Dominion® SX

User Guide

Release 3.1

Copyright © 2007 Raritan, Inc.

DSX-0N-E

September 2007

255-60-2000-00

This page intentionally left blank.

Copyright and Trademark Information

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、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス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。

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.

CE c(UL)US LISTED 1F61 I.T.E.

For assistance in North or South America, please contact the Raritan Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail tech@raritan.com

Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, Eastern.

For assistance around the world, please see the last page of this guide for regional Raritan office contact information.

Safety Guidelines

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.

Rack Mount Safety Guidelines

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 **Appendix A: Specifications**).

- 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.

Contents

⚡ Raritan.

Figures

Tables

Preface

The Dominion SX User Guide provides the information needed to install, set up and configure, access devices such as routers, servers, switches, VPNs, and power strips, manage users and security, and maintain and diagnose the Dominion SX secure console server.

Audience

The primary audiences for this guide are infrastructure administrators and installers who are responsible for installing and setting up devices such as secure console servers. Other interested audiences are operators and observers who use the Dominion SX to reach other devices.

Conventions

This guide uses the following conventions:

EXAMPLE	DESCRIPTION
`/usr/local/java`	Monospaced text indicates file names, paths, directories, or screen text.
Enter	Menu items, Key words and Keyboard keys are bolded.
`<ip address>`	Monospaced, italicized text indicate where the user would substitute a value in a command.

Acronyms

This guide uses the following acronyms:

ACRONYM	MEANING
AD	Active Directory
CC	Command Center
CLI	Command Line Interface
CSC	Common Socket Connection
DPA	Direct Port Access
HTTP	Hypertext Transfer protocol
HTTPS	HTTP Secure (over SSL)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAP/S	Lightweight Directory Access Protocol/Secure
NFS	Network File System
NTP	Network Time Protocol
PPP	Point to Point Protocol
RADIUS	Remote Authentication Dial In User Service
RSC	Raritan Serial Console
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer Protocol
SNMP	Simple Network Management Protocol
TACACS+	Terminal Access Controller Access Control System (PLUS)
TLS	Transport Layer Security
UTC	Universal Time Coordinated
VLAN	Virtual Local Area Network

ACRONYM	MEANING
VPN	Virtual Private Network

Notices

Important: cautionary information that warns of possible affects on the users, corruption risks, and actions that may affect warranty and service coverage.

Note: general information that is supplemental to the text.

Chapter 1: Introduction

Dominion SX Overview

The Dominion 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 Dominion 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 (servers, firewalls, load balancer, and so forth) through the serial port and provides the ability to remotely and securely manage the device using a Web browser.

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

Figure 1 Dominion SX16 Unit

Product Features

Comprehensive Console Management

- Remote Management: Access, monitor, administer, and troubleshoot up to 48 target devices (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 device 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.
- SNMP traps.
- SYSLOG.
- Logging to Network File System (NFS) Server.
- Comprehensive SNMP traps.
- Port alerts with keyword triggers.
- Three Levels of User Access:
  o *Administrator:* Has read and write access to the console window; can modify the configuration of unit.
  o *Operator:* Has read and write access to the console window; cannot modify the configuration of unit (except own password).
  o *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.

Simplified User Experience

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

Package Contents

Each Dominion SX ships with the following:

- (1) Dominion SX unit with mounting kit (Rack-mount kit is optional on some units)
- (1) Raritan **Dominion SX User Guide** CD-ROM, which contains the installation and operations information for the Dominion SX
- (1) Printed **Dominion SX Quick Setup Guide**
- (1) Power cord
- (1) Release Notes
- (1) Packing List page
- (1) RJ45 serial loop-back plug
- A DB9 Factory Reset Adapter for some units (Other units have a reset switch and do not require an adapter).

This page intentionally left blank.

Chapter 2: Installation

There are two ways of completing the initial network installation of the Dominion 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 Dominion SX for use on a local area network (LAN). The following table describes the factory default network settings that come with the Dominion SX. After units are connected to the network, these factory default settings allow you to configure the Dominion SX for normal use.

Table 1 Factory Default Network Settings

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)

Pre-Installation

Ensure that you have the correct cabling ready to connect to the serial consoles of the target server (s) or other serially managed devices that provide a console port.

The following sections describe information that you must supply to complete the configuration of the Dominion SX. Obtain all required configuration information prior to performing the configuration steps. If you are uncertain of any information, contact your system administrator for assistance.

Client Configuration

1. Disable **Proxies** in the installation computer Web browser.
   Use "no Proxies" or temporarily add **192.168.0.192** to the list of URLs for which no proxy is configured.
2. Enable **Java Applet Execution** in the installation computer Web browser for the console client application (RSC).
3. Access the unit through your installation computer Web browser on the same subnet by typing the URL **https://192.168.0.192** into the address/location field.

Hardware Installation
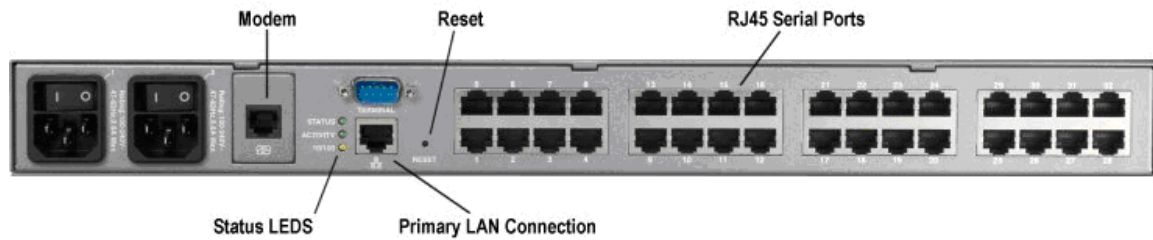
Figure 2 Rear Panel of the DSXA-32

Physical Installation of Dominion SX for Initial Configuration

1. Use a computer with a network card and crossover network cable. This computer will be referred to as the 'installation computer.'
2. Physically mount the unit in an ergonomically sound manner. The unit is designed to be easily rack-mounted, and rack mounting is recommended.
3. Connect the crossover network LAN cable to the primary LAN connection (LAN 1 on models with two Ethernet interfaces) on the back of the chassis.
4. Connect the other end of the network LAN cable to the network card in the installation computer.
5. Connect the female end of the external power cord to the back of the chassis.
6. Connect the male end of the external power cord to the power supply outlet.
7. Power ON the Dominion SX unit.

   Note: The unit will perform a hardware and firmware self-test then start the software boot sequence, which takes a short time and is complete when the light turns on and remains on.

After completion of the hardware and firmware self-test and the software boot sequence, perform the initial configuration tasks using the Graphical User Interface (GUI) or the Command Language Interface (CLI) as described in the following sections.

LED State

On the front panel of the Dominion SX unit, there exists a LED indicator right next to the model name label. The LED indicator will blink blue in the following three cases:

1. Ethernet packets are received or transmitted.
2. Serial data are received or transmitted.
3. When 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.

Initial Configuration Using the Graphical User Interface (GUI)

To initially configure the Dominion SX unit from the Graphical User Interface, follow the steps below.

Network Access

1. Ensure that the installation computer has the route for 192.168.0.192 and that it can communicate with IP address 192.168.0.192.

2. To check the route table in Windows, type the command **`route print`** in a Command window on the installation computer. If 192.168.0.192 is on the gateway list, proceed to step 3. Otherwise, add 192.168.0.192 to the gateway list using the appropriate DOS or UNIX CLI command:

   - Windows 98/2000/NT system: **`route add 192.168.0.192`** **`<INSTALLATION COMPUTER IP ADDRESS>.`** [*Example: route add 192.168.0.192 15.128.122.12*

   - UNIX (including Sun Solaris) system: **`route add 192.168.0.192 <CLIENT_HOST IP ADDRESS> -interface.`** [*Example:* **`route add 192.168.0.192 15.128.122.12 –interface`***]*

3. Type **`ping 192.168.0.192`**. Go to step 4 if you receive a successful reply from the Dominion SX unit. If an error occurs, verify that the default IP address is entered correctly and that a route to that IP address exists.

4. Use the installation computer to connect to the unit by launching a browser and typing the factory default IP address **`192.168.0.192`** in the Web browser's address box.

5. The computer displays the security screens before you can log in.

6. If you click **View Certificate** on the Security Alert-Certificate screen a Certificate screen appears.
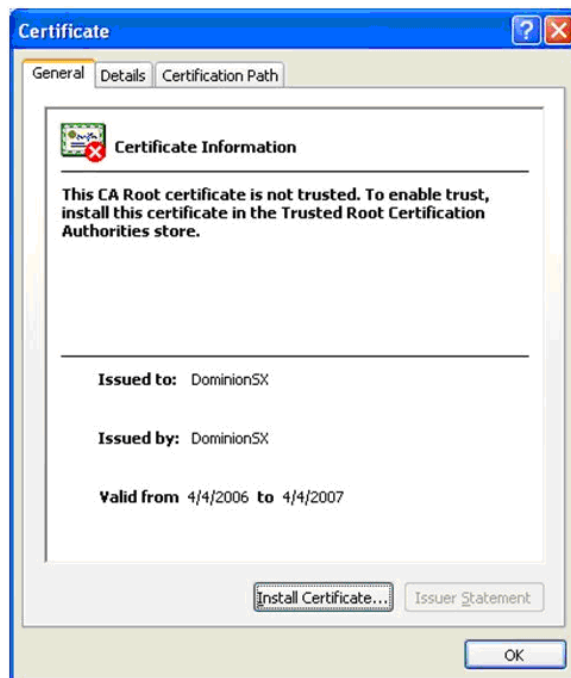
Figure 3 Certificate Information

See **Chapter 8: Security** and **Appendix C: Certificates** for information about installing certificates.

Raritan.

The login screen appears after you finish viewing the security alerts and the Certification Information screen.

Figure 4 DSX Login Screen

7. Log in with the default username **admin** and password **raritan.** Use all lowercase letters. A Restricted Service Agreement Screen appears:

Figure 5 Restricted Service Agreement Screen

Note: Once you click Accept after login, the Dominion SX prompts you to change the default password.

A Change Password screen appears:

Figure 6 Change Password Screen

8. Type a new secure password then retype it (Remember the new password).
9. Click **OK.**
10. Click **Exit**.
11. Log in again using your new password.

The Dominion SX Port Access Screen appears. (See **Chapter 3: Initial Software Configuration**)

Initial Configuration Using the Command Line Interface

To initially configure the Dominion SX unit from the Command Line Interface, follow the steps below.

1. Connect the serial port of your Installation Computer to the Terminal serial port on your Dominion SX. This port is a DB9-Male port on most models, except ALL dual-power dual-LAN models, including DSXA-48, which have an RJ45 connector for a terminal port.

2. Open a terminal emulation program, such as HyperTerminal, to connect to the Dominion SX unit. The serial communication parameters are 9600 bps, No parity, 8 data bits, 1 stop bit and None flow control.

3. Power ON the Dominion SX.

4. Log in using the default username **admin** and the default password **raritan** when prompted. Once logged in a prompt to change the password appears.

5. Type a new password, and then retype it (Remember this password).

   A display will appear showing the Dominion SX unit's status and serial channel ports.

Note: If the password entered does not follow the password rules, an error message will appear as a warning. The user will then be logged out and need to start over again for password setting.

Network Access

1. Ensure that the installation computer has the route for 192.168.0.192 and that it can communicate with IP address 192.168.0.192.

2. To check the route table in Windows, type the command **route print** in a Command window on the installation computer. If 192.168.0.192 is on the gateway list, proceed to step 3. Otherwise, add 192.168.0.192 to the gateway list using the appropriate DOS or UNIX CLI command:

   - Windows 98/2000/NT system: **route add 192.168.0.192 *<INSTALLATION COMPUTER IP ADDRESS>.*** [*Example: route add 192.168.0.192 15.128.122.12*

   - UNIX (including Sun Solaris) system: **route add 192.168.0.192 <CLIENT_HOST IP ADDRESS> -interface.** [*Example:* **route add 192.168.0.192 15.128.122.12 –interface***]*

3. Type **ping 192.168.0.192**. Go to step 4 if you receive a successful reply from the Dominion SX unit. If an error occurs, verify that the default IP address is entered correctly and that a route to that IP address exists.

4. Use the installation computer to connect to the unit by launching a browser and typing the factory default IP address **192.168.0.192** in the Web browser's address box.

Set Date and Time

1. Type **Configuration** to change the unit's configuration.

2. Type **Time** to select the Date / Time configuration.

3. Type **Timezonelist** and find the number code that corresponds to your time zone.

4. Type `clock [tz timezone] [datetime datetime-string]`. The following is an example:

```
admin > Config > Time > clock tz 9 datetime "2007-02-05
09:22:33"
```

In this example, 9 is the time zone code (Step 3) and `"2007-02-05 09:22:33"` the date/time string in the format "YYYY-MM-DD HH:MM:SS" (quotes required).

Network Configuration

1. Type **Configuration** to change the unit's configuration.
2. Type **Network** to select the network configuration.
3. Type:
   ```
   admin > Config > Network > interface enable true if lan1 ip
   192.16.151.12 mask 255.255.255 gw 192.168.51.12
   ```

.Upon successfully entering the data, a report will display the new network configuration and you will be prompted to reboot the unit.

4. Type **yes** to reboot the Dominion SX.
5. You can now remove the serial cable.
6. Reconnect from the installation computer browser to the Dominion SX using the new IP address and password and proceed.

User Configuration

1. Type **Configuration** to change the unit's configuration.
2. Type **Users** to select the user configuration.

To add a user group

Type **addgroup name** <group name> class <class type> ports <n1,n2,n3...> where <group name> is the name of the group and <class type> is

- Op for operator
- Ob for observer.

<n1,n2,n3...> is a list of port numbers this group has access to, separated by comas and no spaces. You could configure port ranges using the same parameters as well, or use the wildcard asterisk (*). For example:

- "config port 3-7 exitstring #0"(this disables exit strings for ports 3,4,5,6,7)
- config port * bps 115200 (this sets all ports to a communications speed of 115200 bps)

To add a user

1. Type **adduser user** <user name> fullname <full name> group <group name> password <password> info <information> dialback <dialback number> active <status> ...
   where *<user name>* is user's login name,
   <full name> is a user's descriptive name (no spaces),
   <group name> is the user's assigned group,
   <password> is the user's password,
   <information> is extra information (optional, no spaces),
   <dialback number> is the user's phone number (optional),
   <status> is true or false, allowing the user to login or not.
2. Type **top** to return to the top level of the CLI menu.

Chapter 3: Initial Software Configuration

After the hardware installation, perform the initial software configuration. Do this by logging onto the Dominion SX from either a browser or through a Command Line Interface (See **Chapter 12: Command Line Interface** for CLI information.)

Dominion SX Initial Software Configuration

1. Log on to the Dominion SX using your new password. A Port Access screen appears according to your user type:

Figure 7 Dominion SX Port Access Screen for Operators/ Observers

Figure 8 Dominion SX Port Access Screen for Administrators.

2. Click the **Setup** tab. The Setup screen appears. It contains links to the Configuration and Logging screens.

Figure 9 Setup Screen

Important: After you complete each configuration task, you must return to the Setup tab to perform the next configuration task.

Date / Time Configuration

1. Click the **Date / Time** in the Configuration section of the Setup Screen. The Date / Time Configuration screen appears.

Figure 10 Date / Time Configuration Screen

2. Select the correct time zone from the **UTC Offset** drop-down menu.
3. Choose one of the following:
    - **User Specified Time –** Click this radio button and enter the date and time manually in the corresponding fields.
    - **Synchronize with NTP Server** – Click this radio button and enter the IP address of a Network Time Protocol (NTP) server in the **Primary Time Server**. If you have a backup NTP server, enter its IP address in the **Secondary Time Server** field.
4. Type the **Interface Name** in the Interface field.
5. Click **OK**.

Note: Features such as certificate generation depend on the correct Timestamp, used to check the validity period of the certificate. In addition, the Syslog and NFS logging features also use the system time for time-stamping log entries.
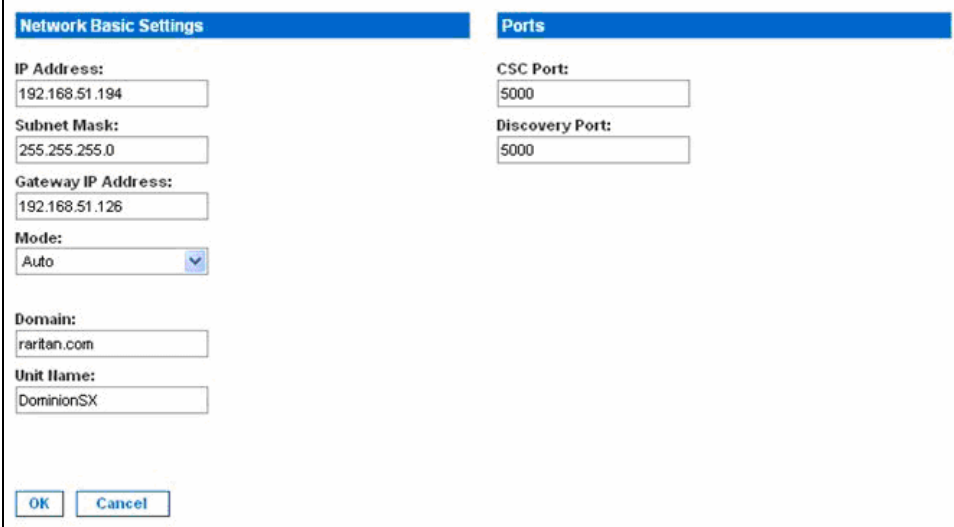
After you click **OK,** the system displays one of the following screens:
- A confirmation screen, which contains the settings you chose and a confirmation message at the top of the screen.
  Date / Time Settings successfully applied.
- An error screen, which contains the original Date / Time screen and the error message.
  ERROR: Date / Time Settings NOT successfully applied.

Network Configuration

1. Click **Network** in the Configuration section of the Setup screen. The Network Configuration Screen appears.

Note: If you have a dual LAN model, there is an Eth Failover checkbox that is selected by default, but can be turned off. The screen below represents a single LAN model and does not show this checkbox.

Figure 11 Network Configuration Screen

Note: Your network administrator usually assigns the values for the following parameters:

2. Type the data in the following fields:
   - **IP Address:** Network address for this unit
   - **Subnet Mask**: Subnet mask for the network where this unit will reside
   - **Gateway IP Gateway:** Default gateway for this unit
3. Select the **Mode** from the Mode drop-down menu.
4. Type the **Domain Name** in the **Domain** field.
5. Type your Unit Name in the **Unit Name** field.
6. In the Ports section:
   - Type 5000 or another port number in the **CSC Port** field.
   - Type 5000 or another port number in the **Discovery Port** field.
7. Click **OK**.

Dominion SX displays either a confirmation or error screen.
1. Click **OK** when the confirmation window appears. After the confirmation screen, Dominion SX automatically disconnects to update the configuration then restarts.
2. Remove the crossover cable between the SX unit and your computer.
3. Connect one end of a straight-through Cat 5 cable to the SX.
4. Connect the other end of the cable to the network.
5. Use the newly assigned IP Address to access your SX unit.

Deployment

1. You can remotely access the Dominion SX through a: LAN connection or a modem connection (optional).
2. The Dominion SX can access target devices only through a serial connection.

LAN Connection

After the initial software configuration phase, configure the DSX unit for operation on the LAN.

1. Ensure that you have an Ethernet cable connected to the network for use with the unit.
2. Physically mount the unit in an ergonomically sound manner.
3. Connect the LAN cable to the primary LAN connection (LAN 1) on the back of the chassis. If the unit has a failover module, connect the secondary network LAN connection (LAN 2).
4. Perform a quick connectivity check by connecting to the device using the Web browser.
5. Enter `https://<IPAddress>` in the address line, where `<IPAddress>` is the IP address of the unit as previously configured.

   The login display should appear verifying that the unit has been properly configured and can be accessed from the network.

6. Log in with username **admin** and the password you created earlier.
7. From the Home page, click the **Setup** tab and select the various configuration options for configuring the DSX and each console port.

Modem Connection (Optional)

To configure the DSX for a modem connection:

1. Connect a phone line to the modem port.
2. Write down the phone number for this line because it will be needed when you configure a client for dialup networking.

See **Appendix E: Modem Configuration** for more information**.**

Chapter 4: Network Settings and Services

This chapter explains how to configure the basic network settings for the DSX, and how to configure the various access protocols (SSH, telnet, etc.) It also explains how to configure the DSX for modem access, and how to enable IP forwarding and create static routes.

Configuring the Basic Network Settings

To configure the basic network settings and discovery ports, click the **Setup** tab, and then click **Network**. The Network Basic Settings and Ports screen appears (Figure 12).

Figure 12 Network Basic Settings and Ports Screen

Give the DSX a Name

To give the DSX unit a name to help identify it:

1. Type a name in the **Unit Name** field.
2. Click **OK**.

Configure the DSX's Network Settings

To configure the network settings:

1. Type an IP address for the DSX in the **IP Address** field.
2. Type the subnet mask in the **Subnet Mask** field.
3. Type the IP address of the gateway router in the **Gateway IP Address** field.
4. Select the speed from the drop-down menu in the **Mode** field. Your choices are **Auto** (default) or **100 Mbp**s.
5. Type your domain name in the **Domain** field.
6. Click **OK**.

Change the Discovery Ports

The DSX has two discovery ports:

- TCP 5000 Common Socket Connection (CSC) discovery

- UDP 5000 Command Center (CC) discovery

If either of these ports is used by another application, you can change the discovery port number in the DSX in the appropriate field and click **OK**.
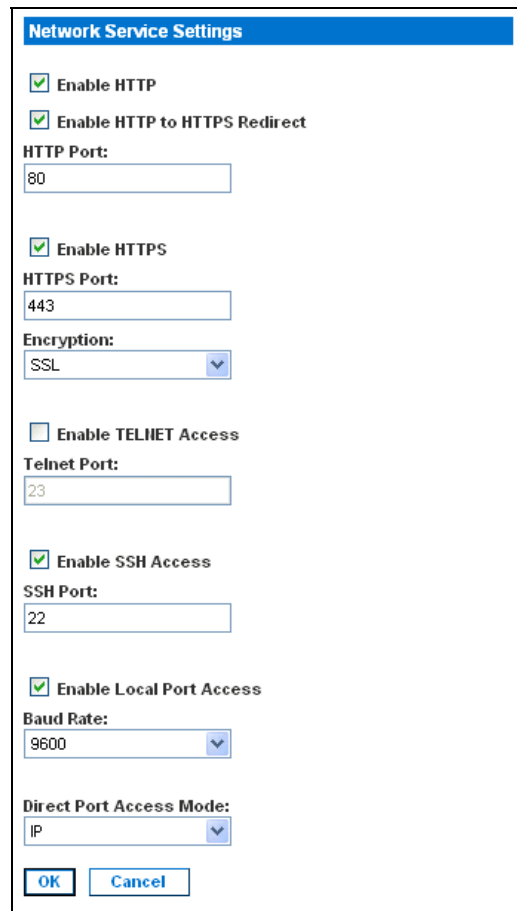
Configuring the Network Service Settings

The table below indicates 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 is set to SSL, but this can be changed to TLS.
Telnet	Disabled for security reasons. This can be enabled and the port configured.
Local Port Access	Enabled. The baud rate is set to 9600 bps, but this can be changed.
Direct Port Access	Set to IP, but this can be changed to Normal or TCP port.

To change any of these network service settings:

1. Click the **Setup** tab, and then click **Services**. The Network Service Settings screen appears.

Figure 13 Network Service Settings

2. Make any necessary changes to the appropriate fields.

3. Click **OK**.

Configuring Modem Access

You can access the DSX via a modem. To set this up:

1. Click the **Setup** tab, and then click **Modem**. The Modem Settings screen appears.

Modem Settings

☐ **Enable Modem**

PPP Server IP:

`10.0.0.1`

PPP Client IP:

`10.0.0.2`

☐ **Enable Modem Dial Back**

OK   **Cancel**
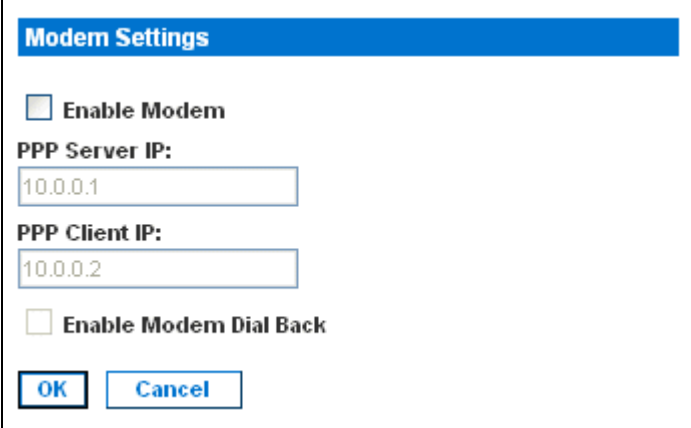
Figure 14 Modem Settings Screen

2. Click the checkbox labeled **Enable Modem** to enable modem access.

3. Type the IP addresses of the Point-to-Point (PPP) server in the PPP Server IP field. The default is 10.0.0.1

4. Type the IP address of the PPP client in the **PPP Client IP** field. The default is 10.0.0.2.

5. If you want to enable modem dialback, click the **Enable Modem Dial Back** checkbox.

6. Click **OK**. Modem access is enabled.

Configuring IP Forwarding and Static Routes

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

Enable IP Forwarding

To enable IP forwarding:

1. Click the **Setup** tab, and then click **Static Routes**. The Static Routes screen appears. It consists of an Enable IP Forwarding panel and a Static Routes List.

2. Go to the IP Forwarding panel and click the checkbox labeled **Enable IP Forwarding**.

IP Forwarding

☑ **Enable IP Forwarding**

OK   **Cancel**
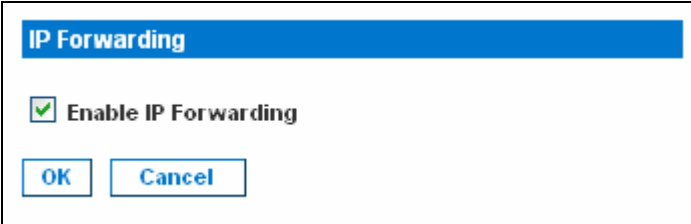
Figure 15 IP Forwarding Panel

3. Click **OK**. IP forwarding is enabled.

Add a New Static Route

To add a new Static Route:

1. Click the **Setup** tab, and then click **Static Routes**. The Static Routes screen appears. It consists of an Enable IP Forwarding panel and a Static Routes List.

Figure 16 Static Routes List

2. Go to the Static Routes List and click **Add New Route**. The Static Route screen appears.

Figure 17 Static Route Screen

3. On a DSX with one LAN interface, **LAN1** appears automatically in the **Interface** field. On a DSX 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 th**e** 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 it for a subnet.

9. Click **OK**.

Delete a Static Route

To delete a static route:

1. Click the **Setup** tab, and then click **Static Routes**. The Static Routes screen appears. It consists of an Enable IP Forwarding panel and a Static Routes List.

2. Go the Static Routes List and click 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 5: User Profiles and Groups

This chapter explains how to create and manage user profiles and user groups.

Managing User Profiles

User profiles serve two purposes:

- To provide users with a username and password to log into the DSX

- To associate the user with a user group. The user group determines which system functions and ports the user can access.

The DSX is shipped with one user profile built in. This is 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.

You can create as many other user profiles as necessary. You can create individual user profiles for each person who will be logging into the DSX, 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, click the **User Management** tab, and then click **User List**. The User List screen appears (Figure 18).

User List

	▲ Username	Full Name	Dialback	Group	Active
☐	Alexander	Alexander		Designers	Yes
☐	Andre	Andre		Managers	Yes
☐	Charle	Charles Kord		Designers	Yes
☐	Elaine	Elaine		Admin	Yes
☐	Emma	Emma Kall		Admin	Yes
☐	Lauren	Lauren		Managers	Yes
☐	Maureen	Maureen Rand		Admin	Yes
☐	Stan	Stan		Admin	Yes
☐	Vic	Victor		Admin	Yes
	admin	Administrator		Admin	Yes

Delete   **Add New User**

Figure 18 User List Screen

2. The User List screen shows every user profile created to date, and for each one gives the:

- Username

- Full name

- Dialback number (if one has been defined)

- User group

3. The User List screen also indicates whether the user profile is active or inactive.

Create a User Profile

To create a new user profile:

1. Click the **User Management** tab, and then click **User List**. The User List screen appears (Figure 18).

2. Click **Add New User**. The New User screen appears.

Figure 19 New User Screen

3. Type a login name in the **Username** field. This is the name the user enters to log into the DSX. 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. It 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 16.

    - You can enter any printable character.

    - The password is case sensitive.

Note: If the strong password feature is enabled, there are other password requirements. Refer to Chapter 8 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, clear this checkbox. You can return at any time and activate the user when necessary.

10. Click **OK**. The user profile is created. It should appear in the User List screen.

Modify a User Profile

To modify an existing user profile:

1. Click the User **Management** tab, and then click **User List**. The User List screen appears (Figure 18).

2. Click the Username of the profile you want to edit. The Edit User screen appears. It looks exactly like the New User screen (Figure 19).

3. You can change any of the fields except the **Username** field.

4. 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.

5. Click **OK** when finished. The user profile is modified.

Delete a User Profile

To delete an existing user profile:

1. Click the User **Management** tab, and then click **User List**. The User List screen appears (Figure 18).

2. Click the checkbox to the left of the user profile you want to delete. You can select more than one.

3. Click **Delete**. You are prompted to confirm the deletion.

4. 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 DSX is shipped with one user group built in. This is 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, click the **User Management** tab, and then click **User Group List**. The Group List screen appears (Figure 20).

Group List

	▲ Group	Class
	Admin	Administrator
☐	Designers	Observer
☐	Managers	Operator
☐	Support	Operator
☐	Writers	Operator

[Delete]   [Add New User Group]

Figure 20 Group List Screen

The Group List screen 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. Click the **User Management** tab, and then click **User Group List**. The Group List screen appears (Figure 20).

2. Click **Add New User Group**. The New Group screen appears.

New Group

Group Name:

Class:
Operator

Port Access:
☐ Select All

☐ 01: Port1   ☐ 02: Port2
☐ 03: Port3   ☐ 04: Port4

[OK]   [Cancel]

Figure 21 New Group Screen

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. 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.

6. Click **OK**. The user group is created. It should appear in the User List screen.

Modify a User Group

To modify an existing user group:

1. Click the **User** Management tab, and then click **User Group List**. The Group List screen appears (Figure 20).

2. Click the **Group Name** of the group you want to edit. The Edit Group screen appears. It looks exactly like the New Group screen (Figure 21).

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. Click the **User Management** tab, and then click **User Group List**. The Group List screen appears (Figure 20).

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.

4. Click **OK**. The selected user groups are deleted.

Chapter 6: Remote Authentication
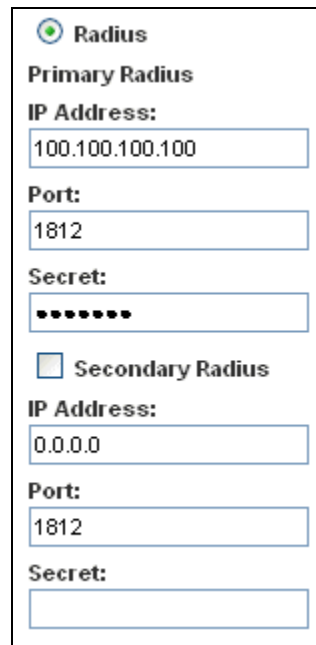
This chapter explains how to configure RADIUS, LDAP, and TACACS+ authentication.

> *Tip: If you are setting up remote authentication, it is a good idea to still keep local authentication enabled. When an authentication request reaches the DSX, it looks to authenticate the user remotely first, and then looks to authenticate the user locally. Keeping local authentication enabled ensures that if remote authentication is misconfigured or otherwise unavailable, you are not locked out or the DSX because you can always be authenticated locally.*

Configuring RADIUS

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

1. Click the **Setup** tab, and then click **Remote Authentication**. The Remote Authentication screen appears. It contains a RADIUS panel.

Figure 22   RADIUS Panel

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 the RADIUS server is listening on (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 DSX users instead of local authentication. To configure LDAP:

1. Click the **Setup** tab, and then click **Remote Authentication**. The Remote Authentication screen appears. It contains an LDAP panel.

Figure 23 LDAP Panel

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 DominionSX, an attribute named DominionSX must be added under the given domain specified by the **Search** field. On top of that, a user group must have been created in DSX 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.
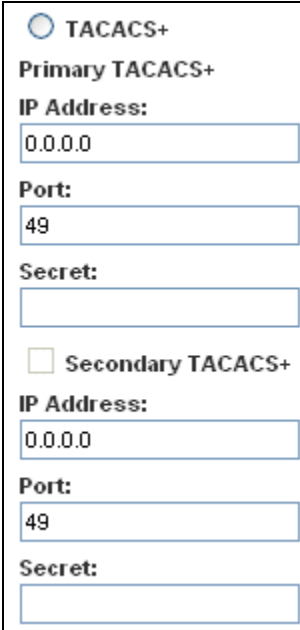
   In other words, it is the domain name. This is where the search starts for the user name. The user name is created in this domain (for example, Search: dc=raritan, dc=com) to process LDAP authentication queries from Dominion SX.

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 DSX users instead of local authentication. To configure TACACS+:

1. Click the **Setup** tab, and then click **Remote Authentication**. The Remote Authentication screen appears. It contains a TACACS+ panel.

Figure 24   TACACS+ Panel

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 it is listening on (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 uses **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 7: Port Configuration and Port Access Application

Port configuration allows Administrators to define the serial/console port settings in order to communicate with remote target devices.

Note: You can access the Raritan Serial Console (RSC) from the Port screen. See the Raritan Serial Console section of this chapter for RSC information.

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, then and only then will a corresponding message be logged in a local/NFS port log. A corresponding event will be sent via SMTP (if configured) and corresponding trap will be sent via SNMP (if configured).

This is very useful for local/remote NFS logging, as it logs just the information you need and no junk messages, thus providing ease of traceability.

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

1. Click the **Setup** tab, and then click **Port Keywords**. The Port Keywords screen appears.
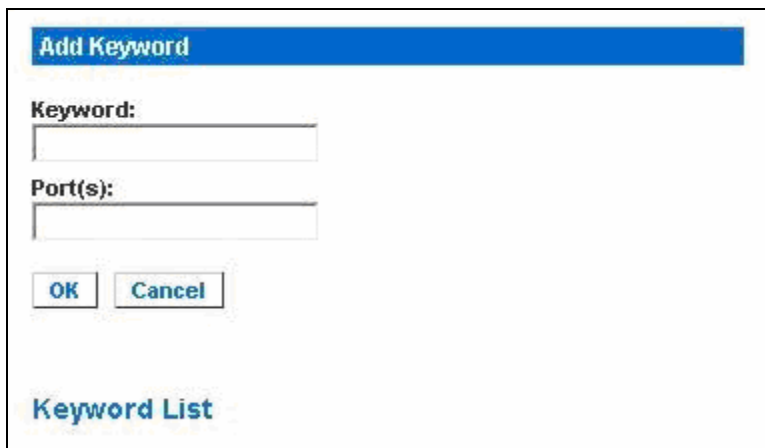
Figure 25 Port Keywords Screen

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. Click the **Setup** tab, and then click **Port Configuration**. The Port Configuration screen appears.

Port Configuration

	▲ No	Name	Application	Baud Rate	Parity Bits	X on / X off	H/W Flow
☐	1	Port1	RaritanConsole	9600	None/8	Enabled	Disabled
☐	2	Port2	RaritanConsole	9600	None/8	Disabled	Disabled
☐	3	Port3	RaritanConsole	9600	None/8	Disabled	Disabled
☐	4	Port4	RaritanConsole	9600	None/8	Disabled	Disabled

Select All   Edit

Figure 26 Port Configuration Screen

2. Select the port(s) you want to configure. You can select one port or several ports, so long as the port configurations are all the same.

    *   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 screen appears.

Port 1

Name:
Port1

Application:
RaritanConsole

Baud Rate:
9600

Parity Bits:
None/8

Flow Control:
None

Detect:
Do Not Detect Physical Connection to the Target

Exit Command:

Escape Mode:
control

Escape Character:
]

Emulation:
VT100

DPA IP Address:
0.0.0.0

DPA SSH TCP Port:

DPA Telnet TCP Port:

OK   Cancel

Figure 27 Edit Port Screen

3. Make sure the port values match the target system's serial port configuration for the first three values.

   - Select the **Baud Rate** from the **Baud Rate** drop-down menu.

   Note: The minimum baud rate supported for local port access is 9600.

   - 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 Dominion SX to detect or not detect the physical connection to the target. The default is Not detect. Change 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. This is the command that will be sent to your system when a port disconnection occurs, for example, logout.

6. Select the escape mode. The default is **None**. Change as follows:
    - Select **Control** from the drop-down menu in the **Escape Mode** field.
    - Type the **Escape Character.** The default for the Dominion SX is **]** (closed bracket).

7. Select the terminal emulation type from the drop-down menu in the Emulation field. The choices are:
    - VT100
    - VT220
    - VT320
    - ANSI

8. If you plan to use Direct Port Access (DPA), you must enter the DPA IP Address, as well as one or both of the following:
    - 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 .

9. Click **OK**.

Direct Port Access

To configure direct port access:

1. Click the **Setup** tab, and then click **Services**. The Network Service Settings screen appears. The **Direct Port Access Mode** field is at the bottom of the screen.
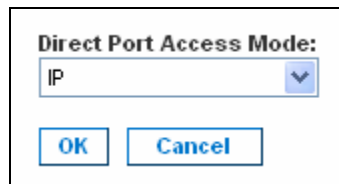
Figure 28 Direct Port Access Mode Field

2. Go to the **Direct Port Access Mode** field. The default is **Normal**, which means disabled. To enable DPA, select either **IP** or **TCP Port** from the drop-down menu.

3. Click **OK** to save this information. The screen displays the following message: *The system will need to be rebooted for changes to take effect.*

4. Reboot now or reboot after completely configuring for DPA.

5. Click the **Setup** tab, and then click **Port Configuration**. The Port Configuration screen appears. (Figure 26).

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, lick **Edit**.
    - To select all the ports, click **Select All**.

    The Edit Port Configuration screen appears (Figure 27). The DPA fields are at the bottom of the screen.

7. Type the DPA IP address of the DSX, and the DPA ports used for SSH and Telnet in the appropriate fields.

8. Click **OK** to save this information.

9. Reboot the DSX unit. This is necessary for the direct port access settings to take effect.

    .

Anonymous Port Access

Anonymous port access allows users to access DPA configured ports without entering a password. To enable the feature:

1. Click the **Security** tab, and then click **Login Settings**. The Login Settings screen appears (Figure 54).
2. Make sure the **Anonymous Port Access** checkbox at the bottom of the screen is checked.
3. Click the **User Management** tab, and the click **User Group List**. The Group List appears (Figure 20).

Note: Refer to Chapter 5 for additional information about user groups.

4. Click **Add New User Group**. The New Group screen appears (Figure 21).
5. Type **Anonymous** in the **Group Name** field.
6. Select **Observer** from the drop-down menu in the **Class** field.
7. **Select** the ports for which you want anonymous port access in the **Port Access** field.
8. Click **OK**.

Important: The Dominion SX unit must be rebooted to apply new direct port access settings.

Raritan Serial Console

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

1. Select the **Port Access** tab.

▲ 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

Figure 29 Port Access Screen

2. Click on the **Name** of the port you want to access for the RSC, for example, Port1 or Port2.

Note: A Security popup screen appears only if you used https to connect to the RSC.

3. Click **Yes**. A **Warning – Security** popup screen appears.
4. Click **Yes** to access the Raritan Serial Client from the Port Screen.

Note: If you click Always, you will not receive the security screen for future access.

The Raritan Serial Console window appears. Refer to the Raritan Serial Client Interface section in this chapter.

Raritan Serial Client Requirements for Java

The Raritan Serial Client (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 will function 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, of course for 1.5.0_02).

Depending on your operating system and browser, it is possible that you need to adjust some 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

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 browser based RSC does not need to make any changes to the Runtime parameters for Java Applets. Do the following 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/1.4.2/docs/guide/plugin/developer_guide/control_panel.html

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

1. Launch the Java Control Panel, which is located in the:
   - **Advanced Tab** in JRE 1.4.x
   - **Java Tab** in JRE 1.5
2. Locate **Java Runtime Settings.**
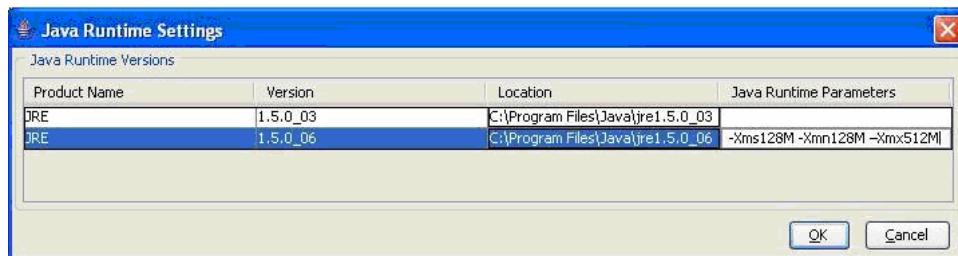
Figure 30 Java Runtime Settings

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

Table 2 Java Runtime Parameters

VALUES -SYNTAX	DESCRIPTION	DEFAULT / COMMENTS
–Xms<Size> in bytes	Sets the initial size of the Java heap.	**2097152 (2MB)** • The `-server` flag increases the default size to 32M. • The values must be a multiple of, and greater than, 1024 bytes (1KB). • Append the letter "m" or "M" to indicate megabytes and "k" or "K" to indicate kilobytes.
–Xmn<Size> in bytes	Sets the initial Java heap size for the Eden generation.	**640K** • The `-server` flag increases the default size to 2M. • **Append the letter "m" or "M" to indicate megabytes and "k" or "K" to indicate kilobytes.**
–Xmx<Size> in bytes	Sets the maximum size to which the Java heap can grow.	**64M** • The `-server` flag increases the default size to 128M. • The maximum heap limit is approximately 2 GB (2048MB). • Append the letter "m" or "M" to indicate megabytes and "k" or "K" to indicate kilobytes. .

Command Example:

```
–Xms128M –Xmn128M –Xmx512M
```

Refer to the following links for additional information and for all the non-standard options:g
http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/java.html
http://java.sun.com/docs/hotspot/VMOptions.html

≡≋≡ Raritan.

Raritan Serial Client Interface

Important: The Raritan Serial Client (Console) Screen usually opens in a separate window in back of the Port Screen. With some versions of Java on Windows, the screen opens in front of the Port Screen.

Minimize the **Port Access** screen to access the Raritan Serial Console screen. The RSC contains drop-down menus that provide the user with the ability to:

- Modify emulation settings such as fonts and window size.
- Manage the history of the session.
- Request Write Access to the port.
- Get a Write Lock on the port.
- Send a Break signal (used for Solaris servers).
- Get a list of users connected to this port.
- Edit text in the window.
- Manage client workstation-based logging of data from the target device.
- Send Keystroke (combinations).
- Send Text files.
- Send power commands to a Power Distribution Unit (PDU).
- Chat among other users on the same port.
- Get help.
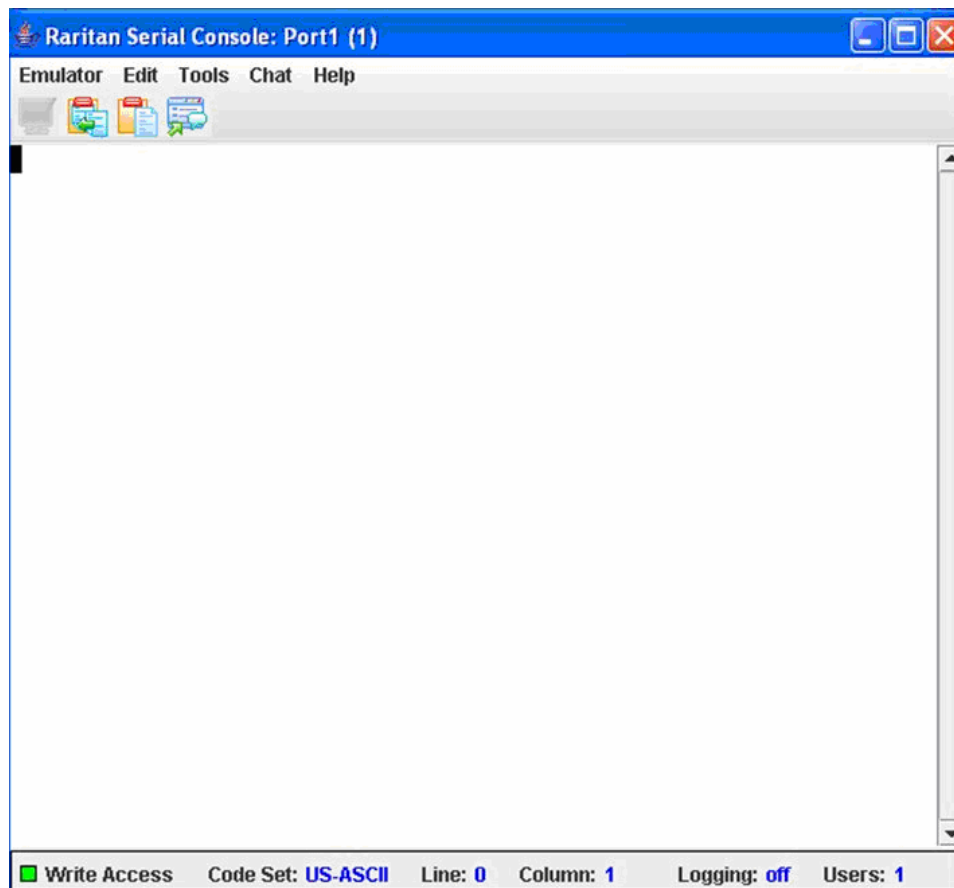
Figure 31 Raritan Serial Client Window

Emulator

1. Change the default user Idle Timeout setting before launching the RSC for the first time or it will timeout in 10 minutes and display a host termination message. See the Security section of the Dominion SX User Guide for changing the Idle Timeout setting..

2. Click on the **Emulator** drop-down menu to display a list of topics.
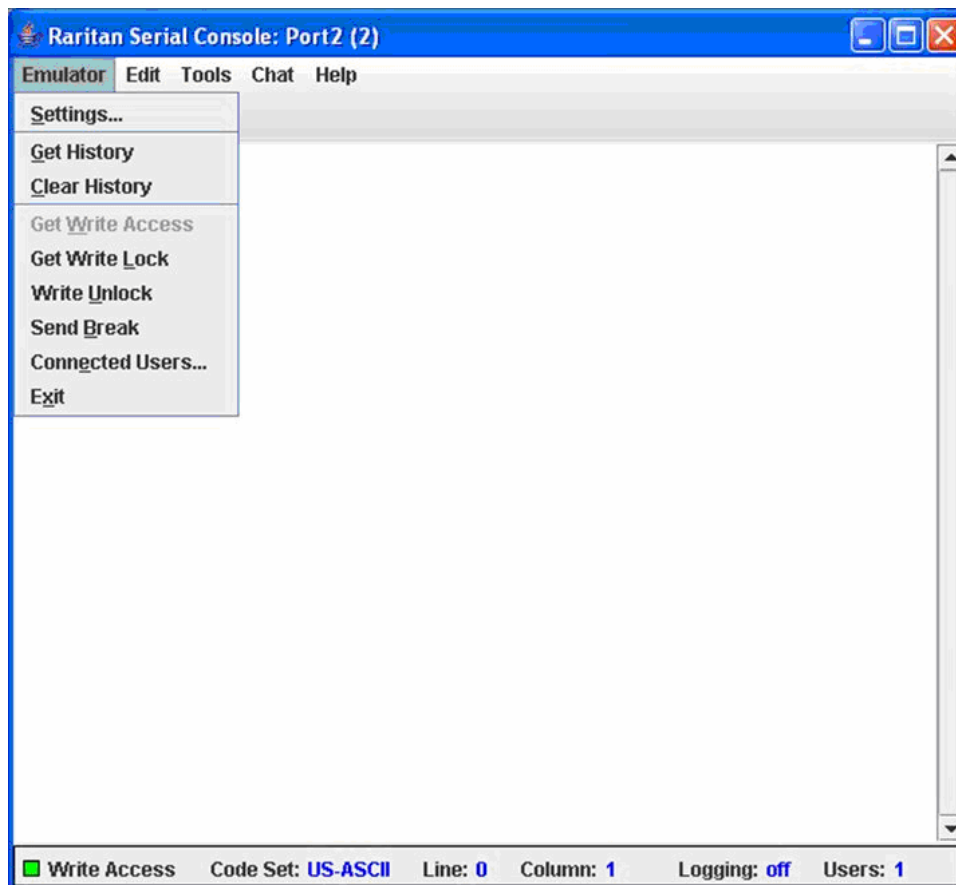
Figure 32 Emulator Drop-Down Menu

IMPORTANT: You must change the default user Idle Timeout setting on the Dominion SX GUI before you begin using the RSC or it will timeout in 10 minutes and display a host termination message. See the Security chapter of the Dominion SX User Guide for changing the Idle Timeout setting.
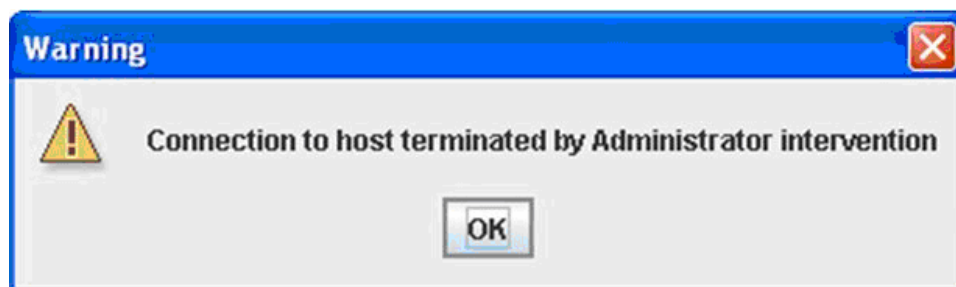
Figure 33 Connection Terminated Warning

3. Change the default **Idletimeout** setting and then launch the RSC.

Note: If the RSC Idletimeout expires, the Dominion SX Idletimeout period begins.

Settings

Note: Terminal emulation settings are set with the port by an Administrator using the Setup->Port Configuration menu.

1. On the **Emulator** menu, click **Settings.** The Settings screen displays the **General** tab with the default settings.
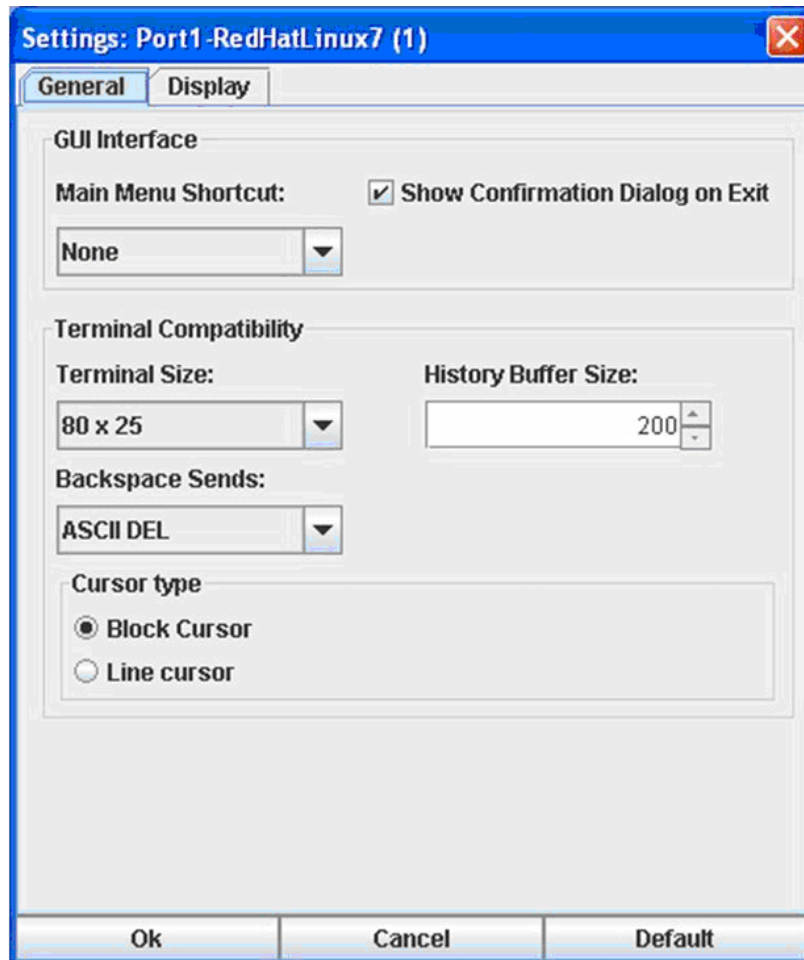
Figure 34 General Settings Window

2. Accept the **Main Menu Shortcut:** default of **None** or choose one of the following from the **Main Menu Shortcut:** drop-down menu.

   - F10
   - Alt

3. Accept the **Show Confirmation Dialog on Exit** default or uncheck it.

4. Accept the **Terminal Size:** default or choose a size from the **Terminal Size:** drop-down menu.

5. Accept the **Backspace Sends:** default of **ASCII DEL** or choose **Control-H** from the **Backspace Sends:** drop-down menu.

6. Accept the **History Buffer Size:** default of **200** or use the arrows to change the buffer size.

7. Accept the **Cursor type:** default of **Block Cursor:** or select **Line Cursor.**

8. Click **Ok.**

Display Settings

1. Return to the **Emulator** menu, select **Settings** and then click the **Display** tab.
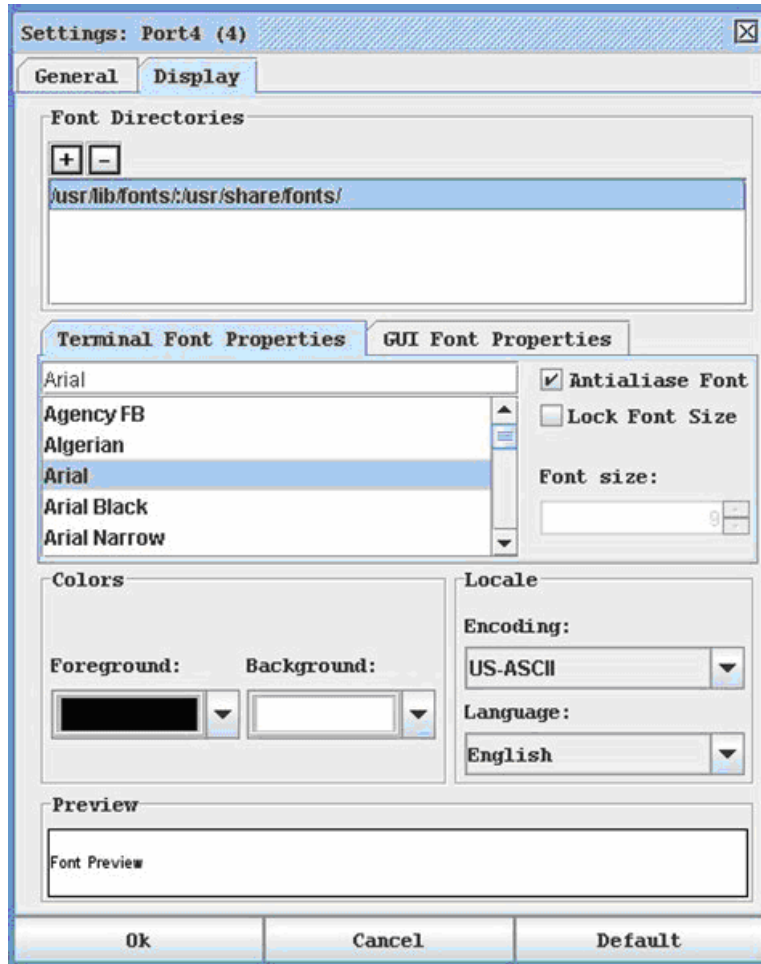
Figure 35 Display Settings Window

2. Click **Default** to accept the **Default** settings. Then click **Ok** to close the Display Settings window**;** however, if you want to change the settings, perform the following steps:
3. Accept the **Terminal Font Properties** default of **Arial** or choose a font from the **Terminal Font Properties** scrolling list.
4. Accept the **Antialiase Font** default or uncheck it.
5. If you want to change the size of the font, check the **Lock Font Size** box and choose a font size from the **Font size:** drop-down menu.

6. Click on the **GUI Font Properties** tab and accept the default of Monospaced or choose a font from the **GUI Font Properties** scrolling list.
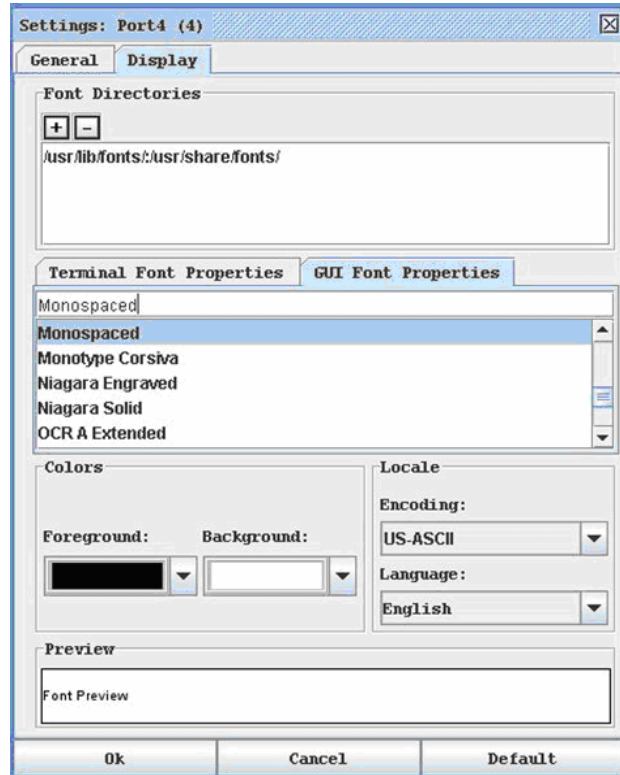
Figure 36 Display Settings: GUI Font Properties

7. Choose the following from their drop-down menus:
    - **Foreground** Color
    - **Background** Color
8. Choose one of the following from the **Encoding** drop-down menu:
    - US-ASCII
    - ISO-8859-1
    - ISO-8859-15
    - UTF-8
9. Choose one of the following from the **Language** drop-down menu:
    - English
    - Japanese
    - Korean
    - Chinese
10. 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, please 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 will wrap, 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, click **Get History** on the **Emulator** menu**.**

Clear History

To clear the history, click **Clear History** on the **Emulator** menu.

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 Client via the Get Write Access command.

10. To enable Write Access, click **Get Write Access** on the **Emulator** menu.

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

Get Write Lock

1. To get write lock, click **Get Write Lock** on the **Emulator** menu.
2. If the Get Write Lock is not available, a request rejected message appears:

Write Unlock

To get Write Unlock, click **Write Unlock** on the **Emulator** menu.

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 Operator or 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. Click **Send Break** on the **Emulator** menu.
   A **Send Break Ack** (Acknowledgement) pop-up 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. Click **Connected Users** to view the connected users on the **Emulator** menu.
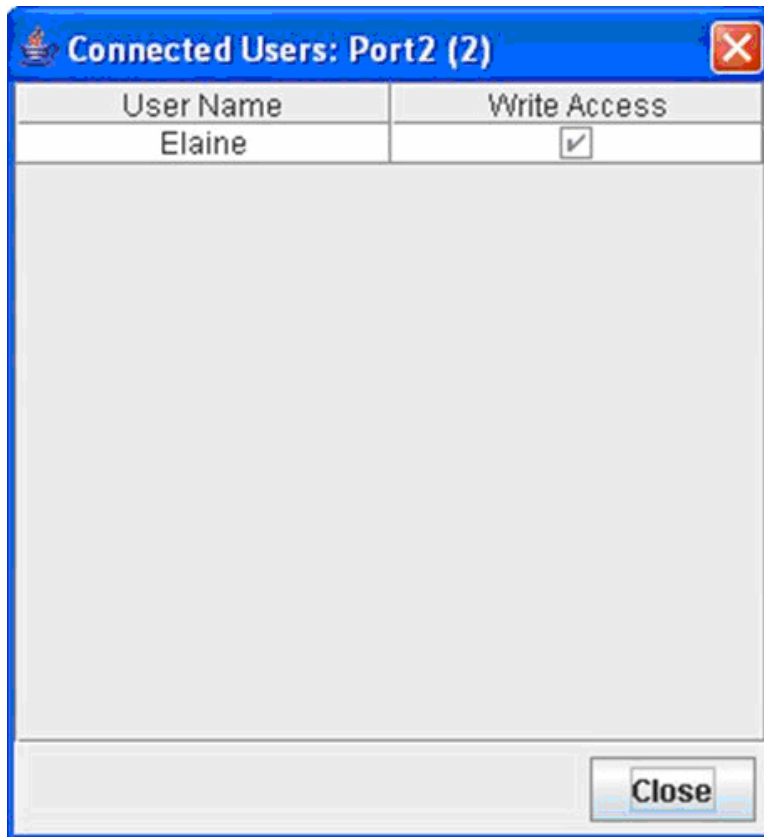
Figure 37 Connected Users Window

11. A check mark appears in the **Write Access** column after the name of the User who has Write Access to the console.

2. Click **Close** to close the Connected Users window.

Exit

1. Click **Exit** on the **Emulator** menu to close the Raritan Serial Console.

    The Exit Confirmation screen appears.

2. Click **Yes.**

Edit

Use the **Copy, Paste**, and **Select All** text commands to relocate and/or re-use important text.
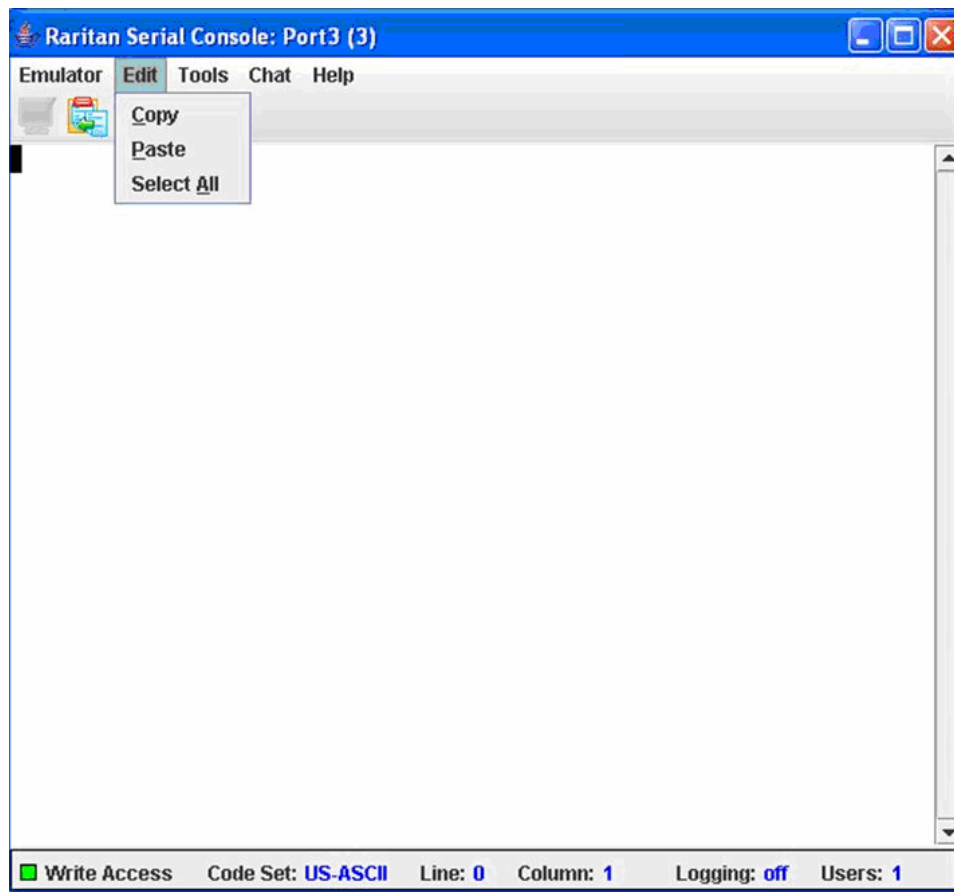
Figure 38 Edit Commands - Copy, Paste, and Select All Text

Copy and Paste All Text:

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

Note: Here are keyboard shortcuts that you can use to highlight, copy, and paste all or partial lines of text:

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

The text copy limit in Raritan Serial Client is 9999 lines.

Tools

1. Click on the **Tools** drop-down menu to display a list of topics.
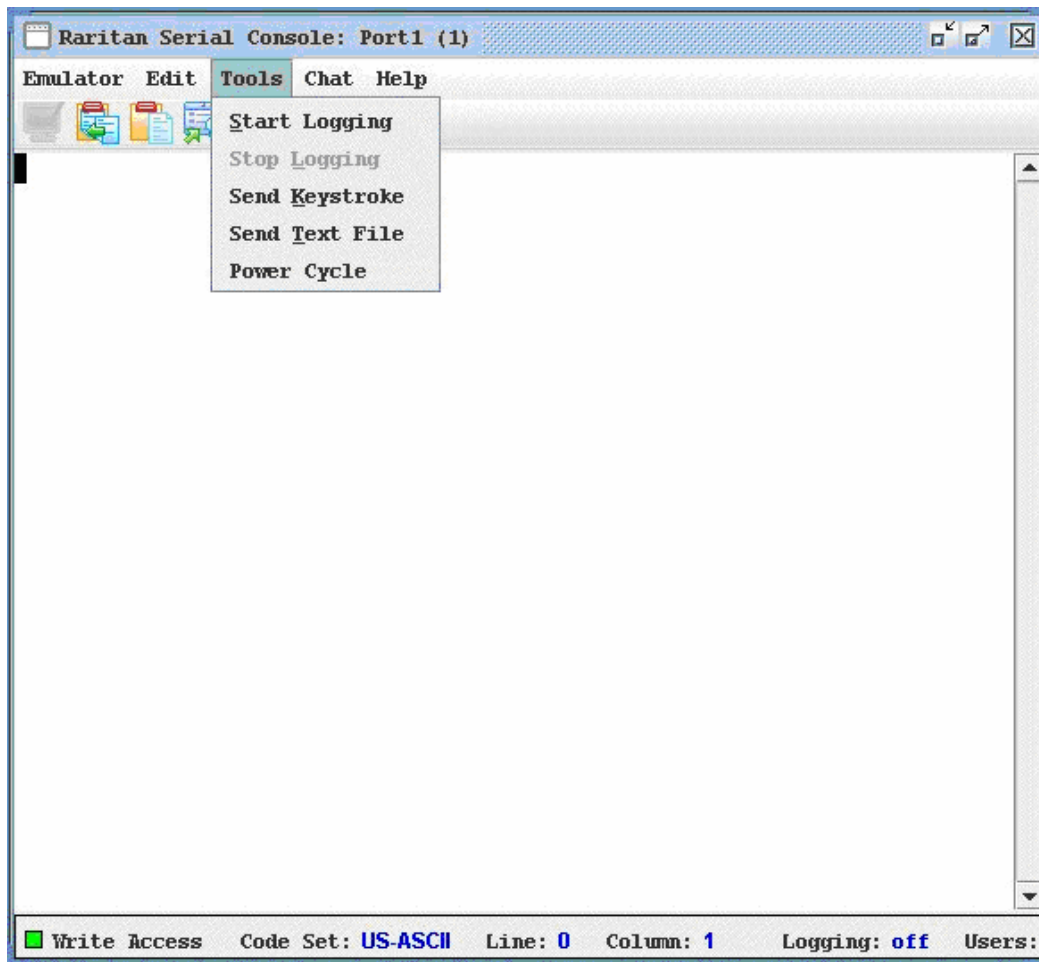
Figure 39 Tools Menu

Start Logging

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

1. On the **Tools** menu, click **Start Logging**.
2. Choose an existing file or provide a new file name in the **Save RSC Log** dialog box.

   - When an existing file is selected for logging, data gets appended to the contents.
   - Providing a new file name results in new file being created.
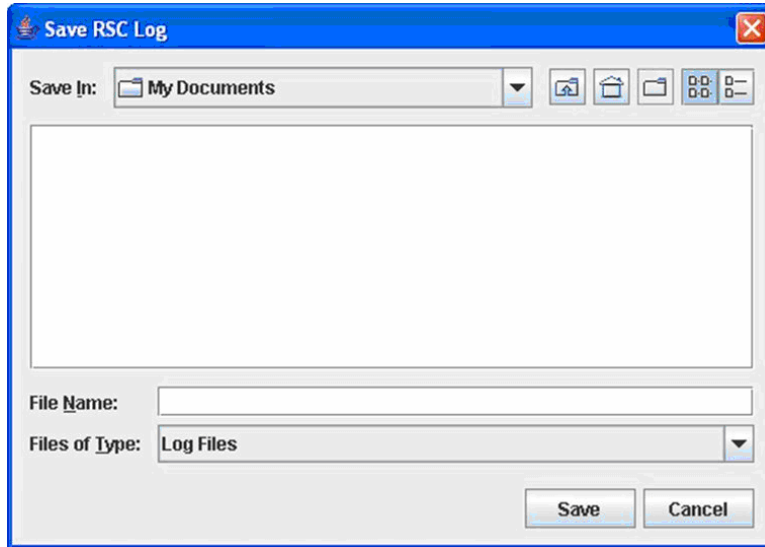
Figure 40 Start Logging Command Window

3. Click **Save** after selecting or creating a file.

Stop Logging

On the T**ools** menu, click **Stop Logging**. The logging stops.

Send Keystroke

1. On the T**ools** menu, click **Send Keystroke.**
   A **Send Keystroke** screen appears:
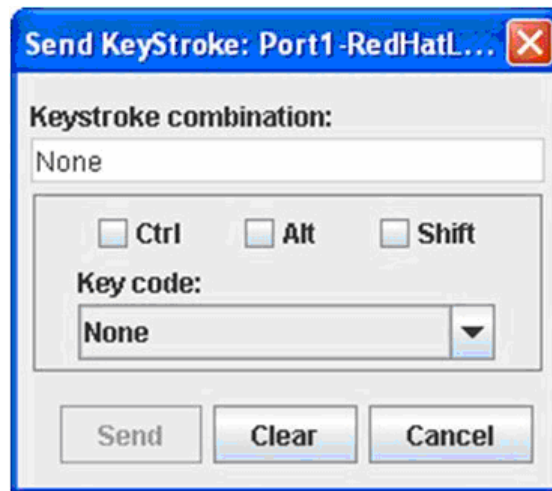
Figure 41 Send Keystroke

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. On the T**ools** menu, click **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**.

   - As soon as you click the **Open** dialog box, it sends whatever file you selected directly to the port.
   - If there is a loopback plug inserted, you see the file displayed.
   - If there is currently no target connected, then nothing will be visible on the screen.

Chat

When using browser access over SSL, an interactive chat feature called **Chat** provides you and other users on the same port to communicate. You can conduct an online dialog for training or collaborative diagnostic activities. 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, chat messages will not be shown to the same user.

To use Chat:

1. Click **Chat** on the **Chat** menu**.**
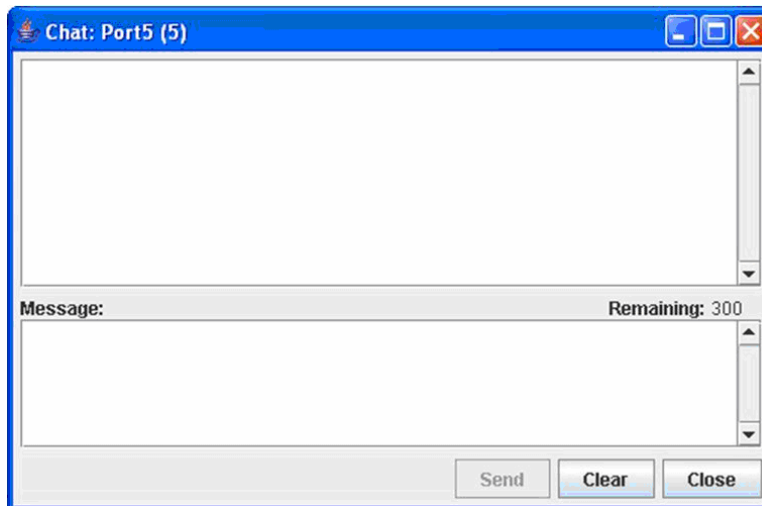
Figure 42 SecureChat Command and User Chat Window

2. Type a message in the **Message** text field.
3. Click **Send** or press **ENTER** to send the message.
4. Click **Clear** to delete the typed text, or click **Close** to exit and close the Message window.

Help

Help Topics include on-line assistance for operating the Raritan Serial Console, and release information about Raritan Serial Console.

Help Topics

To Access Help Topics:

1. Click **Help Topics** on the **Help** menu**.**
2. Use the navigation bar on the right side of **Table of Contents** window to scroll to the topic you need or click on the links.
3. Close this window when you are finished.

About Raritan Serial Console

The **About Raritan Serial Console** window 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:

1. Click **About Raritan Serial Console** on the Help menu.

   An **About Raritan Serial Console** message appears on top of the Raritan Serial Console drop-down menu:

Figure 43 Sample of the About Raritan Serial Console Window

2. Click **OK** to close the About Raritan Serial Console window.

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

The standalone Raritan Serial Client (RSC) is used to make direct connections to the target without going through the Dominion SX GUI application. The user specifies the Dominion 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 will function 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, of course for 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. Browse to the page at **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** 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, environment variables must be configured. Make a note of the exact path where Java was installed. (The path information will be used later.)

Setting Windows OS Variables

1. Open the Start menu, and then open the Control Panel and choose **System**.
2. Go to **Advanced** and open **Environment Variables**.
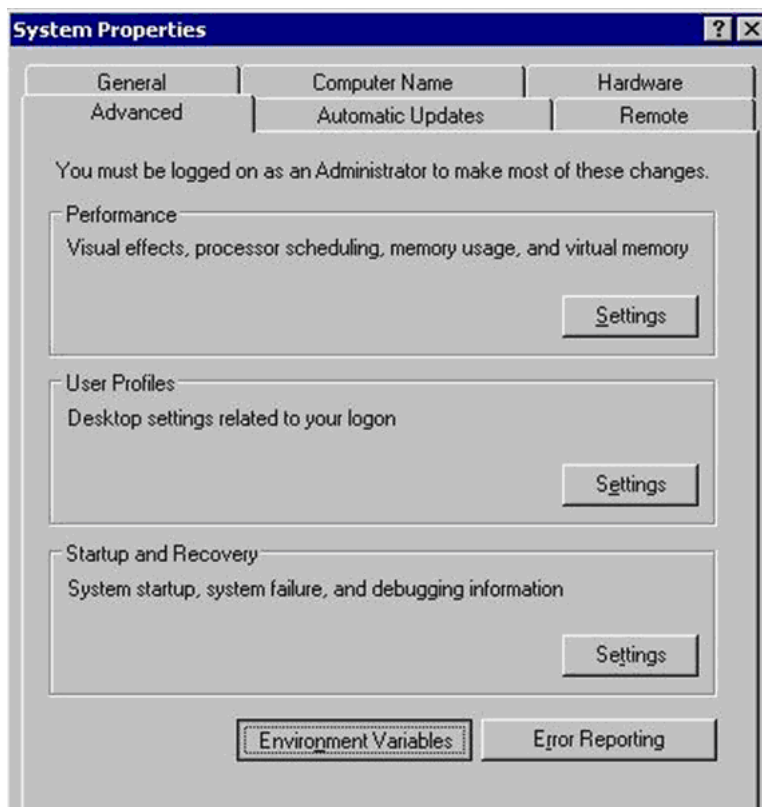
Figure 44 Windows OS: System Properties

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**.
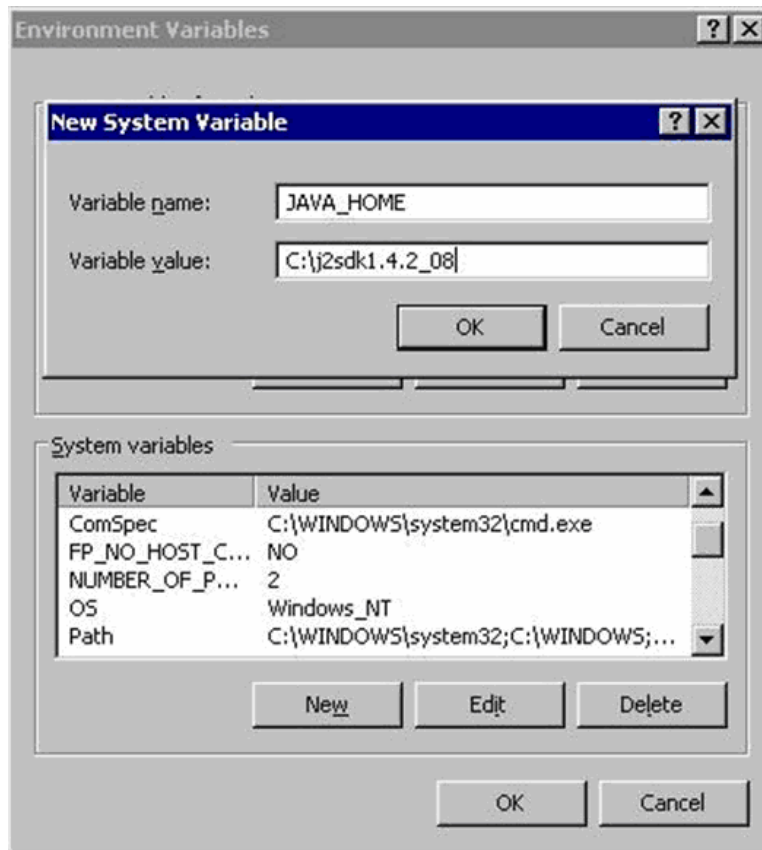
Figure 45 Windows OS: New System Variable

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**.
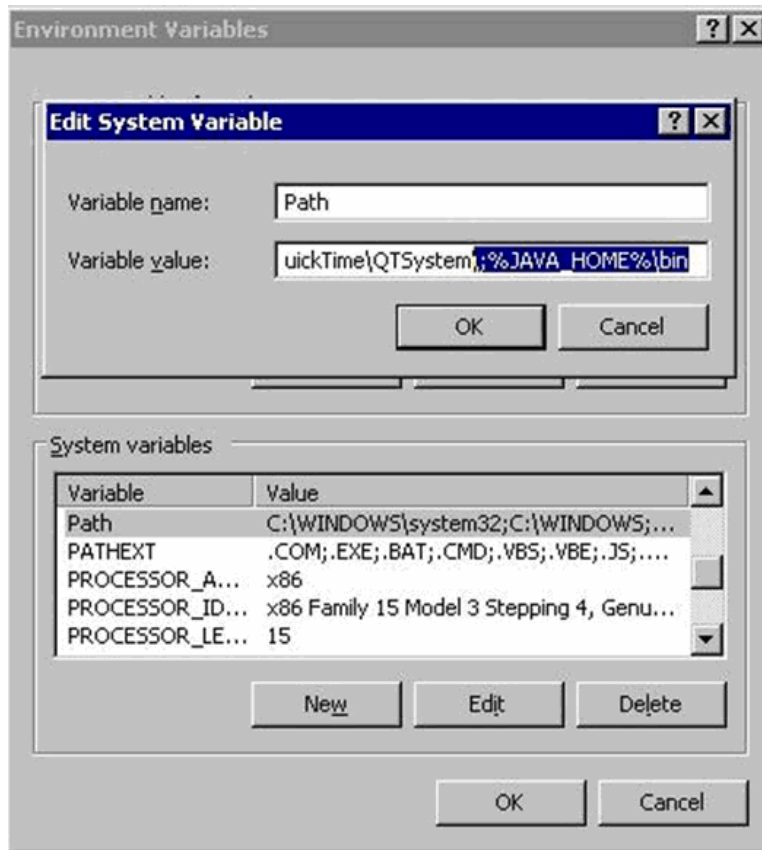
Figure 46 Windows OS: Edit System Variable

9. Select the CLASSPATH variable and click **Edit**.

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.
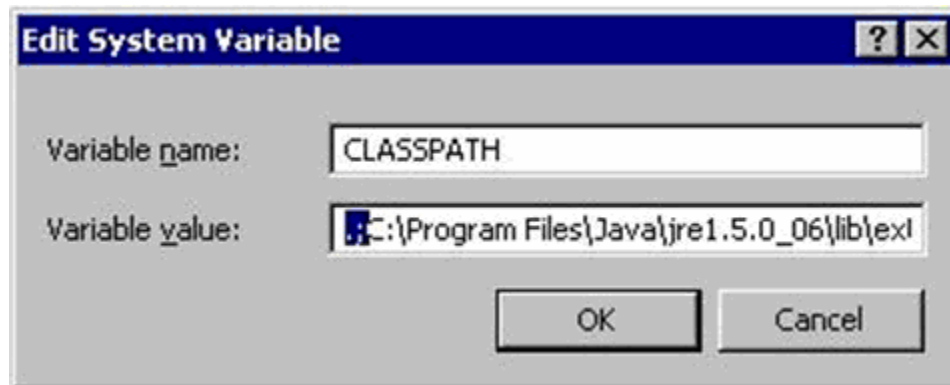
Figure 47 Windows OS: CLASSPATH Variable

Setting Linux OS Variables

If you want to set Java for this user only, open and edit **.profile** file located in the
/home/Username folder.
If you want to set Java for all users, open **.profile** file in your /etc folder

1. Find the line where you set your PATH

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

2. Before that line you must set your JAVA_HOME and then modify your PATH to include it.
    To achieve this, add the following lines:

    export
    JAVA_HOME=/home/username/j2sdk1.4.2/
    export PATH=$PATH:$JAVA_HOME/bin

3. Save the file and you are finished.

Setting UNIX OS Variables

Perform the following steps 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.
    *   To set your path: Assuming JRE 1.4.2_05 is installed in /usr/local/java: you must
        set your PATH variable.
    *   To set path for bash shell:
        export PATH=$PATH:/usr/local/java/j2re1.4.2_05/bin**.**
    *   To set path for tcsh or csh:
        set PATH = ($PATH /usr/local/java/j2re1.4.2_05/bin)**.**
    *   These commands can either be typed at the terminal each time you log in, or you can add
        them to your .bashrc for bash shell or .cshrc for csh or tcsh so that each time you log in,
        the PATH is already set. See your shell documentation if you encounter problems.

Figure 48 Check JRE Version in Sun Solaris

3. If the JRE is version **1.4.2_05** or later, but not version 1.5.0_02 , proceed with the RSC
    installation. If the version is older, go to the Sun Web site 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 on 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 screen appears.
4. Click **Next**. The installation path screen appears.
5. Change the path, if desired.
6. Click **Next**. The installation progress screen appears.

Note: The standalone version of Raritan Serial Console (RSC) is available from the Raritan Support website: http://www.raritan.com/support/sup_upgrades.aspx
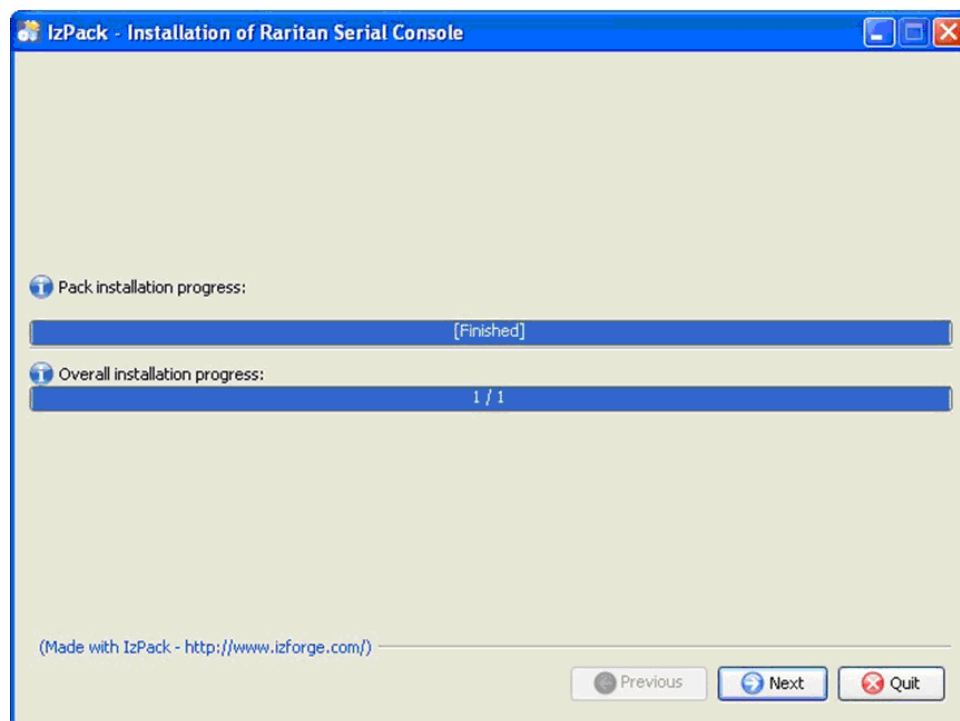
Figure 49 RSC Windows Install Progress Screen

7. Click **Next.** The Windows shortcut screen appears.
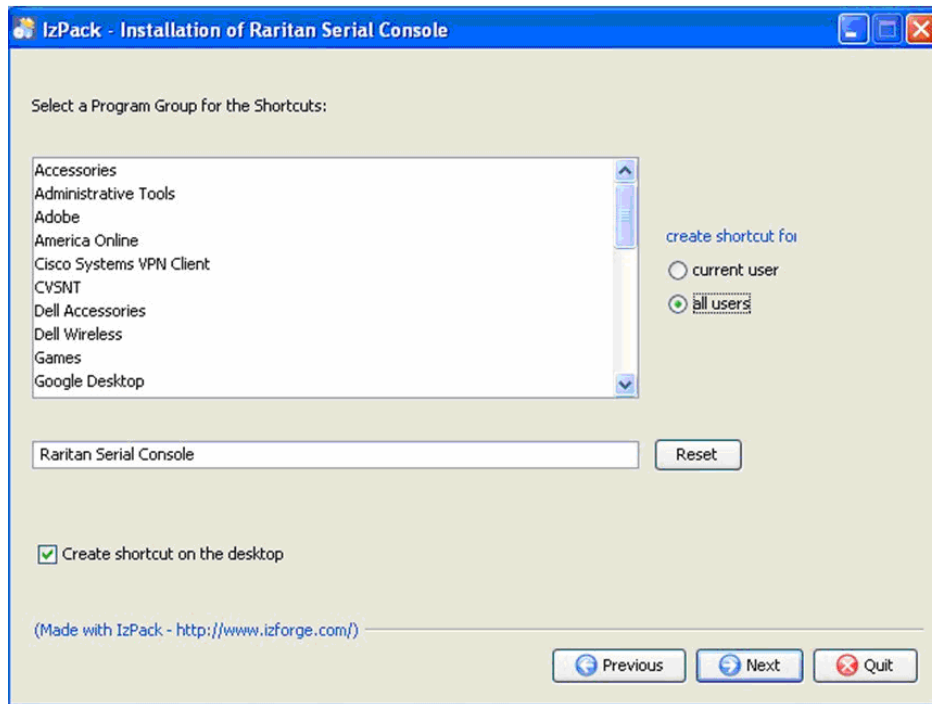
Figure 50 RSC Windows Shortcut Screen

8. Specify the desired Program Group for the Shortcut.
9. Click **Next**. The installation finished screen appears.
10. Click **Done**.

Launching RSC on Windows Systems

1. Double-click on the **shortcut** or use **Start Programs** to launch the standalone RSC. The **Raritan Serial Console Login** connection properties window appears.
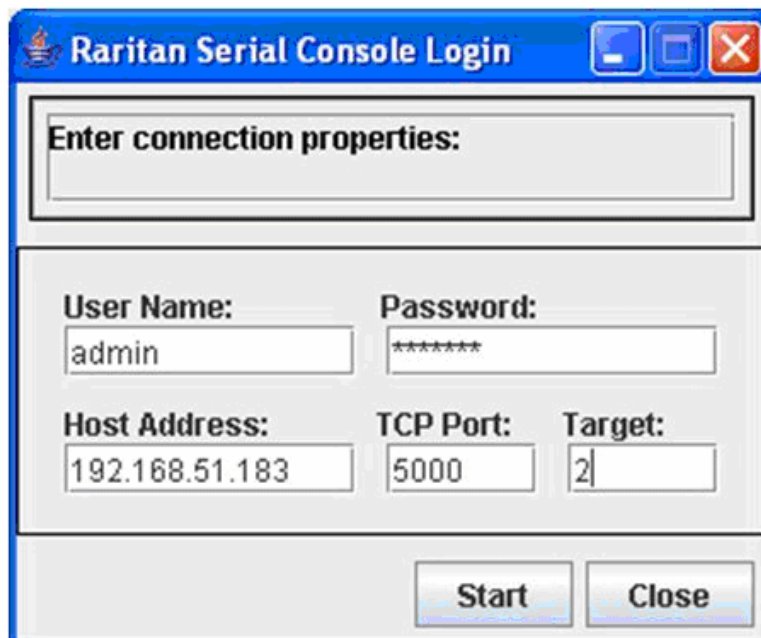
Figure 51 Standalone RSC Login Screen

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.
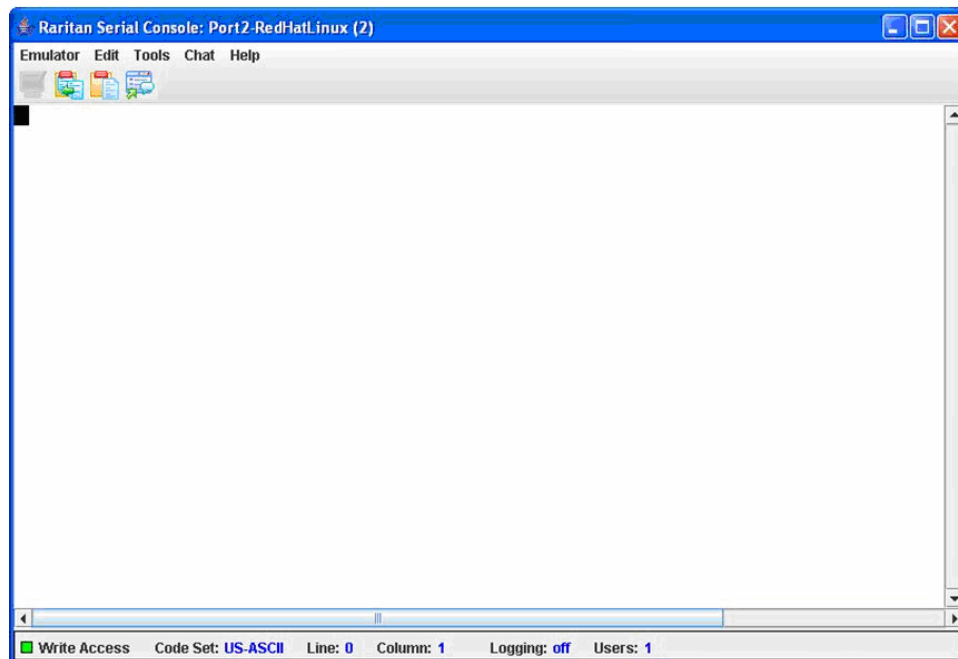
Figure 52 Standalone RSC Connected to Port Window

Note: In case of unrecognized characters or blurry screens that might appear in RSC window due to localization support, please try changing the font to Courier New. Go to: Emulator → Settings → Display, and select Courier New for Terminal Font Properties or GUI Font Properties.

Installing RSC for Sun Solaris

You must have administrative privileges to install RSC.

1. Log on 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 screen loads.

6. The **Set Installation Path** screen appears.
    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 screen indicates where you will find an uninstaller program, and allows the option of generating an automatic installation script.
    e) Click **Done** to close the Installation window.

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 **ENTER** 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 on.

Chapter 8: Security

There are a number of elements to consider when addressing security for console servers. The following are some of the Security aspects:

- Encrypting the data traffic sent between the operator console and the DSX unit.
- Providing authentication and authorization for users.
- Logging data relevant to the operation so it can later be viewed for auditing purposes. In some cases, this data is required for compliance with governmental or company regulations.
- Encryption of port data log sent to a remote nfs server.
- Security profile
- "Man in the Middle"

The Security function provides the Dominion SX administrator with the following tools:

- Specify login authentication and handling parameters.
- Kerberos settings.
- Certificate specifications.
- Banner to be displayed.
- Security profile management.
- Manage firewall rules.

Security Settings

Select the **Security** tab to bring up the security-related tools. The Security Settings screen appears.

Figure 53 Security Settings Screen

Login Settings

Click **Login Settings** on the Security Settings screen to access the Login Settings screen, which contains the Local Authentication, Login Handling, and Strong Password Settings panels..

Figure 54 Login Settings Screen

Local Authentication

1. Go to the Local Authentication panel and click the **Enable Local Authentication** checkbox.
2. 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 is to 0, which effectively disables this feature.
2. To enable single login only, click the **Single Login per User** checkbox. Only one user can log in at a time using the same profile.
3. Click the **Anonymous Port Access** checkbox to turn this feature on. An Anonymous User Group is created by default and it can't be deleted even by the Administrator. It is visible/not visible in Group List if Anonymous Port Access is unchecked/checked.

Note: Refer to Chapter 7 for additional information about anonymous port access.

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.

Configure Kerberos

Figure 55 Kerberos Settings

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 DSX, and install a user certificate on the DSX.

Generate a Certificate Signing Request

To generate a Certificate Signing Request (CSR):

1. Click the **Security** tab, and then click **Certificate**. The Certificate screen appears.

Figure 56 Certificate Signing Request

2. Click the checkbox labeled **Generate a Certificate Signing Request**.
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 DSX:

1. Click the **Security** tab, and then click **Certificate**. The Certificate screen appears.
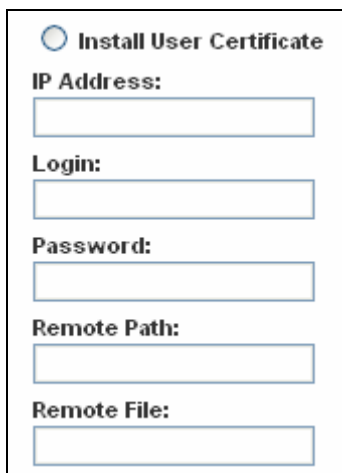
Figure 57 Install User Key

2. Click the checkbox labeled **Install User Key**.
3. Type the following information in the corresponding fields:
    - The IP address of the host with the key
    - A login and password on the host
    - The path and name of the file containing the key
6. Click **OK**.

Install a User Certificate

To install a user certificate on the DSX:

1. Click the **Security** tab, and then click **Certificate**. The Certificate screen appears.

Figure 58 Install User Certificate

2. Click the checkbox labeled **Install User Certificate**.
3. Type the following information in the corresponding fields:
    - The IP address of the host with the certificate
    - A login and password on the host
    - The path and name of the file containing the certificate
4. Click **OK**.

SSL Client Certificate

SSL Security certificates are used in browser access to ensure that the device that you are attached to is the device that is authorized to be connected. See **Appendix C: Certificates** 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

Figure 59 SSL Client Certificate Screen

Enabling Client Certificate Authentication:

To enable Client Certificate Authentication:
1. Click **Enable SSL Client Certification**.
2. Click **OK** to enable the Client Certificate authentication.

Installing a New Trusted Certificate Authority

To install a new trusted Certificate Authority (CA) to the DSX, the CA certificate must be on an accessible FTP server.
1. Click **Install Certificate Authority**.
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 DSX.

Removing a User-Added Certificate Authority

To remove a user-added CA from the DSX:
1. Click **Remove Certificate Authority**.
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.

Viewing a Certificate Authority

To view a CA:
1. Click **View Certificate Authority**.
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.

Managing the Client Certificate Revocation List (CRL)

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

Adding a New Certificate Revocation List to the DSX

To add a new CRL to the DSX, the CRL list must be on an accessible FTP server.
1. Click **Add Certificate Revocation List**.
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.

Deleting a Certificate Revocation List from the DSX

To delete a CRL from the SX:
1. Click **Delete Certificate Revocation List**.
2. In the **CRL Name** field, type the name of the CA this CRL belongs to.
3. Click **OK** to delete the CRL.

Viewing a Certificate Revocation List

To view a CRL:

1. Click **View Certificate Revocation Lis**t.
2. Click **OK** to retrieve the list of CRLs.

Banner

Dominion SX optionally supports a customizable (maximum 5000 words, 8 words per row) welcome banner that is displayed after login. The banner identifies where the user has logged into. In addition, there is the ability to add a consent banner that forces the user to accept the stated conditions prior to advancing into operation of the console server.
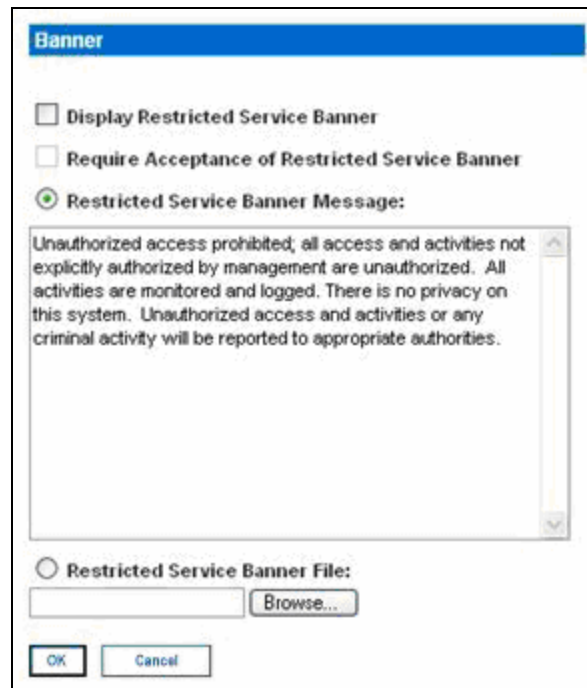
Figure 60 Banner Screen

1. Check one of the following fields.
    *   **Display Restricted Service Banne**r
    *   **Require Acceptance of Restricted Service Banner**
2. Check one of the following fields:
    *   **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 DSX login screen.
5. Click **OK**.

Security Profiles

The DSX provides three security profiles that you can use. They simplify the assigning of 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 have to disable the profile in order 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 unchecked, and you enable the Secure profile, this feature becomes checked. When you disable the Secure profile, the **TLS Required** feature remains checked.

Select a Security Profile

To select a security profile:

1. Click the **Security** tab, and then click **Security Profiles**. The Security Profiles screen appears.
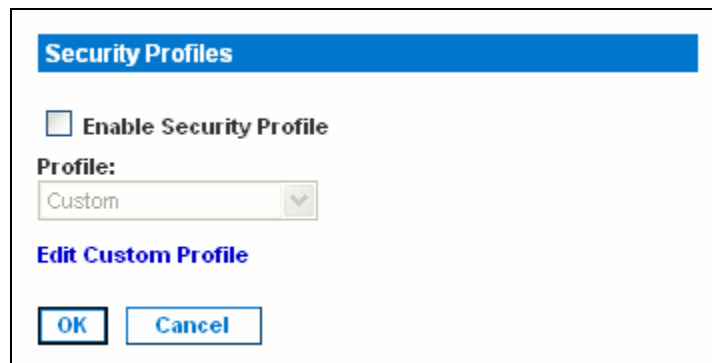
Figure 61 Security Profiles
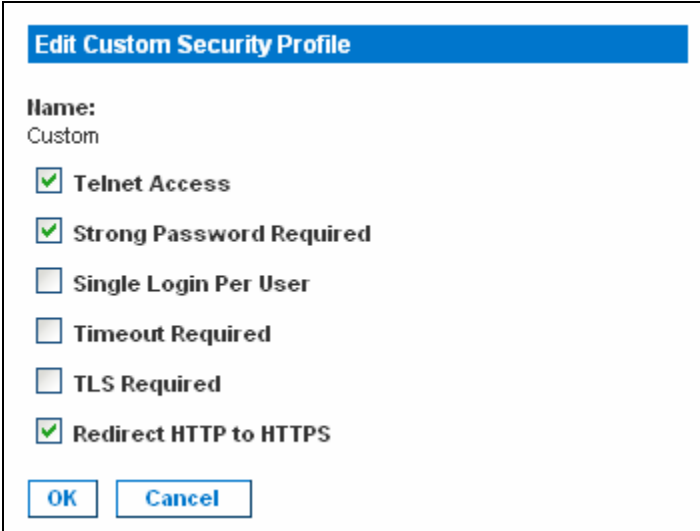
2. Click the checkbox labeled **Enable Security Profile**.
3. Select the profile from the drop-down menu in the **Profile** field.
4. Click **OK**.

Edit the Custom Profile

To edit the Custom profile:

1. Click the **Security** tab, and then click **Security Profiles**. The Security Profiles screen appears.

2. Click the **Edit Custom Profile** link. The Edit Custom Security Profile screen appears.

Figure 62 Edit Custom Security Profile Screen

3. Check one or all of the following fields.
    - Telnet Access
    - Strong Password Required
    - Single Login Per User
    - Timeout Required
    - TLS Required
    - Redirect HTTP to HTTPS

4. Click **OK**.

Firewall

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

Enable the Firewall

To enable the firewall:

1. Click the **Security** tab, and then click **Firewall**. The Firewall Screen appears. The Firewall screen displays the existing IPTables rules.

Figure 63 Firewall Screen

2. Click the check box labeled **Enable Firewall**.
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. Click the **Security** tab, and then click **Firewall**. The Firewall Screen appears. The firewall screen displays the default IPTables rules.
2. Go to the **Add/Delete IP Tables 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.
5. Add **new rules if you choose.**

   Note: Rules are added using the IP Tables command to the kernel. These rules take effect immediately but persist permanently only after clicking the Save button.

   Note: If there is a mistake in the rules and as a result, the unit becomes inaccessible, 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 9: Logging

This chapter explains how to enable and configure the various DSX logs.

Configuring Local Event Logging

To configure the local log settings, click the **Setup** tab, and then click **Log**. The Log Settings screen appears. 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 DSX unit. To set this feature up:

1. Go to the Event Log panel and click the **Enable Event Log File** checkbox. (To turn this feature off, clear this checkbox.).
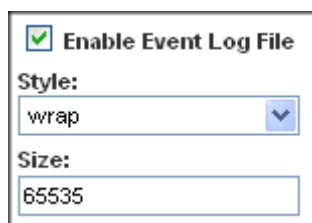
Figure 64 Event Log Panel

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 Dominion 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.)
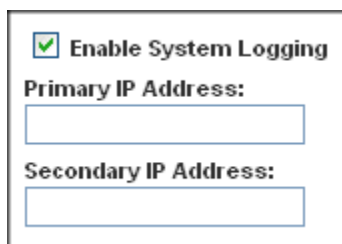
Figure 65 System Logging Panel

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 Logging

You need to configure port logging **after** you have enabled NFS logging (see "Configuring NFS Logging" below).

This feature enables port data to be logged to a Network File System (NFS) server. This allows 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 DSX 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 click the **Enable Port Logging** checkbox. (To turn this feature off, clear this checkbox.)

Figure 66 Port Logging Panel

2. Type the prefix to the port data file's name on the NFS server in the **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 DSX will not create 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 will disable timestamps in the log file. The maximum value is 99999. This field is optional.

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**.

Figure 67 shows an example of an output file.

```
Mon Nov 06-2006 13:46:20 -------- admin connected to port--------
Mon Nov 06-2006 13:46:21 -------- admin got write access --------
Password:
Authentication failure.
Username: admin
Password:
Authentication successful.


------------------------------------------------------------------------
Welcome to the DominionSX.  [Model: SX32]
UnitName:sx181        FirmwareVersion:3.0.1.5.1      Serial:WAOF300029
IP Address:192.168.51.181   UserIdletimeout:5min

Port Port               Port Port               Port Port
No.  Name                No.  Name                No.  Name
1  - Port1 [U]           2  - Port2 [U]           3  - Port3 [U]
4  - Port4 [U]           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 - Port31 [U]          32 - Port32 [U]
Current Time: Mon Nov  6 16:34:35 2006

admin > log
admin >
-- sx240_16ports UP -- Mon Nov 06-2006 13:46:38
lgo^G
admin > logout

Username:

Mon Nov 06-2006 13:46:47 -------- admin disconnected from port --------
```

Figure 67 Sample Output File

Configure Input Port Logging

To enable input port logging:

1. Go to the Input Port Logging panel and click the **Enable Input Port Logging** checkbox. (To turn this feature off, clear this checkbox.)
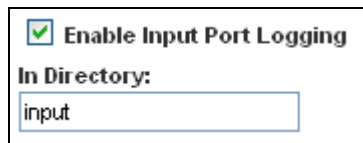
Figure 68 Input Port Logging Panel

2. Type a directory for input in the **In Directory** field.

3. Click **OK**.

Configuring Encryption

To configure encryption:

1. Go to the Encryption panel and click the **Encryption** checkbox. (To turn this feature off, clear this checkbox.)

Figure 69 Encryption Panel

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

3. Click **OK**.

Configuring SMTP Logging

To configure SMTP logging, click the **Setup** tab, and then click **Events**. The SMTP Logging screen appears. This screen contains and SMTP Settings panel and a New SMTP Event panel.

Enable SMTP Logging

To enable SMTP logging:

1. Go to the SMTP Settings panel and click the Enable SMTP Server checkbox to enable SMTP logging.

Figure 70 SMTP Settings Panel

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 the new event in the **Event** field.
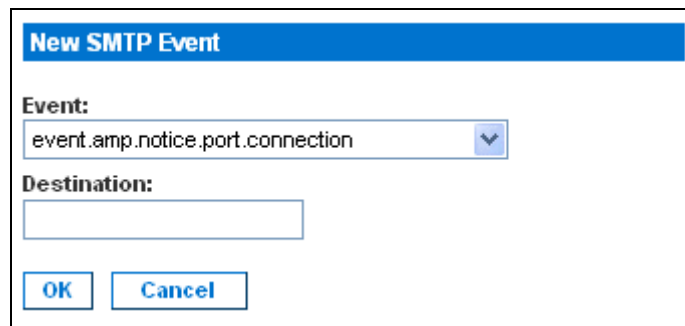
Figure 71 New SMTP Event Panel

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.strongpasssword

- 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. Type the email address to send the event in the **Destination** field.

3. Click **OK**.

Test the SMTP Logging

It is important that the SMTP server information be accurate so that the Dominion 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" above.

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

To configure NFS Logging:

1. Click the **Setup** tab, and then click **NFS**. The NFS Settings screen appears.

Figure 72 NFS Settings Screen

2. Click 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 DSX supports Simple Network Management Protocol (SNMP) traps and logging.

Enable SNMP Logging

To enable SNMP logging:

1. Click the **Setup** tab, and then click **SNMP**. The SNMP screen appears.

2. Go to the SNMP Setting panel and click the **Enable SNMP** checkbox to enable the SNMP feature.
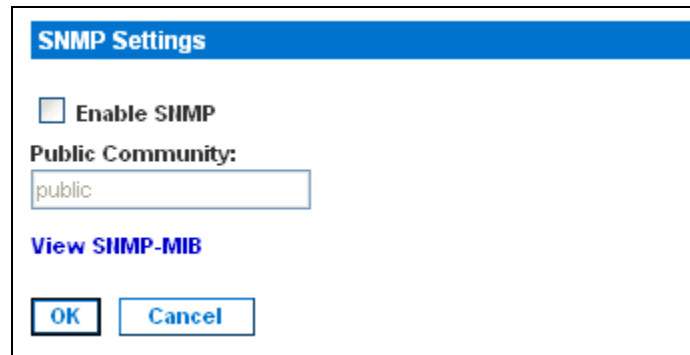
Figure 73 SNMP Settings Panel

3. 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.

4. Click **OK.**

Create a New SNMP Destination

SNMP destinations determine which SNMP management stations receive SNMP traps. To create a new SNMP destination:

1. Go the SNMP Destination panel and type the IP address of the new destination in the **IP Address** field.
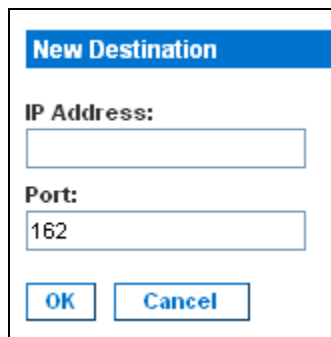
Figure 74 SNMP Destination Panel

2. By default, the new destination will use the standard SNMP port of 162. You can change this to another port, if you wish, by entering a different port number in the **Port** field.

3. Click **OK**.

Note: To display the SNMP Management Information Base (MIB), click the View SNMP-MIB link in the SNMP Settings panel (Figure 73).

≡Σ Raritan.

Chapter 10: Maintenance

The Dominion SX maintenance features presented in this chapter allow the administrator perform the following tasks:

- Manage event logs.

- View configuration report.

- Backup and restore the SX unit settings.

- Upgrade firmware and track upgrade history.

- Reset to factory default settings.

- Reboot the unit.

Managing the Local Event Log

The DSX 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, click the **Maintenance** tab, and then click **View Event Log**. The event log is displayed. Figure 75 shows a typical event log.

Date/Time	Event
Feb 1 16:30:35	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for Logging.
Feb 1 16:30:35	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for User.
Feb 1 16:30:40	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for DominionSX.
Feb 5 11:12:23	DominionSX DomSX: DominionSX notice SXRebootCompleted
Feb 5 11:12:25	DominionSX DomSX: DominionSX notice SXSystemReady
Feb 5 11:13:24	DominionSX DomSX: DominionSX info SXUserLogin LAN Local Elaine 192.168.50.153
Feb 5 12:02:04	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for SNTP.
Feb 5 12:02:04	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for User.
Feb 5 12:02:09	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for SNTP.
Feb 5 12:40:16	DominionSX DomSX: DominionSX notice SXUserDeleted Admin user deleted user "Tricia"
Feb 5 12:40:16	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for User.
Feb 5 12:40:45	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for Group.
Feb 5 12:53:51	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for Device.
Feb 5 12:53:59	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for Interface.
Feb 5 12:54:00	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for CSCDiscovery.
Feb 5 12:54:00	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for CSC.
Feb 5 12:55:23	DominionSX DomSX: DominionSX notice SXRebootCompleted
Feb 5 12:55:25	DominionSX DomSX: DominionSX notice SXSystemReady
Feb 5 12:58:20	DominionSX DomSX: DominionSX info SXUserLogin LAN Local Elaine 192.168.50.153
Feb 5 13:04:37	DominionSX DomSX: DominionSX notice SXSettingSaved User Elaine changed configuration for User.

Figure 75 Event Log

Note: If the number of events in the log exceeds the size of one screen, a Next link is added 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. Click the **Maintenance** tab, and then click **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. Click the **Maintenance** tab, and then click **Send Event** Log. The Send Event Log screen appears.
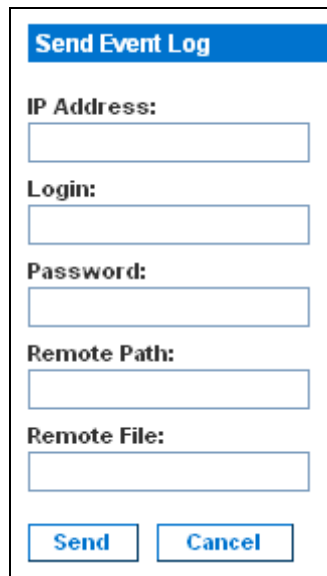
Figure 76 Send Event Log Screen

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 will be 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 is a report that provides detailed information about the DSX unit. To display the report, click the **Maintenance** tab, and then click **Configuration Report**. The report shows:

- Version and firmware information
- Port settings
- User and group settings
- HTTP, HTTPS, SSH and Telnet ettings
- RADIUS, LDAP, TACACS+, and Kerberos settings
- Local authentication settings
- Other settings
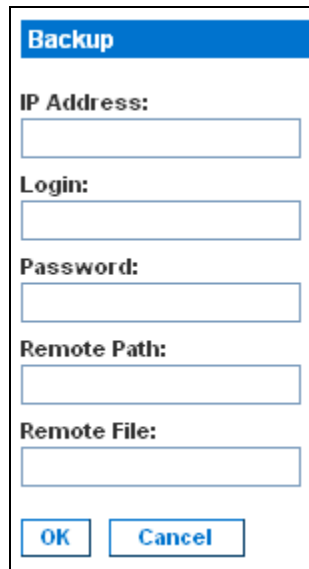
Backing Up and Restoring the DSX

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

Backing Up the DSX

To back up the DSX unit:

1. Click the **Maintenance** tab, and then click **Backup**. The Backup screen appears.

Figure 77 Backup Screen

2. In the **IP Address** field, type the IP address of the target FTP server where the backup will be written.

3. In the **Login** field, type the login name of the account on the system where the backup will be stored.

4. In the **Password** field, type the password of the account on the system where the backup will be stored.

5. In the **Remote Path** field, type the path to the backup file.

6. In the **Remote File** field, type the name of the file in which the backup will be saved.

7. Click **OK**.

Restoring the DSX

Restoring the DSX retrieves a copy of the DSX configuration from the FTP server where it has been backed up and writes the file to the DSX. To perform a restore operation

1. Click the **Maintenance** tab, and then click **Restore**. The Restore screen appears.
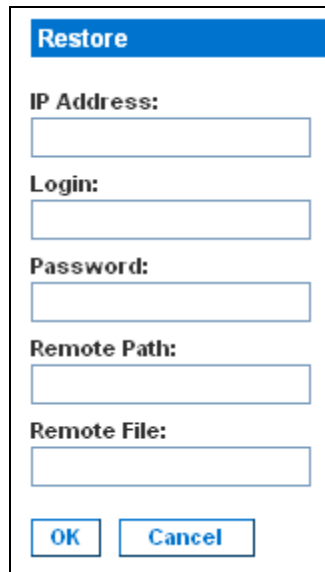
Figure 78 Restore Screen

2. In the **IP Address** field, type the IP address of the source FTP server system from which the restore data will be retrieved.

3. In the **Login** field, type the login name of the account on the system where the restore data will be stored.

4. In the **Password** field, type the password of the account on the system where the restore data will be stored.

5. In the **Remote Path** field, type the path to the restore file.

6. In the **Remote File** field, type the name of the file in which the restore will be saved.

7. Click **OK**.

Upgrading the DSX Firmware

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

Display the Current Firmware Version

To display the current version of firmware running on a DSX unit, click the **Maintenance** tab, and then click **Firmware Version**. The Firmware Version screen appears. This screen shows the firmware version, RSC, kernel, and PMON.

Firmware Version

Firmware Version:	3.1.0.1.2
RSC:	1.0.0.5.2
Kernel:	2.4.12
PMON:	2.0.1

Figure 79 Firmware Version

Upgrade the Firmware

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 Dominion 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. Click the **Maintenance** tab, and then click **Firmware Upgrade**. The Firmware Upgrade screen appears.

Figure 80 Firmware Upgrade Screen

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 (e.g. /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 DSX will turn off, flash once while it is extracting more files, turn off, then turn on and remain on. You will be 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 a DSX unit, click the **Maintenance** tab, and then click **Firmware Upgrade History**. The Firmware Upgrade History screen appears. It gives the version of each past firmware upgrade and the date and time the upgrade was performed.

Figure 81 Firmware Upgrade History Screen

Performing a Factory Reset on the DSX

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

To perform a factory reset, click the **Maintenance** tab, and then click **Factory Reset**. You will be 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 DSX GUI to perform a factory reset, you may want to try resetting from the DSX hardware. To do so, insert a pin into the RESET hole on the back panel of DSX unit and hold for about 15 seconds. Then the DSX is reset back to factory defaults.

Rebooting the DSX

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

To perform a reboot, click the **Maintenance** tab, and then click **Reboot**. You will be prompted to confirm the reboot. Click **Yes** to proceed. If you change your mind, click **No**.

Chapter 11: Diagnostics

The Diagnostics function provides the administrator with the tools to test the network and monitor processes.

Select the **Diagnostics** tab to display the Diagnostics screen. It provides links to Network Infrastructure Tools and Administrator Tools.

Figure 82 Diagnostics Screen

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. Click **Status of Active Network Interfaces** on the Diagnostics screen**.** The system displays status information about the active network interfaces.
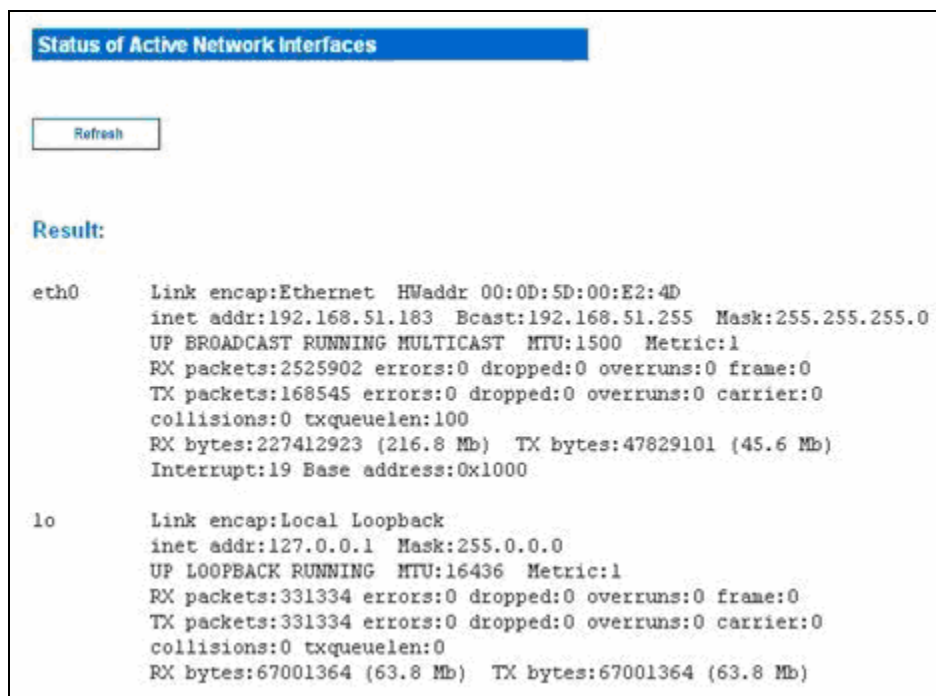
Figure 83 Active Network Interface Status

2. Click **Refresh** to update the information.

Network Statistics

1. Click **Network Statistics** on the Diagnostics screen. The system displays network statistics.

```
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_rdmp
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
```

Figure 84 Network Statistics

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:
    o   Route
    o   Interfaces
    o   Groups
    o   Statistics
    o   Program
3. Click **Refresh** to update the information.

Ping Host

1. Click **Ping Host** on the Diagnostics screen. The Ping Host screen appears.
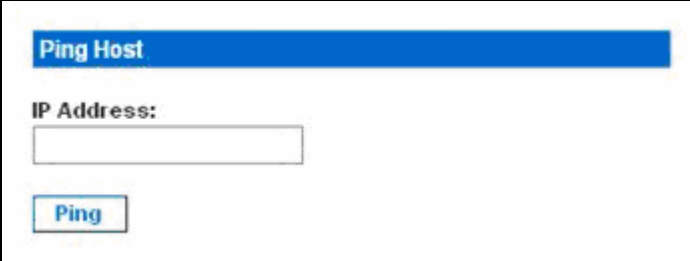
Figure 85 Ping Host

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

Trace Route to Host
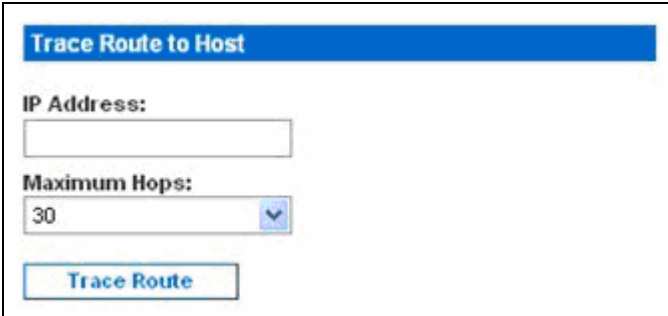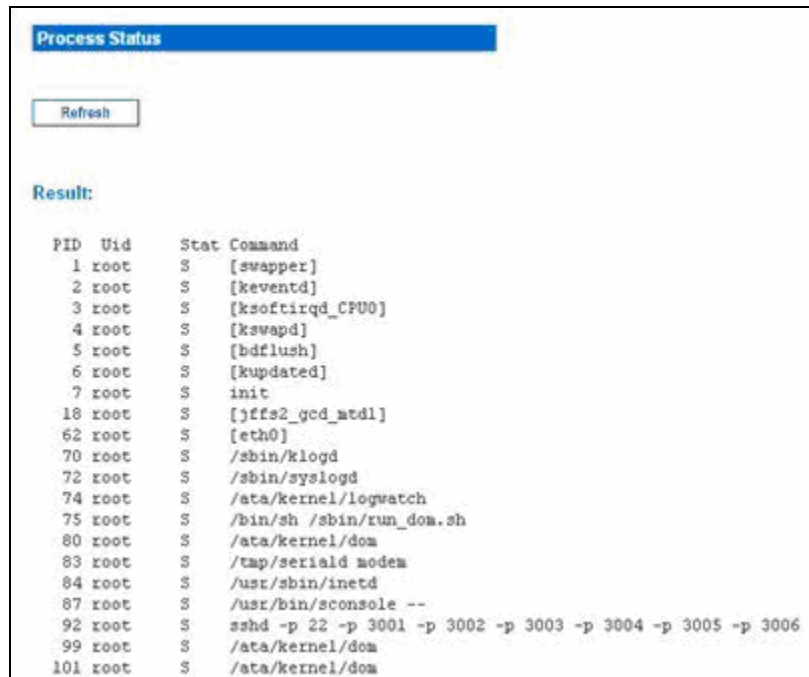
Figure 86 Trace Route to Host

1. Click **Trace Route to Host** on the Diagnostics screen. The Trace Route to Host screen appears.
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 screen displays the results of the Trace Route.

Administrator Tools — Process Status

1. Click **Process Status** in the Diagnostics Screen. The screen displays the results of your request.

Figure 87 Process Status

2. Click **Refresh** to update the information.

Chapter 12: Command Line Interface

Command Line Interface Overview

The Dominion SX Serial Console supports all serial devices such as:

- 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 Dominion 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 Dominion SX or to connect to target devices. The RS-232 interface may operate at all standard rates from 1200 bps to 115200 bps.

Note: The following figures describe an overview of the CLI commands. See CLI Commands for a list of all the commands, which include definitions, and links to the sections in this chapter that give examples of these commands

CLI Command Overview – Part 1

configuration

authentication

- ldap
  - ldaps
    - getservercert
    - removeservercert
    - viewservercert
  - primaryldap
  - secondaryldap
- radius
  - primaryradius
  - secondaryradius
- tacacsplus
  - primarytacacs
  - secondarytacacs

events
- add
- delete
- smtp

log
- cleareventlog
- eventlogfile
- eventsyslog
- nfsgetkey
- nfssetkey
- portlog
- sendeventlog
- vieweventlog

modem
- dialback
- dialin

network
- ethernetfailover
- interface
- ipforwarding
- name
- ports
- route
- routeadd
- routedelete

nfs
- nfs

ports
- config
- keywordadd
- keyworddelete

services
- dpa
- encryption
- http
- https
- logout
- lpa
- ssh
- telnet

snmp
- add
- delete
- snmp

time
- clock
- ntp
- timezonelist

users
- addgroup
- adduser
- deletegroup
- deleteuser
- editgroup
- edituser
- groups
- users

CLI Command Overview – Part 2

Connect

(port sub-menu, reached using escape key sequence)

- clearhistory
- close
- gethistory
- getwrite
- return
- sendbreak
- writelock
- writeunlock

Diagnostics

- ifconfig
- netstat
- ps
- traceroute

history

ipmi
- ipmidiscover
- ipmitool

listports

Maintenance

- backup
- cleareventlog
- factoryreset
- firmware
- logoff
- password
- reboot
- restore
- sendeventlog
- upgrade
- upgradehistory
- upgradestatus
- userlist
- vieweventlog

Security

banner
- banner
- ftpgetbanner

certificate
- client
- server

firewall
- firewall
- iptables

kerberos
- gethostnamefile
- getkrbconfig
- kadmin
- kerberos
- kinit
- klist

loginsettings
- idletimeout
- inactiveloginexpiry
- invalidloginretries
- localauth
- lockoutperiod
- singleloginperuser
- strongpassword
- unauthorizedportaccess

securityprofiles
- profiledata
- securityprofiles

show

(available in all menus)

top

userlist

The following common commands can be used from all levels of the CLI to the preceding figure: top, history, logout, quit, show, and help.

Accessing the Dominion SX Using CLI

Access the Dominion SX by using one of the following methods:

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

A number of SSH/Telnet clients are available and can be obtained from the following locations[1]:

- Putty - http://www.chiark.greenend.org.uk/~sgtatham/putty/
- SSH Client from ssh.com – www.ssh.com
- Applet SSH Client – www.netspace.org/ssh
- OpenSSH Client - www.openssh.org

SSH Connection to the Dominion SX

The SSHv2 Server is configured to run on the Dominion SX by default. Use any SSH client that supports SSHv2 to connect to it.

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

Specific information about configuring particular SSH clients is beyond the scope of this document.

SSH Access from a Windows PC

To open an SSH session from a Windows PC:

1. Launch the SSH client software, such as PuTTY.
2. Enter the IP address of the DSX server `192.168.0.192`.
3. Select **SSH**, which uses the default configuration port 22.
4. Click the **Open** button.
5. The following prompt appears:
   `login as:`

See the **Login** section for login information.

SSH Access from a UNIX Workstation

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

`ssh -l admin 192.168.0.192`

The following prompt appears:
`password:`

See the **Login** section for login information.

---

1 Raritan does its best to keep these links accurate. If you find inaccuracies with this information, please contact Raritan.

Telnet Connection to the Dominion SX

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

Enabling Telnet

If you wish to use Telnet to access the DSX, first access the DSX from the CLI or a browser.

CLI

1. Use the following command:
   ```
   admin > 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 > 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 DSX Unit

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

Telnet Access from a Windows PC

To open a Telnet session from a PC:

1. Select **Run** from the Startup menu.
2. Type **Telnet** in the Open text box.
3. Click **OK**. The Telnet window opens.
4. At the prompt enter the following command
   ```
   Microsoft Telnet> open <IP address>
   ```
   where *<IP address>* is the DSX IP address set up in Chapter 3.
5. Press **Enter**. The following message appears:
   ```
   Connecting To <IP address>...
   ```

The following prompt appears:
```
login as:
```

See the **Login** section for login information.

Local Port Connection to the Dominion SX

The local port of the Dominion SX must be connected to the COM port of a computer system, a terminal, or some other serial capable device using a null modem cable with DB-9F null on both ends.

If there is an RJ 45 interface, 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 device as a serial target to another SX.

Port Settings

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

- Bits per second = 9600
- 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 Dominion SX unit.
3. Disable Flow control.
4. Press **Enter** and the following prompt appears: *username:*

See the **Login** section for login information.

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, for example, to change the baud rate from the default 9600 bps to 115200 bps, enter:

```
admin > Config > Services > lpa enable true 115200
```

To disable local port access:

```
admin > Config > Services > lpa enable false
```

Login

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

```
login as: admin
```

The password prompt appears. Enter the default password: **raritan**

```
Password:
```

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

```
login as: admin
Password:
Authentication successful.


------------------------------------------------------------------
Welcome to the DominionSX  [Model: SX4]

UnitName:DominionSX        FirmwareVersion:3.0.0.5.1  Serial:WACEA00008

IP Address:192.168.51.194  UserIdletimeout:99min
------------------------------------------------------------------
Port Port                        Port Port

No.  Name                        No.  Name

1  - Port1 [U]                    2  - Port2 [U]

3  - Port3 [U]                    4  - Port4 [U]


Current Time: Wed Sep 20 16:17:15 2006



admin >
```

Figure 88 Sample Administrator Login

```
5. login as: Janet

6. Password:

7. Authentication successful.

8.  --------------------------------------------------------------
Welcome to the DominionSX  [Model: SX4]

UnitName:DominionSX        FirmwareVersion:3.0.0.5.1  Serial:WACEA00008

IP Address:192.168.51.194  UserIdletimeout:99min

9. --------------------------------------------------------------

10.

11.  Port Port                        Port Port

12.  No.  Name                        No.  Name

13.  1  - Port1 [U]                    2  - Port2 [U]

14.  3  - Port3 [U]                    4  - Port4 [U]

15.

16.  Current Time: Wed Sep 20 16:05:50 2006

17.

18.

19.  Janet >
```

Figure 89 Sample Operator or Observer Login

After reviewing the following **Navigation of the CLI** section, perform the <u>Initial Configuration</u> tasks.

Navigation of the CLI

Before using the CLI, it is important to understand CLI navigation and syntax; additionally, there are combinations of keystrokes that simplify CLI use.

Completion of Command

The CLI supports the completion of partially entered commands. After entering the first few characters of an entry, hit 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 greater than one possible match is found, the CLI also displays the valid entries.
- The user can enter additional text to make the entry unique and 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.
- A question mark (?) after a command gives help for that command.
- A vertical line (|) indicates a choice within an optional or required set of keywords or arguments.

Shortcuts

- Press the **Up-Arrow** to display the last entry.
- Use the **Backspace** key to delete the last character typed.
- Use **Ctrl/C** to terminate a command or cancel a command if you typed the wrong parameters.
- Use **Enter** to execute the command.
- Press **Tab** to complete a command, such as:

  `admin > Conf`

  The system displays the `admin > Config >` prompt.

Common Commands for all Command Line Interface Levels

Table 3 lists the commands that are available at all CLI levels. These commands also help navigate through the CLI.

Table 3 Commands Common to All CLI Levels

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 DSX CLI.
show	Show the settings for the given parameter or show all configuration 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 [localauth | ldap | radius | tacacs | smtp | network | nfs|
modem | port | http | lpa | ssh | telnet | snmp | ntp |
users | groups | idletimeout | events ] [all]<>
```

Command Example

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

```
admin > show

Dominion 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
```

Initial Configuration

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

1. Reset the administrator password.
   All Dominion 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 DSX device.
2. Assign the IP address, subnet mask, gateway IP address to allow remote access.
3. Set the time and date.

≡ **Raritan.**

Once the preceding parameters are set, the following areas can be configured from either the local console port or over the network:

- service
- security
- users
- serial ports

Setting Parameters

To set parameters the user must be logged in with administrative privileges. At the top level the user will see the "Username" > prompt, which for initial configuration is "admin" >. If the user has logged in with a different user name, that user name will appear instead of admin. Enter the top command to return to the top menu level.

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 > 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 > Config > Time > timezonelist`
2. `admin > Config > Time > clock tz 21 datetime 2006-09-23 13:22:33`

Setting Network Parameters

Network parameters are configured using the interface command.

```
admin > Config > Network > 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 DSX will need to be reset to the factory default from the reset button on the rear panel and the initial configuration tasks will need to be performed again.

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

CLI Prompts

The Command Line Interface prompt indicates the current command level. The root portion of the prompt is the login name; **admin** is the root portion in the following command:

admin > Config > Port >

CLI Commands

Table 4 lists and describes all available CLI commands.

Table 4 Available CLI Commands

COMMAND	DESCRIPTION
backup	*System command to backup the console server settings*
cleareventlog	*Clears the contents of the local event log*
config	*Port configuration command* *Switch to the Configuration menu.*
connect	*Connect to a port.*
diagnostics	*Switch to diagnostic commands menu.*
encryption	*Select the encryption method for HTTPS.*
eventlogfile	*Controls and configures the local event log.*
eventsyslog	*Controls system event logging.*
factory_reset	*System command to reset to the factory settings.*
firmware	*System command to display the versions of the firmware.*
help	*Display an overview of the CLI syntax.*
history	*Display the current session's command line history.*
http	*Enable http connections.*
ifconfig	*Show detailed network configuration.*
interface	*Configure the DSX network interface.*
ipmi	*IPMI Configuration commands.*
listports	*List accessible ports.*
Kerberos	*Kerberos based Network Authentication*
ldap	*LDAP Configuration .*
localauthentication	*Local Authentication Configuration .*
logout	*Logout of the current CLI session.*
maintenance	*Switch to System Maintenance commands.*
netstat	*Print network connections*
nfsget	*Generates an encryption key.*
nfssetkey	*Enables encryption of log data.*
password	*Set the current user's password.*
ping	*Ping a remote system.*
portlog	*Enables and configures the logging of port data.*
ps	*Report system process status*
quit	*Return to previous command*
radius	*Switch to the RADIUS Configuration menu.*
reboot	*System command to reboot the system.*
restore	*System command to restore the system*

security	Switch to the security menu.
sendeventlog	Sends the local event log to a remote FTP server.
show	Show configuration options.
tacacsplus	Switch to the TACACS+ Configuration Menu.
telnet	Enable telnet communication and specify the port.
top	Return to the root menu.
traceroute	Print the route to a remote system
upgrade	System command to upgrade the firmware.
upgradehistory	System command to show the upgrade history.
userlist	List users.
vieweventlog	Displays the local event log.

Security Issues

There are a number of elements to consider when addressing security for console servers:

- Encrypting the data traffic sent between the operator console and the DSX 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.
- Encryption of port data log sent to a remote nfs server.
- Security profile
- "Man in the Middle"

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

Configuring Encryption of Traffic

Encryption of traffic between the operator console and the DSX 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, the user must manually enable the HTTP and Telnet services.

Welcome Banner Configuration

Dominion SX optionally supports a customizable (maximum 6000 words) welcome banner that is displayed after login. The banner identifies where the user has logged into. In addition, there is the ability to add a consent banner that forces the user to accept the 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 device you are attaching to is the device that is authorized to be connected. This section describes only how to configure the certificates on the console server. See Appendix C for details on SSL Certificates.

Enabling Firewall Protection

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

Enabling Security Profiles

Dominion 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 Dominion SX, facilities are provided to log data and to provide alerts based on activities between the users, Dominion SX and the target device. These facilities provide an audit trail allowing the authority responsible to review what has happened in the system and determine who implemented what action and when.

Among the facilities provides 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. Dominion SX allows the administrator to define groups with common permissions and attributes. They can then add users to the groups and each user takes o the attributes and permissions of that group. By enabling groups, the permissions for each user do not have to be configured reducing the time to configure users.

Command Language Interface Permissions

Administrators can execute all commands.

Operators and Observers can only execute the following commands:

- Connect
- Help
- Listports
- Logout.
- Password

Target Connections and the CLI

The purpose of the Dominion SX unit 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 is displayed. The Dominion SX unit also provides the ability to share ports among users.

Set Emulation on Target

To set emulation on the target:

- Ensure that the encoding in use on the host matches the encoding configured for the target device. For example, 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.
- Ensure that the terminal emulation on the target host connected to the Dominion 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. For example, 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 Dominion SX unit is a property associated with the port settings for a particular target device. Ensure that the settings for terminal emulation in the client software, for example, 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 Dominion 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

It is possible for Access Client users to share ports with other authenticated and authorized users, regardless of whether they are Access Client users(RSC) 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.

Administering the Dominion SX Console Server

Configuration Commands

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

The commands available under the configuration menu provide the ability to configure the Dominion SX.

The following commands are available in the configuration menu:

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

Configuring Authorization and Authentication (AA) Services

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

- Idle time out for inactive users
- User defined certificates
- Security profiles.

Table 5 Configuration: Authentication Commands: ldap

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 "raritan: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 DSX.

If you use older (SX 2.5 and older release) formats of "op:1:2:4" or "a:" , the system will allow you to log in and will restrict the ports accessibility according to user types and their limitations. The DSX 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 there is no way for the client to know which port limitations exist.

LDAP Configuration Menu

The **ldap** configuration menu provides access to setting up ldap and ldaps.

The ldap is entered by typing ldap at the following prompt:

admin > Config > Authentication > ldap

The ldap command options are described in Table 6.

Table 6 LDAP Command

COMMAND OPTION	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 Example

```
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.

The syntax of the radius menu commands are:
```
primaryraduius                                                          <>
```

RADIUS Command Example
```
admin > Config > Authentication > radius > primaryradius
```

TACACSPLUS Command

The **tacacsplus** menu provides access to commands used to configure access to a TACACS+.

The syntax of the `tacacsplus` command is:
```
primarytacacs <>
```

Command Example

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

Configuring Events

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

Table 7 Configuration: Events Commands

COMMAND OPTION	DESCRIPTION
add	Add an SMTP event.
delete	Delete an SMTP event.
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** command provides the administrator with the following commands to manage the logging features of the Dominion SX server:

- cleareventlog
- eventlogfile
- eventsyslog
- nfsget
- nfssetkey
- portlog
- sendeventlog
- vieweventlog

Cleareventlog Command

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

The syntax of the cleareventlog command is:

```
cleareventlog
```

Cleareventlog Command Example
```
admin > Config > Log > cleareventlog
```

Eventlogfile Command

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

The syntax of the eventlogfile command is:

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

The eventlogfile command options are described in Table 8.

Table 8 Eventlogfile Command

COMMAND OPTION	DESCRIPTION
enable <true|false>	Enable or disable the system event log logging.
size value	Maximum size of local log file (in bytes)
style <wrap|flat>	Specifies what action to take when the maximum size is reached: wrap will cause the log to circle around when end is reached. flat will cause logging to stop when the end is reached.

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>] [] [secondary ip <ip>]
```

The eventsyslog command options are described in Table 9.

Table 9 Eventsyslog Command

COMMAND OPTION	DESCRIPTION
`enable <true|false>`	Enable or disable the system event log logging.
`primary ip <ip>`	Primary FTP server address
`secondary ip <ip>`	Secondary FTP server address

Eventsyslog Command Example

```
admin > Config > Log > eventsyslog enable true primaryip
192.168.134.11 secondaryip 192.168.245.11
```

nfsgetkey Command

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

The syntax of the nfsget command is:

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

The nfsgetkey command options are described in the following table.

Table 10 nfsget Command

COMMAND OPTION	DESCRIPTION
`type <rc4|aes128>`	Type of encryption key used for 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. NFS is notoriously insecure. It can be accessed easily and the data misused. With Dominion SX, the administrator has the ability to 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 used to encrypt.

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

The syntax of the nfssetkey command is:

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

The nfssetkey command options are described in Table 11.

Table 11 nfssetkey Command

COMMAND OPTION	DESCRIPTION
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.

Command Example

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

NFS Encryption Enable Command

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.

The syntax of the portlog command is:
```
portlog  [enable  <true|false>]  [prefix  name]  [size  value]
[timestamp interval] [update interval] [inputlog <true|false>]
[indir name] [outdir name] [encrypt <true|false>]
```

The portlog command options are described in Table 12.

Table 12 Portlog Command

COMMAND OPTION	DESCRIPTION
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 max value is 99999.
update interval	Time interval (in seconds) between two updates to the remote log file The default interval is 30. 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 (SX1Input)
outdir name	Filename for storing output log.(SX1Output) Output implies data sent from target to the DSX port.
encrypt <true|false>	Enable/Disable Encryption of log data sent to the remote NFS Server.

Portlog Command Example

```
admin > Config > Log > portlog enable true prefix DomSX1 size
1000000 timestamp 1 update 20 inputlog false indir /nfs SX DomIn
outdir SXDom 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
```

Decrypting Encrypted Log on Linux-based NFS Server

To decrypt nfs encryption on Linux platform, follow the instructions stated below:

1.   Retrieve the current nfs encryption key:

    `admin > Config > Log > nfsgetkey type rc4`

    (cut and paste the response of this command into a file, such as: dsx-encrypt.key)

2.   Retrieve decryption application and place it on the Linux machine, or compile its source.

3.   Save the encryption key file (e.g. dsx-encrypt.key) in the same directory where the decryption application is stored.

4.   Copy the encrypted portlog file to the same directory.

5.   Decrypt the file using the command:

    `./decrypt -f <portlogfile> -e <keyfilename> -o  <outputfile>`

    The decrypted file should be saved in `<outputfile>`.

Sendeventlog Command

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

The syntax of the sendeventlog command is:

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

The sendeventlog command options are described in Table 13.

Table 13 Sendeventlog Command

COMMAND OPTION	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

```
admin > Config > Log > sendeventlog 72.236.162.187 login acy
password pasraritansword path sxlogfile file log 32
```

Vieweventlog Command

The **vieweventlog** command displays the local log file.

The syntax of the vieweventlog command is:

```
vieweventfile
```

Vieweventlog Command Example

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

Configuring Modem

The **modem** menu provides access to 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 dialin. Configure modem dialin first and then enable dialback. Dialin and Dialback should be enabled on the device used for modem communication (local, RADIUS, LDAP, or TACACS+).

Table 14 Configuration: Modem Commands

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|disable>][server IP] [client IP]

Modem Menu Command Examples

```
admin > Config > modem > dialin enable true serverip 10.0.13.211
clientip 10.0.13.212
admin > Config > modem > dialback enable true
admin > Config> Modem > show modem
```

```
Modem Settings:
```
```
        Dialin Enabled: 1
        Server IP : 10.0.13.211
        Client IP : 10.0.13.212
```

```
        Dialback : Enabled
```
Dialback with local user.

Before a modem connection can be established, the local user that is going to be used for dialin authentication should be configured. A new user can be added or an existing one could be reconfigured with a correct dialback. The correct configured user (Dialback number is 129) should have the following settings:

```
User Settings:
        Login : Modem
        Name : Dialback
        Info: SX
        Dialback: 129
```

```
          Group :Admin
          Active : 1
```

Dialin and Dialback should be enabled on the device used for modem communication.

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

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

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

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


RADIUS Server Settings

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

Primary Server
        Enabled - true
        IP Address - 10.0.0.188
        Port - 1812
        Secret - qaz1wsx
```

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)

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

```
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)

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

```
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 are used to configure the SX network adapter.

Table 15 Configuration: Network Commands

COMMANDS	DESCRIPTION
ethernetfailover	Enable/Disable network failover
interface	Configure the SX unit network interface.
ipfowarding	IP forwarding configuration
name	Network name configuration
ports	Network port configuration
route	Show kernel routing table
routeadd	Add route to kernel routing table
routedelete	Delete route of kernel routing table

Ethernetfailover Command

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

The syntax of the ethernetfailover command is:

```
ethernetfailover <enable|disable> <interval>
```

Interface Command

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

The syntax of the interface command is:

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

The network command options are described in Table 16.

Table 16 Interface Command

COMMAND OPTION	DESCRIPTION
enable <true|false>	Enable/Disable Interface
if <lan1	lan2>	Select LAN interface you are configuring
ip ipaddress	IP Address of the DSX assigned for access from the IP network
mask subnetmask	Subnet Mask obtained from the IP 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)

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

IPForwarding Command

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

The syntax of the ipfowarding is:

```
ipforwarding <>
```

The network command options are described in Table 17.

Table 17 Ipforwarding Command

COMMAND OPTION	DESCRIPTION

Ipforwarding Command Example

The following command enables the IP Forwarding:

```
admin > Config > Network > ipforwarding
```

Name Command

The **name** command is used to configure the network name.

The syntax of the name is:

```
name <>
```

The network command options are described in Table 18.

Table 18 name Command

COMMAND OPTION	DESCRIPTION

name Command Example

The following command sets the network name:

```
admin > Config > Network > name
```

Ports Command

The **ports** command is used to configure the network ports.

The syntax of the ports is:

```
ports <>
```

The network command options are described in Table 19.

Table 19 ports Command

COMMAND OPTION	DESCRIPTION

Ports Command Example

The following command :

```
admin > Config > Network > ports
```

Route Command

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

The syntax of the command is:

```
route <>
```

The command options are described in Table 20.

Table 20 Route Command

COMMAND OPTION	DESCRIPTION

Route Command Example

The following command displays the route table:

```
admin > Config > Network > route
```

Routeadd Command

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

The syntax of the command is:

```
routeadd <>
```

The command options are described in Table 21.

Table 21 Routeadd Command

COMMAND OPTION	DESCRIPTION

Routeadd Command Example

The following command adds a route to the route table:

```
admin > Config > Network > routeadd
```

Routedelete Command

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

The syntax of the routedelete is:

```
routedelete <>
```

The command options are described in Table 22.

Table 22 Routedelete Command

COMMAND OPTION	DESCRIPTION

Routedelete Command Example

The following command remove a route from the route table:

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

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
```

The syntax of the nfs command is:

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

The **nfs** command options are described in Table 23.

Table 23 NFS Command

COMMAND OPTION	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
option option	softmount | hardmount

Command Example

The following command displays the current NFS settings:

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

```
NFS Settings :
        Enable : 0
        Primary IP : 0.0.0.0
        Pimary 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 option softmount
```

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. Those services are:

- The escape sequence used to disconnect from the port to access the emulator to send breaks or control multi user functions. (Example: Ctrl a)
- Set the exit string that is to be sent to the target when an idle timeout occurs. By sending the exit string, the port is disconnected from the DSX and the next user logging into the port will have to log into the target as well. (Cisco router example: logout)
- Define the addresses to be 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 the **Direct Port Addressing** section for details of this feature.

Ports Config Command

The syntax of the config command is:

```
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]
[exitstring <cmd[#delay;]>] [dpaip ipaddress] [telnet port] [ssh port]
```

The command options are described in Table 24.

Table 24 Port Configuration Command

COMMAND OPTION	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|28800|38400|57600|115200)
parity <none|even|odd>	Port parity type

`flowcontrol` `<none|hw|sw>`	Port flowcontrol type hw = hardware flow control 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
`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

Command Example

```
admin > ports config port 1 name ld1 bps 115000 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: 115200
        Parity: 0
        Flow control: 0
        RSC Terminal Emulation: VT100
        Disconnect: Disabled
        Application: RaritanConsole
        Exit String: show strongpassword
        Escape: Control-]
        DPA:
                IP: 0.0.0.0
                Telnet Port: 0
                SSH Port: 0
```
The following example configures DPA port settings when the Administrator chooses DPA mode IP. The IP Address is assigned for direct port access using the following command.

```
    admin > Config > Port > config port 1 dpaip 10.0.13.240


    Port 1: Configuration Saved
    DPA changes will not be available until after the SX is
    reebooted.
```

1. The following example configures DPA port settings when the Administrator chooses DPA mode TCPPort. The Administrator needs to set the SSH or Telnet port value assigned for direct port access:

```
admin > Config > Port > config port 1 ssh 7700 telnet 8800


Port 1: Configuration Saved
DPA changes  will  not  be  available  until  after  the  SX  is
rebooted.
```

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>
```

For configuring all ports using a block of contiguous port numbers, <port *> command can be used. If port_range is specified, then a block of contiguous port numbers will be used. The given value of base_tcpport is used as starting value. For individual port configuration, the <port portnumber> command can be used.

Ports Keywordadd Command

Keywords can be configured per port. After a keyword is configured for a port, an SMTP notification, if the corresponding event is selected for notification, is sent upon detecting this keyword in the data coming from the target connected to the port.

The syntax of the keywordadd command is:
```
keywordadd
```
The command options are described in Table 25.

Table 25 Port Keywordadd Command

COMMAND OPTION	DESCRIPTION

Command Example
```
admin > ports > keywordadd
```

Ports Keyworddelete Command

The keyworddelete command removes an existing keyword.

The syntax of the keyworddelete command is:
```
keyworddelete
```
The command options are described in Table 26.

Table 26 Port Keyworddelete Command

COMMAND OPTION	DESCRIPTION

Command Example
```
admin > ports > keywordadd
```

Configuring Services

The following commands provide the ability to configure the Dominion SX server services:

- DPA
- Encryption
- HTTP
- HTTPS
- Logout
- LPA
- SSH
- Telnet

dpa Command

The permitted TCP Port Range is 1024-65535.

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 Table 27.

Table 27 dpa Command

COMMAND OPTION	DESCRIPTION
mode <IP | TCPPort>	Per-port Direct Port Access type mode.
	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.
port_range	A block of contiguous IP addresses.
base_dpaip	Sstarting value for the block of contiguous IP addresses.
IP address	If IP Address = 0.0.0.0 is specified for a port, then the IP access is disabled for that particular port. It is the same as unassigning the IP address for a port.

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 device needs to be rebooted to apply new settings. DPA changes will not be available until after the DSX is rebooted

After a successful DPA connection, the following appears:

```
ssh admin@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.
```

Enabling unauthorizedportaccess to a set of ports assigned to 'Anonymous' group.

Unauthorized port access is only available 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: Observer
        Ports:
```

To configure Anonymous group settings go to **config > user** menu 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, the user name should be "Anonymous" and empty password <blank> as is shown below (The Anonymous access is granted if both fields username and password are empty <blank>):


```
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.*

The syntax of the encryption command is:
```
encryption [prot <TLS|SSL>]
```
The encryption command options are described in Table 28.

Table 28 Encryption Command

COMMAND OPTION	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 define the port.

The syntax of the http command is:

```
http [enable <true|false>] [port value] [redirect <true|false>]
```

The http command options are described in Table 29.

Table 29 HTTP Command

COMMAND OPTION	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.

The syntax of the https command is:

```
https [enable <true|false>] [port value]
```

The https command options are described in the following table.

HTTPS Command

COMMAND OPTION	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 the local port access configuration. Dominion SX units have one or two local ports, depending on the model. (Insert reference to App B for the pinouts for DB9-M and RJ45-F ports):

The syntax of the lpa command is:

```
lpa [enable <true|false>] [bps value]
```

The lpa command options are described in Table 30.

Table 30 Lpa Command

COMMAND OPTION	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 bits-per-second. Possible values are: (1200|1800|2400|4800|9600|19200|28800|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

The syntax of the ssh command is:

```
ssh [enable <true|false>] [port value]
```

The ssh command options are described in Table 31.

Table 31 SSH Command

COMMAND OPTION	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 will need to be rebooted for changes to take effect.
```

Telnet Command

The syntax of the telnet command is:

```
telnet [enable <true|false>] [port value]
```

The telnet command options are described in the following table.

Table 32 Telnet Command

COMMAND OPTION	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
```

Configuring SNMP

The Dominion SX server supports sending SNMP alerts to a predefined SNMP server. The Raritan SNMP MIB may be obtained from the FAQs in the support section of the Raritan web site. (http://www.raritan.com/_downloads/SX-MIB.txt). The following commands configure the SNMP features:

- add
- delete
- snmp

SMNP 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.

The syntax of the add command is:

```
add [dest ipaddress] [port value]
```

The add command options are described in Table 33.

Table 33 SNMP Add Command

COMMAND OPTION	DESCRIPTION
dest ipaddress	SNMP destination IP address
port value	SNMP destination port

SNMP Add Command Example

```
admin > Config > SNMP > add 72.236.162.33 78
```

SNMP Delete Command

The SNMP delete command deletes trap recipients. A recipient is an IP address with an optional space- separated port number. If a recipient with a port number is to be removed, include the port number in the delete command. Traps may be sent to multiple ports with the same IP address.

The syntax of the SNMP delete command is:

```
delete [dest ipaddress]
```

The SNMP delete command options are described in Table 34.

Table 34 SNMP Delete Command

COMMAND OPTION	DESCRIPTION
dest ipaddress	SNMP destination ip address to be deleted

SNMP Delete Command Example

```
admin > Config > SNMP > delete 72.236.162.33
```

SNMP Command

The SNMP command controls SNMP traps and specifies the community name used to send traps.

The syntax of the snmp command is:

```
snmp [enable <true|false>] [public community-string]
```

The snmp command options are described in Table 35.

Table 35 SNMP Command

COMMAND OPTION	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 are:

- clock
- ntp
- timezonelist

Clock Command

The **clock** command lets the administrator set the time and date for the server.

The syntax of the clock command is:

```
clock [tz tz] [datetime datetime] [timezonelist]
```

The clock command options are described in Table 36.

Table 36 Clock Command

COMMAND OPTION	DESCRIPTION
tz tz	The time zone index is a number corresponding to the desired time zone.
datetime datetime	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.

Command Example

The following example sets the Dominion 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 the administrator determine if a Network Time Protocol (NTP) server should be used to synchronize the SX clock to a reference.

The syntax of the command is:

```
ntp [enable <true|false>] [primaryntpip] [secondaryntpip]
```

The command options are described in Table 36.

Table 37 ntp Command

COMMAND OPTION	DESCRIPTION
enable	Enable or disable the use of NTP.
primaryntpip	The NTP server to use first.
secondaryntpip	The NTP server to use if the primary is not available.

Command Example

The following example enables NTP.

```
admin > Config > Time > ntp enable true primaryntpip 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.

The syntax of the command is:

```
timezonelist
```

Configuring Users

The following commands provided the administrators with the ability to manager users:

- addgroup
- adduser
- deletegroup
- deleteuser
- editgroup
- edituser
- groups
- users

Addgroup Command

The **addgroup** command creates a group with common permissions.

The syntax of the addgroup command is:

```
addgroup [name groupname] [class <op|ob>] [ports <number|range|*>]
```

The addgroup command options are described in Table 38.

Table 38 Addgroup Command

COMMAND OPTION	DESCRIPTION
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)

Command Example

```
admin > Config > User > addgroup name unixgroup class op ports 1, 3
```

Adduser Command

The **adduser** command is used to manage information about a specified user.

The syntax of the adduser command is:

```
adduser [user loginname] [fullname user's-fullname] [group name]
[dialback phonenumber] [password password] [info user-information]
[active <true|false>]
```

The adduser command options are described in Table 39.

Table 39 Adduser Command

COMMAND OPTION	DESCRIPTION
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	User's password (required)

password	
info *user- information*	Miscellaneous user information
active *<true|false>*	Activate/Deactivate user account

Adduser Command Example

The following example 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.

The syntax of the deletegroup command is:

```
deletegroup [name groupname]
```

The deletegroup command options are described in Table 40.

Table 40 Deletegroup Command

COMMAND OPTION	DESCRIPTION
name groupname	Group name

Command Example

```
admin > Config > User > deletegroup name unixgroup
```

Deleteuser Command

The **deleteuser** command is used to remove a specified user.

The syntax of the deleteuser command is:

```
adduser [user loginname]
```

The deleteuser command options are described in Table 41.

Table 41 Deleteuser Command

COMMAND OPTION	DESCRIPTION
user *loginname*	Login Name (Required)

Deleteuser Command Example

The following example shows how to delete a user.

```
admin > Config > User > deleteuser user jjones
```

Editgroup Command

The **editgroup** command edits an existing group.

The syntax of the editgroup command is:

```
editgroup [name groupname] [class <op|ob>] [ports <number|range|*>]
```

The editgroup command options are described in Table 42.

Table 42 Editgroup Command

COMMAND OPTION	DESCRIPTION
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)

 Command Example

```
admin > Config > User > editgroup name unixgroup class op ports 1,4
```

Edituser Command

The **edituser** command is used to manage information about a specified user.

The syntax of the edituser command is:

```
edituser [user loginname] [fullname user's-fullname] [group name]
[dialback phonenumber] [password password] [info user-information]
[active <true|false>]
```

The edituser command options are described in Table 43.

Table 43 Edituser Command

COMMAND OPTION	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 example 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.

The syntax of the groups command is:

```
groups
```

Command Example

```
admin > Config > User > groups
```

Users Command

The **users** command shows the details of existing users.

The syntax of the users command is:

```
users
```

Users Command Example

```
admin > Config > User > users
```

Connect Commands

The connect commands provide a means to access ports and their history..

Table 44 Connect Commands

COMMAND	DESCRIPTION
connect	Connect to a port. The port sub-menu, reached using escape key sequence.
clearhistory	Clear history buffer for this port.
close	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.

Diagnostics Commands

The diagnostic commands provide a means to gather information for troubleshooting problems.

Table 45 Diagnostics Commands

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]

IPMI Commands

The IPMIDiscover and IPMITool commands provide the capability 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.

The ipmidiscover tool syntax is:
```
ipmidiscover [OPTIONS] startIP endIP
```

All discovered targets supporting IPMI version 2.0 will be listed, allowing the user to select one and execute the IPMI operations.

The command options are described in Table 46

Table 46 IPMIDiscover Command

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

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. These functions include 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.

The ipmitool syntax is

```
ipmitool [-c|-h|-v|-V] -I lanplus -H <hostname> [-p <port>]
[-U <username>] [-L <privlvl>] [-a|-E|-P|-f <password>]
[-o <oemtype>] [-C <ciphersuite>]
```

The command options are described in Table 47

Table 47 IPMITool Command

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 will be 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.
`[-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>	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

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
```

For additional information: refer to http://ipmitool.sourceforge.net/manpage.html

Listports Command

Table 48 Listports Command

Command	Description
listports	List accessible ports. admin > listports Port Port Port Port No. Name No. Name 1 - Port1 [U] 2 - Port2 [U] 3 - Port3 [U] 4 - Port4 [U]

Port names up to 23 characters are displayed. Longer portnames are truncated to 22 characters, with a $ sign at the end

The letter after the port name describes the state of each port.

- A – Active
- B – Busy
- D – Down
- U – Up

Maintenance Commands

The **maintenance** commands are used by administrators to perform maintenance related tasks on the Dominion SX firmware. The following commands are system commands:

- backup
- cleareventlog
- factoryreset
- firmware
- logoff
- password
- reboot
- restore
- sendeventlog
- upgrade
- upgradehistory
- upgradestatus
- userlist
- vieweventlog

Backup Command

The **backup** command makes a copy of the Dominion SX configuration and writes the backup onto an ftp server. The current SX device configuration is saved to the computer with the IP set in the command parameters in an encrypted format. All device settings are stored in the file EXCEPT network settings. The file can recovered if a Restore operation becomes necessary.

The syntax of the backup command is:

backup [ip IP] <login LOGIN> <passwd PASSWD> [path PATH] [file FILE]

The backup command options are described in Table 49.

COMMAND OPTION	DESCRIPTION
`[ip IP]`	IP address of the target system where the backup will be written.
`<login LOGIN>`	Username of the account on the system where the backup will be stored.
`<passwd PASSWD>`	Password of the account on the system where the backup will be stored.
`[path PATH]`	Specifies the path to the backup file.
`[file FILE]`	Specifies the name of the file in which the backup will be 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 will be 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 qaz1wsx
path /home/ceci file Bac
```

Cleareventlog Command

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

The syntax of the cleareventlog command is:

`cleareventlog`

Cleareventlog Command Example

`admin > Config > Log > cleareventlog`

Factoryreset Command

The **factoryreset** command returns the Dominion 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 Dominion SX because, upon rebooting, the IP address of the unit will be reset to the factory default IP address of 192.168.0.192.

The syntax of the factoryreset command is:

`factoryreset`

Command Example

```
admin > Maintenance > factoryreset

Network Settings:
        Name: DominionSX
        Domain : raritan.com
        CSC Port: 5000
        Discover Port: 5000
        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.

The syntax of the firmware command is:

```
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

Table 50 Logoff Command

COMMAND	DESCRIPTION
logoff	Force logoff (terminate) a user or port session.

Password Command

Table 51 Password Command

COMMAND	DESCRIPTION
password	Sets the current user's password. For example, the user is logged in and wants to change the current password.

Reboot Command

The **reboot** command restarts the Dominion SX console server. This command is only available to users with administrative privileges. All user sessions will be terminated without warning, and no confirmation will be 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.

The syntax of the reboot command is:

```
reboot
```

Reboot Command Example

```
admin > Maintenance > reboot
```

The system responds with the following messages:

```
Rebooting the system will logoff 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 Dominion SX system from a system and writes the file to the Dominion SX server.

The syntax of the `restore` command is:

```
restore [ip IP] <login LOGIN> <passwd PASSWD> [path PATH] [file FILE]
```

The restore command options are described in Table 49.

Table 52 Restore Command

COMMAND OPTION	DESCRIPTION
[ip IP]	IP address of the target system from which the restore data will be retrieved.
<login LOGIN>	Username of the account on the system where the restore data is stored.
<passwd PASSWD>	Password for the above account.
[path PATH]	Specifies the path to the backup file to be restored to a similar system with the same port density.
[file FILE]	Specifies the name of the file in which the backup data was saved.

Restore Command Example

In the example below, 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 will be pulled from the top level of the guest account in a file named `backupfile`.

```
admin > system > restore ip 192.168.51.220 login guest passwd
guestpassword path . file backupfile1
```

Sendeventlog Command

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

The syntax of the sendeventlog command is:

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

The sendeventlog command options are described in Table 53

Table 53 Sendeventlog Command

COMMAND OPTION	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

```
admin > Config > Log > sendeventlog 72.236.162.187 login acy
password pasraritansword path sxlogfile file log 32
```

Upgrade Command

Note: in order to perform an upgrade, there should 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.

The syntax of the upgrade command is:

```
upgrade [ip ipaddress] [login login] [password password] [path
pathname]
```

The command options are described in Table 54Table 53

Table 54 Upgrade Command

COMMAND OPTION	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.

The syntax of the upgradehistory command is:

```
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.

The syntax of the userlist command is:

```
userlist
```

Vieweventlog Command

The **vieweventlog** command displays the local log file.

The syntax of the vieweventlog command is:

```
vieweventfile
```

Vieweventlog Command Example

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

Security Commands

Dominion SX controls the ability to hack into the system by using random logins. The following security command menus provide access to the commands needed to configure the Dominion SX security features:

- banner
- certificate
- firewall
- kerberos
- loginsettings
- securityprofiles

Banner Command

The **banner** command controls the display of a security banner immediately after login..

The syntax of the banner command is:

```
banner [display <true|false>] [audit <true|false>]
```

The banner command options are described in Table 55.

Table 55 Banner Command

COMMAND OPTION	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 DSX to go to this site to retrieve the welcome banner because the welcome banner and the audit statement are maintained on an external FTP site.

The syntax of the ftpgetbanner command is:

```
ftpgetbanner [ip ipaddress] [login login] [password password]
[path pathname]
```

The ftpgetbanner command options are described in Table 56.

Table 56 ftpgetbanner Command

COMMAND OPTION	DESCRIPTION
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

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.

The syntax of the certificate command is:

```
certificate <>
```

Note: For a description of how to enable LDAP over SSL with a third-party certification authority, refer to http://support.microsoft.com/default.aspx?scid=kb;en-us;321051. Document requires the exchange of certificate of authority created by the MS Server.

The client command options are described in Table 57.

Table 57 Certificate Client Commands

COMMAND	DESCRIPTION
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

Client Command Example

```
admin > Security > certificate > client
```

The server command options are described in Table 58.

Table 58 Certificate Server Commands

COMMAND	DESCRIPTION
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

Server Command Example

```
admin > Security > certificate > server
```

Firewall Command

The **firewall** command provides control for the turning on or off the firewall.

The syntax of the firewall command is:

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

The firewall command options are described in the following table.

Table 59 Firewall Command

COMMAND OPTION	DESCRIPTION
enable <true|false>	Enable/Disable firewall with true or false

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.

The iptables command options are described in Table 60.

Table 60 iptables Command

COMMAND OPTION	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

To add a default iptable rule for local access:

```
admin > Security >firewall >iptables -A INPUT -t filter -j ACCEPT
-s 127.0.0.1
```

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 acccess 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 ruleset

```
admin > Security >firewall >iptables –list
```

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
```

Execute this command once you have configured all the settings.

Kerberos Command

The **kerberos** command menu provides access to the commands used to configure the Kerberos network authentication protocol. The Kerberos commands are listed in the table below.

Table 61 Kerberos Commands

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 DSX

DSX can use kerberos authentication by using the following steps. As a result , Kerberos-based network mutual authentication and symmetric [a.k.a. private/secret] key cryptography can be achieved in the CLI and GUI of the DSX for remote user authentication.

See the MIT Kerberos website for information about Kerberos, KDC, Kadmind , 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 use : 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, DSX 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 DSX.
- Disable HTTP redirect from the services menu.
- Synchronize the time of the client machine. DSX machine, KDC and kadmind 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, Kadmind, the application server and client machine, refer to : the 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 kadmind 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 provides access to the commands used to configure the systemwide login settings. The loginsettings commands are listed in the table below.

Table 62 Loginsettings Commands

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.

idletimeout Command

The **idletimeout** command sets or changes the amount of idle time allowed before the system disconnects the user.

The syntax of the idletimeout command is:

idletimeout `time [number 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.

The syntax of the `inactiveloginexpiry` command is:

`inactiveloginexpiry [days value]`

The `inactiveloginexpiry` command options are described in Table 63.

Table 63 Inactiveloginexpiry Command

COMMAND OPTION	DESCRIPTION
`days <value>`	`Number of days before 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.

The syntax of the `invalidloginretries` command is:

`invalidloginretries [number value]`

The `invalidloginretries` command options are described in Table 64.

Table 64 Invalidloginretries Command

COMMAND OPTION	DESCRIPTION
`number value`	Number of failed login retries allowed before account is deactivated

Command Example

`admin > Security > LoginSettings > invalidloginretries number 5`

Localauth Command

The localauth command is used to configure local authentication.

The syntax of the localauthentication command is:

Command not yet implemented

Lockoutperiod Command

The **`lockoutperiod`** command defines the lockout period on invalid login attempts.

The syntax of the `lockoutperiod` command is:

`lockoutperiod [time time]`

The `lockoutperiod` command options are described in Table 65.

Table 65 Lockoutperiod Command

COMMAND OPTION	DESCRIPTION
time time	Period of time (in minutes) for which the user cannot login after account deactivation.

Command Example

```
admin > Security > LoginSettings > lockoutperiod time 120
```

Singleloginperuser Command

The **singleloginperuser** command enables or disables multiple logins per user..

The syntax of the `singleloginperuser` command is:

`singleloginperuser [enable <true|false>]`

The command options are described in Table 66.

Table 66 Singleloginperuser Command

COMMAND OPTION	DESCRIPTION
enable <true|false>	Enable/Disable multiple login sessions per user

Command Example

```
admin > Security > LoginSettings > singleloginperuser enable true
```

Strongpassword Command

The Dominion SX server supports both standard and strong passwords.

- Standard passwords have no rules associated with them; that is, 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 list.
- The maximum length of a strong password is 15 characters.

The syntax of the strongpassword command is:

```
strongpassword [StrongPasswordRulesEnable <true|false>]
[PWUppercaseRequired <true|false>] [PWLowercaseRequired
<true|false>] [PWNumberRequired <true|false>] [PWSymbolRequired
<true|false>] [PasswordValidityPeriod <#>] [PasswordHistoryDepth
<#>] [MinPasswordLength <#>] [MaxPasswordLength <#>]
```

The strongpassword command options are described in Table 66.

Table 67 Strongpassword Command

COMMAND OPTION	DESCRIPTION
StrongPasswordRulesEnable	true/false
PWUppercaseRequired	true/false
PWLowercaseRequired	true/false
PWNumberRequired	true/false
PWSymbolRequired	true/false
PasswordValidityPeriod	Number of days before expiration
PasswordHistoryDepth	Number of Passwords until repeat is allowed
MinPasswordLength	Minimum password length
MaxPasswordLength	Maximum password length

Strongpassword Command Example

The following example sets the Strong Password rules in effect:

- Uppercase is required.
- Lowercase is not required.
- Numbers are required.
- Symbols are not required.
- Passwords will expire 90 days after being set.
- Passwords will allow to be repeated after 5 passwords have been set. Until then there will be no repeats allowed.
- Passwords must be at least 8 and not more than 16 characters.

```
admin > Security > LoginSettings > strongpassword
StrongPasswordRulesEnable true PWUppercaseRequired true
PWLowercaseRequired false PWNumberRequired true PWSymbolRequired false
PasswordValidityPeriod 90 PasswordHistoryDepth 5 MinPasswordLength 8
MaxPasswordLength 16
```

Unauthorizedportaccess Command

The syntax of the `unauthorizedportaccess` command is:

`unauthorizedportaccess [enable <true|false>]`

The `unauthorizedportaccess` command options are described in the following table.

Table 68 unauthorizedportaccess Command

COMMAND OPTION	DESCRIPTION
enable <true|false>	Enable/Disable unauthorized access to a set of ports assigned to 'Anonymous' group

Unauthorizedportaccess Command Example

`admin > Security > LoginSettings > unauthorizedportaccess enable disable`

Securityprofiles Commands

The **securityprofiles** command menu provides access to the commands used to configure and control security profiles. The securityprofiles commands are listed in the table below.

Table 69 Securityprofiles Commands

COMMAND	DESCRIPTION
profiledata	View or modify a Security Profile.
securityprofiles	Enable and select a Security Profile.

Profiledata Command

The **profiledata** command is used to modify or view a security profile. The Dominion 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 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.

The syntax of the profiledata command is:

```
profiledata [name <Standard|Secure|Custom>] [telnet <true|false>]
[strongpass   <true|false>]   [timeout   <true|false>]   [single
<true|false>] [redirect <true|false>] [tls_required <true|false>]
```

The profiledata command options are described in Table 70.

Table 70 Profiledata Command

COMMAND OPTION	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 13: Intelligent Platform Management Interface

The Intelligent Platform Management Interface (IPMI lets you manage the IPMI functions of a remote system. The following topics are covered in this chapter:

- Discover IPMI Devices
- IPMI Configuration (thoroug

The Intelligent Platform Management Interface (IPMI) lets you manage the IPMI functions of a remote system.

Figure 90 IPMI Screen

Discover IPMI Devices

To discover IPMI servers on the network:

1. Click the **IPMI** tab, and then click **Discover IPMI Devices**. The Discover IPMI Devices screen appears.

Figure 91 Discover IPMI Devices Screen

1. You can leave the **Options** field blank, or you can enter -t timeout [seconds].
2. Type starting and ending IP addresses in the corresponding fields. The DSX will discover all IPMI devices within this range of IP addresses.
3. Click on the **IPMI Discover** button.

Example

The following is an example of the output when nothing has been entered in the **Option**s field:

Result:
```
 Discovering IPMI Devices ...
--- ipmidiscover statistics ---
448 requests transmitted, 0 responses received in time, 100.0% packet
loss
```

IPMI Configuration

IPMI configuration lets you manage the IPMI functions of a remote system. These functions include printing FRU information, LAN configuration, sensor readings, and remote chassis power control.

1. Click on the **IPMI Configuration** section of the IPMI screen to get IPMI configuration information.

Figure 92 IPMI Configuration

4. Click on the **Help** button to get IPMI configuration information, which appears on the **IPMI Configuration** screen.

Help:
```
ipmitool version 1.8.7

usage: ipmitool [options...]

        -h              This help
        -V              Show version information
        -v              Verbose (can use multiple times)
        -c              Display output in comma separated format
        -I 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 Cipher suite to be used by lanplus interface
        -k key          Use Kg key for IPMIv2 authentication
        -L level        Remote session privilege level
[default=ADMINISTRATOR]
        -A authtype     Force use of auth type NONE, PASSWORD, MD2, MD5
or OEM
        -P password     Remote session password
        -E              Read password from IPMI_PASSWORD environment
variable
        -m address      Set local IPMB address
        -b channel      Set destination channel for bridged request
        -l lun          Set destination lun for raw commands
        -t address      Bridge request to remote target address
        -o oemtype      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
```

5.   Type the IP address in the IP Address field.
6.   Type your username in the Username field.
7.   Type your password in the Password field.
8.   Type an option in the Option field.
9.   Type a command in the Command field.
10. Click on the IPMI Discover button. The system displays the results of your command.

Chapter 14: Power Control

Power Control lets you manage the power functions. The following topics are covered in this chapter:

- Power Control
- Associations Power Control
- Power Strip Power Control
- Power Strip Status

Port Power Associations

You can associate one or more outlets on a powerstrip connected to the DSX to specific DSX ports.

Create a Port Power Association

To create a port power association:

1. Click the **Setup** tab, and then click **Port Power Association List**.
2. Click **Add**. The Port Power Association screen appears.

Figure 93 Port Power Association Screen

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 Command Line Interface. Accessing the power strip directly will display raw character stream of commands responding in between DSX and the power strip, while you are write-

locked from any control.

Note: Power control is not supported on the last port of the DSX unit. The last port of the unit can be used for non-power control device.

Delete a Port Power Association
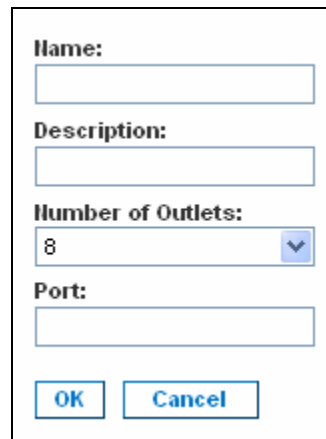
To delete a port power association:
1. Click the **Setup** tab, and then click **Port Power Association List**.
2. Click **Add**. The Port Power Association screen appears.
3. Select the association in the Outlet Association list.
4. Click **Delete**.

Power Strip Configuration

To configure a power strip:
1. Click the **Setup** tab, and then click **Power Strip** Configuration.
11. Click **Add**. The Power Strip Configuration screen appears.

Figure 94 Power Strip Configuration Screen

12. Type a name and description in the **Name** and **Description** fields.
13. Select the number of outlets from the drop-down menu in the **Number of Outlets** field.
14. Type the port number in the **Port** field.
15. Click **OK**.

Power Association Groups

To create a power associations group:

1.   Click the **Setup** tab, and then click **Power Association Groups List**.

16.   Click **Add**. The Power Association Groups screen appears.
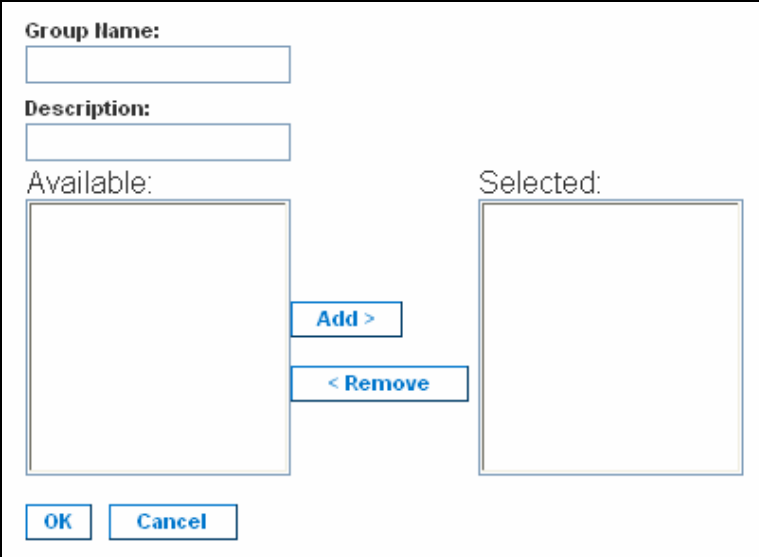
Figure 95 Power Association Group Screen

17.   Type a name and description in the **Group Name** and **Description** fields.

18.   Select the number of outlets from the drop-down menu in the **Number of Outlets** field.

19.   Click **OK**.

Power Control

Select the **Power Control** tab to bring up the power control-related tools.

Figure 96 Power Control

Associations Power Control

Click **Associations Power Control** on the **Power Control** menu to access the tool to manage power control associations.

Group and Port Power Associations

	Name	Type	Outlet Status	
☐	Port2	Port	ON/OFF	Select All

On   Off   Cycle
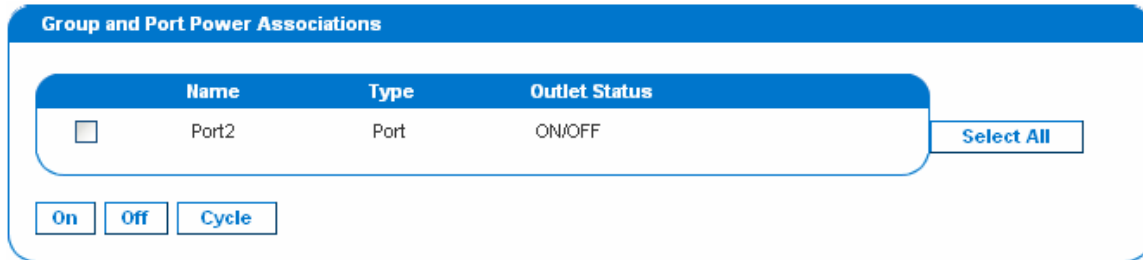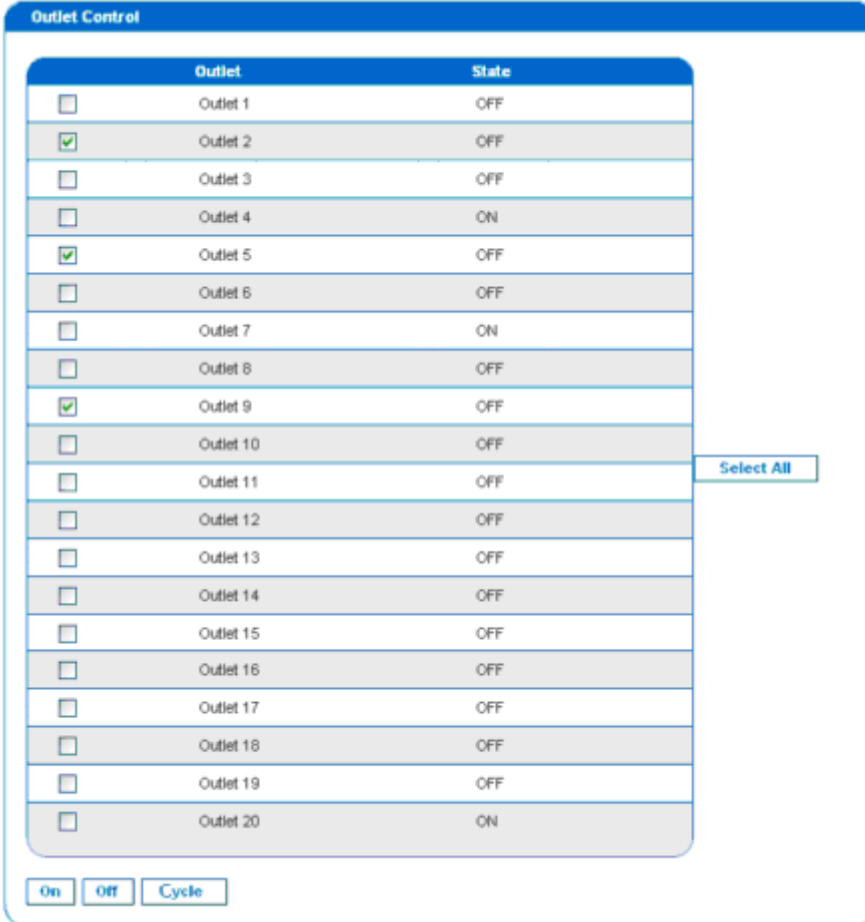
Figure 97 Associations Power Control

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 will be 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 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

Click **Power Strip Power Control** on the **Power Control** menu to access the tool to manage power strips.

Figure 98 Power Strip Power Control

Power Strip Status

Click **Power Strip Status** on the **Power Control** menu 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
```

Figure 99 Power Strip Status

CLI Command for Power Control

CLI Port Power Association

Description: Power Control menu – Associate a power strip outlet to a DSX port

Scenario #1	Port Power Association – Add Outlet.
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) is physically connected to DSX named PowerStr1. User is in power menu.
Action	1. Type command. 2. Press Enter.
CLI Input	Command: associate port 1 powerstrip PowerStr1 outlet 1

Scenario #2	Port Power Association – Associate 6 Outlets to one Port.
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) is physically connected and configured to DSX named PowerStr1. User is in power menu.
Action	1. Type command - associate [port port] [powerstrip powerstrip] [outlet outlet] to associate Outlet1 to Port1 2. Press Enter. 3. Repeat steps 3 and 4 for Outlet 2, 3, 4, 5 and 6.
CLI Input	associate port 1 powerstrip PowerStr1 outlet 1-6

Scenario #3	Port Power Association – Associate 6 Outlets to one port spread across two PDUs.
Pre-condition	Administrator user is logged in via CLI. Two Power Strip devices (DPX) are physically connected and configured to the DSX, respectively named PowerStr1 and PowerStr2. User is in power menu.
Action	1. Type command - associate [port port] [powerstrip powerstrip] [outlet outlet] to associate Outlet1 of PowerStr1 to Port1 2. Press Enter. 3. Repeat steps 1 and 2 for Outlet 2 and 3. 4. Type command - associate [port port] [powerstrip powerstrip] [outlet outlet] to associate Outlet1 of PowerStr2 to Port1 5. Press Enter. 6. Repeat steps 4 and 5 for Outlet 2 and 3.
CLI Input	· associate port 1 powerstrip PowerStr1 outlet 1,2,3 · associate port 1 powerstrip PowerStr2 outlet 1,2,3

Scenario #4	Port Power Association – Associate one Outlet to two Ports.
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) is physically connected and configured to the DSX named PowerStr1. User is in power menu.
Action	1. Enter command 2. Press enter
CLI Input	· associate port 1 powerstrip PowerStr1 outlet 1 · associate port 2 powerstrip PowerStr1 outlet 1

Scenario #5	Port Power Association – Associate all available Outlets to Ports.
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) is physically connected and configured to the DSX named PowerStr1. User is in power menu
Action	1. Enter command. 2. Press enter. 3. 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

Scenario #6	Port Power Association – Associate outlets to one Port from different Power Strips.
Pre-condition	Administrator user is logged in via CLI. Two Power Strip devices (DPX) are physically connected and configured to the DSX respectively named PowerStr1 and PowerStr2. User is in power menu.
Action	1. Enter command to associate Port1 to Outlet1 from PowerStr1. 2. Press Enter. 3. Enter command to associate Port1 to Outlet1 from PowerStr2. 4. Press Enter.
CLI Input	· associate port 1 powerstrip PowerStr1 outlet 1 · associate port 1 powerstrip PowerStr2 outlet 1

Scenario #7	Port Power Association – Associate outlets from 6 different Power Strips to one Port.

Pre-condition	Administrator user is logged in via CLI.
	6 Power Strip devices (DPX) are physically connected and configured to DSX.
	User is in power menu.
Action	1. Enter Command to associate Port1 to Outlet1 of PowerStr1.
	2. Press Enter.
	3. 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

Scenario #8	Port Power Association – Edit outlet names
Pre-condition	Administrator user is logged in via CLI.
	Power Strip device (DPX) is physically connected and configured to DSX named PowerStr1.
	User is in power menu.
Action	1. Enter Command to edit outlet1 name of PowerStr1.
	2. 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 a DSX port.

Scenario #1	Remove Port Power Association
Pre-condition	Administrator user is logged in via CLI.
	Power Strip device (DPX) is physically connected and configured to DSX named PowerStr1.
	User is in power menu.
Action	1. Enter command.
	2. Press Enter.
CLI Input	Command: unassociate port 1 powerstrip PowerStr1 outlet 1

Scenario #2	Delete multiple outlets Association
Pre-condition	Administrator user is logged in via CLI.
	Power Strip device (DPX) is physically connected and configured to the DSX named PowerStr1.
	User is in power menu.
Action	1. Enter command.
	2. Press Enter.
CLI Input	Command: unassociate port 1 powerstrip PowerStr1 outlet 1,4,7

CLI Power Strip Configuration

Description: Power Control Menu

Scenario #1	Configure a DSX Port to contain a Power Strip device (the port is previously connected to a power strip)
Pre-condition	Administrator user is logged in via CLI.
	Power Strip device (DPX) is physically connected to Port1 of DSX.

	Administrator is in power menu.
Action	1. Enter command.
	2. Press Enter.
CLI Input	setpowerport name PowerStr1 type DPCS12 port 1

Scenario #3	Power Strip Configuration after factory reset
Pre-condition	Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX.
	DSX user has already configured the port as a Power Strip.
Action	1. Log in to DSX unit with administrator privileges via CLI.
	2. Go to Maintenance menu
	3. Perform Factory Reset
CLI Input	Command: factoryreset

CLI Power Association Group

Description: Power → PowerGroups menu

Scenario #1	Create new power group.
Pre-condition	Administrator user is logged in via CLI.
	Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX.
	Administrator is in Power → PowerGroups menu.
Action	1. Enter Command.
	2. Press Enter.
CLI Input	Command: addpowergroup name "Test Group" description "Test group"

Scenario #2	Add a port to a power group
Pre-condition	Administrator user is logged in via CLI.
	Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX.
	Administrator is in Power → PowerGroups menu.
Action	1. Enter Command.
	2. Press Enter.
CLI Input	Command: addpowergroupport name "test Group" port port 2

Scenario #3	Add multiple ports to a power group
Pre-condition	Administrator user is logged in via CLI.
	Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX.
	Administrator is in Power → PowerGroups menu.
Action	1. Enter Command.
	2. Press Enter.
CLI Input	Command: addpowergroupport name "test Group" port port 2-4,10

Scenario #4	Remove group member
Pre-condition	Administrator user is logged in via CLI.
	Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX.
	Administrator is in Power → PowerGroups menu.
Action	1. Enter Command.
	2. Press Enter.
CLI Input	Command: deletepowergroupport name "Test Group" port 2

Scenario #5	Delete Power Group
Pre-condition	Administrator user is logged in via CLI. Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Administrator is in Power → PowerGroups menu.
Action	1. Enter Command. 2. Press Enter.
CLI Input	Command: deletepowergroup name "Test Group"

CLI Power Strip Power Control

Description: Power Control Menu

Scenario #1	Switch on/off a single Outlet
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Administrator is in power menu.
Action	1. Enter Command. 2. Press Enter.
CLI Input	on powerstrip PowerStr1 outlet 1 off powerstrip PowerStr1 outlet 1

Scenario #2	Switch on/off all Outlets
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Administrator is in power menu.
Action	1. Enter Command. 2. Press Enter.
CLI Input	on powerstrip PowerStr1 outlet * off powerstrip PowerStr1 outlet *

Scenario #3	Switch on/off group of outlets
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Administrator is in power menu.
Action	1. Enter Command. 2. Press Enter.
CLI Input	on powerstrip PowerStr1 outlet 1,3,7 off powerstrip PowerStr1 outlet 1,3,7

Scenario #4	Power recycle group of outlets
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Administrator is in power menu.
Action	1. Enter Command. 2. Press Enter.
CLI Input	cycle powerstrip PowerStr1 outlet 1,3,7

Scenario #5	Sequence interval for switch off operation
Pre-condition	Administrator user is logged in via CLI.

	Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Administrator is in power menu.
Action	1. Enter command to set sequence interval. 2. Press Enter. 3. Enter command to switch off group of outlets. 4. Press Enter.
CLI Input	· powerdelay sequence 2 · off powerstrip PowerStr1 outlet 1,3,7

Scenario #6	Sequence interval for switch on operation
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Administrator is in power menu.
Action	1. Enter command to set sequence interval. 2. Press Enter. 3. Enter command to switch on group of outlets. 4. Press Enter.
CLI Input	· powerdelay sequence 2 · off powerstrip PowerStr1 outlet 1,3,7

Scenario #7	Power Recycle Interval
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Administrator is in power menu.
Action	1. Enter command to set sequence and power recycle interval. 2. Press Enter. 3. Enter command to power recycle group of outlets. 4. Press Enter.
CLI Input	· powerdelay sequence 2 cycle 5 · cycle powerstrip PowerStr1 outlet 1,3,7

CLI Association Power Control – Port Association

Description: Power Control Menu

Scenario #1	Association Power Control – Recycle Port Association (Target is associated to One Outlet)
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Port Power Association named Target2 is already created and available in the list. Outle1 of PowerStr1 is associated to Target2. Administrator is in Power Control → Associations Power Control menu.
Action	1. Select Port Association named Target2 2. Click on Power Recycle Interval and enter value: 3. Press Recycle button.
CLI Input	Power Recycle Interval value: 1 sec.

Scenario #2	Association Power Control – Recycle Port Association (Target is associated to Two Outlets from one Power Strip)
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Port Power Association named Target2 is already created and available in the list. Outle1 of PowerStr1 is associated to Target2. Administrator is in Power Control → Associations Power Control menu.
Action	1.　Select Port Association named Target2 2.　Click on Power Recycle Interval and enter value: 3.　Press Recycle button.
CLI Input	Power Recycle Interval value: 1 sec.

Scenario #3	Association Power Control – Recycle Port Association (Target is associated to Two Outlets from two different Power Strip devices)
Pre-condition	Administrator user is logged in via CLI. Power Strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Port Power Association named Target2 is already created and available in the list. Outle1 of PowerStr1 is associated to Target2. Administrator is in Power Control → Associations Power Control menu.
Action	1.　Select Port Association named Target2 2.　Click on Power Recycle Interval and enter value 3.　Press Recycle button.
CLI Input	Power Recycle Interval value: 1 sec.

| Scenario #4	Association Power Control – Recycle Port Association (outlets in the association are with different statuses)
Pre-condition	Administrator user is logged in via GUI. Two Power Strip devices (DPX) named PowerStr1 and PowerStr2 are physically connected to SX Ports. Port Power Association named Target2 is already created and available in the list. Outle1 of PowerStr1 and Outlet2 of PowerStr2 are associated to Target2. Outlet1 and Outlet2 are with different statuses. Administrator is in Power Control → Associations Power Control menu.
Action	1.　Select Port Association named Target2 2.　Click on Power Recycle Interval and enter value: 3.　Press Recycle button.
CLI Input	Power Recycle Interval value: 1 sec.

CLI Association Power Control – Group Association

Description: Power Control Menu

Fg.1
Group1
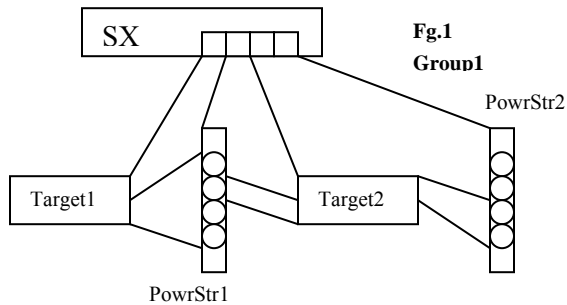
Scenario #1	Turn ON Group Association
Pre-condition	Administrator user is logged in via CLI. Administrator is in power menu. Group Association named Group1 (shown in Fg.1) is already created.
Action	1. Enter Command. 2. Press Enter.
CLI Input	Command: on nodegroup Group1

Scenario #2	Turn ON Group Association (outlets in association are with different statuses)
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	1. Enter Command. 2. Press Enter.
CLI Input	Command: on nodegroup Group1

Scenario #3	Turn OFF Group Association
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	1. Enter Command. 2. Press Enter.
CLI Input	Command: off nodegroup Group1

Scenario #4	Turn OFF Group Association (outlets in association are with different statuses)
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	1. Enter Command. 2. Press Enter.
CLI Input	Command: off nodegroup Group1

Scenario #5	Recycle Group Association
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	1. Enter Command. 2. Press Enter.

CLI Input	· powerdelay sequence 2 cycle 5
	· cycle nodegroup Group1

Scenario #6	Recycle Group Association (outlets in association are with different statuses)
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	1. Enter Command. 2. Press Enter.
CLI Input	· powerdelay sequence 2 cycle 5 · cycle nodegroup Group1

Scenario #7	Turn ON Group and Port Association simultaneously.
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. Port3 is already associated with outlet8 of PowerStr1 which has been created and available in the list.
Action	1. Enter Command. 2. Press Enter.
CLI Input	· powerdelay sequence 2 cycle 5 · on port 3 nodegroup Group1

Scenario #8	Turn OFF Group and Port Association simultaneously.
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. Port3 is already associated with outlet8 of PowerStr1 which has been created and available in the list.
Action	1. Enter Command. 2. Press Enter.
CLI Input	· powerdelay sequence 2 cycle 5 · off port 3 nodegroup Group1

Scenario #10	Recycle Group and Port Association simultaneously.
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. Port3 is already associated with outlet8 of PowerStr1 which has been created and available in the list.
Action	1. Enter Command. 2. Press Enter.
CLI Input	· powerdelay sequence 2 cycle 5 · cycle port 3 nodegroup Group1.

CLI Power Strip Status

Description: Power Control Menu

Scenario #1	Power Strip Status
Pre-condition	Administrator user is logged in via CLI. Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Administrator is in Power menu.
Action	1. Enter Command. 2. 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

Scenario #2	Status of Power Strip that is actually turn off or disconnected
Pre-condition	Administrator user is logged in via CLI. Power strip device (DPX) named PowerStr1 is disconnected from Port1 or turned off. Administrator is in Power menu.
Action	1. Enter Command. 2. Press Enter.
CLI Input	Command: powerstrip name PowerStr1

Scenario #3	Power Strip Status – Outlet status
Pre-condition	Administrator user is logged in via CLI. Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX.
Action	1. Check the current status of outlets – outlet1 is turn on 2. Turn off outlet1. 3. Go to Power menu and check the status of outlet1.
CLI Input	· powerstrip name PowerStr1 · off powerstrip PowerStr1 outlet 1 · powerstrip name PowerStr1

Scenario #4	Power Strip Status – Outlet status when port association is removed
Pre-condition	Administrator user is logged in via CLI. Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX. Outlet1 and Outlet2 are associated with Port1. Outlet1 and Outlet2 are with status "ON". Administrator is in Power menu.
Action	1. Check the current status of outlets – outlet1 is turn on 2. Remove Outlet1 and Outlet2 from outlet association to Port1. 3. Go to Power menu and check the status of outlet1.
CLI Input	· powerstrip name PowerStr1 · unassociated port 1 powerstrip PowerStr1 outlet 1,2 · powerstrip name PowerStr1

Scenario #5	Power Strip Status – Outlet status when group association is removed

ᴤᴤ Raritan.

Pre-condition	Administrator user is logged in via CLI.
	Power strip device (DPX) named PowerStr1 is physically connected to Port1 of DSX.
	Group association named Group1 is created.
	Outlet1 and Outlet2 are with status "ON".
	Administrator is in Power menu.
Action	1. Check the current status of outlets – outlet1 is turn on
	2. Remove Group1.
	3. Go to Power menu and check the status of outlet1.
CLI Input	· powerstrip name PowerStr1
	· deletepowergroup name Group1
	· powerstrip name PowerStr1

Chapter 15: Top-10 Use Cases

This chapter includes 10 of the mostly common cases to help familiarize users quickly with practical operation on DSX unit. Please note that data entered in the case are created as examples, and could vary upon different situations.

Case 1. Upgrading DSX Firmware via Web Browser

1. Purpose: To upgrade DSX firmware version for enhanced features or service patches.
2. Check Raritan support website for availability of latest firmware version: (http://www.raritan.com/support/firmwareupgrades and look for SX under Dominion Family)
3. Download the new SX firmware stored as UpgradePack from Raritan support 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 by an FTP user account that you have.
4. Then, log in the SX through a web browser. Select Maintenance → Firmware Upgrade. Enter FTP server IP address (e.g. 192.168.51.204), 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 firmware upgrade is completed, log in SX and check the firmware version again from: Maintenance → Firmware Version. You can also check firmware upgrade history to make sure: Maintenance → Firmware Upgrade History.
6. Refer to: Upgrading the DSX Firmware section in Chapter 10 for details.

Case 2. Configuring and Using Direct Port Access via SSH

1. Purpose: To allow users to directly SSH into the serial target without using DSX GUI.
2. User may determine an IP address or TCP port on SX IP to use for DPA or any port on SX. Since network administrator has no spare IP address, we will reuse SX IP address with different port.
3. Log back in SX, and select the port enabled for DPA on Setup → Port Configuration.
4. Edit the DPA SSH TCP Port to which SSH client will connect, and then click OK.
5. Log in SX through a web browser. On Setup → Services page, select TCP port on Direct Port Access Mode, and then click OK.
6. Launch the SSH client, such as Plink or PuTTY. Enter the IP address and change the default TCP Port to connect to the port enabled (e.g. plink -ssh -P 2203 192.168.51.9).
7. Refer to: Direct Port Access section in Chapter 7 for details.

Case 3. Using Exclusive Write Access via RSC

1. Purpose: To ensure that you are the only user who has write access to a serial target.
2. After logging in SX via a web browser, "Port Access" tab is selected by default.
3. Connect to a Port 4 by clicking on the hyperlink labled "Port 4".
4. Then, the Raritan Serial Console (RSC) application window launches with Write Access enabled (icon indicated in green on status line at the bottom of the window), unless the port has been occupied by another user.
5. In the RSC window, select Emulator → Get Write Lock (If some other user has previously obtained Write Access, please perform "Get Write Access" first from the Emulator menu of

RSC). The icon on status line will display Write Access (Lock) now, meaning now all users can only view the port connection.

6. Log in the device connected to the port, and try interacting with the device using the RSC panel.

7. Refer to: Get Write Access section in Chapter 7 for details.

8. To relinquish write lock in the RSC window, select Emulator → Write Unlock, and the icon on status line will display Write Access again, meaning any other privileged users will re-gain Write Access now.

Case 4. Configuring LDAP

1. Purpose: To configure DSX to use LDAP/Active Directory server for login authentication.

2. After logging in SX via a web browser, select Setup → Remote Authentication.

3. If the LDAP server has a backup server, enter same parameters (except the IP address) for the secondary LDAP server.

4. Click OK to commit changes.

5. Refer to: Configuring LDAP section in Chapter 6 for details.

Case 5. Creating Power Association Group

1. Purpose: To associate the target server with more than one power outlets physically connected to it.

2. After logging in SX via a web browser, make sure a power strip has been configured previously (To add a power strip: click Add on Setup → Power Strip Configuration page. See Power Strip Configuration section in Chapter 14 for details). Then, click Add on Setup → Port Power Association List page.

3. Select the SX port connected to the dual-powered server device that you wish to associate outlets with from the drop-down menu of Port, and enter a description for it, such as "Internal Web Server Pronto" (see Port Power Association section in Chapter 14 for details).

4. Select the Power Strip and outlet from the drop-down menu to match how the device is connected to power. Then click on Add button and the information will appear in the text box as "[Power Strip Name] \ [outlet 1]". Select the same power strip and another outlet, then press Add button to add it. Another line will display in the text box as "[Power Strip Name] \ [outlet 2]". Click OK to commit the changes.

5. Click Add on Setup → Power Association Groups List page (See Power Association Groups section for details).

6. Enter a group name and description, then the port ID from the "Available" box (multiple selection is permitted), and click Add button to add to the "Selected" box.

7. Click OK to commit changes.

8. Refer to: Power Strip Configuration section for details on how to add power strips to DSX management first. If this wasn't already done, refer to Port Power Associations section to map power strip outlet to a target server connected to a DSX serial port, and then refer to Power Association Groups section for details on how to group multiple power outlets physically connected to that same target server.

Case 6. Performing Factory Reset on DSX

1. Purpose: To set DSX configuration back to factory defaults through GUI.

2. Log in SX via a web browser with your login username and password, such as (admin/raritan).

3. Select Maintenance → Factory Reset. You will be prompted to confirm your decision.

4. Do not power off DSX unit as it reboots with default configuration.

5. You will be re-directed to the login page after the unit is rebooted. If you try to log in for the first time after reset, you'll be advised on the screen that you're now in the factory default mode, and promoted for changing password after logging in with default username and password.

6. Refer to: Performing Factory Reset section in Chapter 10 for details.

Case 7. Managing User Profiles on DSX

1. Purpose: To create, update or delete a DSX user.

2. Log in SX via a web browser with your login username and password, such as (admin/raritan).

3. Select User Management → User List, and the page will display a list of user profiles created.

4. To create a user profile, click Add New User button.

5. To modify an existing user profile, see Modify a User Profile section for details.

6. To delete an existing user profile, see Delete a User Profile section for details.

7. Refer to: Create a User Profile section in Chapter 5 for details.

Case 8. Accessing Port Access on DSX via RSC

1. Purpose: To access a DSX serial target through Raritan Serial Client (RSC).

2. Log in SX via a web browser with your login username and password, such as (admin/raritan).

3. Select the Port Access Tab, and click on the port name you wish to access, e.g. Port 1.

4. Select YES to proceed through security warning(s).

5. The Raritan Serial Console (RSC) will be launched in a separate window – press enter key to "wake up" session.

6. Type in target system's native commands in the RSC window/console.

7. Select Emulator → Exit. Then, select YES on the confirmation dialog box to exit, and the RSC window will close.

8. Refer to: Raritan Serial Console section in Chapter 7 for details.

Case 9. Port Configuration

1. Purpose: To configure DSX serial ports to set up correct serial communications parameters (e.g. baud rate, data bits, stop bit, flow control) and terminal emulation mode to match the serial targets connected to the ports, and name the ports to more easily identify the targets.

2. Log in SX via a web browser with your login username and password, such as (admin/raritan).

3. Select Setup → Port Configuration page, check the box associated with the port number you wish to configure, and click Edit.

4. Refer to: Port Configuration section in Chapter 7 for details.

Case 10. CLI / SSH Connection to SX Port

1. Purpose: To access SX unit itself and SX ports using text-based command lines.
2. SSH access from a Windows PC
    a. Launch the SSH client software (such as Plink or PuTTY).
    b. Enter IP address of DSX server (e.g. 192.168.0.192) and the TCP port if applicable.
    c. Select SSH (using default configuration port 22), and click the **Open** button.
    d. Enter username and password when prompted as below:
        > login as: admin
        >
        > password: raritan (default value)
    e. The console will display all the ports on SX unit with port numbers.
    f. Enter a port number at the prompt, for example:
        > admin> 1
    g. To return back to the SX console, enter the escape sequence characters. For example, simultaneously press the control and closed bracket key (]).
    h. To exit the target serial console session, enter the letter "q" to quit. You will be re-directed back to the SX console, and the port serial console session is now closed.
3. 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 password:
        > login as: admin
        >
        > The password prompt appears. Enter the default password: raritan
    c. The console will display all the ports on SX unit with port numbers.
    d. Enter a port number at the prompt, for example:
        > admin> 1
    e. To return back to the SX console, enter the escape sequence characters. For example, simultaneously press the control and closed bracket key (]).
    f. To exit the target serial console session, enter the letter "q" to quit. You will be re-directed back to the SX console, and the port serial console session is now closed.
4. Refer to: SSH Connection to the Dominion SX section in Chapter 12 for details.

Raritan.

Download from Www.Somanuals.com. All Manuals Search And Download.

Appendix A: Specifications

This appendix contains sections describing:

- DSX models and specifications

- Requirements and tested browser requirements

- DSX hardware for connecting DSX to common vendor models

- DSX Serial RJ-45 pinouts

- DB9 and DB25 Nulling Serial Adapter Pinouts

- DSX Terminal ports

Dominion SX Models and Specifications

The following table lists the Dominion SX models by the number of ports (4 – 48) in the unit.

Table 71 Dominion SX Specifications

MODEL	PORTS	BUILT-IN MODEM	LOCAL PORTS	ETHERNET PORTS	POWER SUPPLY
DSX4	4	No	2	1	Single AC
DSXB-4-M	4	Yes	1	1	Single AC
DSXB-4-DC	4	Yes	2	1	Single DC
DSXB-4-DCM	4	Yes	1	1	Single DC
DSX8	8	No	1	1	Single AC
DSXA-8	8	Yes	1	1	Dual AC
DSXB-8-M	8	Yes	1	1	Single AC
DSXB-8-DC	8	No	2	1	Single DC
DSXB-8-DCM	8	Yes	1	1	Single DC
DSX16	16	Yes	1	1	Single AC
DSXA-16	16	Yes	1	1	Single AC
DSXA-16-DC	16	Yes	1	1	Single DC
DSXA-16-DL	16	No	2	2	Dual AC
DSXA-16-DLM	16	Yes	1	2	Dual AC
DSX32	32	Yes	1	1	Single AC
DSXA-32	32	Yes	1	1	Dual AC
DSXA-32-AC	32	No	2	1	Dual AC
DSXA-32-DC	32	Yes	1	1	Dual DC
DSXA-32-DL	32	No	2	2	Dual AC
DSXA-32-DLM	32	Yes	1	2	Dual AC
DSXA-48	48	Yes	1	2	Dual AC
DSXA-48-AC	48	No	2	2	Dual AC
DSXA-48-DC	48	Yes	1	2	Dual DC

The following table lists the Dominion SX models, their dimensions, and weight.

Table 72 Dominion SX Dimensions and Weight

MODEL	DIMENSIONS (W) x (D) x (H)	WEIGHT
DSX4	11.41"x 10.7"x 1.75"; 290x 270 x 44mm	4.61 lbs; 2.08kg
DSXB-4-M	11.41"x 10.7"x 1.75"; 290x 270 x 44mm	4.61 lbs; 2.08kg
DSXB-4-DC	11.41"x 10.7"x 1.75"; 290x 270 x 44mm	4.61 lbs; 2.08kg
DSXB-4-DCM	11.41"x 10.7"x 1.75"; 290x 270 x 44mm	4.93 lbs; 2.22kg
DSX8	11.41"x 10.7"x 1.75"; 290x 270 x 44mm	4.81 lbs; 2.17kg
DSXA-8	17.32"x 11.41"x 1.75";440 x. 290 x 44mm	8.00 lbs; 3.60kg
DSXB-8-M	11.41"x 10.7"x 1.75"; 290x 270 x 44mm	4.81 lbs; 2.17kg
DSXB-8-DC	11.41"x 10.7"x 1.75"; 290x 270 x 44mm	4.81 lbs; 2.17kg
DSXB-8-DCM	11.41"x 10.7"x 1.75"; 290x 270 x 44mm	5.00 lbs; 2.25kg
DSX16	11.34"x 10.7"x 1.75"; 288 x 270 x 44mm	9.61 lbs; 4.35kg
DSXA-16	17.32"x 11.41"x 1.75";440 x. 290 x 44mm	8.20 lbs; 3.69kg
DSXA-16-DC	17.32"x 11.41"x 1.75";440 x. 290 x 44mm	7.8lbs; 3.51Kg
DSXA-16-DL	17.32"x 11.41"x 1.75";440 x. 290 x 44mm	8.58 lbs; 3.86kg
DSXA-16-DLM	17.32"x 11.41"x 1.75";440 x. 290 x 44mm	8.58 lbs; 3.86kg
DSX32	17.25"x 11.34"x 1.75"; 438 x 288 x 44mm	10 lbs; 4.53kg
DSXA-32	11.34"x 10.7"x 1.75"; 288 x 270 x 44mm	8.7 lbs; 3.98kg
DSXA-32-AC	17.25"x 11.34"x 1.75"; 438 x 288 x 44mm	8.7 lbs; 3.98kg
DSXA-32-DC	17.32"x 11.34"x 1.75"; 440 x 290 x 44mm	8.78 lbs; 3.95g
DSXA-32-DL	17.32"x 11.34"x 1.75"; 440 x 290 x 44mm	8.78 lbs; 3.95kg
DSXA-32-DLM	17.32"x 11.34"x 1.75"; 440 x 290 x 44mm	8.78 lbs; 3.95kg
DSXA-48	17.32"x 11.41"x 1.75";440 x. 290 x 44mm	8.97lbs; 4.04kg
DSXA-48-AC	17.32"x 11.41"x 1.75";440 x. 290 x 44mm	8.97lbs; 4.04kg
DSXA-48-DC	17.32"x 11.41"x 1.75";440 x. 290 x 44mm	8.97lbs; 4.04kg

Requirements

The following table lists the requirements for the DSX.

Table 73 Dominion SX Requirements

REQUIREMENTS	DESCRIPTION
Power	110/220V auto-switching: 50-60 Hz or -36 to -72V DC for DC-powered models
Operating Temperature	32° to 104° F (0° to 40° C)
Operating Humidity	20% - 85% RH non-condensing
Operating altitude	Operates properly at any altitude from 0 to 10,000 feet
Network	One (1) or two (2) 10/100 Ethernet Base-T; RJ-45 connection
Modem (Optional)	Dedicated Modem DB9M Port - many models; Integrated 56K V.92 (RJ11 port)
Protocols (Optional)	TCP/IP, RADIUS, SNMP, SMTP, PAP, TACACS+, NFS, HTTP, HTTPS, SSL, SSH, PPP, NTP, LDAP, LDAP(S), and KerberosV5.

Browser Requirements – Supported

The following table lists the browsers that were tested with the DSX.

Table 74 Browser Requirements

PLATFORM	BROWSER
WIN XP Professional SP2 – SUN JRE 1.5.0_06	IE 6.0
	IE 7.0
	Firefox 2.0
WIN XP Home Edition SP2 – SUN JRE 1.5.0_06	IE 6.0
	IE 7.0
	Netscape 7.1
	FireFox 1.5.0.1
	Mozilla 1.6
WIN 2000 Professional SP4 SUN JRE 1.5.0_06	IE 6.0
	FireFox 1.5.0.1
WIN 2000 Professional SP2 SUN JRE 1.4.2_05	IE 6.0
Fedora Core 4 JRE 1.4.2_05	Mozilla 1.6
	Netscape 7.1
Slackware 10.2	FireFox 1.5.0.6
FreeBSD 6.1	FireFox 1.5.0.7

Connectivity

The following table lists the necessary Dominion SX hardware (adapters and/or cables) for connecting the DSX to common Vendor/Model combinations.

Table 75 Connectivity

VENDOR	DEVICE	CONSOLE CONNECTOR	SERIAL CONNECTION
Checkpoint	Firewall	DB9M	ASCSDB9F adapter and a CAT 5 cable
Cisco	PIX Firewall		
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 Dominion SX-48 models that have this connector to another Dominion SX.
Cisco	Router	DB25F	ASCSDB25M adapter and a CAT 5 cable
Hewlett Packard	UNIX Server	DB9M	ASCSDB9F adapter and a CAT 5 cable
Silicon Graphics	Origin		
Sun	SPARCStation	DB25F	ASCSDB25M 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	ASCSDB9F adapter and a CAT 5 cable
Various	Windows NT		
Raritan	RPCU	RJ-45	CSCSPCS-10 cable or CSCSPCS-1 adapter cable

Go to the following link to obtain a list of commonly used cables and adapters http://www.raritan.com/support

Dominion SX Serial RJ-45 Pinouts

To provide maximum port density and to enable simple UTP (Category 5) cabling, Dominion 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, which is on the back of the DSX.

Table 76 Dominion SX RJ-45 Serial Pinouts and Signals

RJ-45 PIN	SIGNAL
1	RTS
2	DTR
3	TxD
4	GND
5	Signal GND
6	RxD
7	DSR
8	CTS

Go to the following link to find the latest information about the Dominion SX serial pinouts (RJ-45).

http://www.raritan.com/support

DB9F Nulling Serial Adapter Pinouts

Table 77 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

Table 78 DB9M Nulling Serial Adapter Pinouts

RJ-45 (FEMALE)	DB9 (MALE)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

DB25F Nulling Serial Adapter Pinouts

Table 79 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

Table 80 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

Dominion SX Terminal Ports

All Dominion 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 (PC running VT100 emulation software, for example, 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 Dominion SX unit is disabled by default.

Models with two terminal ports support an external modem on only 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.

Table 81 Dominion SX Terminal Port Pinouts-First Port

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 only supports two pins as identified in the following table (Pin 4 and pin 7 are fixed to high).

Table 82 Dominion SX Terminal Port Pinouts-Second Port

DB9M PIN	SIGNAL
1	
2	RxD
3	TxD
4	DTR (H)
5	GND
6	
7	RTS (H)
8	
9	

Dominion SX16 and SX32 Terminal Ports

A modem should not be connected to the DSX16 and DSX32 terminal port 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.

Table 83 Dominion SX16 and SX32 Terminal Port Pinouts

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

Here is some additional information about the Dominion 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 unit. 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 SX2.2 (or higher) release support the local port capability.

- DSX versions through SX2.5 have the local port disabled by factory default.

- In DSX3.1 or higher, the local port is enabled by default.

Appendix B: System Defaults

This appendix contains the system defaults and directions for port access.

Table 84 Dominion SX System Defaults

ITEM	DEFAULT
IP Address	192.168.0.192
Subnet Mask	255.255.255.0
CSC Port Address (**TCP**)	5000
Port address for CC discovery (**UDP**)	5000
Factory default username	admin
Factory default password	raritan
GENERAL SETTINGS	
Direct Port Access (DPA)	Normal Mode (Off)
TACACS+	Disabled
RADIUS	
LDAP	
Local Port Access	
HTTP	Enabled
HTTPS	
SSH	
Syslog	
Event Notification	Disabled
Dialback	
IP-ACL	
Modem	
NTP	
Telnet	
SMTP	
SNMP	
Logging to NFS	
SERIAL PORTS	
Baud Rate	9600
Parity	None
Flow Control	None

≡❆ Raritan.

Use the following information for initiating port access:

Table 85 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
Notes;		
For FTP Upgrades	Port 21 needs to be open	Outgoing
For syslog	UDP port 514 needs to be open	Outgoing

You may need 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.

Appendix C: Certificates

This appendix contains sections describing Certificates and Certificate Authority and provides directions about how to:

- Install Dominion SX CA Certificate to a Browser Certificate
- Install SX Server Certificate for IE Browsers
- Install SX Server Certificate for Netscape Navigator
- Install a Third Party Root Certificate In Browsers
- **Generate a CSR for a Third Party CA to sign.
- **Install Third Party Certificate to SX.
- **Install Client Certificate root into the SX.
- **Install Client Certificate into Internet Explorer
- **Install Client Certificate into Netscape Navigator

A Certificate authority (**CA**) is an entity which issues digital certificates for use by other parties. These certificates contain a public and private key pair as described in standard cryptography references. There are many commercial CAs that charge for their services; however, the Dominion SX acts as a free CA that generates its own certificates. CA and certificates are part of highly available security technology that can be built into browsers and web servers - in particular SSL. Browsers and Operating Systems come with a pre-installed list of trusted Certification Authorities, known as the Trusted Root CA store. The Dominion SX certificates can be added into a browser as Trusted CA.

Default SX Certificate Authority Settings

The **Server Certificate** generated in the Dominion SX unit must be installed in the browser in order for the browser to trust the **Server Certificate**.

Each time you access an SSL-enabled Dominion SX unit, 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 unit's certificate into the browser's certificate store.

These steps will have to be performed for each SX unit to be accessed for each client browser that accesses the Dominion SX.

Install CA Root for IE Browsers

Each time you access an SSL-enabled Dominion SX unit, you see a New Site Certificate window. Eliminate this window's appearance by either accepting a session certificate permanently or by installing the server certificate directly in your browser.

Accept a Certificate (Session-Based)

On initially connecting to a Dominion SX unit will be presented with a certificate warning screen. This certificate by default will be signed by the local SX unit's CA as described above and you will have to accept this certificate to continue. To eliminate the future appearance of this window for this Dominion SX unit permanently, you must install the server certificate in your browser.

This procedure is described in the Install the Dominion SX Server Certificate section that follows.

Install the Dominion SX Server Certificate In Internet Explorer

By installing the Dominion SX Server certificate in IE, you can prevent the Security Alert window from appearing whenever you access the Dominion SX Unit. This step will have to be performed for each SX unit that you wish to access.

1. Launch IE and connect to the Dominion SX unit.
2. The "Security Alert" message will be displayed. Select "Yes".
3. Type **Username** and **Password** when prompted, and log on to the unit.
4. Select the Security tab and then click on the **Certificate** link.
5. Click on the **View Default Certificate** radio button and select OK. A dialog box opens asking to open, save, or cancel the viewing of the certificate. Select save and add the file extension ".cer" e.g. CA_ROOT.cer
6. Open the CA_ROOT.cer file by double-clicking on it. This will open the certificate.
7. Click on the Open button and select the Install Certificate button.
8. Click **Next.**
9. Select the **"Automatically select the certificate store based on the type of certificate" radio button.** If you do not want the Certificate Manager to select the certificate store automatically, click on the **Place all certificates into the following store** radio button and click **Browse** to choose a file.
10. Click **Next**.
11. Click **Finish**.
12. Click **OK**.
13. After installing the certificate, close all IE Browsers, including the IE browser connected to Dominion SX. Then launch a new IE Browser to continue working. The next time you connect to the unit, the trusted certificate warning window will not be displayed.

Remove an Accepted Certificate In Internet Explorer

Removing a certificate that you have previously accepted from the unit is the same process whether removing a Raritan default certificate or a user-installed third-party certificate.

1. Launch IE and on the **Tools** menu, click **Internet Options.** The Internet Options window appears.
2. Click the **Content** tab and click **Certificates**. The Certificates Manager window appears.
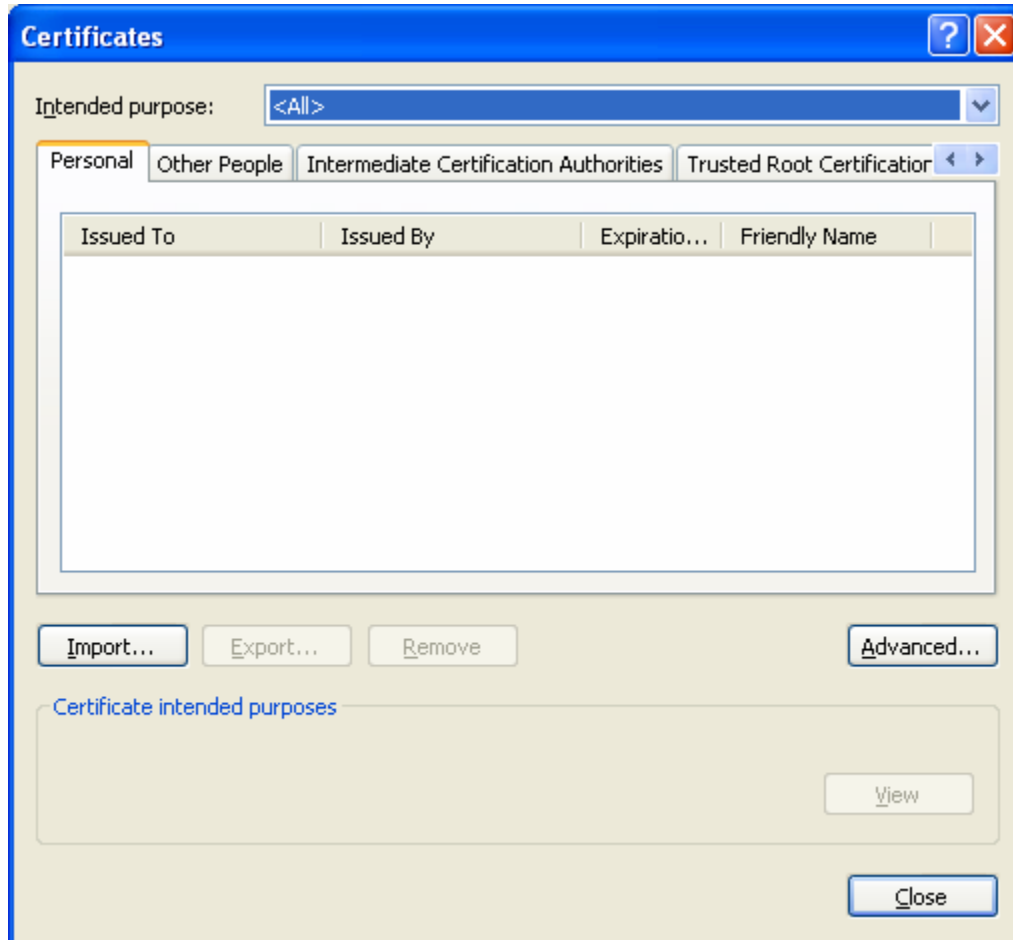
3. Scroll through the list of certificates and select the certificate to be deleted. The Certificate will normally be installed in the Other People tab and will be identified by the name, which should be the IP address of the Dominion SX.
4. Click **Remove**. A message dialog will appear.
5. Click **Yes** to delete the certificate.
6. Click **Close** on the Certificates dialog to close it.
7. Click **OK** on the Internet Options dialog box to close it.

Install Dominion SX Server Certificate for Netscape Navigator

By installing the Dominion SX Server certificate in Netscape, you can prevent the Security Alert window from appearing whenever you access the Dominion SX Unit. This step will have to be performed for each SX unit that you wish to access from each client's browser.

Accept a Certificate (Session-Based)

On initially connecting to a Dominion SX unit will be presented with a certificate warning screen. This certificate by default will be signed by the local SX unit's CA as described above and you will have to accept this certificate to continue. To eliminate the appearance of this window for this Dominion SX unit permanently, you must install the server certificate in your browser. This procedure is described in the **Install the Dominion SX Server Certificate** section that follows.

Install the Dominion SX Server Certificate In Netscape Navigator

1. Launch Netscape Navigator and connect to the IP address of the Dominion SX unit. The "Web Site Certified by an Unknown Authority" window appears.
2. Select "Accept this certificate permanently" and select 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 Dominion SX unit uses the same process whether removing a Raritan default certificate or removing a user-installed third-party certificate.

1. From the Tools menu, select Options.
2. Select the Advanced panel and then double-click on the Certificates category to open it.
3. In the Manage Certificates section, click the Manage Certificates button. This displays Certificate Manager.
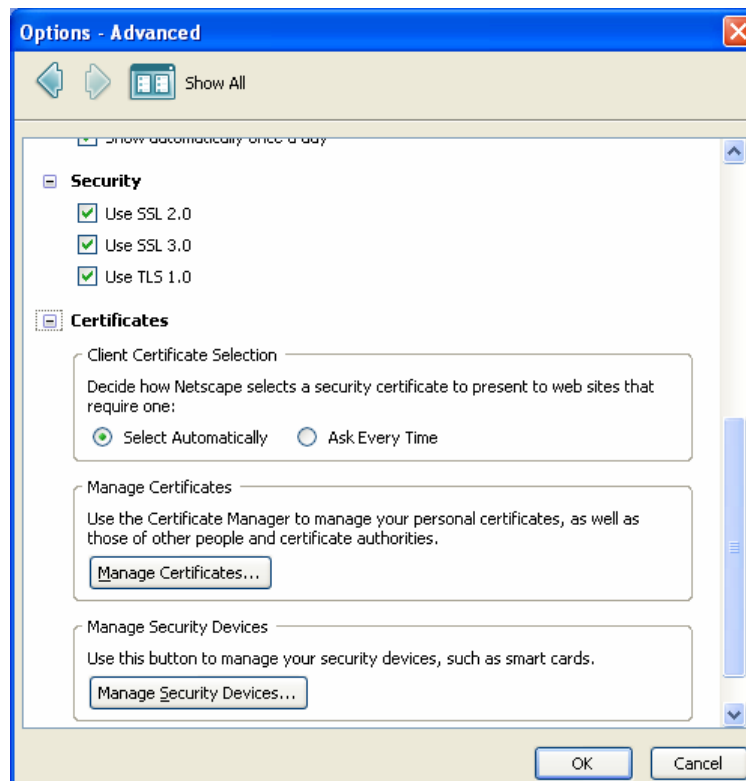
4.   Select the Web Sites tab and select the certificate name that is the common name of the IP address of the Dominion SX, and select the Delete button.
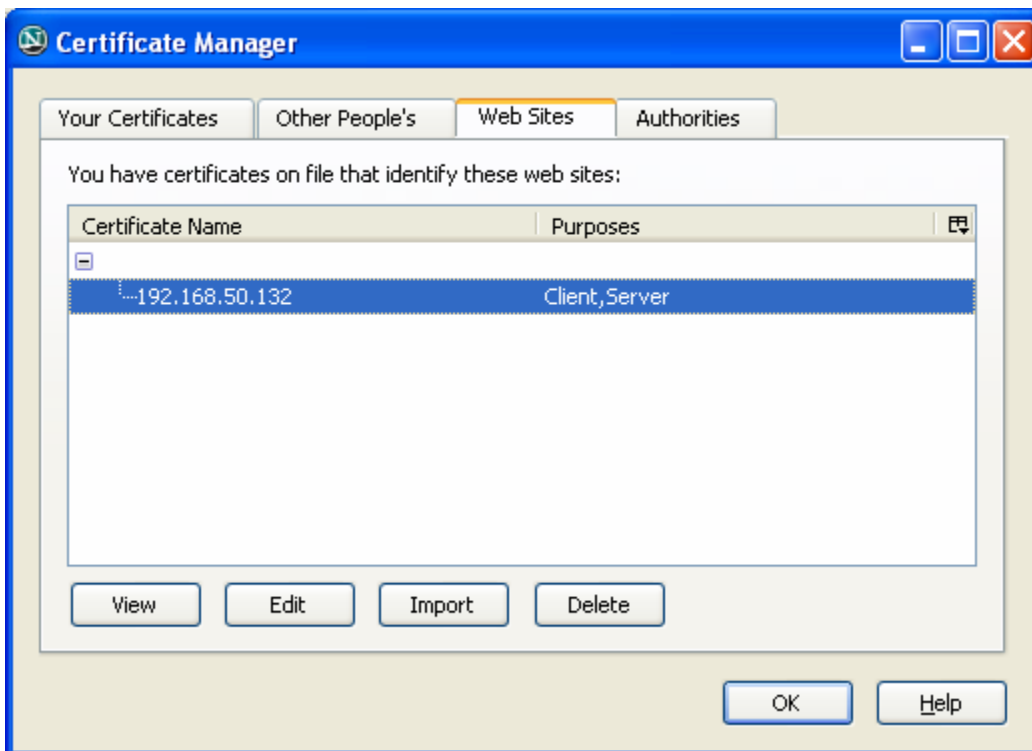
5.   Click OK on the "Delete Web Site Certificates" window to confirm the deletion of the certificate.
6.   On the left side of this window, locate **Certificates** and click **Web Sites**.
7.   Click OK on the Options Advanced Window.

Install a Third-Party Root Certificate

If you have installed a third-party certificate on the unit, you can obtain 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 as an example.

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/
VeriSign Incorporated	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.

Installing a Third-Party Root Certificate to Internet Explorer

In order to install a third party certificate to Internet Explorer you can download the CA certificate and install it following the steps above in the **Install the Dominion SX Server Certificate In Internet Explorer** section.

Installing 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 will appear. Click **Next**, and **Next** in the following screen.
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. Check 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 will have to follow the steps below to remove the currently installed certificate.
7. Click the **Security** button in Netscape, or 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 on **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.

In order to have a third party CA certificate (e.g. Verisign) installed on the SX rather than the internal CA on the Dominion 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 and this certificate must be installed onto the SX with the third party's CA's public key for this third party certificate to be used on the SX. This Certificate and key must then be installed onto the Dominion SX.

1. Go to the Security tab and select Certificate.
2. Select Generate Certificate Signing Request radio button.
3. Fill in parameters underneath the radio button, (bits, name, etc). Note that the email address is mandatory.
4. Click OK.
5. Select view CSR, and save file.
6. Have CSR signed by third party CA, receive back Certificate and public key of the CA.

Install Third Party Certificate to SX.

In order to have a third party CA certificate installed on the SX a Certificate Signing Request (CSR) must be generated by the SX to be signed. The CA will take this CSR and generate a Certificate and this certificate must be installed onto the SX with the CA's public key for this third party certificate to be used on the SX. This Certificate and key must then be installed onto the Dominion SX.

1. Place the certificate and public key on an accessible ftp server.
2. Go to **Security** tab and select **Certificate.**

3. Select the **Install User Key** radio button.
4. Insert the ftp parameters to retrieve the CA Public key file.
5. Click **OK.** The SX will show "User Key Installed" at top of pane.
6. Select the **Install User Certificate** radio button.
7. Fill in the ftp parameters to retrieve the CA signed Certificate.
8. Click **OK.** The SX will show "User Certificate Installed" at top of pane.
9. Restart the SX device for the settings to take place.

Install Client Root Certificate into the SX.

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 unit with the following steps:

1. Retrieve CA's Root certificate used to sign the client certificates and place it on an accessible FTP server
2. Go to **Security tab** and select **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 device 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.mspx?mfr=true

Appendix D: Server Configuration

This appendix contains sections describing the steps to configure Dominion SX units and authentication servers for the following authentication protocols:

- Microsoft Internet Authentication Service (IAS) RADIUS Server
- Cisco Access Control Server (ACS) Radius Server
- TACACS+ (Terminal Access Controller Access-Control System Plus)

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 Dominion SX to use an IAS server.

Configure the Dominion SX to Use an IAS RADIUS Server

The tasks to set up the Dominion SX unit to use an IAS RADIUIS server are:

- Configure a Primary Radius Server (and optional secondary Radius server)
- Configure a Radius port
- Configure a secret (shared secret) that will be 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 the **Add/Remove Windows Components** button.
3. Highlight **Networking Services** then click the **Details...** button.
4. Place a checkmark next to the **Internet Authentication Service** then click **OK**.
5. Click the **Next>** button and continue to complete 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 (Start->All Programs-> Administrative Tools->
   Internet Authentication Service).
2. Right click on Internet Authentication Service (Local) and select Register Server in Active Directory.

Note: Refer to the following Microsoft URL for information about Active Directory:
http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

Add Dominion 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 DSX unit.
3. Select the **RADIUS Standard** in the **Client-Vendor** dropdown menu, and type a **Shared Secret** that matches the Dominion SX configuration.

Create an IAS Policy

The following section describes the steps to create a policy to allow Radius users to access the Dominion SX. The example in this section requires two conditions, the client source IP address of the Dominion SX and the UserID is a member of the SX User Group:

- NAS-IP-Address = Type the IP address of Dominion SX
- Windows-Group = SX User Group

Note: If you have multiple Dominion 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 Dominion SX unit.
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. Select the **Authentication** tab. Remove other checkmarks and add a checkmark to enable Unencrypted authentication (PAP, SPAP)

Note: This version of Dominion SX does not support Challenge Authentication Protocol (CHAP).

11. Select the **Advanced** tab. Remove **Framed-Protoco**l.

Note: Each policy has conditions that must be met. If the conditions are not met then IAS goes to the next policy and examine the conditions.

12. Click the **Add...** button. The RADIUS attributes list appears.
13. Select **Filter-Id Name** and click the **Add** button. Click on **Add** in the Attribute values section. Type the attribute value, **Raritan:G{Admin}**.
14. Click **OK**.
    The value in G{} is the name of a group locally on the DSX, 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 Dominion SX.
    - The Dominion SX comes from the factory with the default Admin group.
    - Additional user groups can be created on Dominion SX unit 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 Dominion SX unit

≡ Raritan.

15. 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).

---

16. Ensure that the service is started.
17. 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 Dominion SX unit. For the Dominion SX to support RADIUS, both the unit and the user information must be added into the RADIUS configuration.

Configure the Dominion SX to use a Cisco ACS Server

The following procedure configures the Dominion SX unit to work with a Cisco Radius Server.

1. Select the **User Management** tab on DSX screen.
2. Go to the **Configuration** section.
3. Select the **User Group List**.
4. Click on **Add New User Group**.

You can define port access and user class (operator or observer). This user group will be used later as a value to the Filter-Id attribute on the Cisco Radius Server. The Dominion SX comes with factory default group **Admin** that will be used as an example in this section; however, any local group can be used as value to the Filter-Id attribute on the Cisco ACS Server.

Notes: Group names are case sensitive and must match exactly those defined in the Filter-Id attribute on the Radius server.

Only Version 3.1 of the Cisco Radius Server has been tested; however, other versions of the RADIUS server should operate with the DSX.

Configure the Cisco ACS Server

1. Log on to Cisco ACS Server using the browser.
2. Type your **Username** and **Password.**
3. Click **Login**.
4. Click **Network Configuration** in the left panel of the screen and select **Add Entry** to add/edit an AAA Client. This must be done for each unit that is going to be accessed via RADIUS.
5. Click on the **Authenticate Using** drop-down menu and select **RADIUS (IETF)**.
6. Click **Submit.**
7. Click **Interface Configuration** in the left panel of the screen.
8. Click on the **RADIUS (IETF)** link to edit properties.
9. Under the **User** and **Group** columns, place a checkmark in the check boxes before **Filter-Id**.
10. Click **Submit.**

11. To add new users and configure RADIUS (IETF) attributes, click **User Setup** in the left panel of the screen.

12. Type the user's name and click **Add/Edit.**

13. To edit existing users, click **User Setup** in the left panel of the screen and click **List All Users.**

14. Select a user from the list.

15. Once you have selected a user, on the user properties page, scroll down to the **IETF RADIUS Attribute** section.

16. Click on the **Filter-Id** check box and add the following value for this attribute:
    Raritan:G{Admin}

    The value in G{} is the name of a group locally on the DSX, in this case the default Admin group.

    - The value can be Raritan:G{Admin}:D{1234567890} if using 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 Dominion SX unit

    - The Dominion SX comes from the factory with the default Admin group.

    - Additional user groups can be created on Dominion SX unit by using the **User Management>User Group** option.

    - Appropriate port access and user class (Operator or Observer) can be defined and the group name should be specified in the Filter-Id attribute value accordingly in order to authorize the RADIUS user to access the Dominion SX unit

17. Click **Submit.**

Note: If there is more then one Radius user requiring the same authorization on the Dominion SX, the Filter-Id attribute and its value can be defined at the group level on the Cisco ACS as long as these users belong to the same group.

TACACS+ Server Configuration

The Dominion SX unit has the capability to use Terminal Access Controller Access-Control System Plus (TACACS+) for authentication services.

The Dominion 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 Dominion SX. Group name specified for this attribute on TACACS+ Must exactly (case sensitive) match with group name on Dominion SX unit or else authentication for TACACS+ user on Dominion 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: Refer to the following URL: http://cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a00 8007cd49.html#12231

1. Add Dominion SX as a client on Cisco ACS TACACS+.

Figure 100 Cisco ACS AAA Client for TACACS+

2.   Select **Interface Configuration**.
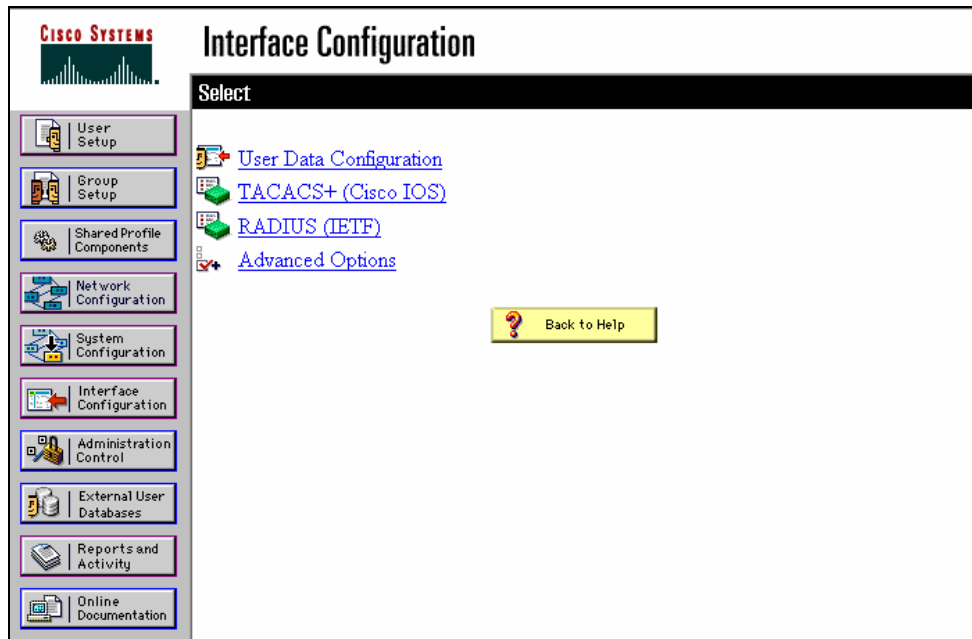
Figure 101 Cisco ACS Interface Configuration

3.   Select **TACACS+ (Cisco IOS)**.

4.   Add **dominionsx** service under the heading **New Services**.
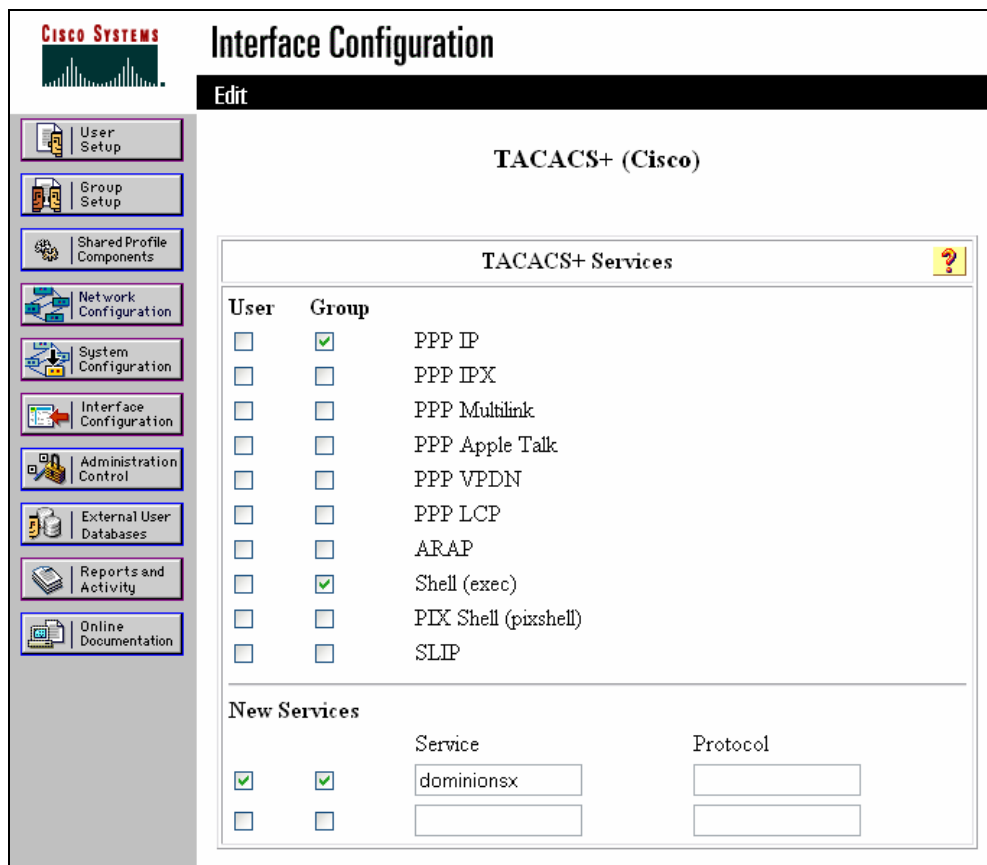
Figure 102 TACACS+ Properties

5. 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** check boxes. Add the attributes (user-type) and the appropriate values to the text box.

Note: The value for the user-group attribute is case sensitive so ensure that it matches exactly the same as the local group name on Dominion SX unit.

Figure 41 TACACS+ Settings

Active Directory

See the following Microsoft URL for information about active directory.
http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

Appendix E: Modem Configuration

Client Dial-Up Networking Configuration

Configuring Microsoft Windows Dial-Up Networking for use with Dominion SX allows configuration of a PC to reside on the same (Define?)PPP network as the Dominion SX. After the dial-up connection is established, connecting to a Dominion 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 NT
- Windows 2000
- Windows XP

Windows NT Dial-Up Networking Configuration

1. Select Start → Programs → Accessories → Dial-Up Networking.
2. Click **New.**
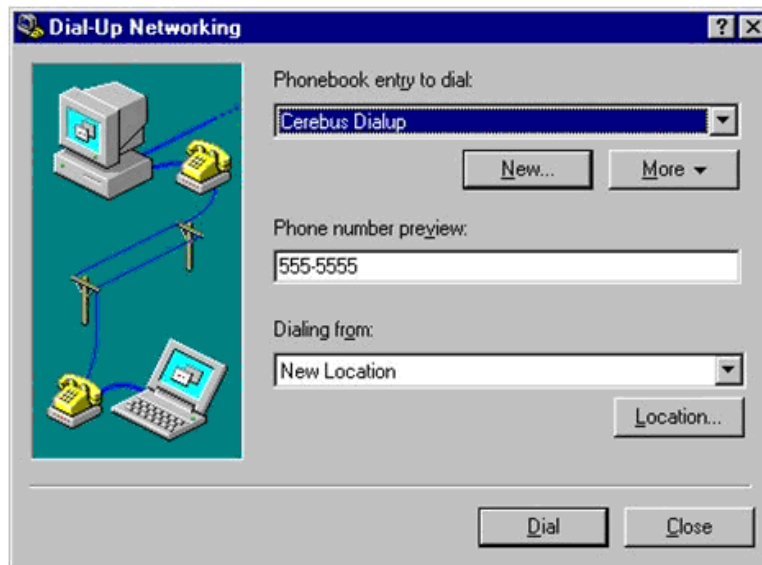
Figure 103 Dial-Up Networking Display

The New Phonebook Entry window allows you to configure the details of this connection.
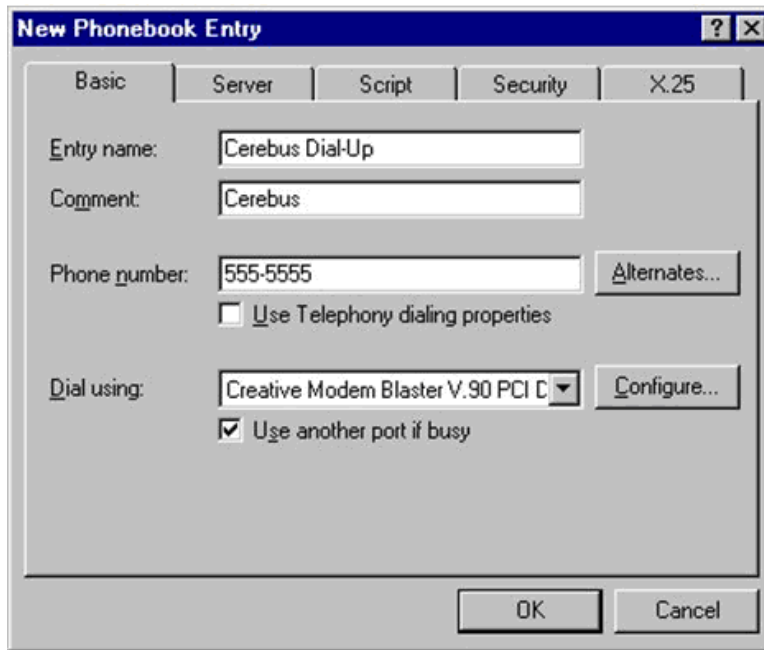
Figure 104 New Phone Entry Display

3. Click on the **Basic** tab and complete the following fields:
    o   **Entry name**: Name of the Dominion SX connection
    o   **Phone number**: Phone number of the line attached to the Dominion SX unit
    o   **Dial using**: Modem being used to connect to Dominion SX; if there is no entry here, there is no modem installed in your workstation
4. Click on the **Security** tab.
    The Security section allows you to specify the level of security to use with the modem connection. When connecting to the Dominion SX unit, security is provided by SSL/ with RC4 encryption, therefore no dialup security is required.
5. Click on the **Accept any authentication including clear text** radio button.

6. Click **OK** to return to the main Dial screen.
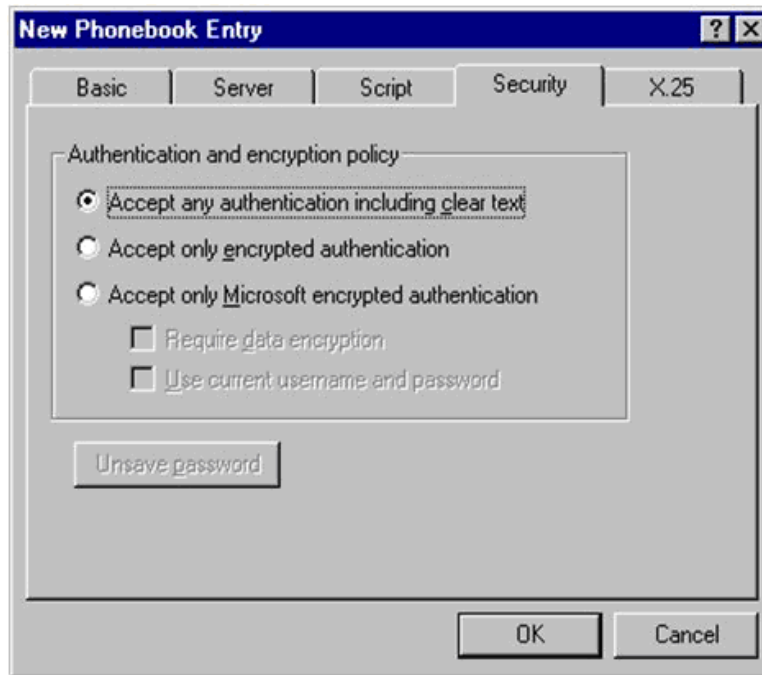
Figure 105 Dial-Up Security Display

7. Click **Dial.** See the Windows NT Users Guide if you receive any error message.

Windows 2000 Dial-Up Networking Configuration

1. Select Start → Programs → Accessories → Communications → Network and Dial-Up Connections.
2. Double-click on the **Make New Connection** icon when the Network and Dial-Up Connections window appears.
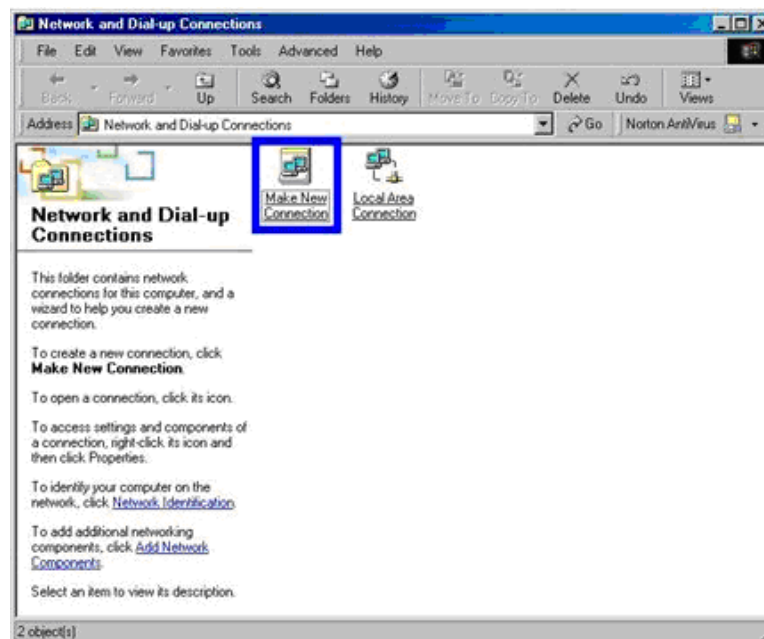
Figure 106 Windows 2000 Network and Dial-Up Connections

3. Click **Next** and follow the steps in the **Network Connection** Wizard window to create custom dialup network profiles.

4. Click the **Dial-up to private network** radio button and click **Next.**
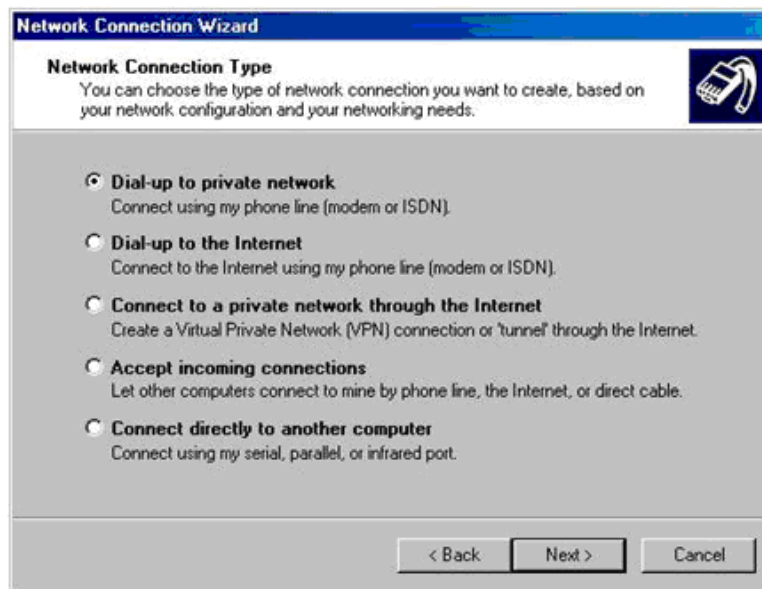
Figure 107 Network Connection Type

5. Select the check box before the modem that you want to use to connect to the Dominion SX unit and then click **Next.**
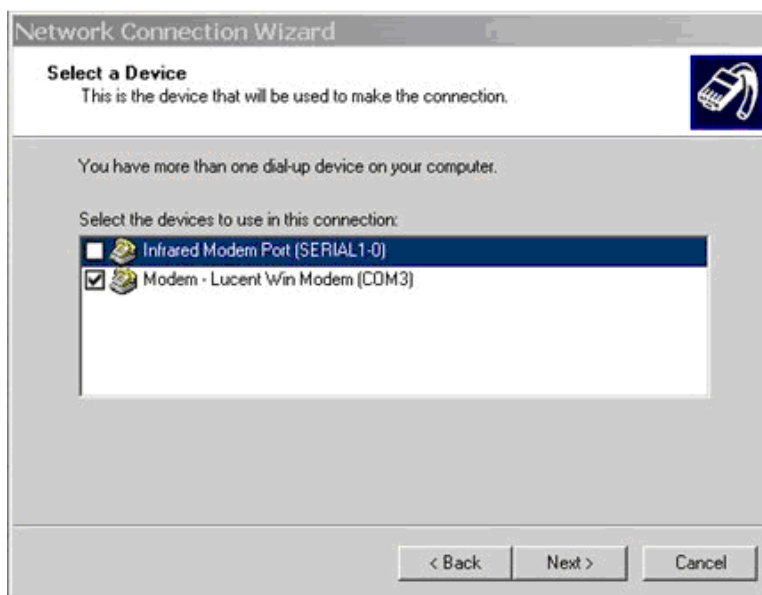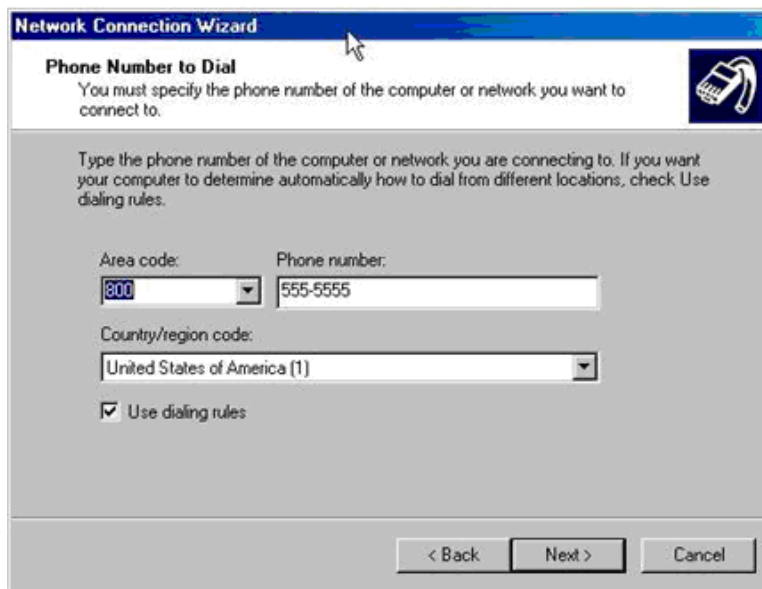
Figure 108 Device Selection

6. Type the **Area code** and **Phone number** you wish to dial in the appropriate fields.
7. Click on the **Country/region code** drop-down arrow and select the country or region from the list.

8. Click **Next.**

Figure 109 Phone Number to Dial

The Connection Availability Screen appears.

    1. Click on the **Only for myself radio button** in the Connection Availability screen.

    2. Click **Next.**

Figure 110 Connection Availability

The Network Connection has been created

    3. Type the name of the Dial-up connection.

    4. Click **Finish**.

    5. Click **Dial** to connect to the remote machine when the Dial Window appears.

A window 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 XP Dial-Up Networking Configuration

1. Select Start → Programs → Accessories → Communications → New Connection Wizard.

2. Click **Next** and follow the steps in the **New Connection Wizard** to create custom dialup network profiles.

3. Click the **Connect to the Internet** radio button and click **Next.**
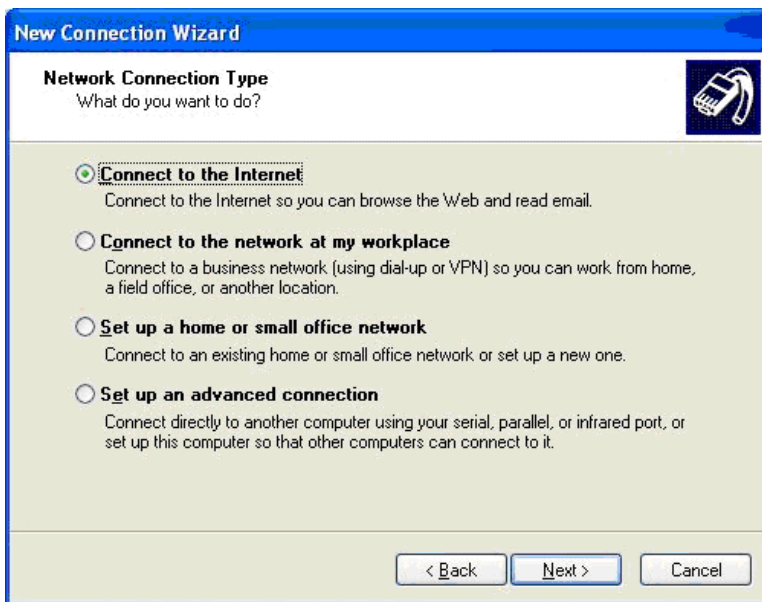

Figure 111 Network Connection Type

4. Click the **Set up my connection manually** radio button and click **Next.**

Figure 112 Device Selection

5. Click on the radio button before **Connect using a dial-up modem** and click **Next.**
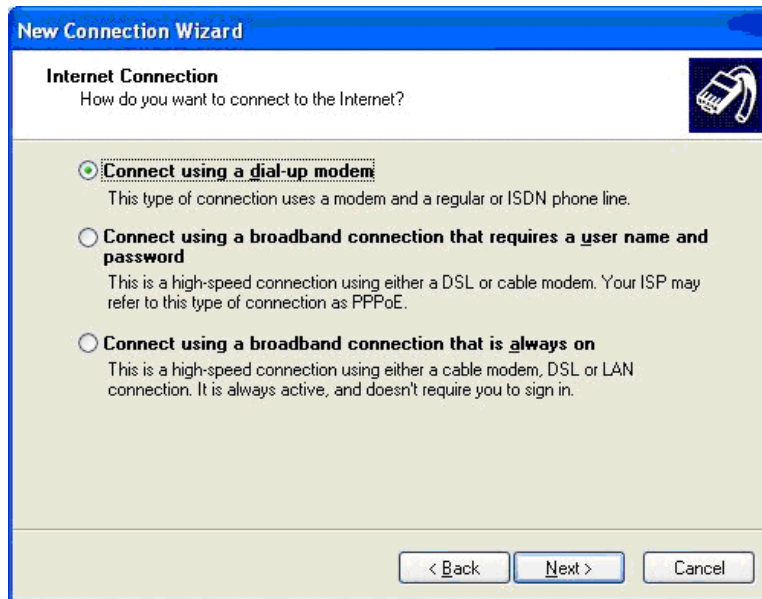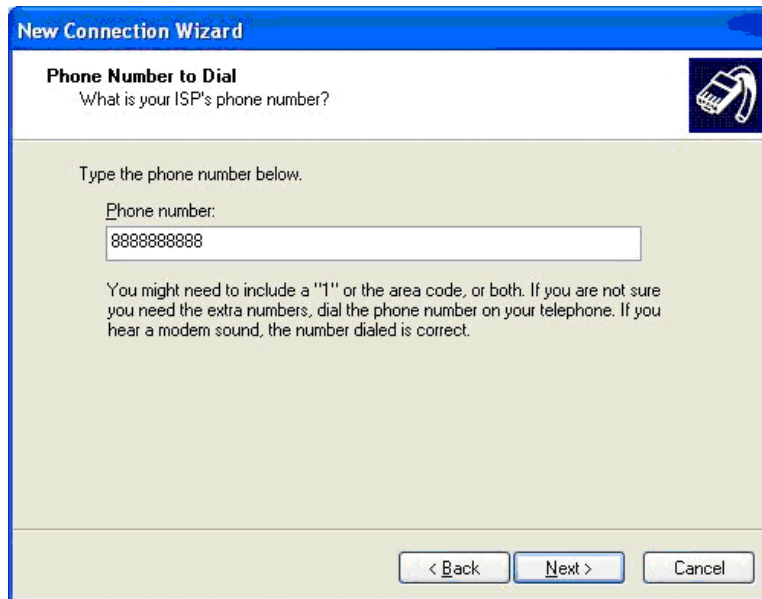
Figure 113 Internet Connection

6. Type a name to identify this particular connection in the **ISP Name** field and click **Next.**

Figure 114 Connection Name

7. Type the phone number of this connection in the **Phone number** field and click **Next.**

Figure 115 Phone Number to Dial

8. Type your ISP information; type the User name and Password in the appropriate fields, and retype the password to confirm it.
9. Click on the checkbox before the appropriate option below the fields and click **Next.**

Figure 116 Internet Account Information

10. Click **Finish**.
11. Click **Dial** to connect to the remote machine when the Dial Window appears.

A window indicating that you connected successfully appears. If you get any errors, consult Windows XP Dial-up Networking Help.

Appendix F: Troubleshooting

The following tables describe problems and suggested solutions for the problems.

Page Access

Table 86 Troubleshooting Page Access

PROBLEM	SOLUTION
Cannot login – what are factory defaults? (only for Dominion SX units running firmware version 2.5 or higher)	username: **admin** (all lower case) password: **raritan** (all lower case)
Cannot login – non defaults.	1. Check multiple login per user status. If disabled and there is already a session established opening anew one fails. 2. 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: 1. Verify that the unit is powered on. 2. Verify that the unit is properly connected to a network. 3. Ping the unit from a computer on the same network to ensure that network communication with the unit occurs. • Should the *ping* fail, contact your network administrator. There may be a problem with your network configuration that is preventing communication with the unit. • Should the *ping* succeed, consult the following topics.
DNS Error/Server Unreachable	When attempting to connect to the Dominion SX URL using Microsoft IE, a web page may appear indicating a DNS error and reading that the server is unreachable. Remove any installed Dominion SX certificates and restart the browser.
Unsupported Encryption	The unit supports only 128-bit SSL encryption. • In Internet Explorer, view **Help→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. • In Netscape, view **Communicator→Tools→Security Info→SSL v3.0 Configuration** and ensure that 128-bit SSL is supported

☰ Raritan.

PROBLEM	SOLUTION
Number of Users Exceeded	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. Wait for a few minutes and attempt to login again. You may need to refresh or <**Shift**+**Refresh**> your browser to successfully log on.

Firewall

Table 87 Troubleshooting Firewall

PROBLEM	SOLUTION
Unable to Access the Web Page	Firewalls must allow access on port 80 (for http) and 443 (for https) for the unit to operate through a firewall. Contact your system administrator and request port 80 and 443, or other custom configured ports for access.
Login Failure	Firewalls must be configured to allow connections using the Dominion SX configurable port network parameter (Default 51000). If the firewall does not allow these connections, the applet indicates that the login has failed. Contact your system administrator and request that connections be allowed on the configurable port.
SSL Security Warnings	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. This is normal behavior. The warning message does not affect operation of the unit.

Login

Table 88 Troubleshooting Login

PROBLEM	SOLUTION
Login Failure	To provide additional security, the unit login screen expires after three minutes. Therefore, all login attempts after this time period will fail. Reload the browser to reset this timer. Hold down the **SHIFT** key and click **Reload** in your browser. This will refresh the login screen from the unit itself (not from a local cache) and allow login to the unit.
RADIUS Users	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. If the RADIUS server is not reachable for user authentication for any reason, the unit will not allow the user to log on until the unit receives the result of the authentication request from the RADIUS server. 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.

Port Access

Table 89 Troubleshooting Port Access

PROBLEM	SOLUTION
Port Access Refresh	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 screen until the **Port Access** button is activated. • You must log out and log in again for the new restriction to be applied. Then the restricted ports are invisible. • Whenever possible, it is recommended that Administrators not change port access rights to a user who is already logged in to the unit.

Upgrade

Table 90 Troubleshooting Upgrade

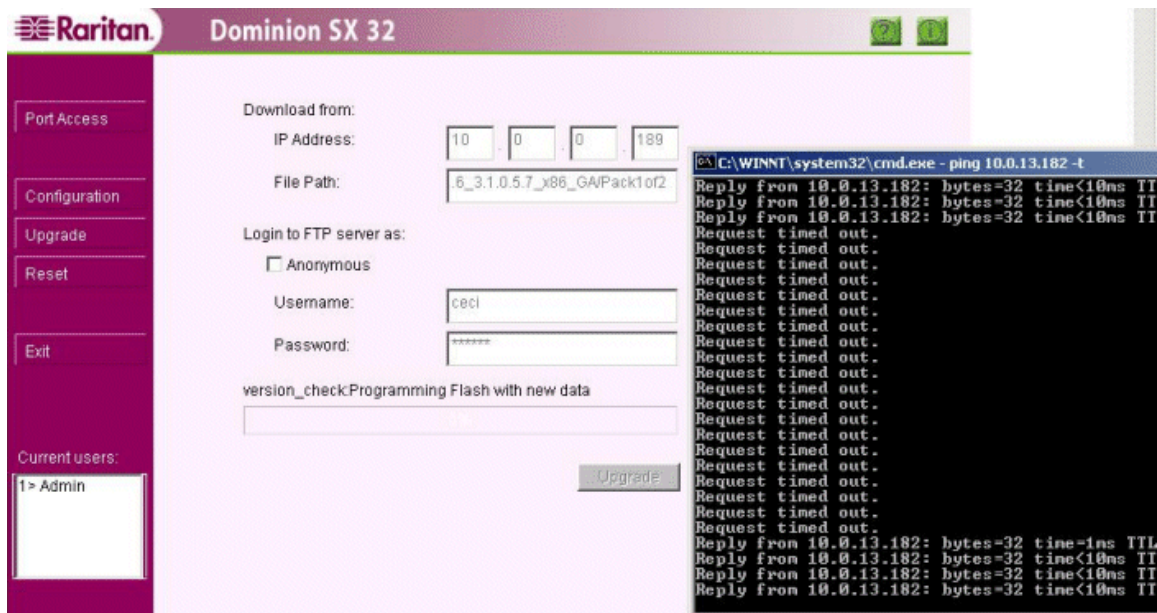| PROBLEM	SOLUTION
FTP - Server Unreachable	If FTP server specified in the upgrade panel is unreachable or incorrect, the upgrade process halts until a response is received from the FTP server or until a timeout occurs. Wait and allow the FTP *Server Unreachable* message to appear.
FTP - File Not Found	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. Verify that the upgrade package is in the correct directory and confirm the upgrade path and IP address of the FTP server. If the upgrade still fails, reinstall the upgrade package and begin again.
Insufficient Partition Size	The latest 3.1.0.5.7 firmware is specifically applicable to Dominion SX models – DSX-16 and DSX-32 only (purchased before August 2004). This version also supports the use with CC-SG 3.1 (CommandCenter SecureGateway) or higher. **Please note** that the attempt to upgrade firmware to the latest 3.1.0.5.7 version will be aborted if the DSX unit 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).

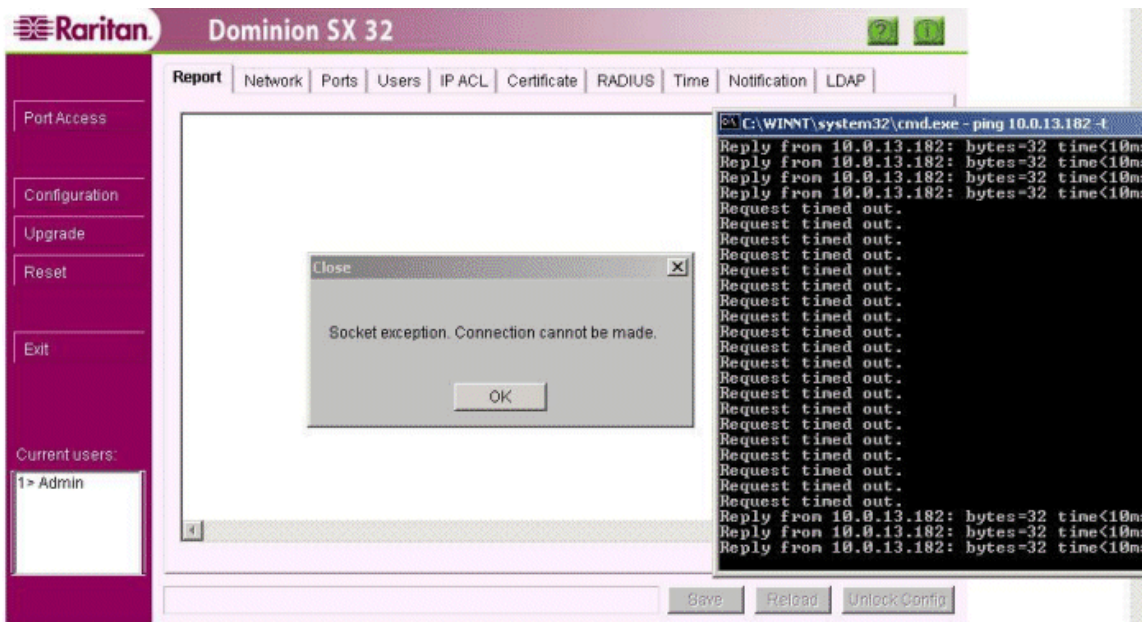*Figure 117 Firmware Upgrade – Timeout*
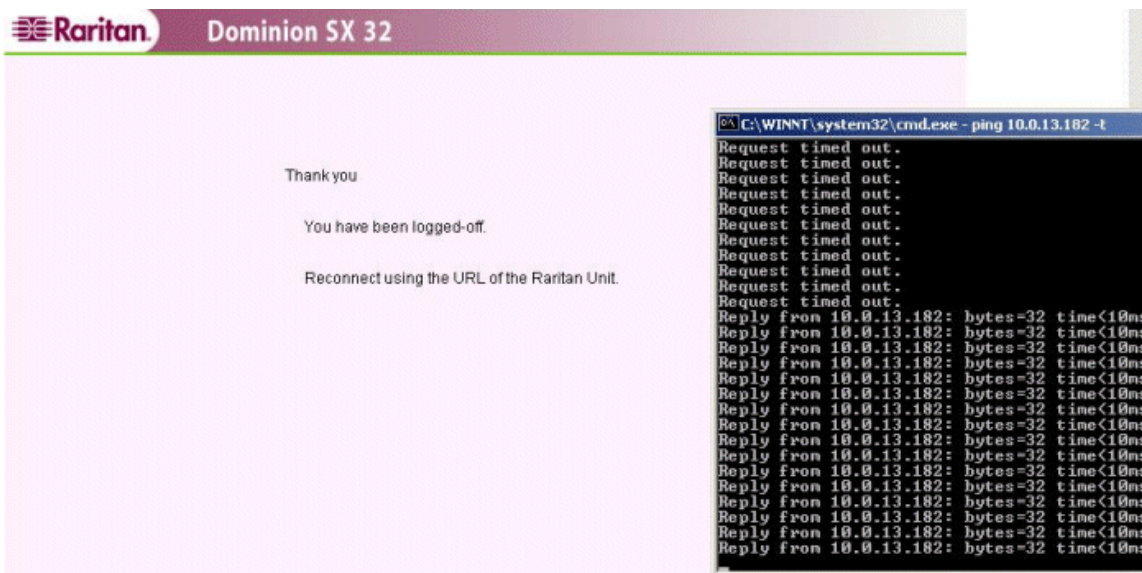
Figure 118 Firmware Upgrade – Connection Fail

Figure 119 Firmware Upgrade – Auto Logout

Modem

Table 91 Troubleshooting Modem

PROBLEM	SOLUTION
Login Failure	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 on to the unit via the modem. 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.

255-60-2000-00

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 8 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

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5994
Email: support.japan@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT+1 CET
Phone +44 20 7614 77 00

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: tech.rap@raritan.com

Sydney, Australia

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +61-2-9029-2558

Germany

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +49-20 17 47 98 0

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33 1 47 56 20 39

GuangZhou

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

Shanghai

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

Beijing

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Korea

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +82-2-5578730

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com