cisco IOS).
4. Add dominionsx service under the heading New Services.

**CISCO SYSTEMS** Interface Configuration

Edit

**TACACS+ (Cisco)**

TACACS+ Services

User	Group	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

New Services

	Service	Protocol
<input checked="" type="checkbox"/>	dominionsx	
<input type="checkbox"/>		

- When adding or editing a user or group, the dominionsx service will appear under the heading TACACS+ Settings. The service can be enabled per user or per group by selecting the dominionsx and Custom Attributes checkboxes. Add the attributes (user-type) and the appropriate values to the text box.

*Note: The value for the user-group attribute is case sensitive; ensure that it matches exactly the same as the local group name on the SX.*

**CISCO SYSTEMS**

### User Setup

Failed attempts exceed:  
5  
Failed attempts since last successful login: 0  
 Reset current failed attempts count on submit

---

#### TACACS+ Settings

**dominionsx**  
 Custom attributes  
user-group=Admin

---

#### IETF RADIUS Attributes

[011] Filter-Id

# Appendix E Modem Configuration

## In This Chapter

Client Dial-Up Networking Configuration .....	285
Windows NT Dial-Up Networking Configuration.....	285
Windows 2000 Dial-Up Networking Configuration .....	288
Windows Vista Dial-Up Networking Configuration .....	292
Windows XP Dial-Up Networking Configuration.....	293

---

## Client Dial-Up Networking Configuration

Configuring Microsoft Windows® Dial-Up Networking for use with SX allows configuration of a PC to reside on the same PPP network as the SX. After the dial-up connection is established, connecting to a SX is achieved by pointing the web browser to the PPP Server IP. Modem installation guidelines are provided for the following client based systems:

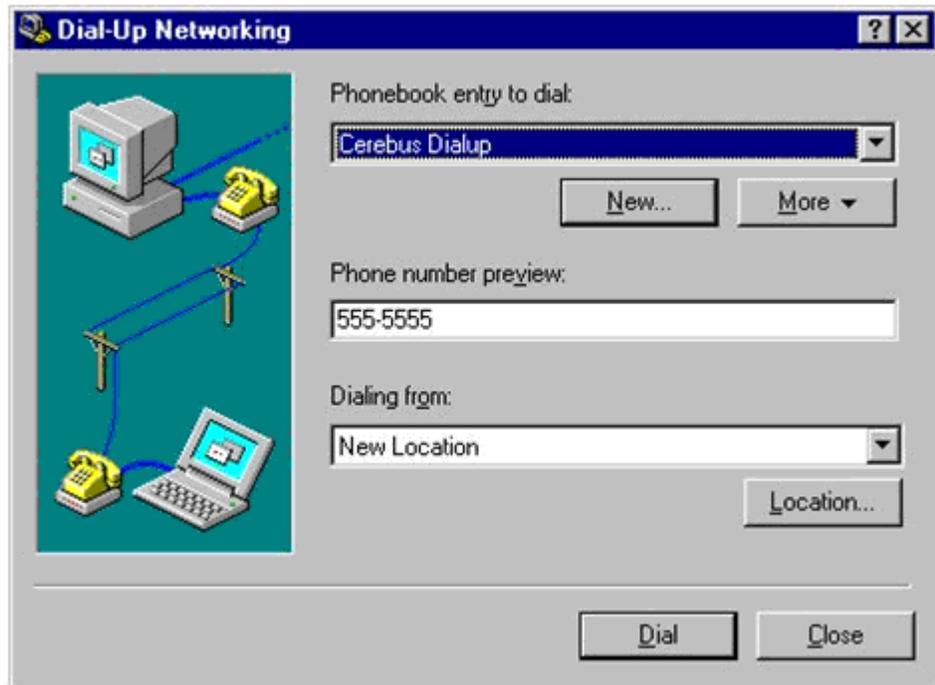
- Windows 7®
- Windows XP® operating system
- Windows Vista®

---

## Windows NT Dial-Up Networking Configuration

1. Choose Start > Programs > Accessories > Dial-Up Networking.

2. Click New in the Dial-Up Networking dialog. The New Phonebook Entry dialog allows you to configure the details of this connection.



3. Click the Basic tab and complete the following fields:
  - Entry name - Name of the SX connection
  - Phone number - Phone number of the line attached to the SX

- Dial using - Modem being used to connect to SX; if there is no entry here, there is no modem installed in your workstation

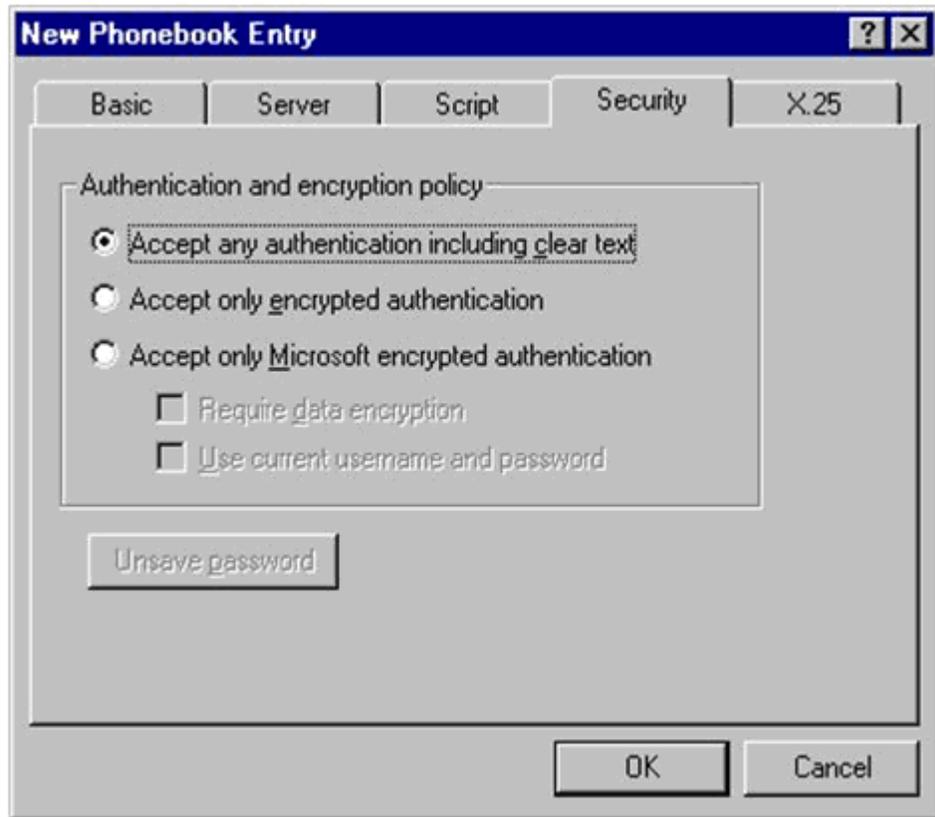
The screenshot shows a Windows-style dialog box titled "New Phonebook Entry". It has five tabs: "Basic", "Server", "Script", "Security", and "X.25". The "Basic" tab is active. The fields are as follows:

- Entry name: Cerebus Dial-Up
- Comment: Cerebus
- Phone number: 555-5555 (with an "Alternates..." button)
- Use Telephony dialing properties:
- Dial using: US Robotics 56k Sportster Modem (with a "Configure..." button)
- Use another port if busy:

At the bottom right, there are "OK" and "Cancel" buttons.

4. Click the Security tab. The Security section allows you to specify the level of security to use with the modem connection. When connecting to the SX, security is provided by SSL/ with RC4 encryption, therefore no dial-up security is required.

5. Click the "Accept any authentication including clear text" radio button.



6. Click OK to return to the main Dial page.
7. Click Dial. See the Windows NT® Users Guide if you receive any error messages.

---

## Windows 2000 Dial-Up Networking Configuration

1. Choose Start > Programs > Accessories > Communications > Network and Dial-Up Connections.

2. Double-click the Make New Connection icon when the Network and Dial-Up Connections window appears.



3. Click Next and follow the steps in the Network Connection Wizard dialog to create custom dial-up network profiles.

- Click the Dial-up to private network radio button and click Next.

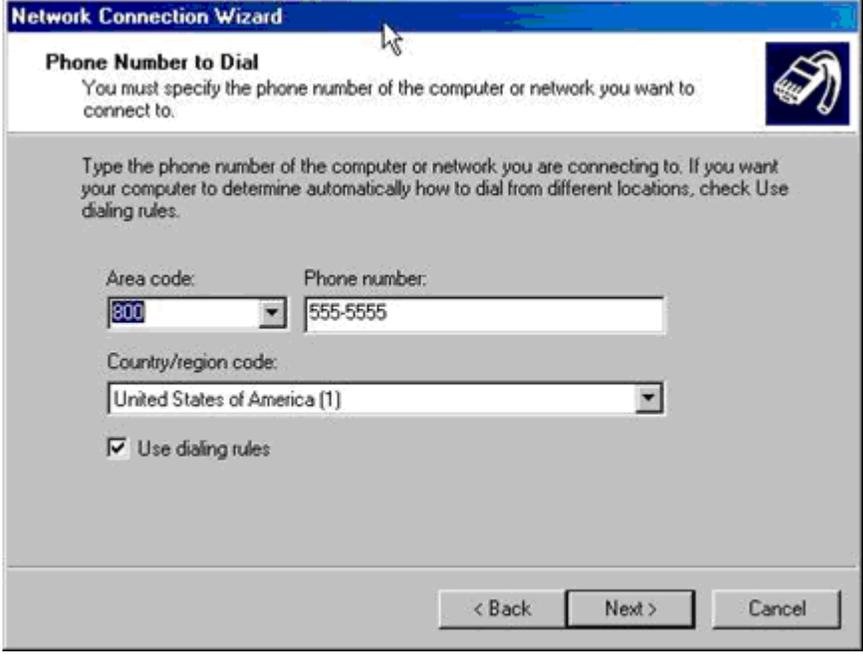


- Select the checkbox before the modem that you want to use to connect to the SX and then click Next.



- Type the area code and phone number you wish to dial in the appropriate fields.

- Click the Country/region code drop-down arrow and select the country or region from the list.



The screenshot shows the 'Network Connection Wizard' dialog box, specifically the 'Phone Number to Dial' step. The title bar reads 'Network Connection Wizard'. Below the title bar, the section is titled 'Phone Number to Dial' with a sub-header 'You must specify the phone number of the computer or network you want to connect to.' and a modem icon. The main text says: 'Type the phone number of the computer or network you are connecting to. If you want your computer to determine automatically how to dial from different locations, check Use dialing rules.' There are two input fields: 'Area code:' with a dropdown menu showing '800' and 'Phone number:' with a text box containing '555-5555'. Below these is a 'Country/region code:' dropdown menu showing 'United States of America (1)'. A checkbox labeled 'Use dialing rules' is checked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Click Next. The Connection Availability dialog appears.
- Click the Only for myself radio button in the Connection Availability dialog.



The screenshot shows the 'Network Connection Wizard' dialog box, specifically the 'Connection Availability' step. The title bar reads 'Network Connection Wizard'. Below the title bar, the section is titled 'Connection Availability' with a sub-header 'You may make the new connection available to all users, or just yourself.' and a modem icon. The main text says: 'You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.' There are two radio buttons under the heading 'Create this connection:'. The first is 'For all users' and is selected. The second is 'Only for myself'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

10. Click Next. The Network Connection has been created.
11. Type the name of the Dial-up connection.
12. Click Finish.
13. Click Dial to connect to the remote machine when the Dial dialog appears. A dialog indicating that a successful connection has been established will appear.

Consult the Windows 2000® Dial-up Networking Help if you receive any error messages.

---

## Windows Vista Dial-Up Networking Configuration

1. Click Start and then click Network. The Network window opens.
2. Select Network and Sharing Center at the top of the window. The Network and Sharing Center window opens.
3. Select "Set up a Connection or Network".
4. Select "Set up a dial-up connection". The "Set up a dial-up connection" dialog appears.
5. Enter the dial-up number.
6. Enter your username and password.

---

*Note: In order to access the SX, the username and password cannot use a \ (backslash).*

---

7. Click Connect.



The screenshot shows the 'Set up a dial-up connection' dialog box in Windows Vista. The title bar reads 'Set up a dial-up connection'. The main content area is titled 'Type the information from your Internet service provider (ISP)'. It contains the following fields and options:

- Dial-up phone number:** A text input field with a [Dialing Rules](#) link to its right.
- User name:** A text input field.
- Password:** A text input field with a  **Show characters** checkbox below it and a  **Remember this password** checkbox below that.
- Connection name:** A text input field.
- Allow other people to use this connection**  
This option allows anyone with access to this computer to use this connection.
- [I don't have an ISP](#) link at the bottom left.

At the bottom right, there are two buttons: **Connect** and **Cancel**.

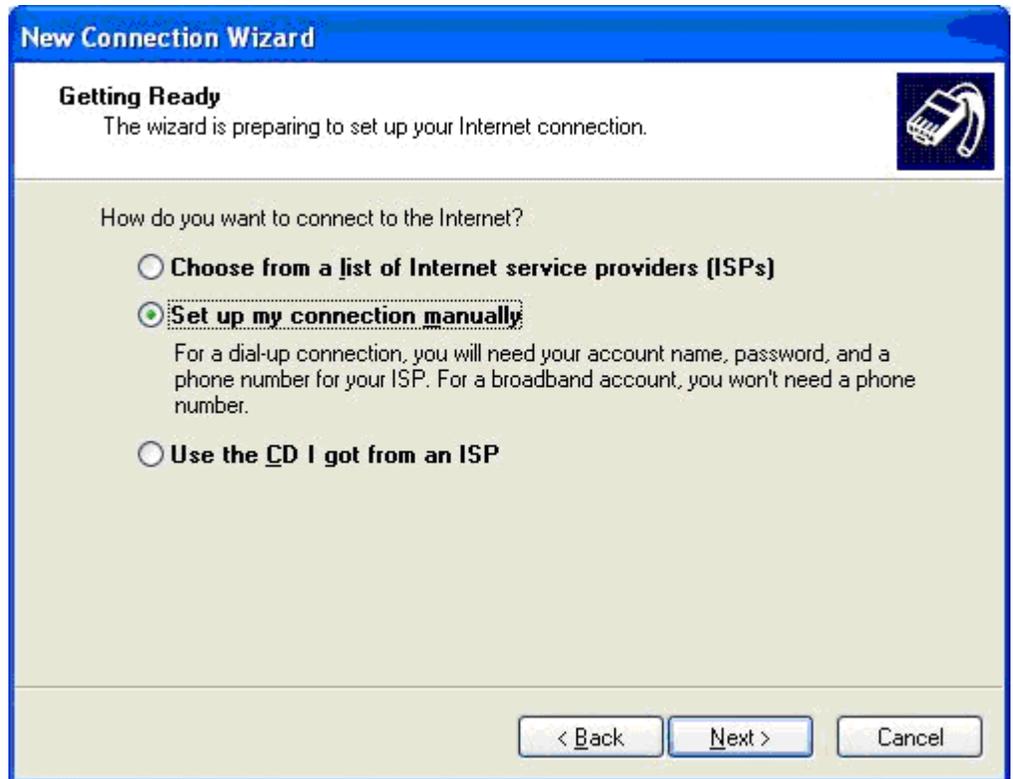
---

## Windows XP Dial-Up Networking Configuration

1. Choose Start > Programs > Accessories > Communications > New Connection Wizard.
2. Click Next and follow the steps in the New Connection Wizard to create custom dial-up network profiles.
3. Click the Connect to the Internet radio button and click Next.



4. Click the "Set up my connection manually" radio button and click Next.



5. Click the "Connect using a dial-up modem" radio button and click Next.



6. Type a name to identify this particular connection in the ISP Name field and click Next.

**New Connection Wizard**

**Connection Name**  
What is the name of the service that provides your Internet connection?

Type the name of your ISP in the following box.

ISP Name

DominionKSX

The name you type here will be the name of the connection you are creating.

< Back   Next >   Cancel

7. Type the phone number for the connection in the Phone number field and click Next.



The screenshot shows a Windows-style dialog box titled "New Connection Wizard". The main heading is "Phone Number to Dial" with a sub-question "What is your ISP's phone number?". A small icon of a modem is in the top right corner. Below the heading, it says "Type the phone number below." followed by a text input field labeled "Phone number:" containing the text "8888888888". A paragraph of instructions follows: "You might need to include a '1' or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct." At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

8. Type your ISP information. Type the user name and password in the appropriate fields, and retype the password to confirm it.

9. Select the checkbox before the appropriate option below the fields and click Next.



The screenshot shows a Windows XP-style dialog box titled "New Connection Wizard". The main heading is "Internet Account Information". Below the heading is a sub-heading "Internet Account Information" and a note: "You will need an account name and password to sign in to your Internet account." To the right of this text is a small icon of a modem. Below the note is a paragraph of instructions: "Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)" There are three input fields: "User name:" with the text "admin", "Password:" with ten dots, and "Confirm password:" with ten dots. Below these fields are two checkboxes: the first is "Use this account name and password when anyone connects to the Internet from this computer" and the second is "Make this the default Internet connection". At the bottom right of the dialog are three buttons: "< Back", "Next >", and "Cancel".

10. Click Finish.
11. Click Dial to connect to the remote machine when the Dial dialog appears. A dialog indicating that you connected successfully appears. If you get any errors, consult Windows XP® Dial-up Networking Help.

---

*Note: The maximum modem speed connecting to the SX is 33,600 bps, as it is a Linux® default limitation.*

---

# Appendix F Accessing a PX2 from the SX

## In This Chapter

Overview .....	299
Connecting the SX to the PX2 Serial Port .....	299
Connecting the SX to the PX2 FEATURE Port .....	300

---

### Overview

The SX provides the following options when connecting a PX2 to a SX:

- Connecting the SX to the PX2 Serial port to connect to and access the PX2.

In this configuration, access to the PX2 is done through the PX2 CLI.

- Connecting the SX to the Feature port on the PX2.

In this configuration, the PX2 is managed from the SX interface like any other powerstrip. See **Power Control** (on page 229).

See the **PX2 Help** for information on using the PX2 device.

---

### Connecting the SX to the PX2 Serial Port

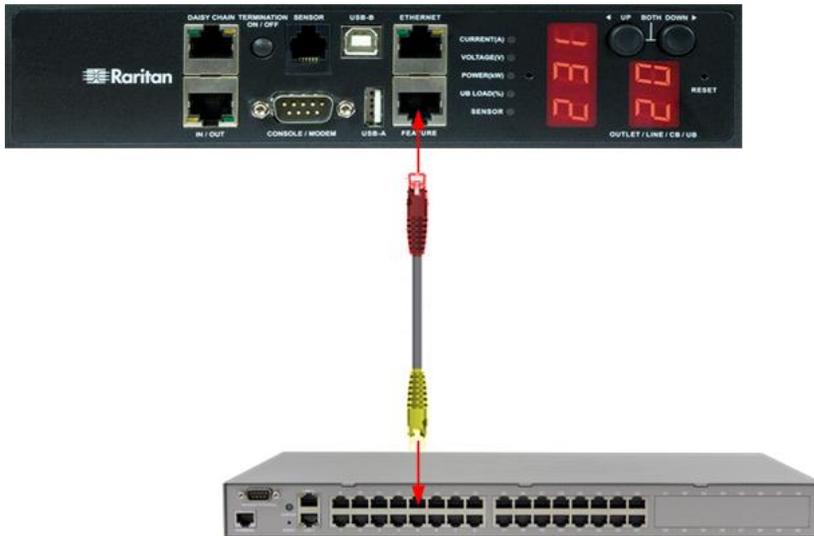
In this configuration, after the PX2 is connected to the SX, access to the PX2 is done through the PX2 CLI.

► **To connect the SX to the PX2:**

1. Connect the ASCSDB9F adapter to the PX2 DB9 console/modem port.
2. Plug a Cat5 cable into the ASCSDB9F adapter and the other end into an RJ45 Serial port on the SX.



3. Power on the PX2. You can now add the PX2 as a managed powerstrip to the SX.



# Appendix G Troubleshooting

## In This Chapter

Page Access.....	302
Firewall .....	303
Login.....	304
Port Access .....	304
Upgrade.....	305
Events Not Captured in Event Log .....	306
Modem.....	306
SSH Connection .....	306
iptables --list Hanging .....	307
Display Issue with Japanese Characters when Using Teraterm 3.1 .....	307
Lines are Overwritten after Column 80 in Linux .....	308
AIX Terminal Settings Not Displaying Correctly .....	308

---

## Page Access

Problem	Solution
Cannot login - what are factory defaults? (only for SX units running firmware version 2.5 or higher)	username: admin (all lower case) password: raritan (all lower case)  Check multiple login per user status. If disabled and there is already a session established opening anew one fails.
Cannot login - non defaults.	Check Local Authentication status. If it is not enabled only remote users may login.
Server Unreachable	If a unit appears to be unreachable by a given browser, run through the following troubleshooting list: <ul style="list-style-type: none"> <li>▪ Verify that the unit is powered on.</li> <li>▪ Verify that the unit is properly connected to a network.</li> <li>▪ Ping the unit from a computer on the same network to ensure that network communication with the unit occurs.</li> <li>▪ Should the ping fail, contact your network administrator. There may be a problem with your network configuration that is preventing communication with the unit.</li> <li>▪ Should the ping succeed, consult the following topics.</li> </ul>
DNS Error/Server Unreachable	When attempting to connect to the SX URL using Microsoft IE, a web page may appear indicating a DNS

Problem	Solution
	<p>error and reading that the server is unreachable.</p> <p>Remove any installed SX certificates and restart the browser.</p>
Unsupported Encryption	<p>The unit supports only 128-bit SSL encryption.</p> <p>In Internet Explorer®, view Help &gt; About Internet Explorer and determine the maximum SSL bit strength for the browser. If it is not at the desired strength, it is recommended that the browser be upgraded.</p> <p>In Netscape®, view Communicator &gt; Tools &gt; Security Info &gt; SSL v3.0 Configuration and ensure that 128-bit SSL is supported</p>
Number of Users Exceeded	<p>The unit has a security measure that allows only a specific number of login pages to be authenticated at any given time. Should this number be reached when attempting to login to the unit, a pop-up window displays indicating that the maximum number of users is exceeded. This is normal behavior for the unit.</p> <p>Wait for a few minutes and attempt to login again. You may need to refresh or &lt;Shift+Refresh&gt; your browser to successfully log in.</p>

---

## Firewall

Problem	Solution
Unable to Access the Web Page	<p>Firewalls must allow access on port 80 (for http) and 443 (for https) for the unit to operate through a firewall.</p> <p>Contact your system administrator and request port 80 and 443, or other custom configured ports for access.</p>
Login Failure	<p>Firewalls must be configured to allow connections using the SX configurable port network parameter (Default 51000). If the firewall does not allow these connections, the applet indicates that the login has failed.</p> <p>Contact your system administrator and request that connections be allowed on the configurable port.</p>

Problem	Solution
SSL Security Warnings	<p>The unit embeds its Internet Address (IP) in its SSL certificate. Should the firewall perform Network Address Translation (NAT), the SSL certificate will not match the IP address recognized by the browser generating a security warning.</p> <p>This is normal behavior.</p> <p>The warning message does not affect operation of the unit.</p>

---

## Login

Problem	Solution
Login Failure	<p>To provide additional security, the unit login page expires after three minutes. Therefore, all login attempts after this time period will fail. Reload the browser to reset this timer.</p> <p>Hold down the SHIFT key and click Reload in your browser. This will refresh the login page from the unit itself (not from a local cache) and allow login to the unit.</p>
RADIUS Users	<p>The unit can be configured to support RADIUS authentication. Any user not defined as a local user is considered to be a RADIUS user when RADIUS is enabled.</p> <p>If the RADIUS server is not reachable for user authentication for any reason, the unit will not allow the user to log in until the unit receives the result of the authentication request from the RADIUS server.</p> <p>Authentication may take up to 20 seconds. Be patient and wait until either the user successfully logs in, or the Authentication Denied message is displayed.</p>

---

## Port Access

Problem	Solution
Port Access Refresh	<p>The unit does not automatically refresh the Port Access list. It is refreshed only when the user clicks Port Access. Therefore, it is possible that a user will have permissions revoked and these changes will not be visible on the port access page until the Port Access button is activated.</p> <hr/> <p><b>You must log out and log in again for the new restriction to be applied. Then the restricted ports are invisible.</b></p> <hr/>

Problem	Solution
	Whenever possible, it is recommended that Administrators not change port access rights to a user who is already logged in to the unit.

## Upgrade

Problem	Solution
FTP - Server Unreachable	<p>If FTP server specified in the upgrade panel is unreachable or incorrect, the upgrade process halts until a response is received from the FTP server or until a timeout occurs.</p> <p>Wait and allow the FTP Server Unreachable message to appear.</p>
FTP - File Not Found	<p>The unit requires a package of upgrade files to be in the directory specified by the upgrade path. This package must have all included files and an upgrade.cnf file. Should this file not exist, or if the contents of the file are not in the indicated places, the File Not Found message will appear.</p> <p>Verify that the upgrade package is in the correct directory and confirm the upgrade path and IP address of the FTP server.</p> <p>If the upgrade still fails, reinstall the upgrade package and begin again.</p>
Insufficient Partition Size	<p>The latest 3.1.0.5.7 firmware is specifically applicable to SX models - DSX16 and DSX32 only (purchased before August 2004). This version also supports the use with CC-SG 3.1 (CommandCenter SecureGateway) or higher.</p> <p>Note that the attempt to upgrade firmware to the latest 3.1.0.5.7 version is aborted if the SX is detected with less than 32mb partition size. Then the upgrade will not be performed, and the unit's operation will not be impacted. The unit will auto restart after the upgrade is attempted. Following screen shots exhibit a sample upgrade attempted for such unit (IP Address for the unit is 10.0.13.182).</p> <p>(See the figures shown below for details.)</p>

Problem	Solution
Upgrade failed in dual-LAN units	While upgrading dual-LAN units from 2.5.x versions, an error message appears stating "The upgrade has failed. Check your upgrade directory and/or your connections, and try again.". (See the figure below for details.) In order to properly complete the upgrade, do not reboot the unit when the message appears, but re-apply the

Problem	Solution
	upgrade pack again.

---

## Events Not Captured in Event Log

The `eventlogfile` command can fail to be captured in the SX event log for three possible reasons:

- The log file size is set to greater than 10000000
- The log file size is set to less than 1024
- Saving the event to the event log file causes the log file size to exceed 50% of the available flash memory on the SX. SX does not allow this to occur.

To fix the problem, set the event log file to save at a smaller file size.

Note that each SX model has a different amount of flash memory available. Use the log file sizes that can cause failures described here as your guidelines when setting the event log file size.

---

## Modem

Problem	Solution
Login Failure	<p>The unit supports Web-browser access through the modem at connection speeds of 28.8K bps or greater. If the baud rate is insufficient, the user may be unable to log in to the unit via the modem.</p> <p>28.8K bps minimum connection speed is recommended for browser-based modem authentications (login). For CLI-based access, using SSH or Telnet, speed as low as 9600bps is adequate.</p>

---

## SSH Connection

Problem	Solution
SSH Access to SX from a client running the Windows Vista® operating system failed to connect.	<p>There may be a problem experienced by some users of Vista's Enterprise (and Business) edition with SX where the SSH window starts and fails to open. This is independent of the SX firmware version and does not require an upgrade of SX firmware to resolve.</p> <p>This problem seems to stem from the Vista's implementation of</p>

Problem	Solution
	<p>TCP auto tuning.</p> <p>Vista's Enterprise (and Business) editions utilize an aggressive scaling factor, which causes issues in packet segmentation, leading to SSH handshake messages being split apart and connection to never complete. The problem with Vista, is what Vista is doing when it sees that the SX cannot support the window scaling size of 8. Microsoft has described this problem at <a href="http://support.microsoft.com/kb/929868/">http://support.microsoft.com/kb/929868/</a> <a href="http://support.microsoft.com/kb/929868/">http://support.microsoft.com/kb/929868/</a>. SX cannot support a window scaling of 8 at all, because there is insufficient memory to support this level of packet buffering. When this scaling factor is shrunk or disabled entirely, the SSH handshaking completes correctly and the connection can be established.</p> <p>To perform this on vista, run a cmd.exe shell at an elevated admin level and execute the following command:</p> <pre>netsh interface tcp set global autotuninglevel=highlyrestricted</pre> <p>- Or -</p> <pre>netsh interface tcp set global autotuninglevel=disable</pre>

---

### iptables --list Hanging

If iptables --list hangs, it may be because the current rules are preventing access to the DNS server from the SX. Execute iptables -n --list to prevent DNS lookups from hanging this command.

---

### Display Issue with Japanese Characters when Using Teraterm 3.1

When connecting to a SX serial port via Teraterm 3.1 and then setting the terminal language to Japanese (ja\_JP:UTF8), the characters are not displayed correctly. To avoid this issue, use RSC or Putty.

---

## Lines are Overwritten after Column 80 in Linux

The default Linux® terminal display is set up for 80 columns, while RSC can be configured to have a different number of columns. If the RSC is configured to a different column number than the terminal, the last line in the columns may be overwritten when you perform a carriage return at the end of the last line.

To avoid this, set the default display columns in RSC to the same value as the terminal, or execute 'stty cols <numberofcols>' on the terminal.

---

## AIX Terminal Settings Not Displaying Correctly

If you encounter a display issue where the AIX terminal settings do not match up with the rows and columns in the RSC interface or the SSH terminal, do the following:

- Connect from the terminal window and execute the `stty rows <X>` command on the AIX shell

where <X> is the number of rows visible on the RSC or SSH terminal.

# Appendix H Frequently Asked Questions

## In This Chapter

FAQs.....	310
-----------	-----

## Chapter 14

### FAQs

Questions	Answers
How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
Why do I get a "This page contains secure and insecure items" prompt when using IE6?	This message may or may not be displayed, depending on the settings of IE6.
Why do I get an "Invalid certificate message" when using some browsers?	The Certificate Authority (CA) used by Raritan, Inc. may not be on the CA list of the browser.
What is the purpose of the Disable Local Authentication option?	For security reasons, some users do not want to allow any locally authenticated users to log into the Dominion SX unit. This option allows only for remotely authenticated users to log into the Dominion SX unit. This option should only be enabled AFTER remote authentication has been successfully tested and configured.
When I Disable Local Authentication, how come I cannot log into the Dominion SX unit?	<p>This is because of a couple of reasons:</p> <ul style="list-style-type: none"> <li>• A valid remote authentication source has not been entered</li> <li>• The remote authentication source is not reachable</li> <li>• The Disable Local Authentication option should only be enabled AFTER remote authentication has been successfully tested and configured</li> </ul>
Why do I lose connectivity to the Dominion SX unit after resetting it to factory default?	By default the unit in factory reset mode enables DHCP to get an IP address. If there is no DHCP server, it will reset to the IP address 192.168.0.192 with the username "admin" and password "raritan".

Questions	Answers
How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
What settings will be lost when restoring a unit to factory default?	All user-entered settings: usernames, passwords, all networking parameters – including IP address, security profiles, firewall rules, all services, TCP port numbers for services, idle logout timer, strong password rules.
Why does the Device disconnect indication not work with all my devices and servers?	Device disconnect indication requires both hardware (RS232) control signal support, and the right serial cabling to work. If either of these is missing, device disconnect indication cannot correctly track the loss of connection to a serial device. Most, but not all, servers and devices support these control signals.
Why does my device show "Down" in the port access menu on the GUI and the CLI, but I can still log into it?	If a device is configured for device disconnect indication, but the device cannot support the control signal or (RS232) serial cabling is not correctly made, the device will indicate "Down" on the Port access screen (GUI) and on the CLI, but it can may still be accessible when connected. Disable the device disconnect indication option to show default indication that the device is "Up".
How many lines can I cut and paste with the Dominion SX?	With SX release 3.0, this user-configurable and can be set up to copy-paste an industry-leading 9999 lines.
Where can I get a copy of the MIB for Dominion SX?	The SX MIB is available from the SX User Interface on the GUI SNMP configuration page. Also from the Firmware, Software and Product Documentation page for the SX: <a href="http://www.raritan.com/support/dominion-sx">www.raritan.com/support/dominion-sx</a>
With Dominion SX release 3.0 or higher, do I still need to type dominion before I get the username and password prompt using SSH/Telnet?	No. Beginning with release 3.0, enter the username in the "Login as:" or Username prompt.

Questions	Answers
<p>How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?</p>	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
<p>When I SSH into Dominion SX, I am unable to log in, even when I use a local account that I know works through the web/GUI interface.</p>	<p>[Only applied to firmware releases 2.1 though 2.5] The initial login name for Dominion SX over SSH interface is dominion (no password). Once this account is accessed you will see the "Welcome to Raritan Dominion Server" message and be prompted to enter a username. At this prompt, type the account that exists locally on the SX or the remote account (this assumes that the SX unit is configured with remote authentication information).</p>
<p>My Dominion SX has just been configured with a network address and I can successfully ping the SX IP, but when I try to access it using a Web browser, the message reads "Page cannot be found or server error, please contact System Administrator".</p>	<p>Check your Web browser settings and confirm that a proxy server is being used. If so, click on the checkbox to 'Bypass local addresses or configure DSX IP in the exception list.' Next, make sure the Web browser has 128-bit cipher strength. From the Help menu, click on "About" to find this information.</p>
<p>When I select the "Send Break" option from the Emulator menu in Raritan Console (on my DSX), it does not send a break to my Sun server. What could be wrong and how can I address it?</p>	<p>If the SUN machine does not respond to the break signal, verify that the line 'KEYBOARD_ABORT=disable' is commented out in the /etc/default/kbd file (on the SUN machine). If this line is not commented out, it will disable a keyboard abort sequence; comment out this line to enable the sequence.</p>

Questions	Answers
How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
Is there any software requirement for PCs connected to Dominion SX?	<p>Depends. For access using a web-browser, the Dominion SX does not require any software to be loaded on the client; the browser does have to be Java-enabled. It is 100% operating system independent. When using an SSH/Telnet client, the customer has to provide an SSH/Telnet client. In some operating systems, like Linux®, an SSH client is included in the distribution. Also, OpenSSH.org has an SSH client.</p>
How can I consolidate the sites where I have a Dominion SX installed?	<p>Raritan's CommandCenter® Secure Gateway is designed specifically to provide centralized management. It is the ideal solution if you are looking to consolidate management of devices such as Dominion SX and other Raritan network-based products.</p>
Is the Ethernet port on the Dominion SX unit 10/100Mbps auto sensing?	<p>Yes.</p>
Can the network port(s) on the Dominion SX be set to 100Mbps Full-Duplex?	<p>Yes.</p>
Does Dominion SX support RS422 and RS485?	<p>No. Currently Dominion SX supports only asynchronous RS232 (also commonly called serial, even though serial is a broad term that covers more than RS232). RS 422 and RS485 are used in industrial automation and other markets. Dominion SX is currently designed for connection to serially managed servers and other devices typically found in the data-center and server rooms. This includes serially controlled power strips like Raritan's line of remote power control units.</p>
Do I need to be a UNIX expert to install Dominion SX?	<p>Dominion SX is the easiest to install of all the secure console servers on the market. From power-up, typical time for installation is less than 3 minutes, with no need to edit files and use the command-line. Dominion SX does not require an external server to operate.</p>

Questions	Answers
<p>How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?</p>	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
<p>I have a server/serially managed device that is more than 300 feet from the Dominion SX - how do I connect?</p>	<p>You will need to purchase a 3rd party RS232 to RS422/485 converter for each end (two units total)-one at the Dominion end and one connected to the device.</p>
<p>Does Dominion SX provide an integrated interface that allows you to view all the Serial devices that are connected?</p>	<p>Yes, Dominion SX provides a single, consolidated view of all serial devices via one-sign-on. A single IP address gives access to all connected serial devices while any Java-enabled Web browser provides terminal emulation. Or, use an SSH/Telnet client.</p>
<p>Can I open multiple windows and "tile" to monitor multiple servers and other IT equipment?</p>	<p>Yes, you may monitor and "tile" as many windows as there are serial ports on the Dominion SX. For example, up to 32 serial ports on a 32 port unit, 16 on a 16-port unit and 48 on a 48-port unit. This is assuming one (1) user session per port; in some applications more than one user session per port is possible.</p>
<p>I manage many servers. How do I select a server to connect to?</p>	<p>From a browser, a simple menu provides the user-assigned name of each server. Users simply click on a server to connect to its console port. When using SSH/telnet, the user gets a list of ports they are authorized to connect with when they log in.</p>
<p>As a user, do I see all servers connected to a Dominion SX?</p>	<p>No. Each user sees only a list of servers they are authorized to manage/view. The administrator of the Dominion SX sets up the access privileges to each server by user group, or under control of privileges from a directory service like LDAP, Active Directory®, or authentication system - TACACS+, RADIUS, or Kerberos.</p>

Questions	Answers
How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
Does Dominion SX work with Raritan's CommandCenter® Secure Gateway?	<p>Yes, Dominion SX is deployable as part of an enterprise-wide management solution with Raritan's CommandCenter Secure Gateway; hundreds of Dominion SX units can be managed via CommandCenter Secure Gateway.</p>
Is the modem used only for administering the Dominion SX itself?	<p>No. Unlike other products in its category, Dominion SX offers modem access to administer the box and get to the target servers.</p>
Is a modem standard on any Dominion SX models?	<p>Many Dominion SX Models with 4- to 48-serial ports include a built-in 56K modem. Competitors charge for an additional PCMCIA modem; other models have a dedicated modem port via a DB9-Male connector.</p>
What level of control does Dominion SX have over attached target servers?	<p>The remote user has direct command line access and total control of target devices for maintenance, administration, troubleshooting, and even rebooting. User rights are only restricted by their log-on privileges on Dominion SX and the server itself.</p>
What is the MTBF for the power supply in the Dominion SX?	<p>350,000 hours. But, keep in mind that the life of a power supply depends on environmental factors like temperature, humidity, variation in power, and other factors.</p>
What is the ESD (electro-static discharge) protection on the Dominion SX serial ports?	<p>15KV (Kilo volts)</p>
Why do I need to use a serial adapter to connect to some servers?	<p>While EIA published a standard for RS232 on DB25 and DB9 connectors, there is no standard for RS232 on RJ45 connectors. Also, some manufacturers have chosen not to follow the pin out assignments of the EIA on DB25 and DB9 connectors.</p>

Questions	Answers
How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
Is the Dominion SX unit SUN® "break-safe"?	All Dominion SX units are SUN "break-safe" for use with SUN Solaris; and, the units are Solaris Ready certified by SUN.
I have lost my Admin password to the Dominion SX. Is there a back door or secret password?	For security reasons, there is no back-door password. The only option is to restore the unit to its factory default settings. A hardware reset function to restore the unit to factory default settings is provided.
Does Dominion SX include the 19" rack mount kit or is there an extra charge for this option?	Dominion SX comes standard with a complete ready-to-install 19" rack mount kit on the models with 16 or greater serial ports. One 8-port model with dual-power also comes with a rack-mount kit. Some competitors charge extra for a rack mount kit. On models with less than 16 ports, a rack mount kit is available as an option.
What remote access connection methods can Dominion SX accommodate?	Dominion SX provides multiple choices for remote access. These include: HTTP/HTTPS, SSH/Telnet, or dial-up modem. That means servers can be accessed both in and out of band so remote access to mission critical target servers is always available-even if the network is down.
Which ports need to be open on the corporate firewall for a secure console session using Dominion SX?	Port 443 (for https); optionally port 80 (http) for user sessions. For units running software version 2.2 or higher, port 51000 (or other port between 1024-65536). On software releases PRIOR to firmware 2.2 (2.0Bx or 2.1.x) either port 23 or a user-designated port between 2000 and 2400. When using SSH, port 22 needs to be open. Starting with Dominion SX firmware 3.0, the TCP ports for HTTP, HTTPS, Telnet, SSH are all user configurable. These user configured ports will need to be open for access. Also, TCP port 5000.
How do I get access to the operating system of the Dominion SX?	Dominion SX is a secure appliance. Therefore, NO access is possible to the operating system.

Questions	Answers
How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
I have a few serial devices located a distance away from my server closet and the Dominion SX. Can I connect these devices to my Raritan switch?	<p>Yes. EIA RS232 specifications defined in the 1970s recommend that the maximum distance serial devices be 30 feet (10 meters). However, with good cables, no patch panels, and lower baud rates, customers report success up to 200 feet.</p>
How do I upgrade the software on my Dominion SX?	<p>Use the Administrator option for Upgrade from a menu. The upgrade is done over the Ethernet port of the Dominion SX. Access to an FTP server is required.</p>
Are updates to Dominion SX software free?	<p>Yes. Currently, all software upgrades are free.</p>
Does Dominion SX require any additional client software?	<p>No. Dominion SX is truly "Plug-and-Play" making installation quick and set-up easy. It is not necessary to buy any additional client software or hardware. In addition, no special networking equipment or design is necessary.</p>
What code-sets does the terminal emulator in Dominion SX support?	<p>Dominion SX release 3.0 or higher supports VT100/VT220/VT320 and ANSI with the following code-sets:</p> <ul style="list-style-type: none"> <li>• US-ASCII (ISO 646)</li> <li>• ISO 8859- (Latin-1)</li> <li>• ISO-8859-15— (Latin -9)</li> <li>• UTF-8</li> </ul>
What is the name of the terminal emulation package included with Dominion SX?	<p>Beginning with Release 3.0 it is called the Raritan Serial Console (RSC). For firmware releases 2.00 through and including 2.5, it was called RaritanConsole.</p>

Questions	Answers
<p>How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?</p>	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
<p>Can I use Dominion SX over a VPN connection?</p>	<p>Yes, Dominion SX fits into most any network configuration utilizing TCP/IP. Set up the VPN (typically IPSec) connection then start the web-browser and enter the URL for the Dominion unit. The session to the Dominion runs transparently over the VPN tunnel.</p>
<p>The Dominion SX uses the Web browser to access serial devices. What are the advantages of Java-enabled Web browser access?</p>	<p>For many Solaris™/Unix®/Linux system administrators, the de facto standard for accessing serial hosts is SSH. However, the SSH clients available for Unix/Linux do not support Apple Macintosh. Additionally, Java-enabled browsers are available on many platforms, including PDAs and handheld PCs. The easy "point-and-click" access offered by Dominion SX allows administrators secure access from any Java-enabled Web browser.</p>
<p>I need an IP-enabled console switch. Now that Dominion SX support local (direct) Port access, beginning with release 2.2, by using the AUATC, can I connect a Dominion SX to the Paragon network, instead of using an SCS232 Console Switch (or equivalent)?</p>	<p>Yes. Connect the AUATC to the Paragon switch, and connect the AUATC (DB-25-Male connector) to the Dominion SX (DB9-Male connector) using a DB25-female to DB9-female cable. Then Enable the local port access (LPA) feature on the Dominion SX; ensuring that the communication parameters (baud rate, parity, etc.) matches between the AUATC and the Dominion SX.</p>
<p>What Authentication mechanisms does the Dominion SX support?</p>	<p>Local database, RADIUS, LDAP/S, TACACS+, Active Directory, and Kerberos V5.</p>
<p>What Authentication and Authorization mechanisms does the Dominion SX support?</p>	<p>Local database, RADIUS, LDAP/S, TACACS+, Active Directory, Kerberos V5. Optionally, local authentication can be Disabled.</p>

Questions	Answers
How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
Can the Dominion SX support Authorization at a per port level?	Yes. Dominion SX can support Authorization at a per port level – via Local database, RADIUS, LDAP/S, TACACS+, Active Directory, Kerberos V5.
Does Dominion SX support SNMP?	Yes. Dominion SX supports SNMP traps via the Raritan Enterprise MIB. SNMPv2 and v3 are supported.
Does Dominion SX support syslog	Yes. Dominion SX supports syslog – to primary and secondary servers.
Can I log every keystroke of a session (input from user and response from a server/device) with a server?	Yes. Dominion SX supports logging over NFS. Beginning with Release 3.0, the session can be optionally encrypted with a used-defined key.
Does Dominion SX support telnet?	Yes. Dominion SX supports enabling of the telnet daemon on the Dominion SX unit. Because telnet sends all information "in the clear", enabling telnet is at the customers own discretion, and telnet is disabled by default when the unit ships from the factory. Raritan strongly suggests the use of SSH as a safer alternative to telnet, since all data is encrypted, including the login sequence.
Can I send an intentional "break" signal to the SUN Solaris server when using SSH?	Yes.
Can I send an intentional "break" signal to the SUN Solaris server when using a Web browser?	Yes.

Questions	Answers
<p>How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?</p>	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
<p>Can I send an intentional "break" signal to the SUN Solaris server when using telnet?</p>	<p>Yes.</p>
<p>Can I get the buffered off-line data from a serial port when using SSH?</p>	<p>Yes.</p>
<p>Can I get the buffered off-line data from a serial port when using telnet?</p>	<p>Yes.</p>
<p>Can I get the buffered off-line data from a serial port when using a Java-enabled web-browser?</p>	<p>Yes.</p>
<p>Does Dominion SX support local (direct) port access for "crash-cart" applications in a data center?</p>	<p>Yes. Dominion SX supports local port access. Feature is disabled by default from the factory. Default parameters are 9600-N-8-1. The local port on the Dominion SX 4/8/16/32 is a DB9-Male.</p> <p>2. The local port on the Dominion SX 48 port models with a modem is RJ45 Female. For models with two local ports (models without a modem), the 2<sup>nd</sup> local port is DB9-Male.</p>

Questions	Answers																		
How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>																		
What are the pin-outs of the Dominion SX RJ45 serial ports?	<p>Dominion SX Serial Pin-outs</p> <p>The RJ45 connector on the rear of the unit has the following pinout:</p> <table border="1" data-bbox="560 877 953 1310"> <thead> <tr> <th>RJ45 PIN</th> <th>SIGNAL</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>RTS</td> </tr> <tr> <td>2</td> <td>DTR</td> </tr> <tr> <td>3</td> <td>TxD</td> </tr> <tr> <td>4</td> <td>GND</td> </tr> <tr> <td>5</td> <td>Signal GND</td> </tr> <tr> <td>6</td> <td>RxD</td> </tr> <tr> <td>7</td> <td>DSR</td> </tr> <tr> <td>8</td> <td>CTS</td> </tr> </tbody> </table>	RJ45 PIN	SIGNAL	1	RTS	2	DTR	3	TxD	4	GND	5	Signal GND	6	RxD	7	DSR	8	CTS
RJ45 PIN	SIGNAL																		
1	RTS																		
2	DTR																		
3	TxD																		
4	GND																		
5	Signal GND																		
6	RxD																		
7	DSR																		
8	CTS																		
How do I install Java?	See the Standalone Raritan Serial Console section of Chapter 5: Port Configuration and Port Access Application of the Dominion SX User Guide.																		
Is the status of the unit limited by the status of the device or equipment to which it is attached (that is, Server, router, firewall, load balancer, or other network device)?	<p>No, because the unit is a totally "out of band" solution that runs on its own dedicated microprocessor.</p> <p>Even if the target devices to which the Dominion SX is attached are turned off, you will still be able to access the unit.</p>																		
Can I reset the unit without losing my settings?	Click Maintenance > Reboot to reset the system.																		

Questions	Answers
<p>How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?</p>	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
<p>How do I reset the unit back to its factory-default settings?</p>	<p>Performing a factory Reset returns the Dominion SX unit to its default factory settings. Be very careful when doing this, because it will erase all the data and settings on the Dominion SX unit and return it to the state in which it was originally shipped.</p> <p>To perform a factory reset, choose Maintenance &gt; Factory Reset.</p>
<p>Does the unit need to be on the same physical LAN as the client_host during installation and setup?</p>	<p>No, setup can be performed via the SX's LPA port with a straight serial connection.</p>
<p>Once the physical installation is complete and my ping query elicits a response from the unit, how do I initially access the unit and begin to customize the unit?</p>	<p>Open a supported network-enabled web browser, type "192.168.0.192" in the address line, and press the &lt;Enter&gt; key.</p> <p>The system displays the start-up screen for the unit, and prompts you through the entire set-up process.</p> <p>Once setup is complete, log off the console, and use the IP address you assigned during set-up to re-access the unit.</p>
<p>Once I have assigned the unit a unique IP address, how do I access the unit in the future?</p>	<p>Open your supported Web browser,</p> <p>Type the IP address you have assigned to that unit into the Address field</p> <p>Press the &lt;Enter&gt; key. The login/password screen for the unit will appear.</p>
<p>Can I assign specific port access to a specific user?</p>	<p>Yes, but only if the user is NOT an Administrator. The Administrator will always have access to all the ports.</p>

Questions	Answers
How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
I performed maintenance on my NFS server, which affected my Dominion SX port logging. I had port logging enabled , but I could not access any port on the DSX.	<p>This is a designed feature. The idea of NFS port logging is to avoid missing anything on the ports.</p> <p>Disable port logging when performing maintenance on the NFS server.</p>
Sometimes when I try to log on, I see a message that states my "login is incorrect" even though I am sure I am entering the correct User Name and Password. Why is this?	<p>This is a security feature.</p> <p>There is a session-specific ID that is sent out each time you login to the unit. This ID has a time-out feature. If you do not login to the unit before the time-out occurs, then the session ID becomes invalid.</p> <p>Performing a &lt;Shift-Reload&gt; refreshes the page from the unit, and not from the now-expired cache. Similarly, you may close the current browser, open a new browser, and login again. This provides an additional security feature so that no one can recall information stored in the cache to access the unit.</p>
What should I do if the browser returns with the message that the device timed out?	<p>Try reloading using &lt;Shift-Reload&gt;. If this does not work, check your network connections and network status.</p> <p>You may also want to ping the console or perform a route print (as described in other FAQs) to ensure that proper network communication is occurring.</p> <p>If a web page does not load to your browser, there are probably network difficulties that are preventing the page from loading.</p>
How do I upgrade the Dominion SX software?	<p>Click Maintenance &gt; Firmware Upgrade and fill in the parameters.</p>

Questions	Answers
<p>How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?</p>	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
<p>What if I forget or lose my password?</p>	<p>Any Administrator can assign any user (Administrator, Operator, or Observer) a new password if it is forgotten or lost.</p> <hr/> <p><b>Important: If there is only one Administrator, and he/she forgets his/her password, then the unit must be factory-reset and re-configured from the initial set-up screen. All saved values will be lost.</b></p>
<p>Is there any way for me to optimize the performance of Microsoft Internet Explorer if it is my preferred Web browser?</p>	<p>To improve the performance of Microsoft Internet Explorer when accessing the console:</p> <ol style="list-style-type: none"> <li>1. Select Tools@Internet Options@Advanced from the main menu.</li> <li>2. Scroll through the list until you see the following items and disable them.</li> <li>3. JIT compiler for virtual machine enabled</li> <li>4. Java logging enabled</li> <li>5. Java console enabled</li> </ol>
<p>I am having trouble using the 128-bit SSL on the unit. Do you know what might be causing this?</p>	<p>It is likely that the browser you are using does not support 128-bit SSL encryption. Depending on the version of browser installed on your workstation, you may need to do one of the following:</p> <ul style="list-style-type: none"> <li>• Install a 128-bit SSL compatible version of your browser.</li> <li>• Upgrade your current browser to be 128-bit SSL compatible.</li> </ul> <p>See the browser manufacturer's web site for instructions.</p>

Questions	Answers
<p>How do I enable Direct Port Access with a Dominion SX unit running SX3.1+ firmware?</p>	<p>Enabling Direct Port Access (DPA) from the CLI in Dominion SX.</p> <p>Attached is a sample run for DPA configuration from CLI.</p> <p>The following are main steps:</p> <ol style="list-style-type: none"> <li>1. Configure DPA mode from Configuration-&gt;Services.</li> <li>2. Configure which port need DPA and type of DPA (Telnet-TCP, SSH-TCP, IP ADDR) from Configuration-&gt;ports</li> <li>3. Reboot SX</li> <li>4. Reapply Configuration-Services settings, for SSH, Telnet to take effect of DPA settings.</li> <li>5. Reboot SX</li> </ol> <p>DPA should be functional on 2<sup>nd</sup> reboot</p>
<p>Sometimes when I am trying to dial-in to the unit or when I am connected to the unit via the modem and I lose my connection.</p> <p>If I immediately try to dial-in again, I can't get connected.</p> <p>However, if I wait for a few minutes, the dial-in is successful. Why is this?</p>	<p>In this case, "a few minutes" is the key:</p> <p>The modem has a pre-defined "clean up time" after every connection ends – it does not matter whether the connection is dropped, severed, or intentionally closed by the user.</p> <p>The modem will take about one minute to re-cycle itself to be ready for the next incoming call.</p>
<p>What's the MTBF for Dominion SX?</p>	<p>131,566 Hours. Keep in mind that the life of a SX depends on the environment factors such as temperatures, humidity, variation in power and other factors</p>
<p>How do I select the language and how many languages that RSC can support?</p>	<p>Open RSC - Emulator - Setting - Display - Language. SX 3.1 RSC can support four languages: English, Japanese, Korean and Chinese</p>
<p>Does the SX support a 2048 bit hash key length?</p>	<p>Yes, SX supports the industry standard 2048 bit hash key length.</p>

▶ **U.S./Canada/Latin America**

Monday - Friday  
8 a.m. - 6 p.m. ET  
Phone: 800-724-8090 or 732-764-8886  
For CommandCenter NOC: Press 6, then Press 1  
For CommandCenter Secure Gateway: Press 6, then Press 2  
Fax: 732-764-8887  
Email for CommandCenter NOC: tech-ccnoc@raritan.com  
Email for all other products: tech@raritan.com

▶ **China**

**Beijing**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +86-10-88091890

**Shanghai**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +86-21-5425-2499

**GuangZhou**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +86-20-8755-5561

▶ **India**

Monday - Friday  
9 a.m. - 6 p.m. local time  
Phone: +91-124-410-7881

▶ **Japan**

Monday - Friday  
9:30 a.m. - 5:30 p.m. local time  
Phone: +81-3-5795-3170  
Email: support.japan@raritan.com

▶ **Europe**

**Europe**

Monday - Friday  
8:30 a.m. - 5 p.m. GMT+1 CET  
Phone: +31-10-2844040  
Email: tech.europe@raritan.com

**United Kingdom**

Monday - Friday  
8:30 a.m. to 5 p.m. GMT  
Phone +44(0)20-7090-1390

**France**

Monday - Friday  
8:30 a.m. - 5 p.m. GMT+1 CET  
Phone: +33-1-47-56-20-39

**Germany**

Monday - Friday  
8:30 a.m. - 5:30 p.m. GMT+1 CET  
Phone: +49-20-17-47-98-0  
Email: rg-support@raritan.com

▶ **Melbourne, Australia**

Monday - Friday  
9:00 a.m. - 6 p.m. local time  
Phone: +61-3-9866-6887

▶ **Taiwan**

Monday - Friday  
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight  
Phone: +886-2-8919-1333  
Email: support.apac@raritan.com