

# Dominion<sup>®</sup> SX

## Installation and Operations Manual Dominion SX Series

### **Raritan Computer Inc.**

400 Cottontail Lane  
Somerset, NJ 08873  
USA  
Tel. 1-732-764-8886  
Fax. 1-732-764-8887  
E-mail: [sales@raritan.com](mailto:sales@raritan.com)  
<http://www.raritan.com>

### **Raritan Computer Japan, Inc.**

4th Flr. Shinkawa NS Building  
1-26-2 Shin-kawa, Chuo-ku  
Tokyo 104-0033  
Japan  
Tel. 81-03-3523-5991  
Fax. 81-03-3523-5992  
E-mail: [sales@raritan.co.jp](mailto:sales@raritan.co.jp)  
<http://www.raritan.co.jp>

### **Raritan Computer France**

120 Rue Jean Jaurès  
92300 Levallois-Perret  
France  
Tel. 33-14-756-2039  
Fax. 33-14-756-2061  
E-mail: [sales.france@raritan.com](mailto:sales.france@raritan.com)  
<http://www.raritan.fr>

### **Raritan Computer U.K. Ltd.**

36 Great St. Helen's  
London  
EC3A 6AP  
United Kingdom  
Tel. 44 20 7614 7700  
Fax. 44 20 7614 7701  
E-mail: [sales.uk@raritan.com](mailto:sales.uk@raritan.com)  
<http://www.raritan.com>

### **Raritan Computer Europe, B.V.**

Eglantierbaan 16  
2908 LV Capelle aan den IJssel  
The Netherlands  
Tel. 31-10-284-4040  
Fax. 31-10-284-4049  
E-mail: [sales.europe@raritan.com](mailto:sales.europe@raritan.com)  
<http://www.raritan.com>

### **Raritan Computer Taiwan, Inc.**

5F, 121, Lane 235,  
Pao-Chiao Rd., Hsin Tien  
Taipei Hsien  
Taiwan, ROC  
Tel. 886-2-8919-1333  
Fax. 886-2-8919-1338  
E-mail: [sales.asia@raritan.com](mailto:sales.asia@raritan.com)  
<http://www.raritan.com.tw>

### **Raritan Computer Deutschland GmbH**

Lichtstraße 2  
D-45127 Essen  
Germany  
Tel. 49-201-747-9820  
Fax. 49-201-747-9850  
E-mail: [sales.germany@raritan.com](mailto:sales.germany@raritan.com)  
<http://www.raritan.de>

### **Shanghai Representative Office of Raritan Computer, Inc.**

RM17E, Cross Region Plaza  
No.899 Lingling Road  
Shanghai China 2000030  
Tel. 86-21-5425-2499  
Fax. 86-21-5425-3992  
E-mail: [sales.china@raritan.com](mailto:sales.china@raritan.com)  
<http://www.raritan.com.cn>



Copyright ©2005 Raritan Computer, Inc.

DSX-0H-E

September 2005

255-60-2000

---

*This page intentionally left blank.*

---

### **Copyright and Trademark Information**

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

©Copyright 2005 Raritan Computer, Inc., Dominion, RaritanConsole, SecureChat, Remote Power Control, Paragon, Powerboard and the Raritan company logo are trademarks or registered trademarks of Raritan Computer, Inc. All rights reserved. Java is a registered trademark of Sun Microsystems, Inc. Windows, Windows 98, Windows 2000, NT, XP, Internet Explorer, and Active Directory are registered trademarks of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communication Corporation. Mozilla is a registered trademark of the Mozilla Foundation. RC4 is a registered trademark of RSA Corporation. All other trademarks or registered trademarks are the property of their respective holders.

### **EXPORT NOTICE**

Dominion SX models contain 128-bit encryption software. Export of this product is restricted under U.S. law. Information is available from the U.S. Department of Commerce, Bureau of Export Administration at <a href="http://www.bxa.doc.gov">www.bxa.doc.gov</a> .
---

**Please Note:** Web browser images in this manual were collected using Internet Explorer as the browser. Unless otherwise noted, this documentation applies to all Dominion SX series models.

*For assistance in the U.S., please contact the Raritan Technical Support Team  
by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail [tech@raritan.com](mailto:tech@raritan.com)  
Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm Eastern*

*For assistance outside the U.S., please contact your regional Raritan office.*

---

*This page intentionally left blank.*

# Contents

<b>Chapter 1: Introduction .....</b>	<b>1</b>
Dominion SX Overview .....	1
Product Photos.....	1
Product Features.....	1
Package Contents.....	2
<b>Chapter 2: Installation.....</b>	<b>3</b>
Pre-Configuration Notes.....	3
Hardware Installation .....	4
Initial Software Configuration .....	5
Initial Configuration.....	6
Dominion SX.....	7
Deployment .....	10
<b>Chapter 3: Operation .....</b>	<b>11</b>
Overview .....	11
Accessing the Remote Device .....	11
Browser-Based Access.....	11
Security Dialog for Console Display.....	13
Internet Explorer .....	13
Netscape Navigator .....	14
Sending a Break / Null .....	14
<b>Chapter 4: Console Features.....</b>	<b>15</b>
Emulator .....	15
Settings.....	15
History .....	16
Write Access.....	17
Sending a Break/Null .....	18
User List .....	19
Close .....	20
Edit .....	21
Tools.....	22
Start Logging .....	22
Stop Logging .....	23
Script .....	24
SecureChat .....	25
Help .....	26
Help Topics.....	26
About RaritanConsole.....	27
Direct Port Access.....	28
URL with Password and Username and Port .....	28
URL with Port Number.....	29
Exit the Application.....	30
Dominion SX Management .....	32
Display .....	32
Configuration Lock and the Configuration Save Commands .....	33
Update.....	33
Save and Reload .....	33
Configuration.....	35
Report.....	35
Network .....	36
Ports .....	38
Users .....	40
IP ACL.....	43
Certificate .....	48
RADIUS .....	54
Time.....	58
Notification.....	59
Upgrade .....	63
Reset.....	65
Soft Reset.....	65
Factory Reset .....	66

<b>Chapter 5: Using the Command Line Interface with Secure Shell and Telnet.....</b>	<b>69</b>
Secure Shell (SSH) Access .....	69
Interactive Session.....	69
Command Line Arguments Session: Syntax for initiating a Command Line Session .....	78
Port Sharing Using SSH .....	79
<b>Chapter 6: Authentication and Authorization .....</b>	<b>81</b>
Implementing LDAP Remote Authentication.....	81
TACACS+ Server Configuration .....	82
<b>Chapter 7: Logging .....</b>	<b>85</b>
NFS Per Port Logging Configuration Usage .....	85
Name .....	85
Description.....	85
NFS Server Setup .....	86
<b>Chapter 8: SNMP.....</b>	<b>87</b>
SNMP Trap Configuration .....	87
Name .....	87
Description.....	87
<b>Chapter 9: System Configuration .....</b>	<b>89</b>
Local Port Access Configuration.....	89
Name .....	89
Description.....	89
Name .....	90
Description.....	90
Service (Telnet and SSH) Configuration.....	90
Name .....	90
Description.....	90
<b>Appendix A: Specifications .....</b>	<b>93</b>
Dominion SX Connectivity and Serial Pin-Out Guides .....	94
Connectivity Table.....	94
Dominion SX Serial Pinouts.....	95
<b>Appendix B: System Defaults.....</b>	<b>97</b>
<b>Appendix C: Certificates .....</b>	<b>99</b>
Certificate .....	99
Certificate Contents .....	99
Certificate Authority .....	100
Installing Dominion SX CA-Root Certificate to a Browser .....	101
Installing CA Root for IE Browsers.....	102
Accept a Certificate (Session-Based) .....	102
Install the Raritan Root Certificate .....	102
Remove an Accepted Certificate .....	105
Install CA Root for Netscape Navigator .....	106
Accept a Certificate (Session-Based) .....	106
Install the Dominion SX Root Certificate.....	107
Remove an Accepted Certificate .....	109
Install a Third-Party Root Certificate .....	110
<b>Appendix D: RADIUS Server .....</b>	<b>113</b>
Overview .....	113
Install and Configure the RADIUS Server for Windows 2000.....	114
<b>Appendix E: Configuring Cisco ACS RADIUS Server.....</b>	<b>121</b>
<b>Appendix F: RSA ACE/Server Configuration.....</b>	<b>125</b>
Lightweight Directory Access Protocol (LDAP).....	130

<b>Appendix G: Modem Configuration.....</b>	<b>131</b>
Client Dialup Networking Configuration .....	131
Windows NT Dialup Networking Configuration .....	131
Windows 98 Dialup Networking Configuration.....	133
Windows 2000 Dialup Networking Configuration.....	135
<b>Appendix H: TCL Programming Guide.....</b>	<b>139</b>
Overview .....	139
TCL Architecture with Target System .....	139
Boot Script Support.....	141
File System .....	141
File Directory Structure .....	141
File System API through TCL .....	141
TCL Commands.....	142
Accessing TCL Window .....	143
Resetting TCL Interpreter .....	143
Editing TCL Scripts .....	143
Executing TCL Scripts .....	143
Automatic Execution of a TCL Script upon Power Up.....	144
Generating a User Event.....	145
Extensions to TCL.....	146
Basic TCL Server Example .....	155
Basic CPU Utilization Monitoring Example .....	156
TCL Server designed to interact with a TCL user .....	159
<b>Appendix I: Troubleshooting .....</b>	<b>161</b>
Problems and Suggested Solutions .....	161
Page Access.....	161
Firewall .....	162
Login.....	162
Port Access .....	163
Upgrade.....	163
Modem.....	163
<b>Appendix J: Technical FAQs .....</b>	<b>165</b>

# Figures

Figure 1 Dominion SX32 Unit.....	1
Figure 2 Rear Panel of 32-port single power supply model .....	4
Figure 3 Default Settings for Factory Reset Mode .....	4
Figure 4 Hardware Setup for Initial Software Configuration .....	5
Figure 5 Change Password Screen .....	7
Figure 6 Dominion SX User Screen .....	7
Figure 7 Time and Date Configuration Screen.....	8
Figure 8 Network Configuration Screen .....	8
Figure 9 Confirm Save Window .....	9
Figure 10 Confirm Reboot Screen .....	9
Figure 11 Confirm Disconnection Screen .....	9
Figure 12 Logged off Dominion SX Screen.....	9
Figure 10 Deployment.....	10
Figure 11 Security Alert Display.....	11
Figure 12 Login Display .....	12
Figure 13 Main Display with Available Ports (32-port unit shown) .....	12
Figure 14 Security Dialog in Internet Explorer.....	13
Figure 17 Console Window .....	14
Figure 18 Settings Command and Settings Window.....	15
Figure 19 History Command .....	16
Figure 20 Get Write Access Command.....	17
Figure 22 User List Command and User List Window .....	19
Figure 23 Close Command .....	20
Figure 24 Edit Commands - Copy, Paste, and Select All Text .....	21
Figure 25 Start Logging Command and Select File Window.....	22
Figure 26 Stop Logging Command .....	23
Figure 27 Script Shell Command .....	24
Figure 28 SecureChat Command and User Chat Window.....	25
Figure 29 Help Topics Command and Help File Window.....	26
Figure 30 Sample of About RaritanConsole Command and About Window .....	27
Figure 31 Direct Port Access Initial Display .....	28
Figure 32 Security Warning Display.....	28
Figure 33 Direct Port Access Display.....	29
Figure 34 Invalid Port Number Error Display.....	29
Figure 35 Save the Changed Configuration Window .....	30
Figure 36 Exit Confirmation Display.....	30
Figure 37 Unit Disconnection Display .....	31
Figure 38 Display Overview .....	32
Figure 39 Sample Report Display .....	35
Figure 40 Sample of Network Configuration Display.....	36
Figure 41 Modem Connection to a Dominion SX unit .....	38
Figure 42 Port Configuration Display .....	38
Figure 43 Port Editing Display.....	39
Figure 44 Users Tab Display.....	40
Figure 45 New User Creation.....	41
Figure 46 Sample User Modification Screen.....	42
Figure 47 Inserting a rule into the browser-based IP ACL configuration screen. ....	44
Figure 48 GUI User Interface .....	44
Figure 49 Certificate Tab Display.....	48
Figure 50 Certificate Configuration Display.....	49
Figure 51 Generate Certificate Display .....	50



Figure 52 View Self-Signed Certificate Display .....	50
Figure 53 Activating Default Certificate .....	51
Figure 54 Generate CSR Request Display .....	51
Figure 55 CSR Configurable Parameters .....	52
Figure 56 View CSR Display .....	52
Figure 57 User Certificate .....	53
Figure 58 Schematic of External Certificate Utilization .....	53
Figure 59 RADIUS Users Login Mechanism .....	54
Figure 60 Unsuccessful Login Message Window .....	55
Figure 61 RADIUS Configuration Display .....	56
Figure 62 Current Users List .....	57
Figure 63 Time Configuration Display .....	58
Figure 64 Notification Display .....	59
Figure 65 New Notification Display .....	60
Figure 66 Edit Notification Destination .....	61
Figure 67 Upgrade Display .....	63
Figure 68 Confirmation for Reset .....	65
Figure 69 Confirmation on Users to be Disconnected .....	65
Figure 70 Factory Reset Connector Location .....	67
Figure 71 Sample SSH Session Screen .....	79
Figure 72 Administrative Information .....	99
Figure 73 Hierarchies of Certificate Authorities .....	100
Figure 74 Schematic Diagram of Certificate Authentication Scheme .....	101
Figure 75 Install Session Based Certificate .....	102
Figure 76 View of CA_ROOT.cer .....	103
Figure 77 Certificate Manager Import Wizard .....	103
Figure 78 Import Wizard, Select a Certificate Page .....	104
Figure 79 Certificate Manager Import Wizard, Completion Page .....	104
Figure 80 Internet Options Display .....	105
Figure 81 Certificate Manager Display .....	105
Figure 82 Netscape New Site Certificate Window .....	106
Figure 83 Netscape New Site Certificate Acceptance Window .....	106
Figure 84 Viewing the Certificate .....	107
Figure 85 Netscape New Type Window .....	107
Figure 86 Netscape New Certificate Authority Window .....	108
Figure 87 Netscape Web Site Certificates Window .....	109
Figure 88 Certificate Already Exists Alert Window for Netscape .....	110
Figure 89 Certificate Signers' Certificates Window in Netscape .....	110
Figure 90 New Certificate Authority Window in Netscape .....	111
Figure 91 Cisco ACS Main Display .....	121
Figure 92 Unit Configuration Display .....	121
Figure 93 Interface Configuration Display .....	122
Figure 94 RADIUS Properties Display .....	122
Figure 95 New User Display .....	123
Figure 96 User Properties Display .....	123
Figure 97 Launching RSA Administration Application .....	125
Figure 98 Add Agent Host Selection .....	125
Figure 99 Add Agent Host Display .....	126
Figure 100 RADIUS Secret Key Display .....	126
Figure 101 Add Profile Selection .....	127
Figure 102 Add Profile Display .....	127
Figure 103 Add Attribute Display .....	128
Figure 104 Add User Display .....	128
Figure 105 Profile Selection Display .....	129

---

Figure 106 Unit Selection Display per User .....	129
Figure 107 LDAP Configuration Screen .....	130
Figure 108 Dial-Up Networking Display .....	131
Figure 109 New Phone Entry Display .....	132
Figure 110 Dial-Up Security Display .....	132
Figure 111 Configuring Windows 98 Dialup Networking .....	133
Figure 112 Make New Connection – Connection Name .....	133
Figure 113 Make New Connection – Complete.....	134
Figure 114 Connect to Window.....	134
Figure 115 Windows 2000 Network and Dialup Connections .....	135
Figure 116 Welcome to the Network Connection Wizard.....	135
Figure 117 Network Connection Type.....	136
Figure 118 Device Selection .....	136
Figure 119 Phone Number to Dial.....	137
Figure 120 Connection Availability.....	137
Figure 121 Network Connection Wizard Completion .....	138
Figure 124 TCL Architecture.....	139
Figure 125 Activating TCL Scripting Window.....	143

# Chapter 1: Introduction

## Dominion SX Overview

The Dominion SX Series of Serial over IP Console Servers offers convenient and secure, remote access and control via LAN/WAN, Internet or Dial-up modem of all networking devices. Dominion SX connects to any networking device (servers, firewalls, load balancer, etc.) via the serial port and provides the ability to remotely and securely manage the device using any Web browser. Dominion SX provides a non-intrusive solution for managing network elements and does not require any software agents to be installed on the target device.

## Product Photos

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



Figure 1 Dominion SX32 Unit

## Product Features

### Comprehensive Console Management

- Remote Management: Access, monitor, administer, and troubleshoot up to 48 target devices (depending on model) from any SSH-client Web browser while consuming only one IP address.
- Scripting: Create, store and execute scripts either on demand or on a continuous basis.
- Notification: Create notification messages via email alerts.
- Collaborative Management and Training: Access ports simultaneously; up to 10 users per port at any time.
- SecureChat™: “Instant message” other SSL users securely and collaborate on device management, troubleshooting, and training activities.
- Get History: Get up to 64 KB of recent console history to assist with debugging.
- VT100 Console Window: View VT100/ANSI terminal emulation including copy/paste and record/playback functionality.
- Local port access
- Telnet
- SNMP traps
- SYSLOG
- Logging to NFS Server
- Three Levels of User Access:
  - **Administrator:** Has read and write access to the console window; can modify the configuration of unit.
  - **Operator:** Has read and write access to the console window; cannot modify the configuration of unit (except own password).

- **Observer:** Has read-only access to the console window; cannot modify the configuration of unit (except own password).

### **Strong Security and User-Authentication**

- SSHV2 Support.
- Encryption Security: 128-bit Secure Socket Layer (SSL) handshake protocol and RC4 encryption.
- User Authentication Security: Login Name and Password scheme (MD5 Hash) with global Access Control List (ACL).
- Supports RADIUS (can be configured as a RADIUS client), TACACS+, LDAP, LDAP(S), Microsoft Active Directory, and NTP.
- Supports User-defined and installable security Certificates.

### **Reliable Connectivity**

- Modem Connectivity: For emergency remote access if the network has failed.
- Target Device Connectivity: Simplified RJ45-based CAT5 cable scheme; serial port adapters are available from Raritan.
- Local Access for “crash-cart” applications.

### **Simplified User Experience**

- SSH.
- Browser-based Interface: Graphical User Interface provides intuitive access to target devices (click on the appropriate button to select the desired target device).
- Upgrades: Built-in firmware upgrade capability via FTP/Internet.
- Ability to load specific applications per console port for ease of use; specific applications are available from Raritan.

## **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 User Manual CD-ROM containing the Dominion SX Installation and Operations Manual
- (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 is included on some units (other units have a reset switch, and do not require an adapter)

## Chapter 2: Installation

Beginning with the Dominion SX release 2.5, there are two ways of completing the initial network installation of the Dominion SX – via Ethernet (with an installation computer), and via a serial cable with a VT100/equivalent, e.g., a PC with HyperTerminal. Please refer to the Quick Setup Guide for Command Line/serial cable installation instructions. This section describes the steps necessary to configure Dominion SX for use on a local area network (LAN). All new Dominion SX units come with default network settings, illustrated in the table below. Once units are connected to the network, these default settings will allow the user to configure Dominion SX for normal use.

There are three separate tasks you must complete to use Dominion SX on the network: Hardware Installation, Initial Software Configuration, and Dominion SX Deployment, usually completed in this order, and each described in this chapter.

*Hardware Installation* describes how to connect the Dominion SX unit to a computer to perform the initial configuration of the unit. This step requires an additional computer that will be used to log into the Dominion SX unit and configure it for the first time in the next section.

*Initial Software Configuration* describes how to connect to Dominion SX in its default state and to configure it for use in a specific network environment.

*Dominion SX Deployment* describes how to install a Dominion SX unit on the network once the Initial Software Configuration is complete.

### Pre-Configuration Notes

The following list includes information that you will be required to supply to complete the configuration of the Dominion SX. Obtain all required configuration information prior to performing the configuration steps outlined below. If you are uncertain of any information, contact your system administrator for assistance.

#### Network Information:

- **Raritan Unit Name:** The name of this unit, a generic term for the Dominion SX unit. This can be 64 characters maximum, no minimum, no spaces.
- **IP address:** The IP address of the unit, as directed by your network administrator.
- **IP subnet mask:** The IP subnet mask for the unit, as directed by your network administrator.
- **IP gateway:** The IP gateway for the unit, as directed by your network administrator.
- **Port Address:** As directed by your network administrator (range is 1024-65536, this port number must not be used by any other application, check with your network administrator if unsure, or check IANA's port/application listing from the Internet) default value is 51000.
- **Domain name:** Name, such as mycompany.co.jp, is required for SMTP alerts.

The following information is not required for a standalone Dominion SX installation, but is required for installation with Raritan's CommandCenter-Secure Gateway. Accept the default port for a standalone installation. Port for CC discovery: 5000. Please see the CommandCenter-Secure Gateway User Guide for additional information.

## Hardware Installation

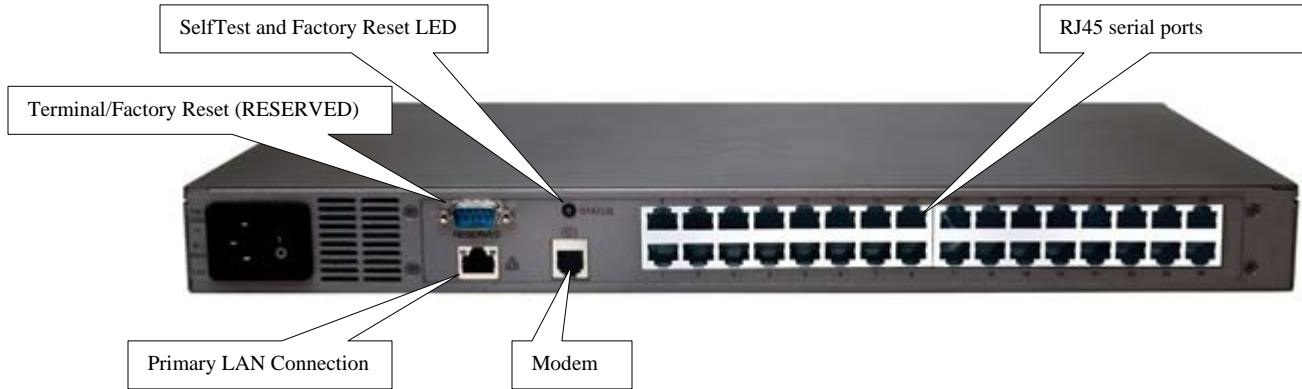


Figure 2 Rear Panel of 32-port single power supply model

### Physical Installation of Dominion SX for Initial Configuration:

1. Obtain 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 on the back of the chassis. Connect the other end to the network card in the installation computer.
4. Connect the female end of the external power cord to the back of the chassis.
5. Connect the male end of the external power cord to the power supply outlet. Power ON the Dominion SX unit.

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

6. Each unit comes with a certain set of configuration defaults henceforth referred to as Factory Reset Mode. The default network settings for this mode are:

Internet Address (IP)	192.168.0.192
Gateway Address	192.168.0.192
Subnet Mask	255.255.255.0
Port Address	51000
Username	admin
Password	raritan

Figure 3 Default Settings for Factory Reset Mode

7. Ensure that your installation computer can communicate with IP address 192.168.0.192. First, verify that the installation computer has the route for 192.168.0.192:
  - a. On the command line interface of the installation computer, enter the command **route print**.
  - b. If 192.168.0.192 is on the gateway list, proceed to the next step. Otherwise, add 192.168.0.192 to the gateway list: type the following commands into either a DOS or UNIX command line interface on the installation computer where your browser is running:
    - i. On a Windows NT/95/98/2000 system: **route add 192.168.0.192 <client\_host IP address>**  
 Example:  
**route add 192.168.0.192 15.128.122.12**
    - ii. On a UNIX (incl. 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***

8. On the command line interface, type: **ping 192.168.0.192**.
  - a. If this command successfully produces a reply from the Dominion SX unit, please proceed to step 9.
  - b. If this does not produce a reply, verify that the default IP address is entered correctly and there is a route to that IP address.
9. Use the installation computer to connect to the unit, typing the factory default IP address **192.168.0.192** in the installation computer Web browser's address line. Once you have reached the unit's initial configuration screen, proceed to the Initial Software Configuration section that follows.

## Initial Software Configuration

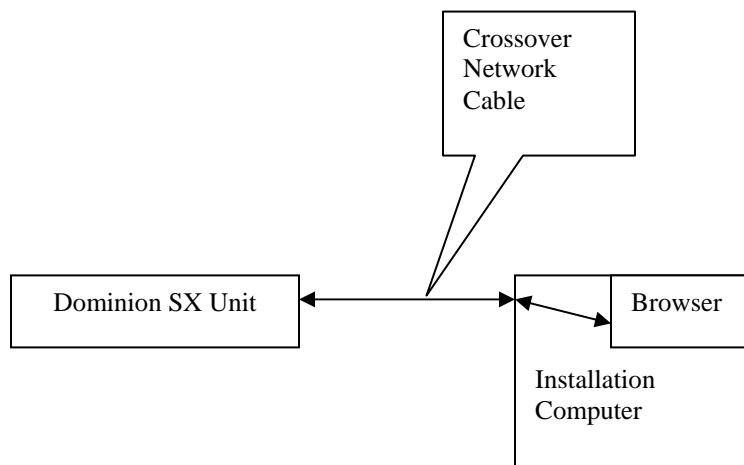


Figure 4 Hardware Setup for Initial Software Configuration

### User Information:

This information should be entered for each user, up to 50 user accounts, with at least one administrator for each Dominion SX unit:

- **User Name:** 32 characters maximum, one character minimum, spaces permitted.
- **Login Name:** 255 characters maximum, one character minimum, no spaces.
- **User Type:**
  - **Administrator:** Can modify configuration of the unit, has read/write access to the console window.
  - **Operator:** Cannot modify configuration of the unit (except own password), has read/write access to the console window.
  - **Observer:** Cannot modify configuration of the unit (except own password), has read-only access to the console window.
- **Information:** Any additional information (text) you want associated with this user. Can be 64 characters maximum, no minimum, spaces permitted.
- **Password:** Alphanumeric text, 6–16 characters in length, no spaces. The first six characters of the password must contain at least two alpha and one numeric character; the first four characters cannot be the same as the user name. Brackets (<>) and quotations (“”) are not allowed.

## **Initial 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.
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.



## Dominion SX

Initial configuration can also be performed through CLI; please see **Chapter 4: Console Features, Factory Reset** for additional information.

1. Initially, you must change the administrator password. Access the unit through your Web browser on an installation computer that is on the same subnet by typing the URL: **https://192.168.0.192**.

The screenshot shows the 'Change Password' interface for Dominion SX 4. The page has a purple header with the Raritan logo and the title 'Dominion SX 4'. On the left, there is a vertical sidebar with a purple background containing the text 'Exit' and 'Current users: 1> Administrator'. The main content area is white and contains the following fields and buttons:

- Login Name:
- New Password:
- Re-enter Password:
- Change:

Figure 5 Change Password Screen

2. Type the new password in the **New Password** field. The default password is **raritan**.
3. Retype to confirm the password in the **Re-enter Password** field and click [**Change**] to register the new password. The Dominion SX user window appears. Please note that if this password is lost, the unit must be reset to factory default and all user-entered settings will be lost.

The screenshot shows the 'User Screen' for Dominion SX 4. The page has a purple header with the Raritan logo and the title 'Dominion SX 4'. On the left, there is a vertical sidebar with a purple background containing the following options: 'Port Access', 'Configuration', 'Upgrade', 'Reset', 'Exit', and 'Current users: 1> Administrator'. The main content area is white and contains four buttons labeled 'Port1', 'Port2', 'Port3', and 'Port4' arranged horizontally.

Figure 6 Dominion SX User Screen

4. Click on the [**Configuration**] button in the left navigation panel to view the Configuration screens, and then click on the **Time** tab to configure the current date and time. 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.

Figure 7 Time and Date Configuration Screen

5. Set the **Current Date** and **Current Time** using the drop-down arrows to select the **Month, Day, Year, Hour, Min.** and **Sec.** values.
6. To use NTP (Network Time Protocol), click on the **Enable Network Time Protocol** check-box and type a valid IP addresses for the **Primary Time Server** and, if required, **Secondary Time Server**.
7. Click on the [**Update**] button.
8. Click on the [**Network**] tab to view the Network Configuration screen.

Figure 8 Network Configuration Screen

9. A network administrator typically assigns the values for these parameters. Please enter the following data – note that all fields are required:
  - **Raritan Unit Name:** Descriptive name for this unit
  - **IP Address:** Network address for this unit
  - **Subnet Mask:** Subnet mask for the network where this unit will reside
  - **IP Gateway:** Default gateway for this unit
  - **Port Address:** Default application communication port – if accessing the unit through a firewall, the TCP port specified during installation must be open.
  - **Terminal Type:** Terminal emulation type; fixed VT100/ANSI
10. Click on the [**Update**] button.

11. Click on the **[Save]** button. A confirmation window will appear; click **[OK]** to accept all data, or click **[Cancel]** to return to the Configuration screens.

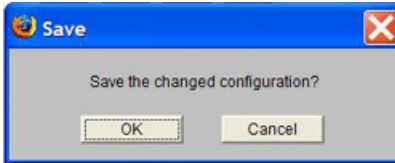


Figure 9 Confirm Save Window

12. If you click **[OK]**, Dominion SX must reboot. A confirmation window will appear; click **[OK]** to reboot the SX, or click **[Cancel]** to return to the Configuration screens.

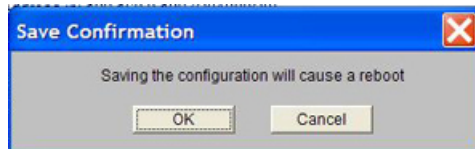


Figure 10 Confirm Reboot Screen

13. Dominion SX will automatically disconnect to update the configuration. A confirmation window will appear; click **[OK]**.

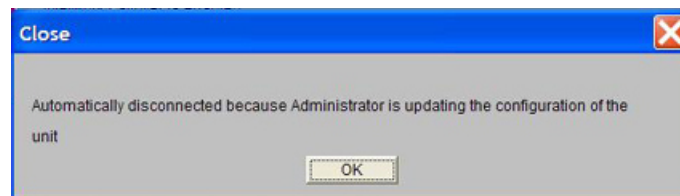


Figure 11 Confirm Disconnection Screen



Figure 12 Logged off Dominion SX Screen

14. Dominion SX will restart; once you see the Login screen, log into the unit and begin using Dominion SX as described starting in **Chapter 3: Operation**.

## Deployment

After the Initial Software Configuration phase, a Dominion SX unit is configured for operation on the LAN.

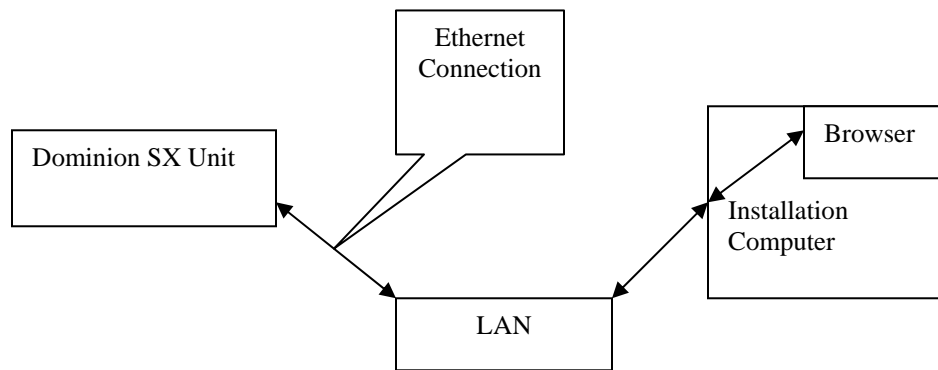


Figure 10 Deployment

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 on the back of the chassis. Connect and/or verify that the other end of the cable is connected to the proper network. If the unit has a failover module, connect the secondary network LAN connection as well.
4. Connect the female end of the external power cord to the back of the chassis.
5. **Serial Connection to Target Devices:** This manual contains detailed information on connecting the Dominion SX unit to the console port of target devices.
6. **Modem Connection (optional):** Connect a phone line to the modem port. Remember to write down the phone number for this line, as it will be necessary later when the user configures a client for dialup networking.
7. Connect the male end of the external power cord to the power supply outlet and power ON the Dominion SX unit.

---

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

---

8. Perform a quick connectivity check by connecting to the device using either IE or Netscape. In the address line, enter **https://<IPAddress>** 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.
9. Enter the Configuration window and enter the various configuration parameters for each console port. Enter specific operational parameters for the unit (please see **Chapter 4: Console Features** for additional information).

## Chapter 3: Operation

### Overview

Once the Dominion SX unit has been deployed in its final destination, you can access the console of the target device. This chapter explains the normal operational procedures.

### Accessing the Remote Device

The remote device can be accessed in one of two ways, either browser-based or by direct port access and used either as a user-based remote device access method or used for application programs to access the target device programmatically.

### Browser-Based Access

---

1. In the address line of a browser on your client desktop, type the IP address of the unit. A security alert window appears.

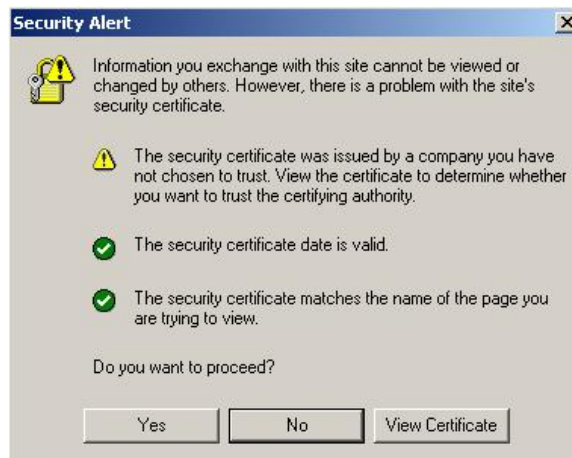
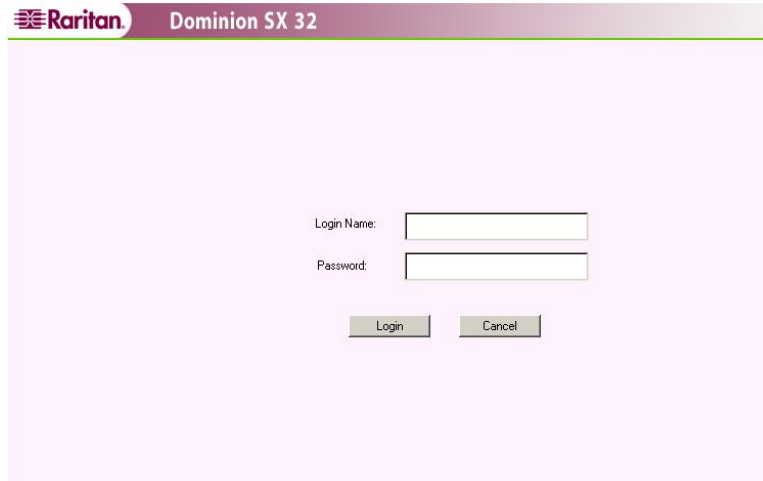


Figure 11 Security Alert Display

The unit is always SSL enabled. When you try to connect to the Dominion SX unit, a Security Alert appears because the CA root certificate is not installed in the browser. Please see **Appendix C: Certificates** for additional information.

2. Click on the [Yes] button to continue.

- When the login screen appears, enter your Login Name and Password, and click on the **[Login]** button. Please note that multiple logins using the same Login Name are permitted.



The screenshot shows the login interface for Dominion SX 32. At the top left is the Raritan logo, and to its right is the text 'Dominion SX 32'. The background is a light purple gradient. In the center, there are two text input fields. The first is labeled 'Login Name:' and the second is labeled 'Password:'. Below these fields are two buttons: 'Login' and 'Cancel'.

Figure 12 Login Display

- When the main display page appears, click on the desired **[Port#]** button to launch that port's console display.

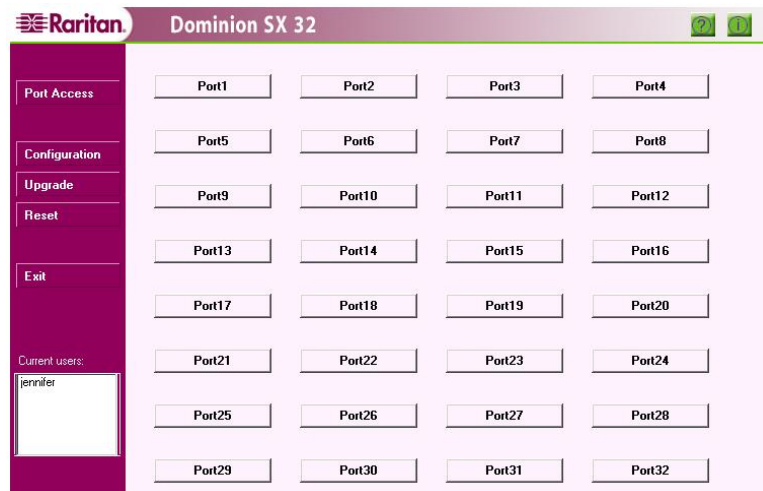


Figure 13 Main Display with Available Ports (32-port unit shown)

## Security Dialog for Console Display

RaritanConsole, an applet included with your Dominion SX unit, is designed to enable access to your computer's resources, including the default code set preferences.

## Internet Explorer

Before the RaritanConsole window appears, a Security Warning screen requests permission to access computer resources. The dialog indicates that the authenticity of the signer, Raritan, has been verified by VeriSign, Inc., and it specifies the permissions requested from the user.



Figure 14 Security Dialog in Internet Explorer

- Click on the [Yes] button to accept all requested permissions. These permissions will not be requested again in the same session. Check the [Always trust content from...] checkbox to avoid being asked for permissions at the start of every new session.
- Click on the [No] button on the dialog box cancels the RaritanConsole window.

---

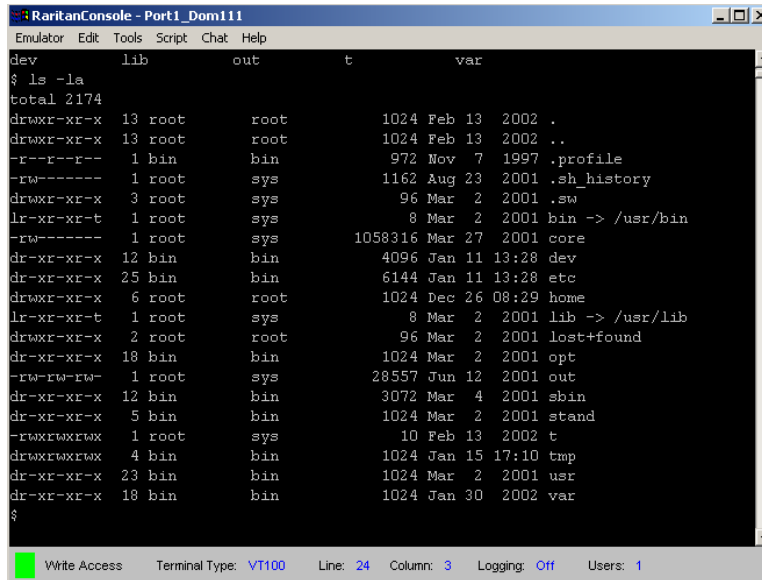
**Important! Once [No] is selected, the console will not pop up until the browser is closed and a new session is started.**

---

## Netscape Navigator

RaritanConsole loads without displaying a Security Warning window. When actions that require user permissions are performed, a security dialog will appear. Each operation requires a unique permission. Once permissions are granted, they will not be requested again in the same session. Users can also check the **[Remember this decision]** checkbox to avoid being asked for permissions every new session.

Once the Security screens are completed, the console window appears, and the user can begin working with the remote target system.



```

RaritanConsole - Port1_Dom111
Emulator Edit Tools Script Chat Help
dev      lib      out      t        var
$ ls -la
total 2174
drwxr-xr-x 13 root    root      1024 Feb 13  2002 .
drwxr-xr-x 13 root    root      1024 Feb 13  2002 ..
-r--r--r-- 1 bin     bin       972 Nov  7  1997 .profile
-rw----- 1 root    sys      1162 Aug 23  2001 .sh_history
drwxr-xr-x  3 root    sys       96 Mar  2  2001 .sw
lr-xr-xr-t  1 root    sys        8 Mar  2  2001 bin -> /usr/bin
-rw----- 1 root    sys     1058316 Mar 27  2001 core
dr-xr-xr-x 12 bin     bin      4096 Jan 11 13:28 dev
dr-xr-xr-x 25 bin     bin      6144 Jan 11 13:28 etc
drwxr-xr-x  6 root    root     1024 Dec 26 08:29 home
lr-xr-xr-t  1 root    sys        8 Mar  2  2001 lib -> /usr/lib
drwxr-xr-x  2 root    root       96 Mar  2  2001 lost+found
dr-xr-xr-x 18 bin     bin     1024 Mar  2  2001 opt
-rw-rw-rw-  1 root    sys     28557 Jun 12  2001 out
dr-xr-xr-x 12 bin     bin      3072 Mar  4  2001/sbin
dr-xr-xr-x  5 bin     bin     1024 Mar  2  2001 stand
-rwxrwxrwx  1 root    sys       10 Feb 13  2002 t
drwxrwxrwx  4 bin     bin     1024 Jan 15 17:10 tmp
dr-xr-xr-x 23 bin     bin     1024 Mar  2  2001 usr
dr-xr-xr-x 18 bin     bin     1024 Jan 30  2002 var
$
Write Access Terminal Type: VT100 Line: 24 Column: 3 Logging: Off Users: 1

```

Figure 17 Console Window

## Sending a Break / Null

### From a Browser:

Some target systems, such as Sun Servers, require a null character (Break) to be sent from the console. To send a break / null, verify that you have write access. If not, use the drop-down menu to obtain write access, as described in the *Write Access* section of **Chapter 4: Console Features**. Then, select **Send Break** from the **Emulator** drop-down list to send a break to the Server running Solaris.



## Chapter 4: Console Features

There are six drop-down menus available in the menu bar of the console window:

- Emulator
- Edit
- Chat
- Tools
- Script
- Help

### Emulator Settings

---

The Settings window displays the Terminal Type and Cursor Type for the console window.

- The unit supports Terminal Type VT100/ANSI, which cannot be changed.
- The Cursor Type can be either Line or Block, depending on your preference. The default cursor is Line type, but can be changed by clicking on the appropriate radio button.

#### To View Settings:

1. Click on **Emulator** in the main menu.
2. Select *Settings* from the drop-down menu.

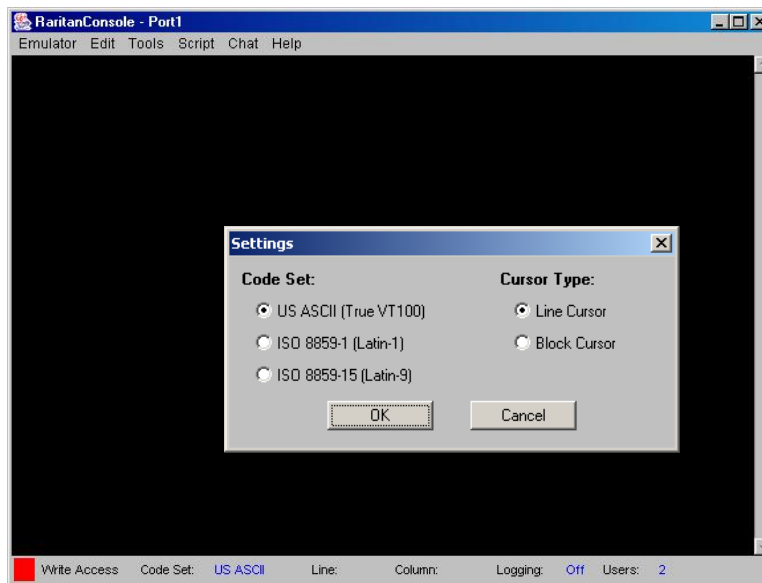


Figure 18 Settings Command and Settings Window

3. Adjust settings as needed.
4. Click on the **[OK]** button to close the Settings window.

## History

The History feature allows you to view the recent history of console sessions by displaying the console messages to and from the target device. This function displays up to 64 kilobytes of recent console message history, allowing 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. History information can be useful when debugging, troubleshooting, or administering a target device.

---

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

---

### To View Session History:

1. Click on **Emulator** in the main menu.
2. Select *History* from the drop-down menu.

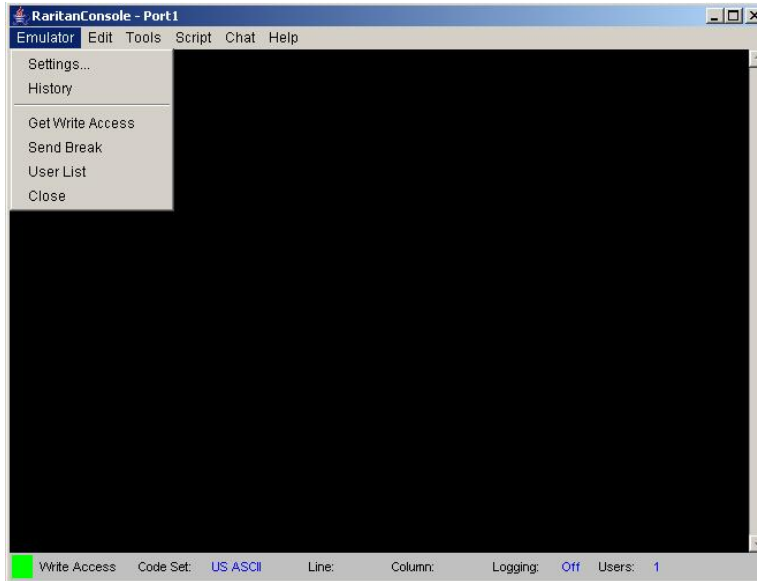


Figure 19 History Command

## Write Access

The user with Write Access can send commands to the target device. Write Access can be transferred among users working in RaritanConsole via the Get Write Access command from the Emulator drop-down menu.

### To Obtain Write Access:

1. Click on **Emulator** in the main menu.
2. Select *Get Write Access* from the drop-down menu.

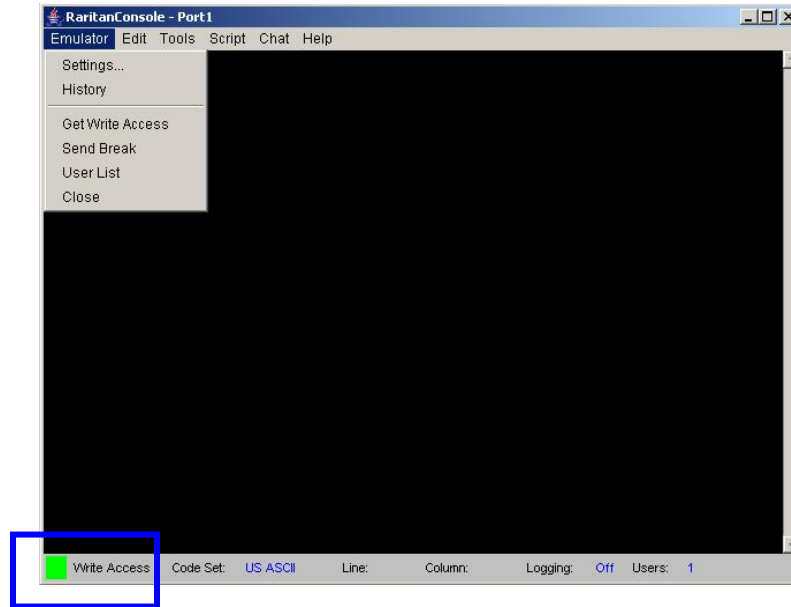


Figure 20 Get Write Access Command

3. You now have Write Access to the target device, as indicated by the green block located before Write Access in the status bar.
4. When another user assumes Write Access from you, loss of Write Access is indicated by a red block before **Write Access** in the status bar. 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.

## Sending a Break/Null

To get access to a certain commands, Sun Solaris servers require a null character (Break) to be sent from the console to get to an **OK** prompt. This is the equivalent of issuing a STOP-A from the Sun keyboard. Only users with Operator and Administrator privileges can send a “break”; users who are Observers cannot send a “break.”

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

1. Verify that you have the Write Access. If not, please follow the instructions in the previous section to obtain write access.
2. Click on **Emulator** in the main menu.
3. Select *Send Break* from the drop-down menu to send a null character to the target Sun Solaris server.

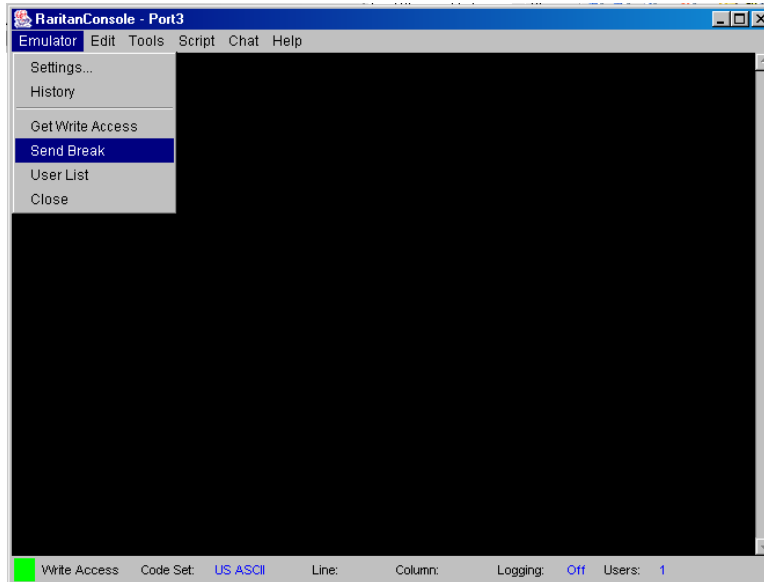


Figure 21 Send Break

## User List

The User List command allows you to view a list of other users who are accessing the same port. An asterisk (\*) appears before the user who has Write Access to the console.

### To View the User List:

1. Click on **Emulator** in the main menu.
2. Select *User List* from the drop-down menu.

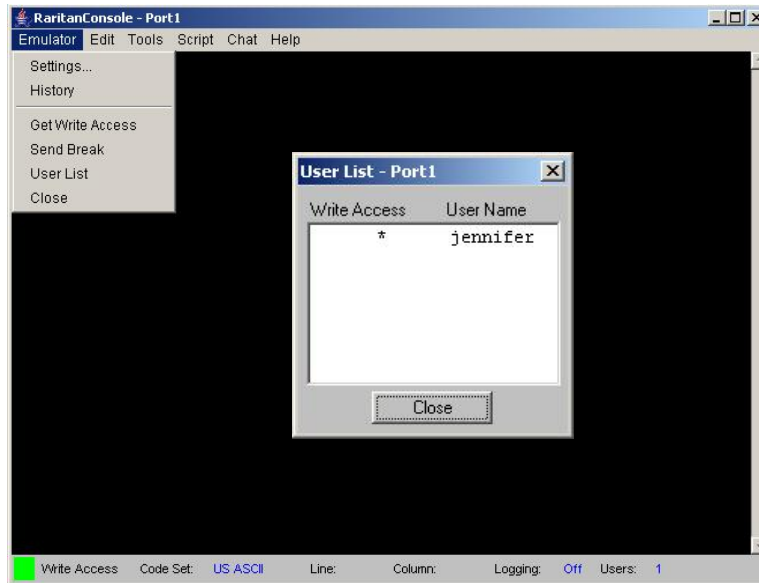


Figure 22 User List Command and User List Window

3. Click on the [Close] button to close the User List window.

## Close

---

### To Close RaritanConsole:

1. Click on **Emulator** in the main menu.
2. Select *Close* from the drop-down menu.

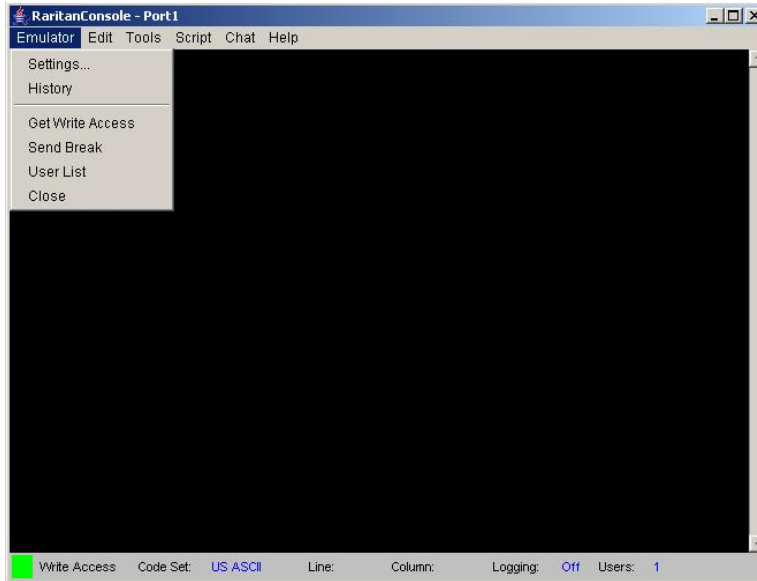


Figure 23 Close Command

## Edit

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

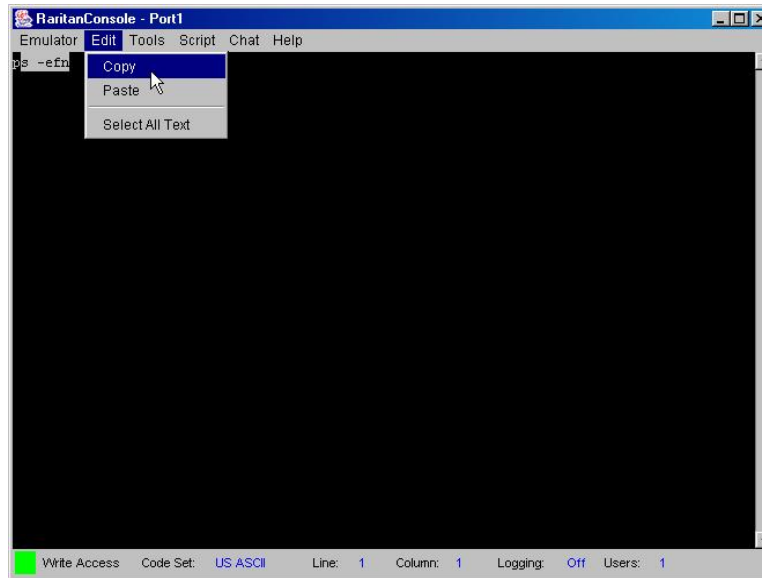


Figure 24 Edit Commands - Copy, Paste, and Select All Text

### To Copy and Paste All Text:

1. Click on **Edit** in the main menu.
2. Select *Select All Text* from the drop-down menu.
3. Click on **Edit** in the main menu.
4. Select *Copy* from the drop-down menu.
5. Position the cursor at the location you wish to paste the text and click once to make that location active.
6. Click on **Edit** in the main menu.
7. Select *Paste* from the drop-down menu.

---

**Note:** There 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 wish to paste the text and click in that location to make it active
- Press <CTRL> and tap the <V> key to paste

**Note:** The text copy limit in RaritanConsole is 999 lines. To increase this amount to 5000 lines, download the RaritanConsole upgrade from Raritan's website:

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

---

## Tools

Raw console data from the target device can be logged to a file in your computer. The Logging indicator on the status bar indicates whether Logging is on or off.

### Start Logging

1. Click on **Tools** in the main menu.
2. Select *Start Logging* from the drop-down menu.
3. Choose an existing file or provide a new file name in the File Dialog box. When an existing file is selected for logging, data gets appended to the contents. Providing a new file name creates a brand new file. Click on the [OK] button after you have selected or created a file.

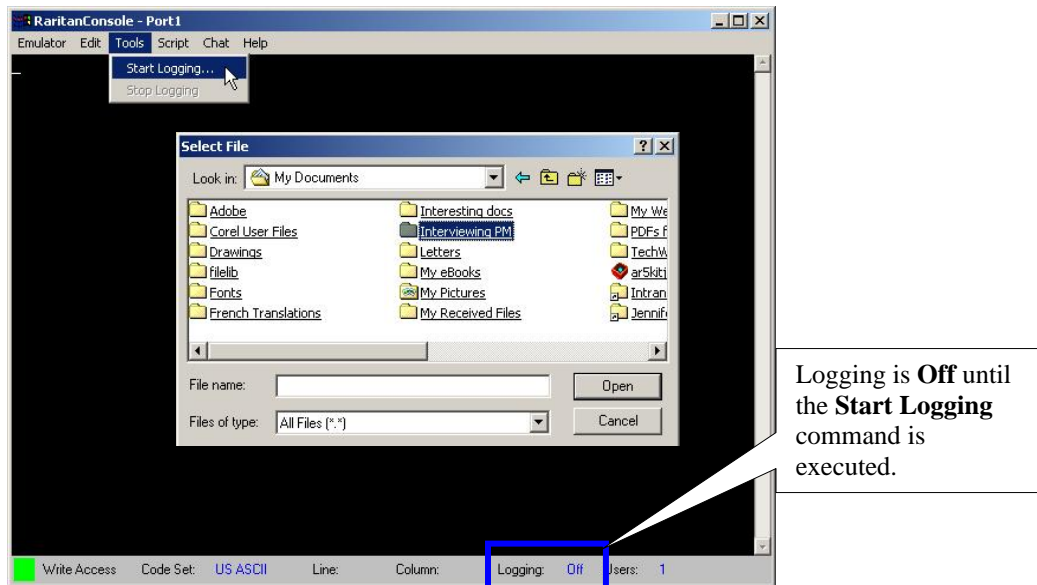


Figure 25 Start Logging Command and Select File Window



## Stop Logging

1. Click on **Tools** in the main menu.
2. Select *Stop Logging* from the drop-down menu.

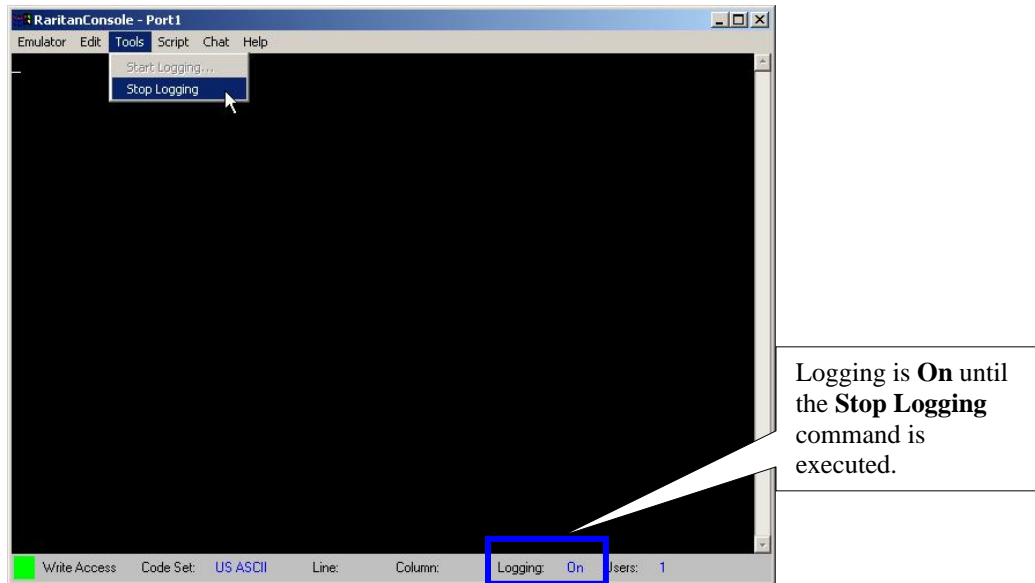


Figure 26 Stop Logging Command

## Script

RaritanConsole supports *TCL* version 7.0, an industry standard scripting engine. Using *TCL* scripting capabilities, system administrators can create their own conditions for event detection, and generate customer-specific notifications and alerts. The unit features a *TCL* engine and a flash file system for the development and storage of *TCL* scripts. Please see **Appendix H: *TCL* Programming Guide** for additional information.

RaritanConsole also comes with User Definable Events that can be generated by *TCL* scripts. Raritan has introduced an extension library to provide an API to the RaritanConsole's functions. Additionally, the unit comes with an extensive list of notification events that can be used to audit, track and trace the conditions of and modifications to the unit itself.

### To Invoke the Script Shell:

1. Click on *Script* in the main menu.
2. Select *Script Shell* from the drop-down menu.

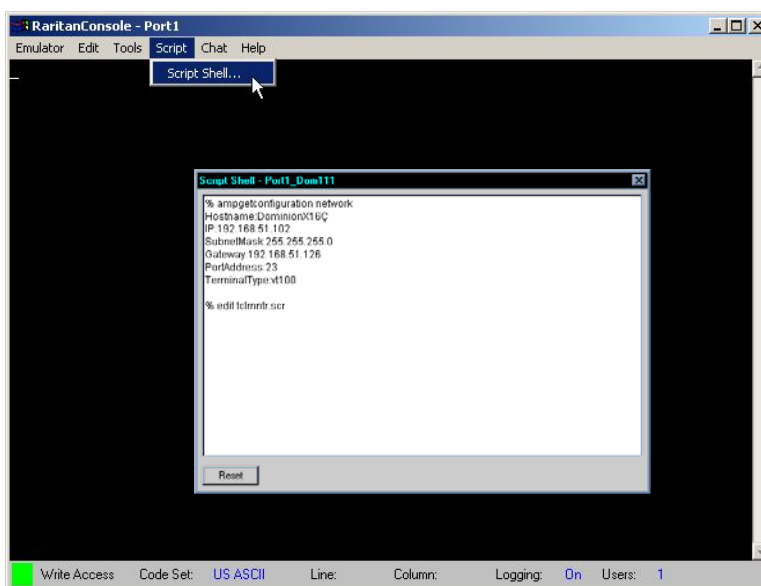


Figure 27 Script Shell Command

3. Enter your command or script and press the **<Enter>** key (please see to **Appendix H: *TCL* Programming Guide** for more information).
4. To reset the script, click **Reset** on the Script Shell window.

## SecureChat

When using SSL (browser access), a real-time interactive chat feature called SecureChat provides you and other users who are accessing the console port of the target device to conduct an online dialog for training or collaborative diagnostic activities. The maximum length of a chat message is 80 characters.

### To use SecureChat:

1. Click on **Chat** in the main menu.
2. Select *User Chat* from the drop-down menu.

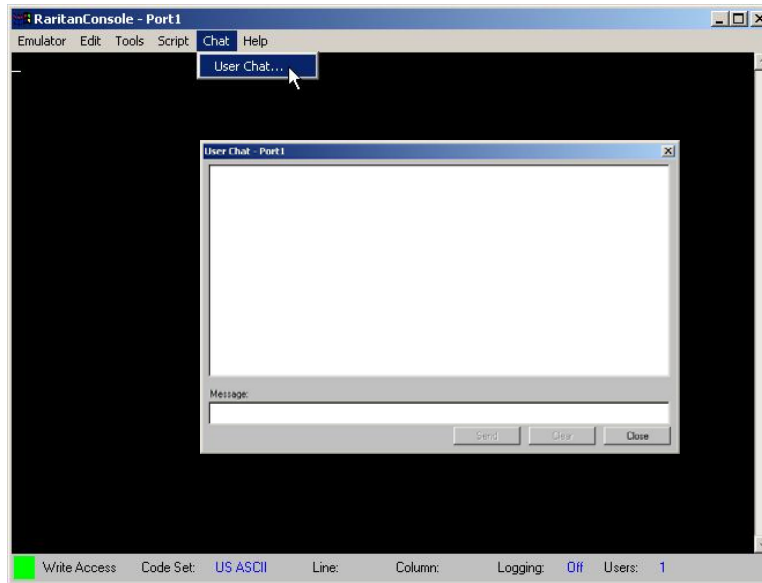


Figure 28 SecureChat Command and User Chat Window

3. Type a message in the **Message** text field.
4. Click on the **[Send]** button or press **<Enter>** to send the message, click on the **[Clear]** button to delete the typed text, or click on the **[Close]** button to exit and close the Message window.

---

*Note:* When a chat is initiated, a chat window will appear on the monitors of all SSL users logged on to the port.

---

## Help

Help Topics include on-line assistance for operating RaritanConsole and the console window, and release information about RaritanConsole.

## Help Topics

---

### To Access Help Topics:

1. Click on **Help** in the main menu.
2. Select *Help Topics* from the drop-down menu.

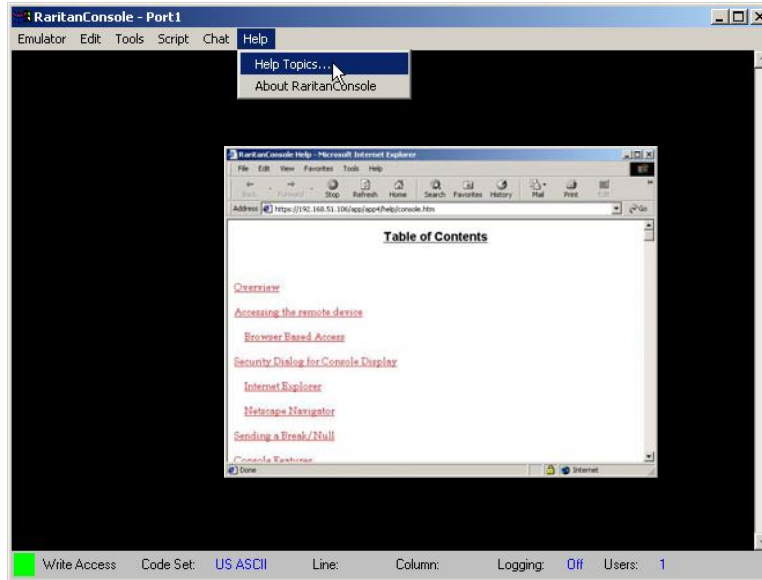


Figure 29 Help Topics Command and Help File Window

3. Use the navigation bar on the right side of the window to scroll to the topic you need, or click on the links. Close this window when you are finished.

## About RaritanConsole

The ‘About’ window displays version information (name and revision number) for the console terminal emulation software, and copyright information. When contacting Raritan for technical support when performing a software upgrade, etc., you may be asked for this information.

### To Access ‘About’ Information:

1. Click on Help in the main menu.
2. Select *About RaritanConsole* from the drop-down menu.

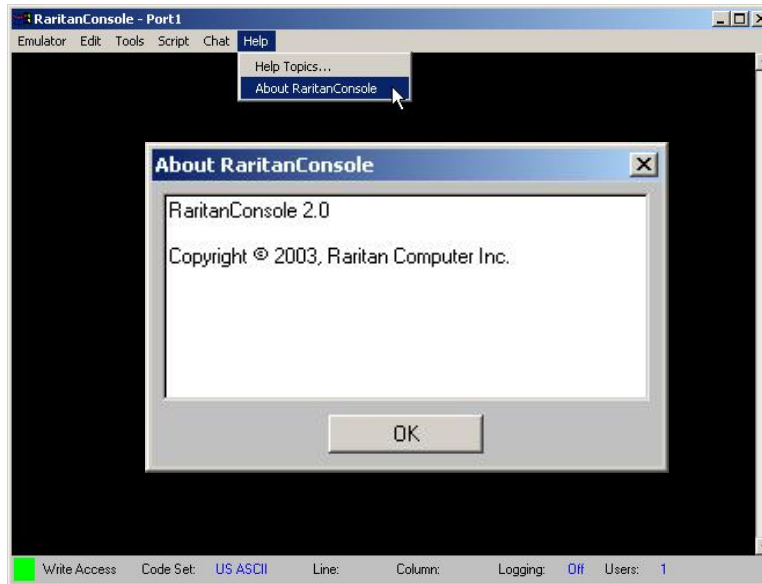


Figure 30 Sample of About RaritanConsole Command and About Window

3. Click **OK** to close the About RaritanConsole window.

## Direct Port Access

This approach provides a quick and direct method of connecting to the console port in order to access unit programmability or the console of the target device directly. There are two ways to access the target device console directly by giving the appropriate URL.

### URL with Password and Username and Port

Type the following URL into the browser's location bar:

**[https://192.168.32.20/dpa.htm?username="username"?password="password"?port="portnumber"](https://192.168.32.20/dpa.htm?username=)**

- **IP Address:** This is the IP Address of the unit – either the actual IP address of the unit or IP Address assigned for a modem
- **“username”:** Login name
- **“password”:** Password
- **“portnumber”:** Port number for which a console is required

*Example:*

For Internet Explorer and Mozilla 1.6 (with supported Java version) the following command line – or entry into the URL field - will connect the user to Port 1; in this example, the username is tanaka, with the password tokyo678:

**[https://192.168.32.20/dpa.htm?username="tanaka"?password="tokyo678"?port="1"](https://192.168.32.20/dpa.htm?username=)**

1. The Direct Port Access display will appear.
2. When the security warning appears (only once for the session); click on the [Yes] button.
3. The console display will appear.

*Note: The user's password will appear in the URL location bar.*

IP Address	192.168.51.228
Port#	1
Port Name	SUN_Solaris_2_6
Application	RaritanConsole

Figure 31 Direct Port Access Initial Display

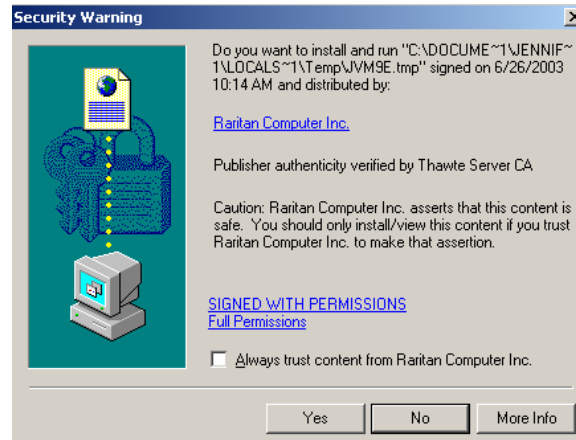


Figure 32 Security Warning Display

**Important! This kind of access will generally be used in applications where the user name and password are retrieved from a database. It is not advisable to place this URL in a HTML page where the user name and password are visible.**

## URL with Port Number

1. Type the following URL into the browser's location bar: **https://<IPAddress>/dpa.htm**
  - **IPAddress**: This is the IP Address of the unit. This can be either the actual IP address of the unit or IPAddress assigned for a modem.
  - **“portnumber”**: Port number for which a console is required.

*Note: https must be used for direct port access. http cannot be used.*

Example:

**https://192.168.50.81/dpa.htm?port="1"**

2. The Direct Port Access display will appear.
3. Enter Login Name and Password and click on the [**Login**] button.
4. When the security warning appears (only once for the session); click on the [**Yes**] button.
5. The console display will appear.

Figure 33 Direct Port Access Display

To exit the application from direct port access, close the Raritan Console window and close the browser window (by selecting **File** → **Close**, or by clicking on the “X” in the top right-hand column).

## Error Conditions

If the user name, password, or port number is invalid or incomplete, an error message will be displayed in the browser.

### Invalid Port Specified:

If the port specified in the URL is invalid, the user is requested to login again with the correct user name and password, and a valid port number:

Figure 34 Invalid Port Number Error Display

## Exit the Application

Click on the **[Exit]** button in the left panel of the Dominion SX window to exit Dominion SX.

If changes to the configuration have been made but not saved, a screen will prompt you to save changes and log out of the unit. Click on the **[Yes]** button to save changes and exit, or click on the **[Cancel]** button to return to the configuration.

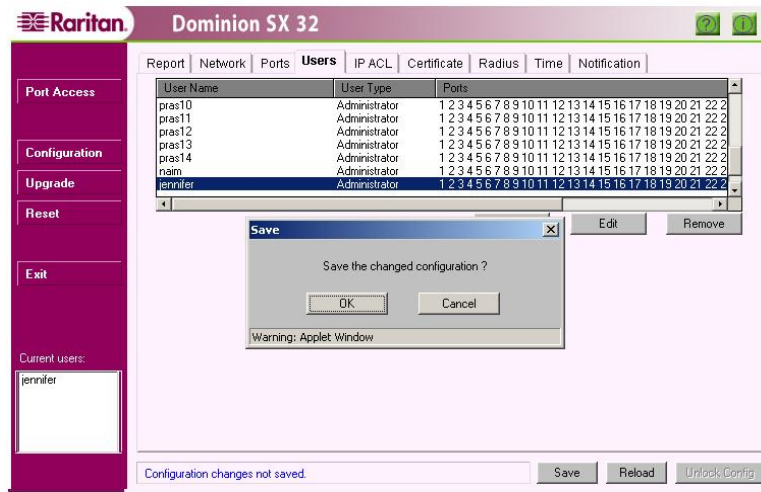


Figure 35 Save the Changed Configuration Window

If changes have been saved already, the unit will confirm the request to exit. Click on the **[OK]** button to log out of the unit.

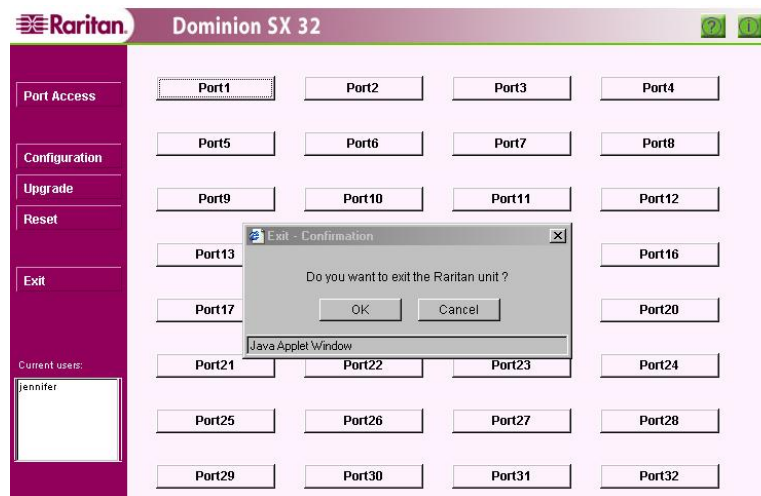
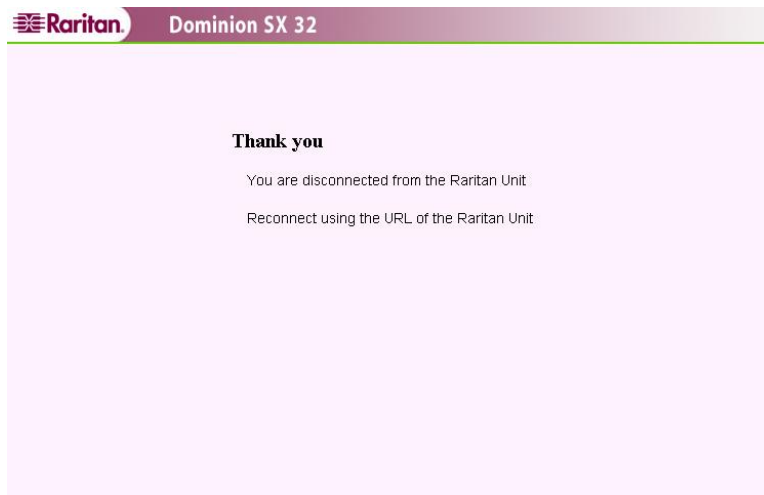


Figure 36 Exit Confirmation Display



A confirmation screen will indicate disconnection from the unit.



*Figure 37 Unit Disconnection Display*

## Dominion SX Management

Some advanced features are configured through a command line interface (CLI) using SSH (and Telnet, if enabled). Aside from providing the capability to manage a remote target device, Dominion SX has a number of powerful built-in features and capabilities available to manage the unit itself. With Dominion SX, users can:

- Change network parameters
- Install custom applications per port
- Restrict access based on IP address
- Add and Delete users and assign permission classes to each user
- Install a user-generated certificate or request a CSR to allow creation of a third-party certificate
- Increase security using RADIUS, TACACS+, LDAP, Microsoft Active Directory
- Use the modem for out-of-band access
- Upgrade the software remotely via the network
- Perform a soft reset on the application

In each case, dedicated displays are provided to allow the adjustment and configuration of the various parameters.

## Display

The display structure is divided into a number of key operational areas:

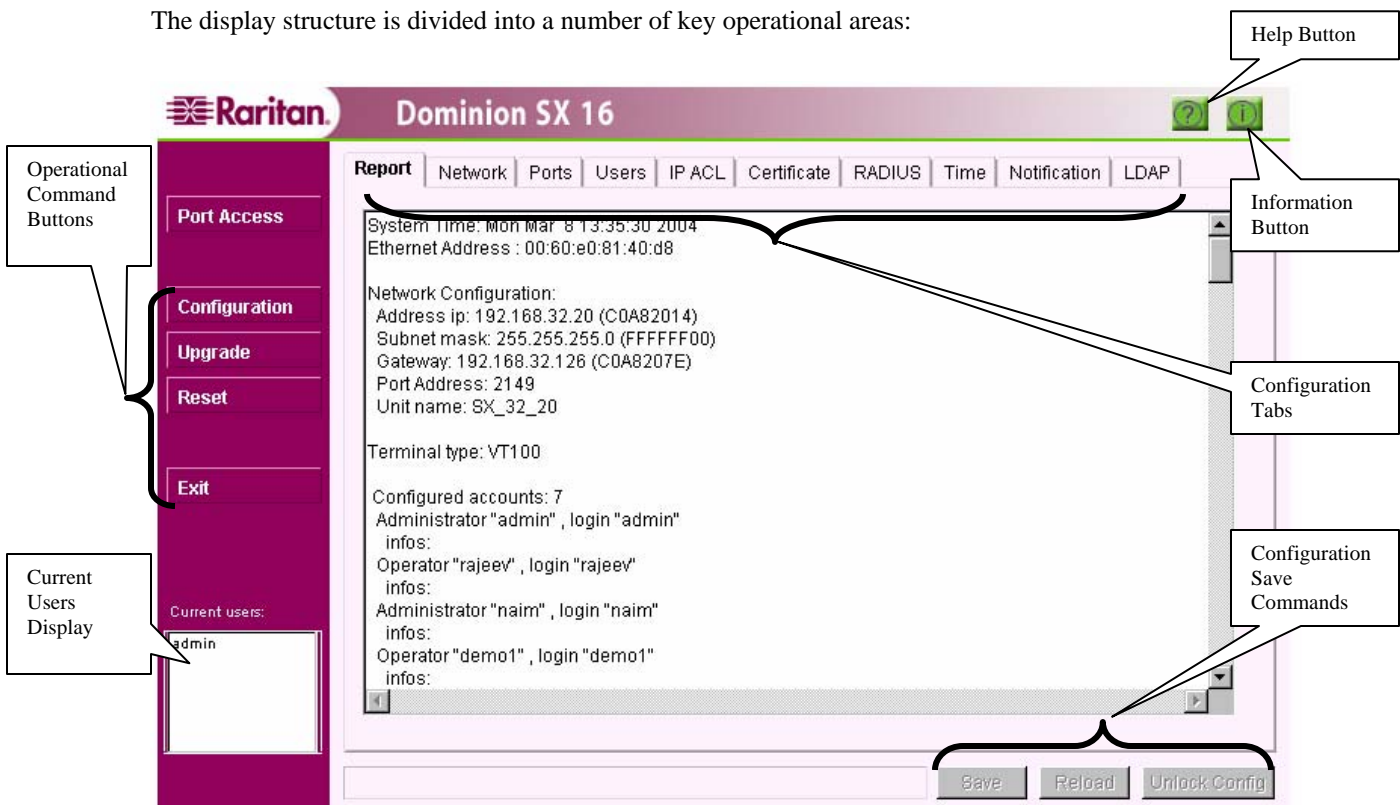


Figure 38 Display Overview

- **Operational Command Buttons:** Used to modify operation of Dominion SX
  - **Port Access:** Connects and displays the remote target device to be managed
  - **Configuration:** Calls up the Configuration Tabs
  - **Upgrade:** Provides a utility to upgrade Dominion SX software through the network
  - **Reset:** Allows a soft reset of the application
  - **Exit:** Logs out of the application and closes the connection to Dominion SX
- **Current Users Display:** Indicates users who are currently connected to Dominion SX
- **Help Button:** Brings up an online help guide on how to use the product
- **Information Button:** Provides copyright notice and software version information

- **Configuration Tabs:** Displays several screens in which the user configures different elements of the application
- **Configuration Save Commands:** Used to save or ignore changes made to configuration

---

## Configuration Lock and the Configuration Save Commands

---

Dominion SX is designed to allow only one user to configure it at any given time. When a user clicks on any of the Configuration tabs, that user acquires the Configuration Lock, preventing others from modifying the configurations. Other users may click on Configuration tabs at the same time, but will view all data in Read-only mode. Only after the lock is released can another user modify configurations.

### To Release the Configuration Lock:

- **Save the Configuration Changes:** Saving the configuration commits the updated information to the unit and automatically releases the Configuration Lock.
- **Reload the Previous Configuration:** Reloading the previous configuration deletes all updated information, reverts to the previously saved data, and automatically releases the Configuration Lock.
- **Unlock the Configuration:** Clicking on the [Unlock Config] button located in the lower right corner of all Configuration screens releases the Configuration Lock only if the user has not updated any configuration changes. If any changes have been updated, only a Save or a Reload can unlock the configuration.

---

*Note: Releasing the configuration lock loses any changes that are not updated.*

---

---

**Important! We recommend releasing the configuration lock once all necessary changes are made. This leaves the configuration available to other users if they must modify the device.**

---

---

## Update

---

Many of the Configuration tab screens feature an [Update] button. A user would click on the [Update] button to notify the system that changes have been made in that Configuration screen. The configuration changes do not take effect until they are saved. This offers two convenient advantages:

- The user can make as many changes as intended in any number of tabs and just keep the changes updated. All changes could be committed to take effect when desired with a single **Save** operation.
- The user can reject all changes made in a single session using the **Reload** option, offering a higher degree of error tolerance for the system. Any accidental deletions or modifications could be rolled back without having to log out of the unit.

---

## Save and Reload

---

Users can apply configuration changes to the Dominion SX unit by clicking on the [Save] button after editing Configuration screens. Users can reject all the configuration changes using the [Reload] button, but it is important to remember that configuration changes cannot be reloaded once they are saved.

### To Save Configuration Changes:

1. Click on the [Configuration] button in the left panel.
2. Click on the tab(s) for the screens in which you want to make configuration changes.
3. When the status bar displays the *Configuration locked* message, other users cannot modify the unit's configuration.
4. Modify data in the screen and click on the [Update] button.
5. The status bar will display the message: **Configuration changes not saved.**
6. Click on the [Save] button.

---

*Note: If you are making changes to several different configuration screens in one session, click on the [Update] button in each screen, but wait until making changes in the final configuration screen, and then click on the [Save] button to save all changes with just one action.*

---

7. The status bar displays the message: **Save in progress...**

---

*Note: When you make changes to **Network** settings on this screen, a warning message alerts you that the system will automatically reboot when you save your changes. Changing **Modem** settings does not require a system reboot.*

---

8. A success message appears.
9. The **Report** screen is updated and displayed after a successful Save.

**To Reload Configuration Changes:**

1. Click on the [**Configuration**] button in the left panel.
2. Click on the tab(s) for the screens in which you want to make configuration changes.
3. When the status bar displays the **Configuration locked** message, other users cannot modify the unit's configuration.
4. Modify data in the screen, and click on the [**Update**] button.
5. The status bar will display the message: **Configuration changes not saved.**
6. Click on the [**Reload**] button to erase any changes in this and any other configuration screen.
7. A successful reload message appears, indicating a successful reload of the original settings and configuration values.
8. The **Report** screen shows that no data has been changed.

# Configuration

## Report

### Overview

The Report configuration screen displays detailed information on how the Dominion SX has been configured, which can be useful if debugging or troubleshooting. This information is accessible only by Administrators.

- System time and date
- DSX unit serial number
- Ethernet MAC address
- Network configuration (Unit Name, IP address, subnet mask, gateway, line speed – Autodetect or 100 FDX, Network failover, and domain name)
- Port configuration – for CommandCenter discovery and SX (communication) port address
- Global session timeout
- Power supply status (for dual-power supply models, status of both power supplies is displayed - an unconnected or failed power supply shows as “Failed”)
- Time configuration
- Number and information of user accounts configured
- IP ACL configuration
- RADIUS, LDAP, NTP configuration
- Modem configuration
- Local ports access
- SSH and telnet
- Certificate configuration
- SMTP configuration
- Application information
- Syslog information
- NFS port log information
- SNMP configuration



Figure 39 Sample Report Display

## Network

### Overview

The Network configuration screen provides an area for Administrators to define both the network and modem (optional) settings for the unit.

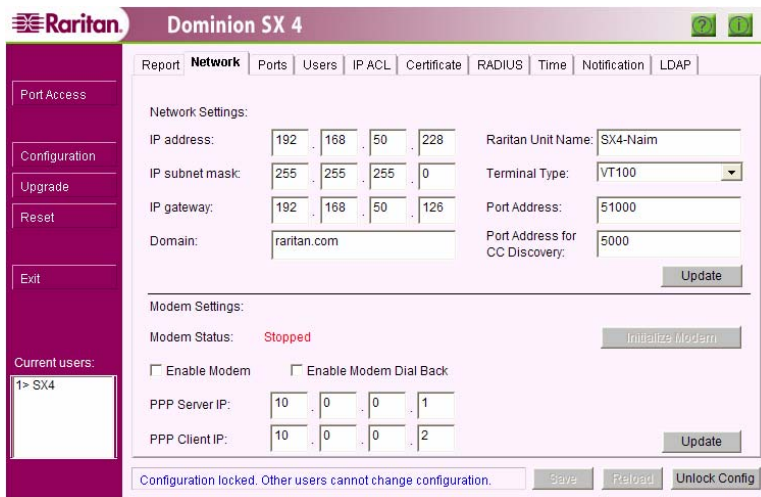


Figure 40 Sample of Network Configuration Display

Some Dominion SX units come equipped with a 56Kbps (Kilobits per second) modem, which allows dial-in access to the unit from virtually any location in the world. On other Dominion SX units, there is a connector on the rear panel for a user-supplied external modem. Client computers connect to the unit by establishing a PPP (Point-to-Point Protocol) link between the client machine and the Dominion SX unit. Once the PPP connection is established, the client computer is physically on the same network as the Dominion SX unit and can access the unit using Internet Explorer or Netscape browsers.

There are three requirements for dialing into the unit:

1. The phone line to the unit must be connected.
2. The modem / PPP connection settings must be configured.
3. If modem Dial Back is enabled, type a valid phone number to ensure successful modem callback connection. Type phone numbers from the command line interface (CLI) (under **Modem**) using SSH (or telnet if enabled). Phone number entries can contain numbers, hyphens, and spaces.
4. The dial-up networking software on the user's personal computer must be configured to establish a PPP connection from the client computer to the unit.

### Configure Network Parameters

- **IP address:** IP address for the unit
- **IP subnet mask:** Subnet mask to be used when deployed in the network
- **IP gateway:** Gateway that the unit uses to communicate with other systems that are not on the same subnet
- **Dominion SX Unit Name:** Name to be associated with the unit, 64 characters in length. Valid characters are A-Z, a-z, -, \_, 0-9, no spaces or special characters allowed
- **Terminal Type:** Type of terminal supported; default is VT100
- **Port Address:** Port address to be used by the unit when communicating with other systems; the default port address is 51000, but can also be set to any value in the range of 1024-65536 (please verify this value with your firewall administrator)
- **Domain name:** For example *mycompany.com*; domain name is required to send SMTP messages by certain mail servers. Unless you the mail server used in your company does NOT require this information to send email, it is safe to fill in this information. Most mail servers will require this information.
- **Port address for CC management:** Port address is required for use by CommandCenter-SG (CC) to discover Dominion SX units in the network. Default value is 5000; this value should NOT be changed unless instructed to do so by the CC administrator. It is possible that other devices connected to the

TCP/IP network may be set to listen to broadcasts on this address; if this is the case, it can be configured to use another port address. However, this port address **MUST** match the port address specified by the CC administrator; otherwise the Dominion SX unit will not be discovered by CC. This port address is relevant only for CC releases 2.3 or higher.

Click on the [**Update**] button to load all the changes.

Click on the [**Save**] button to make the changes permanent.

---

**Important! Remember that saving changes to Network Configuration settings will cause the unit to reboot.**

---

The parameters for configuring modem access include:

PARAMETER	DESCRIPTION
Enable Modem	Configures the modem to answer calls
PPP Server IP	IP address of the PPP server (Dominion SX unit)
PPP Client IP	IP address of the PPP client (remote computer)
Enable modem Dial Back	Enables Modem dial back (phone number for modem dial back is specified in the CLI using SSH [or telnet, if enabled]).

### **Configure Modem Parameters**

1. Check the Enable Modem box.

---

*Note: Click on the checkbox before **Enable Modem Dial Back** and type the phone number for dial back using the command line interface (SSH/telnet). Enabling Modem Dial Back potentially enhances security, and is recommended for most applications.*

---

2. Type the **PPP Server IP** address used by the client to access Dominion SX once the modem connection is established.
3. Type the **PPP Client IP** address assigned by Dominion SX to the client in order for the connection to be established.
4. Click **Update**.
5. Click **Save**.
6. Optionally, enable modem dial back and type the phone number for dial back using the CLI (SSH/telnet). Using modem dial back can potentially enhance security, and is recommended for most applications.

The Modem Status field indicates one of two states:

- **Running:** The modem is configured and is operational.
- **Stopped:** The modem is not operational.

The [**Initialize Modem**] button can be used to reset the modem if it is running but not operating properly.

---

*Note: Be sure to verify the above information with your Network Administrator prior to configuring the unit.*

---

When using Microsoft Windows, once Microsoft dial-up networking has established a connection, a network is constructed with the parameters specified in the Modem Settings area of the Network configuration window. The client computer now can be connected to two separate networks. These networks must have distinct IP addresses if modem access is to function properly. The second network established by the PPP connection has only two devices, the Dominion SX unit with IP address PPP Server IP and the client computer with IP address PPP Client IP.

Please see **Appendix G: Modem Configuration** for additional information on configuring Microsoft dial-up networking on Windows 2000, Windows 98, and Windows NT.

## Modem Usage

Dial-up connection support for the unit allows users to access the connected target device when normal network connectivity to Dominion SX is not available. Once the PPP connection is established between the client computer and the unit, the user can access the unit by using the browser.

**Note:** For browser-based dial-up, access is supported with connection speeds of 28.8 Kbps or higher, with 56Kbps highly recommended. For dial-up access using the Command Line Interface (CLI) (using SSH/Telnet), connection speed of 9600bps or higher is recommended.

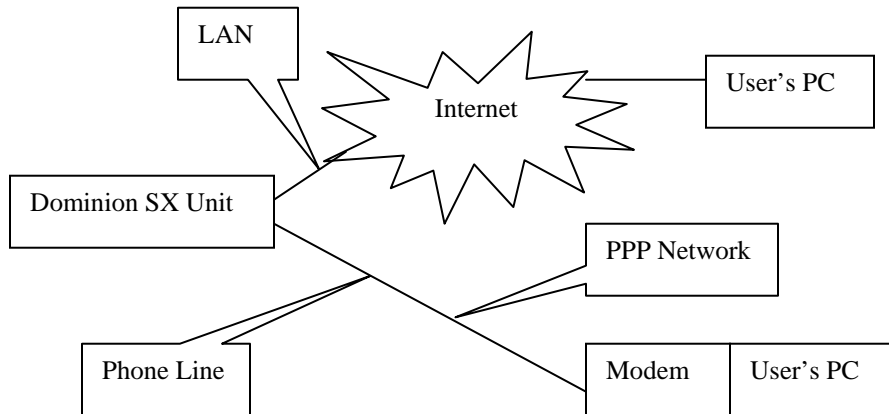


Figure 41 Modem Connection to a Dominion SX unit

## Ports

### Overview

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

No.	Name	Application	Baud Rate	Parity Bits	Parity Check	X on /X off	HW Flow
1	Port1	RaritanConsole	9600	None/8	Disabled	Disabled	Disabled
2	Port2		9600	None/8	Disabled	Disabled	Disabled
3	Port3		9600	None/8	Disabled	Disabled	Disabled
4	Port4		9600	None/8	Disabled	Disabled	Disabled

Configuration locked. Other users cannot change configuration.

Figure 42 Port Configuration Display



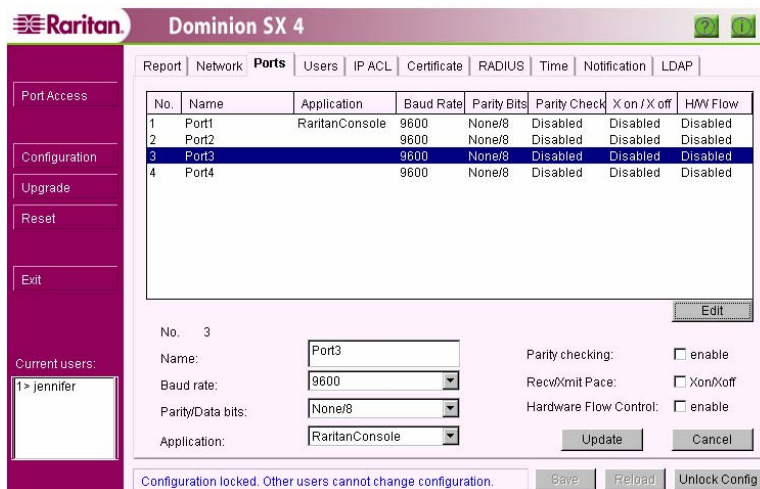


Figure 43 Port Editing Display

## Configure Port Parameters

- **Name:** Name that associates the serial port with the connected target device; can be up to 64 characters in length and must be unique from the other port names (only 20 characters are displayed on Port access buttons)
- **Application:** Application type associated with a specific port, two are provided: default applications RaritanConsole (contact Raritan for additional applications) and PowerBoard (for use with Raritan Power Control units)
- **Baud rate:** Baud rate of the serial port; should match that of the target device connected to the port (valid choices are 1200, 1800, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200)
- **Parity/Data bits:** Parity/Data of the serial port; should match the setting of the target device (valid choices are None/8, Even/7, Odd/7)
- **Parity check:** Enabling or disabling of the Parity function of the serial port; should also match the target device's setting
- **Xon/Xoff:** Can be enabled if the target system supports this feature; will allow the unit to control the data flow and reduce the chance of data loss
- **Hardware Flow Control RTS/CTS:** Can be enabled if the target system supports this feature; will allow the unit to control the data flow using hardware signals and reduce the chance of data loss.

## Edit Port Parameters

1. Select an entry to modify.
2. Click on the [Edit] button.
3. The selected entry appears in the lower half of the screen.
4. Make changes to the fields as needed.
5. Click on the [Update] button to load the changes or click on the [Cancel] button to ignore changes.
6. Click on the [Save] button.

## Users

### Overview

The Users configuration screen provides a place to define a user list with appropriate unit access permissions. There are three classes of users, each with different rights:

- **Administrators:** Can view and modify all configuration information, including the user information for all user types (Administrators, Operators, and Observers). Administrators have write-access rights to the console window.
- **Operators:** Cannot view configuration information; can modify their own passwords through CLI (see **SSH/Telnet, Command Line Interface (CLI) User Interface**, later in this chapter). Operators have write-access rights to the console window
- **Observers:** Cannot view configuration information; can modify their own passwords through CLI (see **SSH/Telnet - Command Line Interface (CLI) User Interface**, later in this chapter). Observers have read-only rights to the console window.

USER TYPE	CONFIGURATION	CONTROL REMOTE TARGET	UPGRADE	RESET
Administrator	All	Yes	Yes	Yes
Operator	Edit own user record	Yes	No	No
Observer	Edit own user record	No	No	No

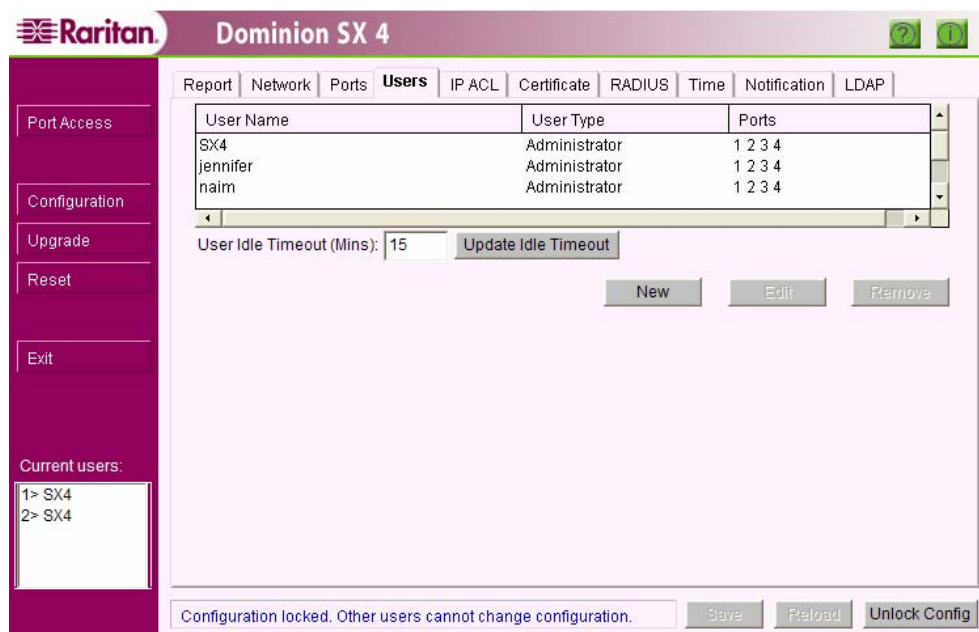


Figure 44 Users Tab Display

### Local Users

The unit can be configured for fifty (50) local user accounts and can support up to ten (10) users simultaneously logged in to the same port.

### Configurable Parameters

- **User Name:** Name used for display purpose as in the Current Users list; alphanumeric text, 1 – 32 characters in length (mandatory)
- **Login Name:** Login name used to log in to Dominion SX; alphanumeric text, 1 – 255 characters in length (mandatory)
- **User Type:** Administrator / Operator / Observer.
- **Information:** Additional informational and/or description to be associated with the user; alphanumeric text, 1 – 64 characters in length

- **Password:** Authentication password; alphanumeric text, 6 – 16 characters in length (mandatory)
- **Ports:** List of ports that the user can access; by default, Administrators are given access to all ports, and can assign ports to Operators and Observers
- **Configure Idle Session Timeout:** Idle session timeout (default value 5 minutes): Set a timeout value between 0 and 999 minutes for idle sessions; system-wide parameter that applies to all users and sessions via web-browser, SSH/telnet. A value of zero means NO timeout. We recommend using the shortest reasonable timeout value.

## Add a New User

Only an Administrator can create a new Administrator, Operator, or Observer. New users' records are valid only after the configuration is saved, and users can change their passwords after the first time they log on.

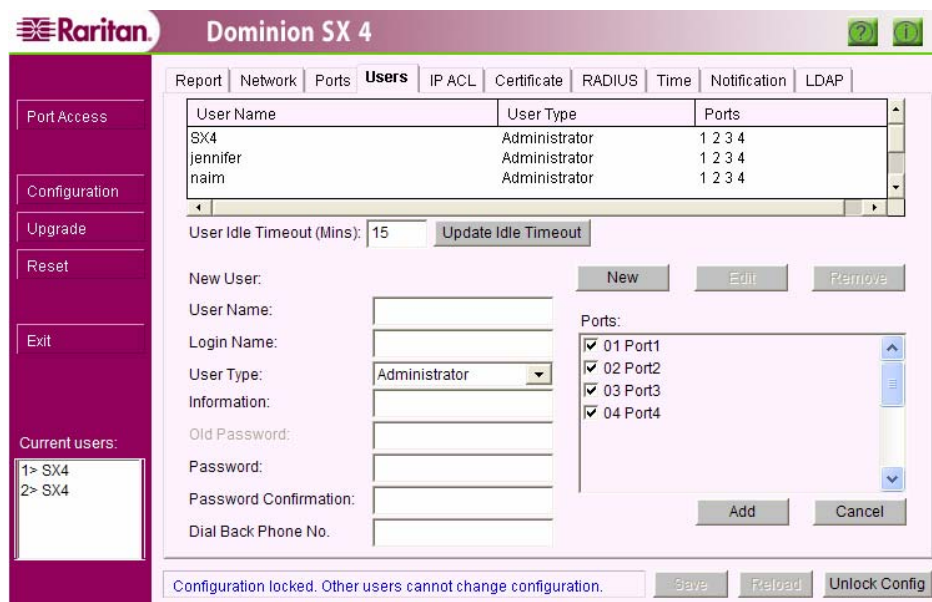


Figure 45 New User Creation

### To Add a New User:

1. Click on the [New] button.
2. Enter the **User Name**, **Login Name**, **User Type**, and **Password**.
3. Retype the password in the **Password Confirmation** field.
4. Type the Dial back phone number in the **Dial Back Phone No** field.
5. Assign the ports that the user can access. Note that Administrator users are automatically granted access to all ports.
6. Click on the [Add] button.
7. Click on the [Save] button.

## Edit Existing User Information

Only Administrators can edit all User information (except **Login Name**). Observers and Operators cannot change any User Information, except their own Passwords, which they can change using CLI.

If the user is logged in at the time the Administrator is editing that User's information, only the **Information** and **Password** fields can be changed.

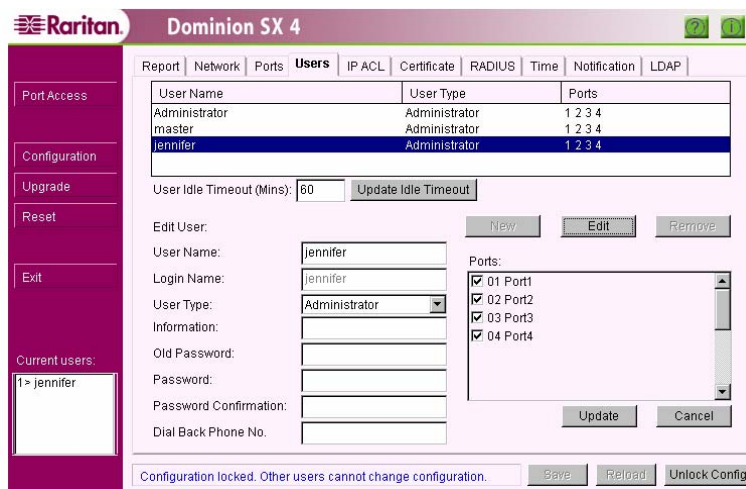


Figure 46 Sample User Modification Screen

### To Edit Existing Information:

1. Click on the **User Name** to modify that user's information.
2. Click on the **[Edit]** button.
3. Update the desired fields.
4. Click on the **[Update]** button.
5. Click on the **[Save]** button.

### Delete a User

#### To Delete an Existing User:

1. Click on the **User Name** of the user to be deleted.
2. Click on the **[Remove]** button.
3. Click on the **[Save]** button.

*Note: If the user being deleted is currently logged in, a warning screen will appear. A logged-in user cannot be deleted until that user has logged out of the system. Please remember that only Administrators can delete users.*

---

## IP ACL

---

**Important: Please make absolutely certain that all IP addresses have been entered correctly before enabling IP ACL. If not, you may be locked out of the unit and be unable to access the unit in the future; the only way to restore access to the unit is to perform a factory reset, removing all user-defined values that you have programmed, forcing you to completely reconfigure the unit.**

---

### Overview

There are two ways for a Dominion SX Administrator to manage IP Access Control Lists (IP ACLs):

- Via the Graphical User Interface (GUI) for configuring and managing IP ACLs
- Via the Command Line Interface (CLI) using SSH/Telnet. Please note that when using the CLI, we highly recommend using SSH, not Telnet, to securely configure the IP ACL.

Because Dominion SX leverages the IPTables firewall functionality to provide IP ACL capability, familiarity with IPTables is strongly recommended, and knowledge of the concepts of Access Control Lists (ACL) is a prerequisite for configuring and administering the Dominion SX IP ACL feature. Explaining IPTables is beyond the scope of this document. Please refer to IPTables documentation for more specific details on creation and management of the IP ACL rule lists. We also suggest the following link:

<http://iptables-tutorial.frozentux.net/iptables-tutorial.html>

### Rule Creation and Execution

*Note: We recommend that you turn IP ACL logging OFF when creating an Allow rule. If not, every accepted packet that matches the rule will be logged, causing the log file to increase in size very quickly.*

---

To create access rules, click on the IP ACL tab on the Dominion SX screen. Click Insert to insert a new rule in the rules table on this screen.

After configuring all IP ACL parameters, you can create rules. Rules in the table begin with the number (No.) zero (0), and continue in numerical order. When attempting to make a connection, Dominion SX will start at the beginning of the rules table list and continue through the list in order until an applicable rule is matched with the command executed.

## Browser - Graphical User Interface (GUI)

The Dominion SX GUI provides a front end to the IPTables.

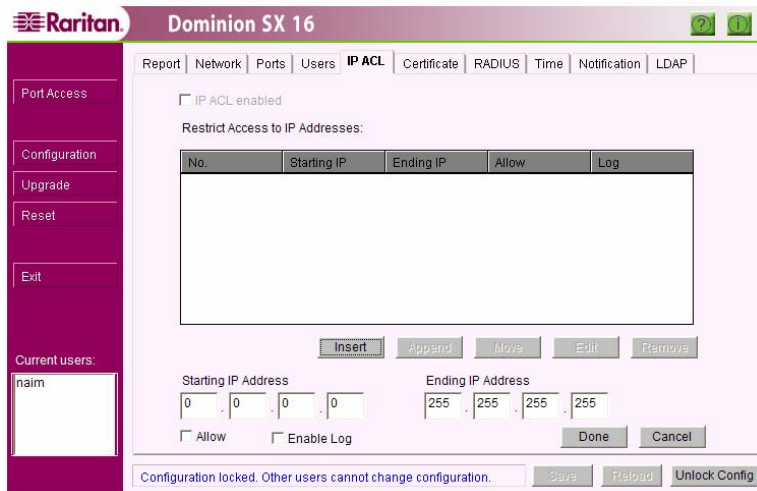


Figure 47 Inserting a rule into the browser-based IP ACL configuration screen.

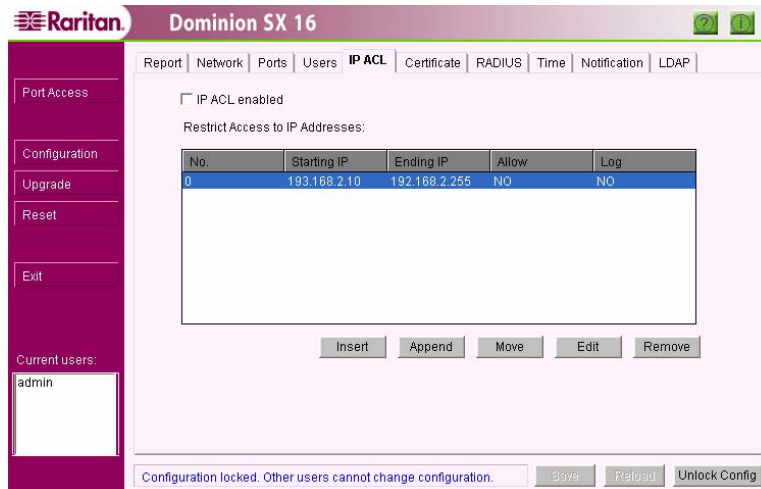


Figure 48 GUI User Interface

We recommend the following link for learning more about IP tables:

<http://iptables-tutorial.frozentux.net/iptables-tutorial.html>

The Dominion SX GUI command buttons assist in editing the Dominion SX configuration:

<b>Insert</b>	Insert a new rule, e.g., rule 0 denies access from all IP Addresses in the range 192.168.2.10 to 192.168.2.255, and will not log the activity.
<b>Append</b>	Allows administrator to append a new rule to the existing rules.
<b>Move</b>	Move a rule up or down on the list; this changes the order in which a rule (filter) is applied. A rule must be selected (highlighted) before it can be moved.
<b>Edit</b>	Allows the administrator to edit the values in a rule already on the list. A rule must be selected (highlighted) before it can be edited.
<b>Remove</b>	Removes a rule from the list. A rule must be selected (highlighted) before it can be removed.
<b>Enable</b>	Enables the IP ACL policy management.

The main screen input consists of the following fields for each policy/rule for Deny/Allow.

<b>Starting IP Address</b>	This is the starting IP Address (Only valid IP addresses in dot notation should be entered).
<b>Ending IP Address</b>	This will be the end range, to apply the policy of Allow/Deny.
<b>Allow</b>	This flag will decide the action based on the filter criteria.
<b>Enable Log</b>	Log flag in the IPTables will be set for this policy.
<b>Done</b>	Saves the current changes and apply the filter to the IPTables.
<b>Cancel</b>	Cancels all the changes and do not save any modifications.

## **Allowing or Denying Access to the Dominion SX**

### **Allowing Dominion SX Access**

To allow access to the Dominion SX from a particular address, set both the **Starting IP Address** and the **Ending IP Address** to a specific address and check the **Allow** checkbox. Click **Done** when finished. Click on the **IP ACL enabled** checkbox, and then click **Save** to save the IP ACL configuration to the non-volatile memory of the Dominion SX. This rule allows connections from this address, and attempts to connect from all other IP addresses will be denied. Please note warnings in the **Overview** section, above.

*Example:* To **Allow** access to the Dominion SX from only one IP address (or a range of IP addresses), see rules, below.

Administrator goal: to allow access to the Dominion SX unit from only IP address 192.168.51.80, and deny access to the Dominion SX unit from ALL other IP addresses.

The following rules will be needed:

**0.) 192.168.51.80 192.168.51.80 Allow No**

**1.) 0.0.0.1 255.255.255.255 Deny No**

Rule 0 is to allow access from the IP address listed; it could be any range of IP address that the user wants.

Rule 1 denies access from all IP addresses, other than those explicitly listed in Rule 0.

Great care must be taken when entering Rule 0, because if a user does not enter the IP address (or address range) in Rule 0 correctly, and then enters Rule 1, the user will functionally be locked out of accessing the Dominion SX unit. The only recovery is to reset the Dominion SX unit to factory default in order to get out of this situation, and, as a result, all user entered settings will be lost.

### **Denying Dominion SX Access**

To deny access to the Dominion SX unit from a particular IP address, set both the **Starting IP Address** and the **Ending IP Address** to a specific address. Do not check the **Allow** checkbox (make certain it is unchecked) to deny access from the particular IP address listed. Click **Done** when finished. Click on the **IP ACL enabled** checkbox, and then click **Save** to save the IP ACL configuration to the non-volatile memory of the Dominion SX. This rule denies all connections from this address. Please note that this will **ALLOW** access to the unit from ALL other IP addresses - other than the one specified in Rule 0. Also, please note warnings in the **Overview** section, above.

## **SSH/Telnet – Command Line Interface (CLI) User Interface for Configuring IP-ACLs**

---

### **Important:**

→ **Make certain that the IP address from which you are connected to the Dominion SX is not accidentally entered into the IP ACL deny list (“Allow=NO”); if the IP Address is in the deny list, the Dominion SX unit will be inaccessible. If this happens, you must reset the Dominion SX unit to factory default settings; when reset, all Dominion SX settings will be lost and must be reconfigured.**

→ **We recommend that you turn IP ACL logging OFF when creating an Allow rule. If not, every accepted packet that matches the rule will be logged, causing the log file to increase in size very quickly.**

---

### **NAME:**

ipacl [enable/disable/status]

### **DESCRIPTION:**

Enable / disable IP Access Control lists.

ipacl status

Display the enable /disable status. Display all configured IPACL rules.

ipacl <enable|disable>

Depending on the parameter, enable or disable ipacl.

### **USAGE EXAMPLE:**

admin:Command>ipacl status

ipacl Status

Enabled: 0 No

ipacl List Count : 3

ipacl Rules: [startip] [endip] [Allow/Deny] [Log]

0.) 1.1.1.1 1.1.1.1 Deny Yes

1.) 2.2.2.2 2.2.2.2 Allow No

2.) 192.168.127.233 192.168.127.233 Allow Yes

### **NAME:**

aclcfg <[list] | [clear] | [move <pos1> <pos2>] |

[delete <pos1> [pos2] ] | [add <ip1> <ip2> <denyflag> <logflag>]>

### **DESCRIPTION:**

Configure IP ACL parameters. The ordering of the rules in the list are followed starting at 0 (zero) and moving downward. When a connection attempt is made, the list is traversed and the first rule that fits will be executed.

See IPTables documentation for more specific details on creation and management of the IPACL rule lists.

aclcfg list

Same as “ipacl status” command, display ipacl configuration and rule list.



aclcfg clear

Remove all the ipacl rules current in the list.

aclcfg move <pos1> <pos2>

Move the ipacl rule at <pos1> to <pos2>.

aclcfg delete <pos1> [pos2]

Delete can have one or two parameters, if there is one parameter, then this command will delete the rule at <pos1>. If there are two parameters, then this command will delete the entire range of rules between and inclusive of <pos1> and <pos2>.

aclcfg add <startingIP> <endingIP> <denyflag> <logFlag>

For the range of IP's specified between <startingIP> and <endingIP> this will either deny, if <denyflag > is 1, or allow, if <denyflag> is 0, access to the DominionSX. If <logFlag> is 1, it will also log any connection attempt that this IPACL rule catches to the Syslog facility.

If you wish to allow or deny a specific IP address, just set the starting and ending IP to that particular address.

#### USAGE EXAMPLE:

```
admin:Command>aclcfg add 1.2.3.4 1.2.3.4 0 0
```

(add a rule allowing IP 1.2.3.4 to connect, do not log connections)

```
admin:Command>aclcfg add 1.2.3.11.2.3.255 1 1
```

(add a rule denying and logging any connection attempt from the IP range 1.2.3.1 to 1.2.3.255)

```
admin:Command>aclcfg del 0
```

(delete the rule at position 0)

```
admin:Command>aclcfg del 2 7
```

(delete rules 2 through 7)

```
admin:Command>aclcfg move 2 4
```

(move the rule from position 2 to position 4 in the list)

#### NOTE:

To enable syslogging of these ipacl messages, the kernel *syslog* messages must be configured using the following:

- 1) "cfglog kernel <parameters>" see the **cfglog** section for parameter values
- 2) "log start kernel" will start the syslog messages
- 3) "log status kernel" will display the kernel's syslog configuration

## Certificate

### Overview

The Certificate configuration screen provides an area for Administrators to define security parameters. Dominion SX supports certificate-based server authentication to establish an encrypted SSL session and to assure the user that they are dealing with a correct web site. The encrypted SSL session, always through HTTPS connection, ensures that personal information sent over the network is secure. Dominion SX supports SSL 128-bit encryption, and will negotiate with the client only at the specified security strength. The unit can act as a Certifying Authority and generate both self-signed CA Certificate and the Server Certificate. The certificate generated uses a 1024-bit public key.

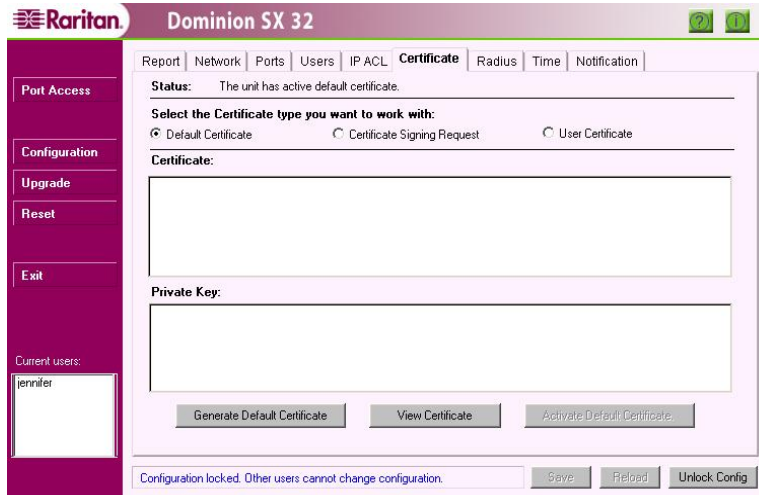


Figure 49 Certificate Tab Display

### Configuration

When the user powers up the unit for the first time, an SSL certificate associated with the default IP address **192.168.0.192** is generated. When the user tries to connect to the unit, a Security Alert is displayed because the CA root certificate is not installed in the browser. Click on the [Yes] button to continue the Configuration process, and configure the unit. Please refer to **Appendix C: Certificates** for more information on how to install the certificate into the browser to prevent the security alert window from appearing. After the configuration is completed, the unit reboots. The server certificate is generated once again, this time for the new IP address assigned to the unit.

### Certificate Generation

Dominion SX provides different methods of generating certificates.

- **Default (or Self-Signed) Certificate:** By default, the unit ships with a self-signed certificate signed by Raritan Computer. The certificate strength is 1024-bits and the certificate is valid for one year.
- **User Certificate:** This method allows the installation of a user-generated certificate, which can be in one the following forms:
  - User certificate generated from the CSR (Certificate Signing request) form. Clicking the “Generate CSR” button generates a CSR. In this case, only the certificate is installed into the unit. The certificate is compared with the private key (already generated) before it is installed into the unit.
  - User Certificate and private key (without pass-phrase) generated by a trusted third-party are installed into the unit.

Once the certificates are installed, the unit will automatically reboot so that the certificates take effect. There is an option that allows users to select either the self-generated or user-installed certificate at any time. Once installed, certificates are maintained in the unit. A status indicator at the top of the Certificate screen indicates the unit’s Certificate status, which might be:

- Active default certificate.
- Active user certificate.

- User certificate and active default certificate.
- Pending CSR and active default certificate

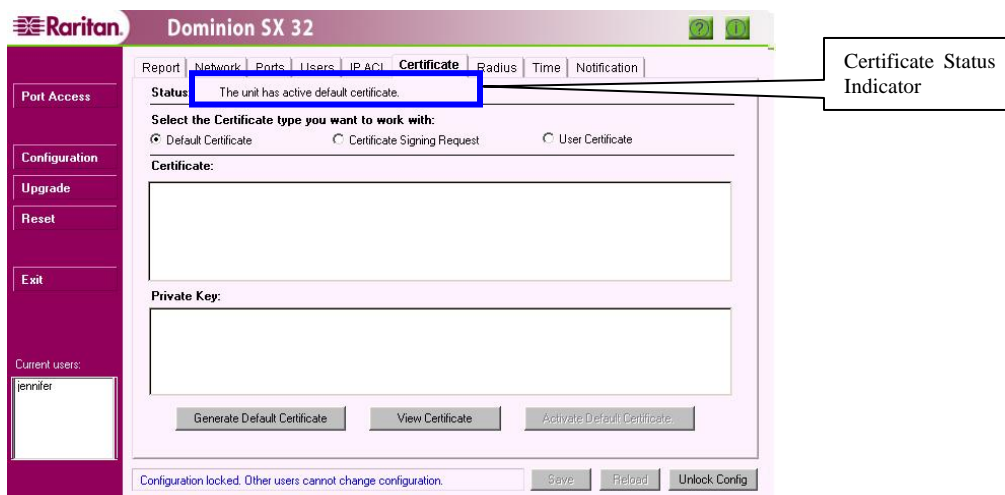


Figure 50 Certificate Configuration Display

## Default Certificate

The unit ships with a 1024-bit self-signed certificate signed by Raritan. When a user powers up the unit for the first time, an SSL certificate is generated that is associated to the default IP address **192.168.0.192**. Once the unit is configured with its new IP address, the unit reboots and uses the new IP address to generate a new certificate. When the **Default Certificate** radio button is selected, three buttons are available at the bottom of the Certificate screen:

1. [**Generate Default Certificate**]: Click on this button to regenerate the certificate provided by Raritan. Please note that generating the certificate will cause the unit to reboot.
2. [**View Certificate**]: Click on this button to view the currently installed default certificate. This option can also be used to copy the certificate (generated by Raritan) and install it on the client desktop. Please refer to **Appendix C: Certificates** for more information.
3. [**Activate Default Certificate**]: Click on this button to activate the default certificate. This option can be used to replace the user-installed certificate with the default certificate provided by Raritan. Please note that activating the default certificate will cause the unit to reboot.

## Generate Default Certificate

This function is used when the certificate has expired and a new one is needed.

1. Click on the [**Generate Default Certificate**] button.
2. When the confirmation window appears, confirm that the correct date is displayed. If not, you must change the date by modifying the information on the Time configuration screen (click on the **Time** tab) before you generate the Certificate, or the Certificate generated may not be valid.
3. The unit will reboot.

**Note:** If you factory-reset the unit and there is no user-installed certificate in the unit, the server Certificate is regenerated for the IP address 192.168.0.192. If the user-installed certificate is active, it will remain active after a factory reset.

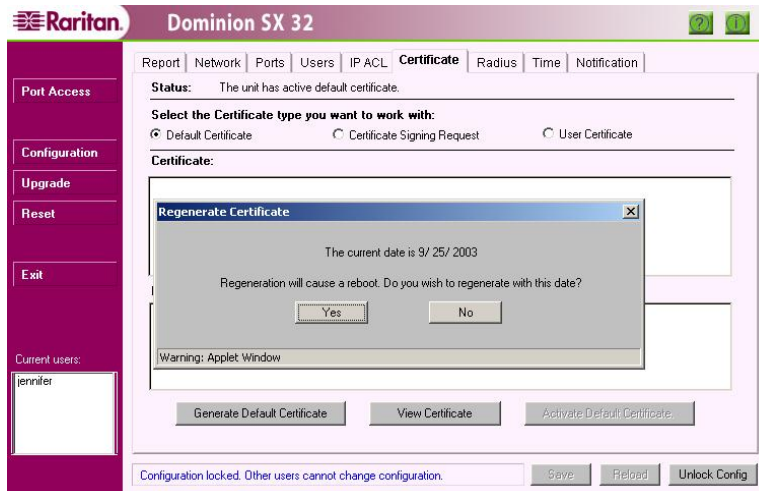


Figure 51 Generate Certificate Display

## View Certificate

This function enables the CA Root Certificate to be generated in the unit.

When you click on the [**View Certificate**] button, the CA Root Certificate appears. Please refer to **Appendix C: Certificates** for more information on installing CA Root.



Figure 52 View Self-Signed Certificate Display

## Activate Default Certificate

This button is active only when a user certificate is installed and active on the unit. When you click on the **[Activate Default Certificate]** button, the default certificate generated by Raritan becomes active. The unit will reboot and use this certificate upon rebooting.

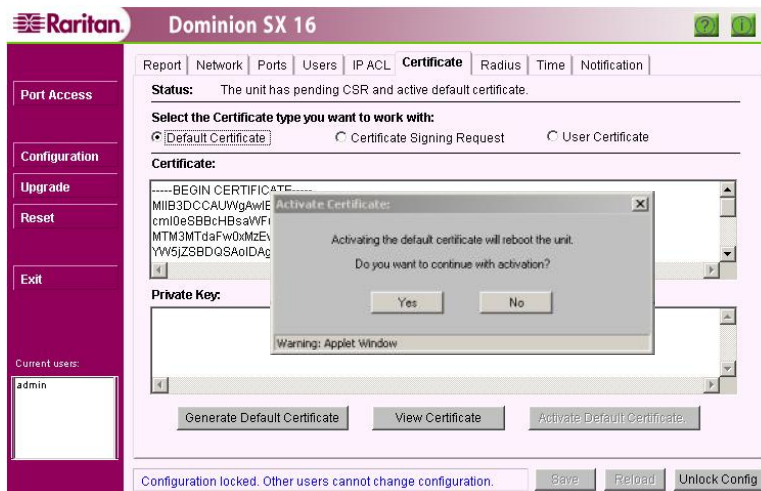


Figure 53 Activating Default Certificate

## Certificate Signing Request (CSR)

Dominion SX will generate a CSR that can be used to obtain a user certificate to be installed in the unit, from a trusted third-party source. Bit strengths of 512, 1024, and 2048 are supported. If a user-installed certificate is active, a CSR cannot be generated. The default certificate from Raritan must be active in order to generate a CSR.

### To Generate a CSR Request:

First click on the **Certificate Signing Request** radio button, and then click on the **[Generate CSR]** button to generate a CSR and a private key that is stored in the unit. When the warning screen appears, click on the **[Yes]** button to continue generating the request and to overwrite the information already on the system.

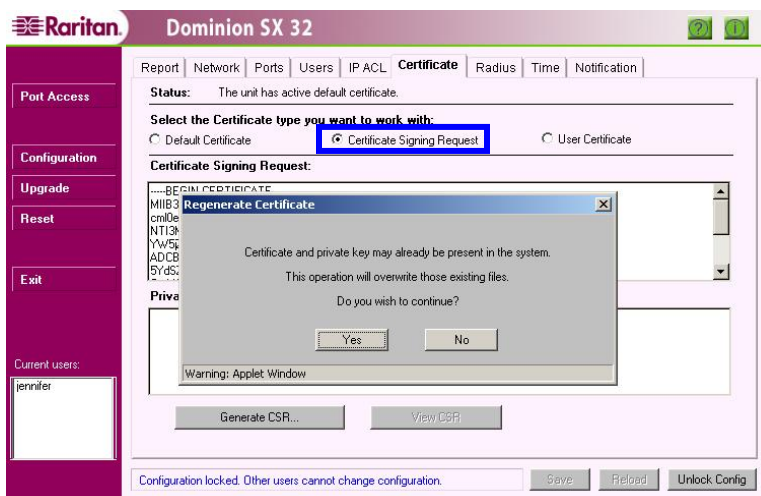


Figure 54 Generate CSR Request Display

**Certificate Request Details:**

Private Key Bit Strength:

Certificate Validity Period:  (in Days)

Common Name:   
(e.g. domain name i.e. www.yourservername.com)

Country Name:  (2 letter code)

State/Province Name:

Locality:  (e.g. city)

Organization:

Organization Unit:  (e.g. Section)

Email Address:

Figure 55 CSR Configurable Parameters

The first three fields in this screen are required; the other fields are optional:

- **Key strength:** 512, 1024, or 2048
- **Certificate validity period:** In days, two years maximum
- **Common name:** Fully qualified host name such as **www.raritan.com** or **10.0.3.65**
- **Country name**
- **State/province name**
- **Locality**
- **Organization**
- **Organization unit**
- **Email address**

Click on the [**Generate CSR**] button to generate and display the request. Cut and paste the result into a text file and use the file to obtain a valid certificate from a third-party. When you receive the new certificate, install it in the unit.

### To View the Certificate Signing Request:

Click on the [**View CSR**] button to view the certificate-signing request that has been generated to obtain a valid certificate.

**Raritan Dominion SX 16**

Report | Network | Ports | Users | IP ACL | **Certificate** | Radius | Time | Notification

**Status:** The unit has user certificate and active default certificate.

**Select the Certificate type you want to work with:**

Default Certificate  Certificate Signing Request  User Certificate

**Certificate Signing Request:**

```
UE0xEDA0BgNVBAMTB1Jhcml0YV4xZ2hBqkqkiG9w0BCQEWFGplbm5pZmVvQHJhcm10YV4uY291MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALypdMeTyePxeIjh7kZMtpoYUuNIHUIuLxKJc0U4CLIR0n0A8DtcCcgJ1WfZG7DAmyGc6ut5hshN4CNrLDn0CAwEAIAAAAMADCCSgS8b3DQEBAUAA0EAYyA9c6mngFX9EL7CGk4MLbA89h5Y3tU64Pk5dJ4g4PttOnd4wYox7BNFUpCINU6MGK7Aea2zknzKjllihw==
```

**Private Key:**

Configuration locked. Other users cannot change configuration.

Figure 56 View CSR Display

## User Certificate (Install Server Certificate)

This function allows the user to install a certificate from various Certificate Authorities (CA) such as VeriSign, Thawte, and Baltimore. If you do not want to use the Certificate generated by the unit, you can obtain one from one of these Certificate Authorities and install it in the unit yourself.

### To Install a User Certificate:

1. Open the certificate and the private key file in a text editor. If the certificate was generated using CSR, only the certificate will be available.
2. Under the **Certificate** Tab, click on the **User Certificate** radio button.
3. Select the text and use the Copy (<Ctrl+C>) and Paste (<Ctrl+V>) commands to copy the certificate and the private key, as applicable, into the respective window.
4. Click on the **[Install User Certificate]** button.
5. If the installation is successful, the unit will reboot, and the next time a user logs into the unit, the User Installed Certificate will appear.

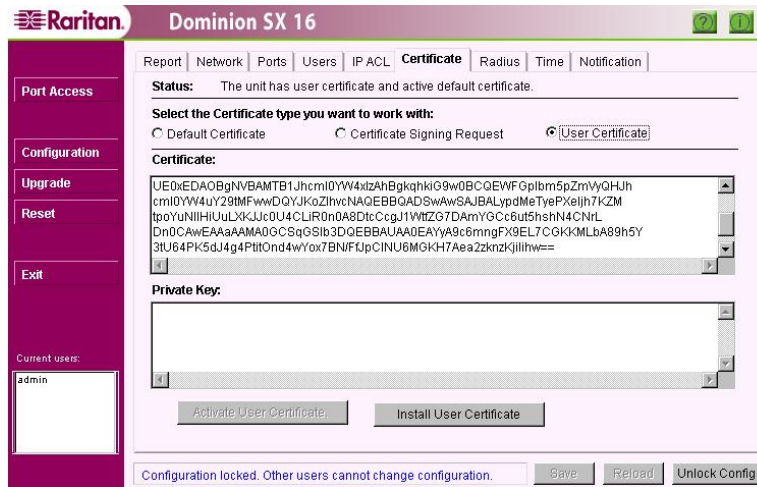


Figure 57 User Certificate

When a user connects to the unit, the Server Certificate is downloaded. The browser trusts the server certificate if the signer of this Certificate, or “CA Root,” is installed in the browser.

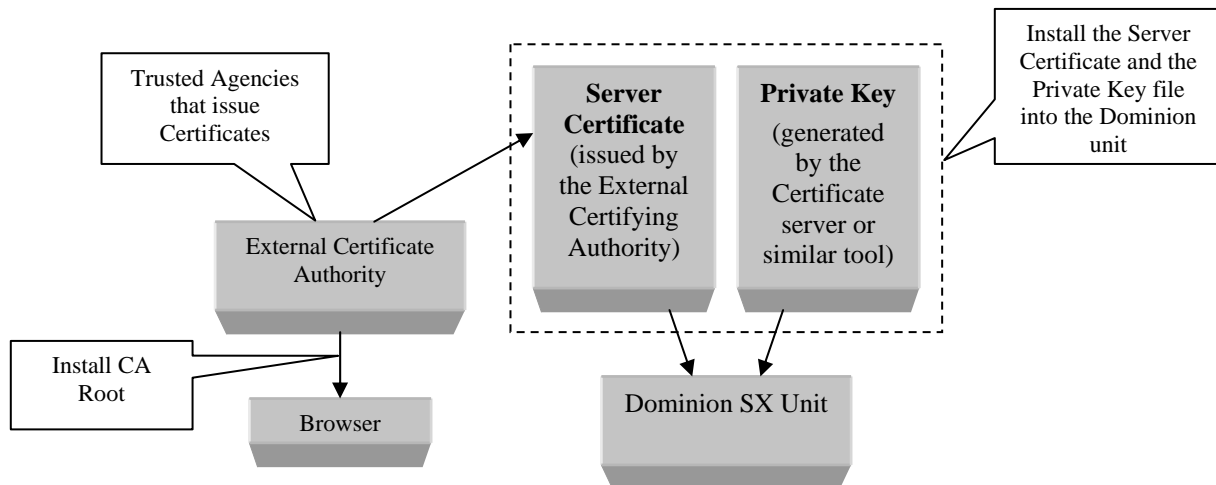


Figure 58 Schematic of External Certificate Utilization

## RADIUS

### Overview

The RADIUS configuration screen allows Administrators to modify information regarding RADIUS, or the Remote Authentication Dial-In User Service, an access server authentication, authorization, and accounting protocol developed by Livingston Enterprises, Inc. RADIUS protocol defines the communication between a RADIUS client and a RADIUS server.

The RADIUS Configuration screen is used to set up the unit for use with a RADIUS protocol server. RADIUS protocol is an Internet standard that provides user authentication, authorization, and accounting services for remote access devices. Dominion SX can be configured as a RADIUS client. The unit will query the RADIUS server for authentication and authorization information each time a user attempts to login to the unit.

The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

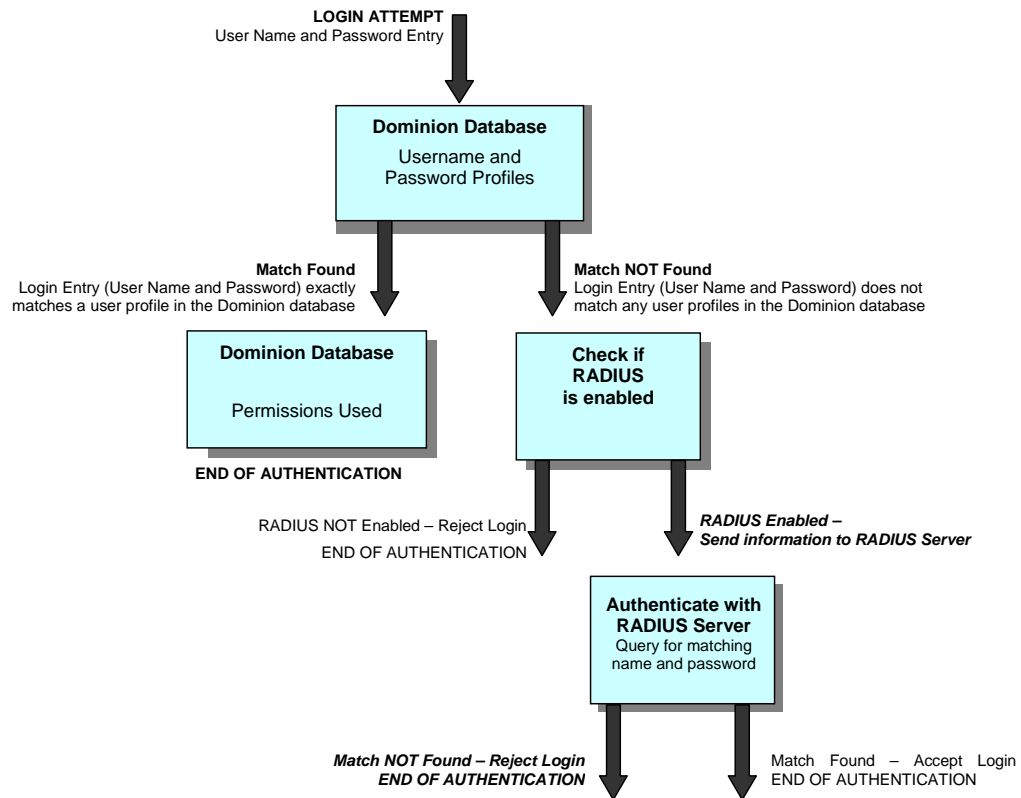


Figure 59 RADIUS Users Login Mechanism

RADIUS Authentication occurs when a user tries to log on to the RADIUS client. After prompting the user for login name and password, the client checks to see if the user is already present in the local list. If not, the client sends this information in an authentication request to the RADIUS server. The RADIUS server checks the validity of the request, then checks its database of user names and passwords. If the name or password **are not** valid, it sends a rejection to the client, who in turn rejects the login. If the login name and password **are** valid, the RADIUS server sends back a packet containing information about this user, and the client uses this information to decide what type of service to supply for the user.



RADIUS users are treated differently from local users only until authentication comes from the RADIUS server. Once the RADIUS server authenticates a particular user, this RADIUS user enjoys the same privileges as any other local user.

When RADIUS, LDAP, or TACACS are enabled, local user authentication is not provided. If the servers are not reachable, then local user authentication is functional.

### **RADIUS Advantages**

- The RADIUS server has a single, unified “database” of users, allowing for authentication of user names and passwords, as well as for configuration information detailing the type of service to deliver to the user. There is no limit to the number of users; it can store as many users as its disk storage permits.
- If you are using many Dominion SX units, you do not have to configure all users on each of the units. Configure a user once on your RADIUS server, then allow all Dominion SX units authenticate their login requests from the same place.

### **RADIUS Configuration**

- Configure the unit for RADIUS as described in the Enabling RADIUS section that follows.
- Configure your RADIUS server for the logon operation to be successful. The steps to configure a RADIUS server are defined in **Appendix D: RADIUS Server**.
- Log on to the unit as a RADIUS user.

In cases where the RADIUS server fails to respond or is improperly configured, network connectivity is too slow, username or password is misspelled , the following error message appears:



*Figure 60 Unsuccessful Login Message Window*

## Enabling RADIUS

Every unit has to be configured for RADIUS Communication to obtain authentication from the RADIUS Server. Administrators should log on to the unit as any non-RADIUS user, and then configure the unit following these steps to obtain authentication:

1. Click on the **RADIUS** Tab.

Figure 61 RADIUS Configuration Display

2. Check the **Enable RADIUS** check box.
3. In the **Primary Server IP** field enter the address of the RADIUS server.
4. In the **Shared Secret** field, enter the password for the client, which was added while configuring the RADIUS server. Please refer to **Appendix D: RADIUS Server** for additional information.
5. In the **Port** field, enter the port number – by default, the port number is **1812**, and should be modified in case the RADIUS server is configured for a different port number. The early deployment of RADIUS was done using the chosen port number **1645**, which conflicts with the “Datametrics” service. *The officially assigned default port number for RADIUS is 1812.*
6. The Information for the Secondary RADIUS Server is optional. This is a mirrored image of the Primary RADIUS Server and it is used only in case the Primary RADIUS Server fails to respond.
7. Click on the [**Update**] button.
8. Click on the [**Save**] button.

---

### Note:

→ When you factory reset your box, all the RADIUS parameters will be lost.

→ RADIUS users are not cached in the memory. Every time you log on as a RADIUS user, authentication comes from the RADIUS server.

→ The RADIUS client sends a packet to the RADIUS server and waits for a reply. If it does not receive a response within 10 seconds, it resends the packet to the same server. If the Primary RADIUS Server again fails to respond, it contacts the Secondary RADIUS Server, if configured to do so. If it does not receive a response from the Secondary RADIUS Server, it informs the user accordingly. Thus, a user may have to wait for as long as 20 seconds if one or both RADIUS server(s) fail to respond or if the Dominion SX unit is not properly configured.

→ RADIUS users will appear in the **Current users** list in the left panel of the main window, but not in the Users list on the Users configuration screen.

---

## Usage

Once you are logged on to the unit as a RADIUS user, you can check your login name in the Current users list in the left panel. This list contains a list of RADIUS and as well as non-RADIUS users currently logged-in to the unit.

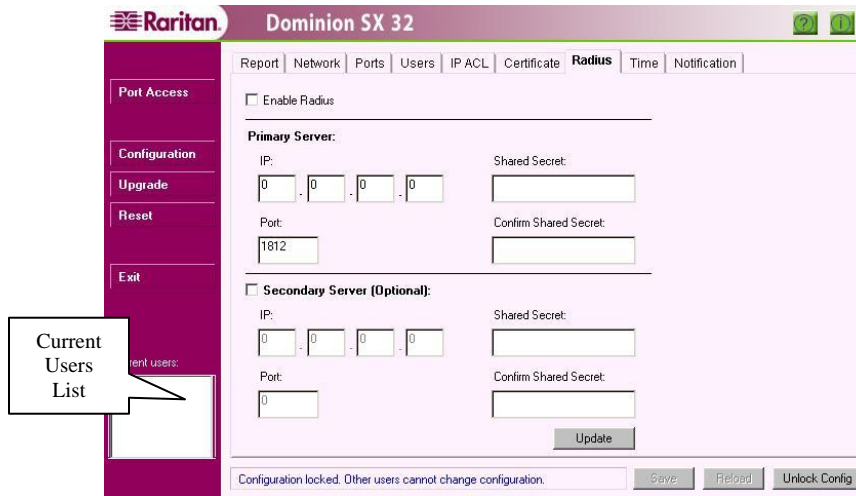


Figure 62 Current Users List

If you have Administrator privileges, you can add new users or edit an existing user. From this stage onwards, there is no difference in behavior between a “local” user and a RADIUS user.

Only non-RADIUS users are listed in the user list on the Users configuration screen under the Users tab. This is because, every time a RADIUS user logs in, authentication comes from the RADIUS server.

## Time

### Overview

The Time configuration screen is important for modifying the time, date, time zone, and NTP server address in the Dominion SX unit. Some features in Dominion SX, for example, Certificate generation, depend on the correct Timestamp, which is used to check the validity period of the certificate.

The screenshot displays the 'Time' configuration page in the Dominion SX 4 web interface. The page is divided into a left-hand navigation menu and a main configuration area. The navigation menu includes options for 'Port Access', 'Configuration', 'Upgrade', 'Reset', 'Exit', and 'Current users'. The main configuration area is titled 'Time' and contains several sections: 'Current Date' with dropdowns for Month (5), Day (16), and Year (2005); 'Current Time' with dropdowns for Hour (16), Min (25), and Sec (2); 'Time Zone' set to '(GMT-05) Eastern Time (US & Canada)'; a checked checkbox for 'Enable Network Time Protocol'; 'Primary Time Server' set to 209.81.9.7; and 'Secondary Time Server' set to 192.43.244.18. An 'Update' button is positioned at the bottom right of the configuration area. At the very bottom of the page, a status bar indicates 'Configuration locked. Other users cannot change configuration.' and includes 'Save', 'Reload', and 'Unlock Config' buttons.

Figure 63 Time Configuration Display

### Configuration

1. Set the Current Date and Current Time.
2. Click **Update**.
3. Click **Save**.

## Notification

### Overview

The Notification configuration screen allows an Administrator to set up notification schemes based on events that occur on the target device. Notification events are sent out as email messages. It is possible to convert the email service to a page so that the notification can be received in a prompt manner. Contact your pager service provider company to find out what email addresses can be used to transmit email messages as pages.

Dominion SX is shipped with a set of predefined notification messages that are based on events that occur within the unit. It is also possible to have user-defined events sent out as email messages. User defined events are defined using the scripting capability.

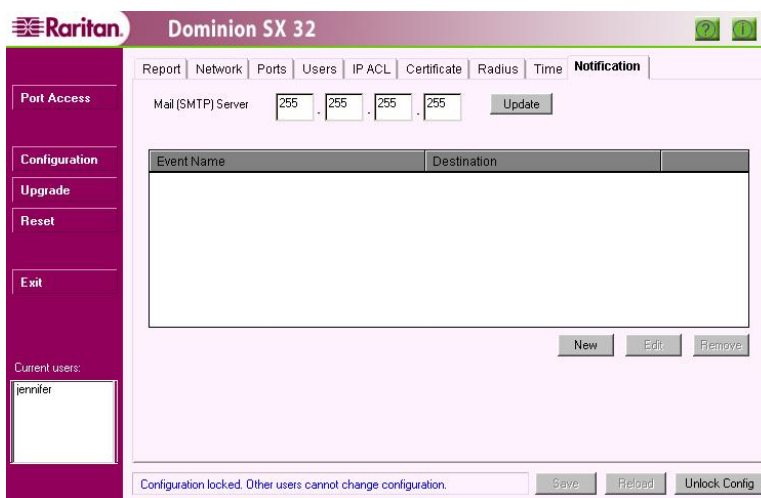


Figure 64 Notification Display

### Configurable Parameters

- **Mail (SMTP) Server:** Type the IP address of the SMTP server. Please ensure that a valid domain name has been set in the Network configuration (e.g., mycompany.com), otherwise SMTP messages may be rejected by certain mail servers including Microsoft Exchange and Sendmail. Type the IP address, click **Update** and then click **Save**. Please note: If the IP address is set to 255.255.255.255 then it will be used to disable the notification task from sending any alerts to the user.
- **Event Name:** Name of event that is to generate an email message, as selected from a predefined list. User-defined events must be entered as they are stated in the TCL scripts.
- **Destination:** Valid email destination address

## Add a New Notification

1. Click on the [New] button.
2. Select the desired event from the **Event Name** drop-down list, for which an email is to be generated. The event list contains events predefined by Raritan. To subscribe to a user-defined event, type the user defined event name.

*Note: This name must match exactly with the event name that has been used when the script was generated.*

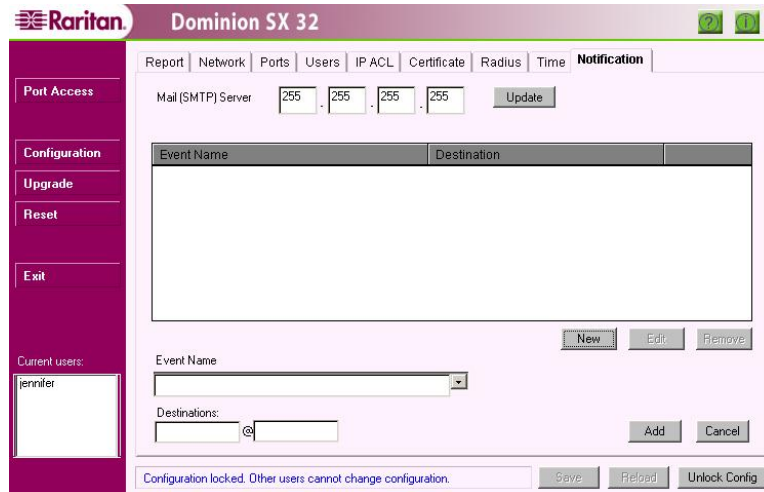
3. Specify the **Destination(s)** as <name>@<domain>.
4. Click on the [Add] button to add this event to the list, or click on the [Cancel] button to discard the changes.
5. Click on the [Save] button.

The screenshot displays the Raritan Dominion SX 32 web interface. The top navigation bar includes tabs for Report, Network, Ports, Users, IP ACL, Certificate, Radius, Time, and Notification. The Notification tab is active. On the left, a vertical menu contains options: Port Access, Configuration, Upgrade, Reset, and Exit. Below this menu, the current user is identified as 'jennifer'. The main configuration area shows the 'Mail (SMTP) Server' field with IP address components (255, 255, 255, 255) and an 'Update' button. A table with columns 'Event Name' and 'Destination' is present, currently empty. Below the table are 'New', 'Edit', and 'Remove' buttons. The 'Event Name' field is a dropdown menu, and the 'Destinations:' field is a text input with an '@' symbol. 'Add' and 'Cancel' buttons are located below these fields. At the bottom, a status bar indicates 'Configuration locked. Other users cannot change configuration.' and includes 'Save', 'Reload', and 'Unlock Config' buttons.

Figure 65 New Notification Display

## Edit a Notification Entry

1. Select the entry to be modified.
2. Click on the **[Edit]** button.
3. Make changes to the entry in the fields that appear in the lower portion of the screen.
4. Click on the **[Update]** button.
5. Click on the **[Save]** button.



The screenshot displays the Raritan Dominion SX 32 web interface. The top navigation bar includes tabs for Report, Network, Ports, Users, IP ACL, Certificate, Radius, Time, and Notification. The left sidebar contains a vertical menu with buttons for Port Access, Configuration, Upgrade, Reset, and Exit. Below the menu, a 'Current users' section shows 'jennifer'. The main content area is titled 'Notification' and features a table with columns for 'Event Name' and 'Destination'. Below the table are 'New', 'Edit', and 'Remove' buttons. A form for editing a notification entry includes an 'Event Name' dropdown menu, a 'Destinations' input field with a '@' symbol, and 'Add' and 'Cancel' buttons. At the bottom, a status bar reads 'Configuration locked. Other users cannot change configuration.' and includes 'Save', 'Reload', and 'Unlock Config' buttons.

Figure 66 Edit Notification Destination

## Delete a Notification Entry

1. Select the entry to be deleted.
2. Click on the **[Remove]** button.
3. Click on the **[Save]** button.

---

**Note:** Click on the **[Reload]** button to recover the deleted item.

---

### **Dominion SX Standard Notification Events**

The following is a list of standard events with their descriptions.

<b>EVENT NAME</b>	<b>DESCRIPTION</b>
event.amp	
event.amp.notice	
event.amp.notice.boot	Unit has successfully booted.
event.amp.notice.reboot	Unit has been requested to be re-booted.
event.amp.notice.upgrade	Unit has been upgraded
event.amp.notice.backup	Unit has been backed up.
event.amp.notice.config	
event.amp.notice.restore	Unit has been restored.
event.amp.notice.config.info	General configuration has been modified.
event.amp.notice.config.user	Access Control List has been modified.
event.amp.notice.config.version	Firmware Version number has been modified.
event.amp.notice.config.system	Port name has been modified.
event.amp.notice.config.network	Network configuration has been modified.
event.amp.notice.config.datacom	Datacom configuration has been modified.
event.amp.notice.config.users	User configuration has been modified.
event.amp.notice.config.ipacl	IP address-based access control list has been modified.
event.amp.notice.config.notif	Notification configuration has been modified.
event.amp.notice.directaccesslockout	Enable Disable local access via CommandCenter
event.amp.notice.port.connection	Target connected to the port has changed state – changed from Offline to Online, or vice-versa.
event.amp.notice.user.logoff	Forces user to log off from unit.

### **Dominion SX Standard Error Notification Events**

The following is a list of standard error events that are internally generated by the unit. Should these notifications occur, please call Raritan Support.

<b>ERROR EVENT NAME</b>	<b>DESCRIPTION</b>
event.amp.error	System related.
event.amp.error.taskInit	System related.
event.amp.error.httpExit	System related.
event.amp.error.outOfMemeory	System related.
event.amp.error.loggingTaskAlreadyDefined	System related.
event.amp.error.ftpReadFailed	System related.
event.amp.error.messagePipeFailed	System related.
event.amp.error.InternalError	System related.
event.amp.error.flashUpgradeFailed	Upgrade failed to write to flash memory.



## Upgrade

The Upgrade feature allows an Administrator to upgrade the Dominion SX unit's firmware/application to a newer version of firmware. Firmware and application upgrades preserve user-defined settings, so the unit does not need to be re-configured after the upgrade procedure is complete.

In order to perform a firmware upgrade, the Administrator must download the upgrades file(s) onto a local FTP server and needs the IP address of the FTP server and the file path to the upgrade file(s). Many upgrades can be performed "anonymously" from the FTP server, and the default settings of this screen are for an anonymous upgrade. However, some FTP servers require a user name and password. If this is the case, the Administrator can uncheck the "Anonymous" box and enter the correct user name and password for the FTP server.

Once the upgrade is initiated, the status bar will indicate the progress of the upgrade and a pop-up window will notify the user once the upgrade procedure is complete.

Figure 67 Upgrade Display

Upgrades can be done of the complete software (AmpAdmin package) and the various applications (AmpApp package) supplied by Raritan. The upgrade steps are similar for both cases.

### To Perform a Complete Software Upgrade:

1. Click on the [Upgrade] button in the left panel.
2. Enter the **IP Address** where the software package is located.
3. Enter the **File Path** to the software package, for example, */pub/Dominion/AmpAdmin*.
4. Enter **FTP Username** and **Password**, if required.
5. Click on the [Upgrade] button.
6. The unit will access the FTP server and download and install the file(s) onto the unit.
7. The unit will automatically reboot after the software is installed.

---

**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.**

---

**To Upgrade the Application:**

Dominion SX has the ability to run different applications on each port; Raritan has a library of applications available for purchase, please contact us for more information.

To load these applications into the unit for deployment:

1. Click on the [**Upgrade**] button in the left panel.
2. Enter the **IP Address** where the software application package is located.
3. Specify the **Path** to the software package, for example, **/pub/Dominion/AmpApp**.
4. Enter the **Username** and **Password** if required.
5. Click on the [**Upgrade**] button.
6. The unit will access the FTP server and download and install the files into the unit.
7. Repeat the above steps for each custom application that has to be installed into the unit.
8. After all applications have been installed, click on the [**Reset**] button.
9. When the unit reboots, log on and go to the **Ports** tab. Select the appropriate ports and configure them to use the correct application.

## Reset

### Soft Reset

Only an Administrator can execute a Soft Reset by clicking on the **[Reset]** button in the left panel of the main window. This resets the unit, logs off all the logged-in users and exits the application. A list of logged-in users who will be logged out upon reset will be displayed. The soft reset is useful when an Administrator wishes to disconnect all users from the unit.

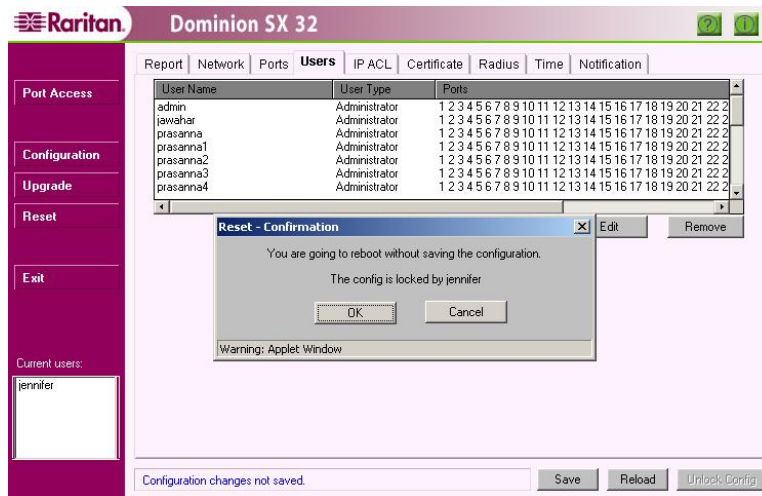


Figure 68 Confirmation for Reset

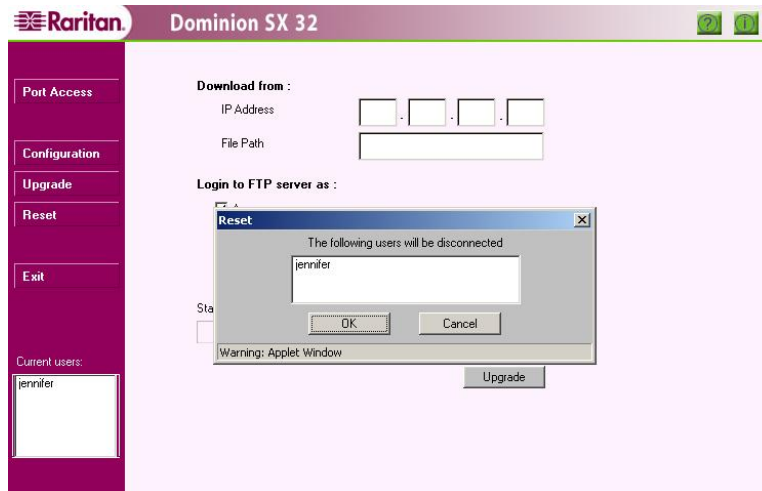


Figure 69 Confirmation on Users to be Disconnected

#### To Perform a Soft Reset:

1. Click on the **[Reset]** button on the left panel.
2. A list of logged-in users, if there are any, is displayed. Click on the **[OK]** button to continue.
3. The unit resets and reboots.
4. Reconnect to the unit.

## Factory Reset

---

You may want to perform a factory reset, or hard reset, to the Dominion SX unit to revert the configuration to known defaults. This is useful if the IP address of the unit is no longer known. Using the following procedure, the network settings of the unit will be reset to the values shown in the table below, and all ports will be reset to 9600 baud, no parity checking, and no flow control.

Internet Address (IP)	192.168.0.192
Gateway Address	192.168.0.192
Subnet Mask	255.255.255.0
Port Address	51000
Port address for CC Discovery	5000
Username	admin
Password	raritan

---

*Note: Factory reset does not remove the user-installed certificate from the unit.*

---

There are two methods for performing factory reset; via CLI, or by using a factory reset adaptor or a reset switch. Both methods are outlined below. When resetting using a factory adaptor or reset switch, it is not necessary to remove the device from all networks (an Administrator should make this decision).

To factory reset via CLI, use the following commands:

```
dominion:Diagnostics> factory_reset
```

Factory Reset Network Settings:

Name: DominionSX

Domain: raritan.com

System Port: 51000

Discover Port: 5000

IP: 192.168.0.192

Net Mask: 255.255.255.0

Gateway: 192.168.0.192

Performing a factory reset will erase ALL system settings.

All system settings will be returned to factory defaults, including network settings (e.g. ip, gateway, et cetera).

Do you wish to continue? (no/yes) (default: no) yes

Reboot the machine; the following text appears:

Welcome to Raritan Dominion Server

Username: admin

Password: raritan

Authenticating [admin].....Authenticated.

User Type [Administrator]

User Name [Administrator]

System is in reset state.

Please enter new administrator password.

New Password:

Re-Enter New Password:

The procedure for performing a factory reset varies depending on the model. For SX16 and SX32 units, the procedure is as outlined below. (For SX4, SX8, and other models with a RESET switch, please see the paragraph that follows):

1. Power OFF the Dominion SX unit.
2. Attach the supplied Factory Reset Connector (serial DB9 female) to the serial DB9 male port on the rear of the unit
3. Power ON the unit.
4. The unit will restore to factory default settings. This process will take approximately 40 seconds.
5. After 40 seconds, reconnect to the unit with the factory default IP address **192.168.0.192**.
6. Unplug the Factory Reset Connector.

---

*Note: It is advisable to remove the unit from the main network while performing a factory reset. Should another device on the network have the IP address of **192.168.0.192**, these two devices will be in conflict.*

---

For SX4, SX8, and other models with a RESET switch on the rear panel, using a ball-point pen (please do not use a graphite pencil), while the unit is powered ON, push in and hold the switch for about 30 seconds (or until the blue LED on the front of the unit goes off), and then release the switch. Only gentle pressure is required. The SX unit will detect the RESET switch and reset the unit to factory default. It will take about 5 seconds for the unit to reboot. On these units, a reset to factory defaults can be performed with the unit powered ON.



Figure 70 Factory Reset Connector Location



# Chapter 5: Using the Command Line Interface with Secure Shell and Telnet

## Secure Shell (SSH) Access

Using a Secure Shell (SSH) client, you can connect and get direct access to the remote target device's console ports. A number of SSH clients are available and can be obtained from the following locations<sup>1</sup>:

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

Once you have obtained and installed an SSH client on your machine, launch the SSH client application. You must enter the appropriate IP address, select **SSH** (which always uses port 22), and click on the **[Open]** button. The example below is done using PUTTY.

Support for SSH is provided in the Dominion SX. By default, the SSHv2 Server is always running. Use any SSH client that supports SSHv2 to connect to it.

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

1. Ensure that the terminal emulation on the host to be accessed is set to VT100.
2. On most UNIX systems, the *env* command can provide the terminal type set on the host. For example, if the terminal type setting on a SUN Solaris server is set to SUN, then the SSH client should also be set to SUN.
3. Also ensure that the character-set in use on the host matches the character-set for the SSH client. For example, if the character-set setting on a SUN Solaris server is set to ISO8859-1, then the SSH client should also be set to ISO8859-1.
4. Ensure that the default Escape sequence set on the Dominion SSH server does not conflict with a key sequence required by either the SSH client or the host operating system. The Escape key sequence is user-configurable.

A Secure Shell (hereinafter, SSH) session can be initiated in two ways:

1. Interactive session - During interactive session, the user provides the commands using menu.
2. Using Command Line Arguments - Using command line mode, all the parameters of a command (including user-name and password) can be provided at the time of invocation of SSH client.

## Interactive Session

---

*Note: CLI commands are the same for SSH and Telnet sessions.*

---

**An SSH session is always started with “dominion” as the login name and IP Address of Dominion SX unit. No password entry is required for this first step.** [Note: This login name is NOT created or /added using Dominion's add user feature, it is a system-defined name for use with SSH/Telnet.]

After an SSH user gets connected with the Dominion SX, then the user is prompted for the authorized user name and password. This user name should have been already created using the Dominion's add-user feature from the HTTP-based configuration menu; it can be local or remote (using RADIUS, TACACS+, or LDAP). After the user name and password is authenticated, then the user is presented with a menu of supported commands in SSH. At this point the user is not connected to any ports.

Operators and Observers are limited in the commands they can execute: help, console\_cmd, list\_ports, user config -> password quit.

---

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

Administrators have access to the following commands currently supported with SSH. Please note that the commands ARE case sensitive:

1. **console\_cmd**: Connect to a serial console target. This command accepts a port number to which the user wants to connect. The serial target is connected at the given port number of Dominion SX unit. It is necessary to enter only the port number. The short form of the command is **lp**. Once the console command has been issued there are additional commands as follows:
  - When a user presses the Escape sequence keys, the control goes to a menu for the console session. The user is presented with a prompt for the console menu (Admin:Port0:Command>). The following commands can be executed from this menu:
    - **send\_break** - intended to be used for SUN targets. It sends “break” command to the serial target (SUN workstation or server).
    - **get\_history** - used to get the history for the console session – from the port buffer, which is accumulating console output even when there is no connected user on that port. Each Dominion SX port has an independent port buffer. The history can be copied and pasted into another program for off-line analysis.
    - **get\_write** – allows users to request write access to the port when in a port-sharing session; shortcut is **gw**.
    - **Help** - displays help for console menu.
    - **Quit** - quits console session and returns to the main menu.

---

*Note: Pressing the <Enter> (Carriage Return) key shall return control back to console session from the console menu.*

---

2. **list\_ports**: displays the list of available ports. Only ports that the user is authorized to see are on the displayed list. The displayed list contains the port name (as assigned by the user to the port) and the application associated with it.
3. **change\_escape**: used to change the escape character used to exit from the serial target session. For example if the user has connected to a serial target at port 2 using “console\_cmd 2”, then the escape character can be used to come back to menu prompt “RaritanCommand>” Default Escape Character is **CTRL** [i.e., Press CTRL key]. The escape character can be a single key or a combination of “Ctrl” key and another key from the following set [‘@’, ‘a – z’, ‘A – Z’, ‘[’, ‘]’, ‘\’, ‘^’, ‘\_’]. Using a single-key for the escape sequence is strongly discouraged.
4. **help** or **h** or **?**: displays the list of supported commands.
5. **user\_list** - displays list of all users who are logged in, their source IP Addresses and any ports they are connected to ; shortcut is **ul**
6. **log** <start|stop|clear|status> - used to start/stop/clear or get status of syslog (use **cfglog** command to configure syslog)
7. **cfglog** <[local <wrap|flat> [FILE SIZE]] | [remote [SERV1] [SERV2]]> - used to configure location and size of syslog (use **log** command to start/stop/clear or get status of syslog); currently, local logging should not be used.
8. **tacacs\_cfg** <enable|disable|status> [<SERVIP> <ServerPort> <keyString>] - used to configure TACACS+ remote authentication and authorization, or to get status.
9. **nfsportlog** <enable|disable|status> [<PREFIX> <SIZE> <SERV1> <SERVDIR> [<SERV2> <SERVDIR2>] - used to configure NFS session/port logging.
10. **snmp** [<<enable|disable> [COMM\_NAME]]<add|del> RECIPIENT>] - configuration of SNMP traps.r
11. **reset**
12. **service** [<telnet|ssh><enable|disable>].
13. **lpa** [<enable|disable|status> [BPS]] – Enable/Disable/Set speed in bits per second (BPS) and show status of local port access (connection of VT100 terminal/PC/workstation with communications software to serial port on SX unit).
14. **diagnostics commands**
15. **modem commands port commands**
16. **network commands**
17. **user config commands**
18. **ipacl** <enable|disable|status>
19. **aclcfg** <[list] | [clear] | [move <pos1> <pos2>] |



```
[del <pos1> [pos2] ] | [add <ip1> <ip2> <denyflag> <logflag>]>
```

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

**20. restore** [ip IP] <login LOGIN> <passwd PASSWD> [path PATH] [file FILE]

**21. logoff** [user NAME] <port PORT>

**22. quit:** exit from SSH session.

---

*Note: Use the standard SSH exit sequence "~." to exit from SSH session at any time.*

---

Some of the usage scenarios using command line SSH client:

Some of the usage scenarios using command line SSH client:

dominion:Command>network

dominion:Network> help

etherspeed:

Force the network speed

[<auto/100FDX>]

failover:

Enable/Disable network failover

[enable/disable] <interval>

network:

Get/Set network parameters.

[name NAME] [domain NAME] [ip IP] [mask MASK] [gw GATEWAY] [port PORT] [discover PORT]

help:

Display help for all commands or one in particular.

[COMMAND]

quit:

Leave the current command context.

dominion:Command>user

dominion:UserCfg> help

idletimeout:

Set the global idle timeout

[timeout]

password:

Set the user password

help:

Display help for all commands or one in particular.

[COMMAND]

quit:

Leave the current command context.

dominion:Command>port

dominion:Port> help

detect:

Enable/Disable the port disconnection detection.

<all|PORT\_NUMBER> [<enable|disable>]

help:

Display help for all commands or one in particular.

[COMMAND]

quit:

Leave the current command context.

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

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

backup example:

```
dominion:Command> backup ip 192.168.51.220 login guest passwd guest_password path . file
backup_file1
```

OK.

dominion:Command>

restore example:

```
dominion:Command> restore ip 192.168.51.220 login guest passwd guest_password path . file
backup_file1
```

Restoring the config settings requires a system restart.

Do you wish to proceed? (yes/no) (default: yes)

Transfer command is part of diagnostics help.

```
#SSH -l dominion <IP Address Of Dominion SX>
```

Welcome to Raritan Dominion Server

Username: admin

password:

Authenticating [admin].....Authenticated.

Type [help] for all commands

Command>help

console\_cmd <port#> [w]

list\_ports

change\_escape

```

help
user_list
log <start|stop|clear|status>
cfglog <[local <wrap|flat> [FILE SIZE]] | [remote [SERV1] [SERV2]]>
tacacs_cfg <enable|disable|status> [<SERVIP> <ServerPort> <keyString>]
nfsportlog <enable|disable|status> [<PREFIX> <SIZE> <SERV1> <SERVDIR> [<SERV2>
<SERVDIR2>]
snmp [<enable|disable> [COMM_NAME]]<add|del> RECIPIENT>]
reset
service [<telnet|ssh> <enable|disable>]
lpa [<enable|disable> [BPS]]
diagnostics commands
modem commands
port commands
network commands
user config commands
ipacl <enable|disable|status>
aclcfg <[list] | [clear] | [move <pos1> <pos2>] |
    [del <pos1> [pos2] ] | [add <ip1> <ip2> <denyflag> <logflag>]>
backup [ip IP] <login LOGIN> <passwd PASSWD> [path PATH] [file FILE]
restore [ip IP] <login LOGIN> <passwd PASSWD> [path PATH] [file FILE]
logoff [user NAME] <port PORT>
quit

```

Command>

Command>list\_ports

User Name [admin]

Total Number Of Ports Available = 6

Port1

Port2-SUN

Port3

Port4

Port5

Port6

Command>

Command>console\_cmd 2 (shortcut would be con 2)

User Type [Administrator]

UserName [admin]

Number Of Accessible Ports = 6

Port# PortName

[1] Port1

[2] Port2-SUN

[3] Port3

[4] Port4

[5] Port5

[6] Port6

Serial Port 2 Connected.

Escape character is Ctrl-\

User [admin] Is Now Master [Write Access Allowed] For This Port.

*[Now user can access serial target connected to port 2 of Dominion SX]*

User Name [test]

Type [help] for all commands

test:Command>?

console\_cmd <port#> [w]

list\_ports

change\_escape

help

user\_list

log <start|stop|clear|status>

cfglog <[local <wrap|flat> [FILE SIZE]] | [remote [SERV1] [SERV2]]>

tacacs\_cfg <enable|disable|status> [<SERVIP> <ServerPort> <keyString>]

nfspportlog <enable|disable|status> [<PREFIX> <SIZE> <SERV1> <SERVDIR> [<SERV2> <SERVDIR2>]

snmp [<enable|disable> [COMM\_NAME]|<add|del> RECIPIENT>]

reset

service [<telnet|ssh> <enable|disable>]

lpa [<enable|disable> [BPS]]

diagnostics commands

modem commands

port commands

network commands

user config commands

ipacl <enable|disable|status>

aclcfg <[list] | [clear] | [move <pos1> <pos2>] |

[del <pos1> [pos2]] | [add <ip1> <ip2> <denyflag> <logflag>]>

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

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

logoff [user NAME] <port PORT>

quit

test:Command>

Inactivity timer logoff of a user:

test:Command>User has been logged out : Your session has been terminated due to inactivity.(System).

User [test] Is Force-Logged-Out From This Session.

User List – shows which users are logged on and port(s) they are connected to – if any. In the example below, user **test** is logged into the Dominion SX but is not currently connected to any port, while user **jennifer** is connected to port 1.

test:Command>ul <<-- note use of short form of the command user\_list

Number Of Users = 2

- 1) test |10:28:36 2005/05/11 |127.0.0.1 Ports:
- 2) jennifer |10:28:50 2005/05/11 |192.168.50.191 Ports: 1

---

**Note:** To view a complete configured user list, use the Users Configuration screen in the Dominion SX interface (please see **Chapter 4: Console Features, Configuration, Users** for additional information).

---

test:Command>

Diagnostics commands:

test:Command>diagnostics

test:Diagnostics> ?

test:Diagnostics> help

factory\_reset:

Reset the unit to default settings.

netstat:

Display current network connections.

Run "help netstat" for more detail.

ping:

See if a host is reachable via IP address.

Run "help ping" for more detail.

traceroute:

Trace the network route to a host.

[-dnrv] [-m max\_ttl] [-p port#] [-q nqueries] [-s src\_addr] [-t tos] [-w wait] host [data size]

log:

Display the system log one screen at a time.

transfer:

Upload the log to a remote FTP server.

[ip IP] <login USER> <password PASSWORD> <path REMOTE\_PATH> <file REMOTE\_FILE>

help:

Display help for all commands or one in particular.

[COMMAND]

quit:

Leave the current command context.

test:Diagnostics>

Ping command:

test:Diagnostics> ping 192.168.50.66

PING 192.168.50.66 (192.168.50.66) 56(84) bytes of data.

Warning: time of day goes back (-8553us), taking countermeasures.

```
64 bytes from 192.168.50.66: icmp_seq=1 ttl=64 time=4.79 ms
64 bytes from 192.168.50.66: icmp_seq=2 ttl=64 time=0.691 ms
64 bytes from 192.168.50.66: icmp_seq=3 ttl=64 time=0.692 ms
64 bytes from 192.168.50.66: icmp_seq=4 ttl=64 time=0.695 ms
64 bytes from 192.168.50.66: icmp_seq=5 ttl=64 time=0.912 ms
```

--- 192.168.50.66 ping statistics ---

```
5 packets transmitted, 5 received, 0% packet loss, time 4043ms
rtt min/avg/max/mdev = 0.691/1.556/4.790/1.619 ms
```

test:Diagnosics>

Traceroute example:

test:Diagnosics> traceroute 192.168.50.66

traceroute to 192.168.50.66 (192.168.50.66), 30 hops max, 40 byte packets

```
1 192.168.50.66 (192.168.50.66) 0.852 ms 1.661 ms 0.843 ms
```

Netstat command example:

test:Diagnosics> netstat

Active Internet connections (w/o servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	192.168.50.228:51000	192.168.50.191:2804	ESTABLISHED
tcp	0	0	192.168.50.228:51000	192.168.50.191:2813	ESTABLISHED
tcp	0	13447	192.168.50.228:443	192.168.50.191:2814	ESTABLISHED
tcp	0	0	localhost:51000	localhost:1043	ESTABLISHED
tcp	0	0	localhost:1043	localhost:51000	ESTABLISHED
tcp	0	0	192.168.50.228:ssh	192.168.50.66:55783	ESTABLISHED

Active UNIX domain sockets (w/o servers)

Proto	RefCnt	Flags	Type	State	I-Node	Path
unix	3	[ ]	STREAM	CONNECTED	340	/dev/log
unix	3	[ ]	STREAM	CONNECTED	333	
unix	3	[ ]	STREAM	CONNECTED	138	/dev/log
unix	3	[ ]	STREAM	CONNECTED	31	

test:Diagnosics>

Modem comands:

test:Command>modem

test:Modem> ?

dialback:

Enable/Disable the modem dial-back. Modem must be enabled for this to work.

[<enable|disable>]

phone:

Get/Set a user's dial-back phone number (in digits only). Pre-requisite modem is enabled and dialback is also enabled.

login [phone number]

modem:

Enable/Disable Modem and PPP settings.

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

help:

Display help for all commands or one in particular.

[COMMAND]

quit:

Leave the current command context.

test:Modem>

admin:Command>network

admin:Network> ?

etherspeed:

Force the network speed

[<auto/100FDX>]

failover:

Enable/Disable network failover

[enable/disable] <interval>

network:

Get/Set network parameters.

[name NAME] [domain NAME] [ip IP] [mask MASK] [gw GATEWAY] [port PORT] [discover PORT]

help:

Display help for all commands or one in particular.

[COMMAND]

quit:

Leave the current command context.

test:Modem>

admin:Command>network

admin:Network> ?

etherspeed:

Force the network speed

[<auto/100FDX>]

failover:

Enable/Disable network failover

[enable/disable] <interval>

network:

Get/Set network parameters.

[name NAME] [domain NAME] [ip IP] [mask MASK] [gw GATEWAY] [port PORT] [discover PORT]

help:

Display help for all commands or one in particular.

[COMMAND]

quit:

Leave the current command context.

## Command Line Arguments Session: Syntax for initiating a Command Line Session

SSH -l dominion -t <IP Address of Dominion SX> "sconsole -u <username> -a <password> -p <port#>"

An example of using this command, with the following parameters:

Dominion IP Address = 192.168.51.225

Username = admin

Password = frst256

Port# = 2

```
$ SSH -l dominion -t 192.168.51.225 "sconsole -u admin -a pass123 -p 2"
```

Authenticating [admin].....Authenticated.

User Type [Administrator]

UserName [admin]

Number Of Accessible Ports = 6



```
Port# PortName
[1] Port1
[2] Port2-SUN
[3] Port3
[4] Port4
[5] Port5
[6] Port6
```

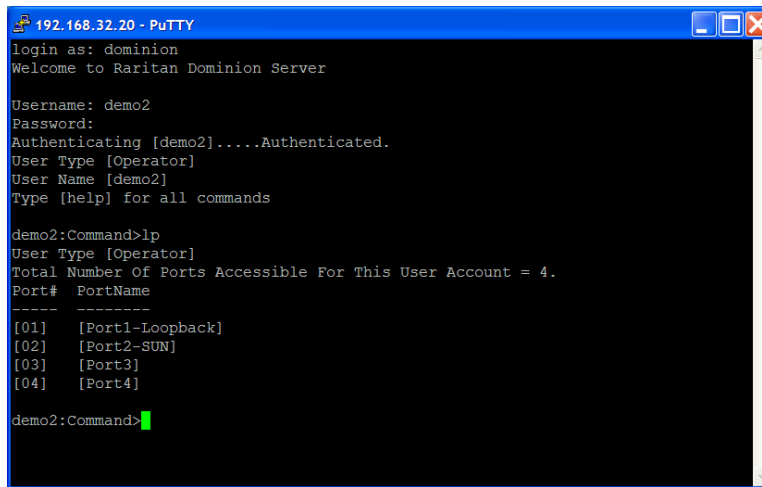
Serial Port 2 Connected.  
Escape character is Ctrl-\

User [admin] Is Now Master [Write Access Allowed] For This Port.

---

*Note: After the serial target is connected, the escape character can be used to exit from the serial target session and come back to “**Command>**” prompt for an interactive session.*

---



```
192.168.32.20 - PuTTY
login as: dominion
Welcome to Raritan Dominion Server

Username: demo2
Password:
Authenticating [demo2]....Authenticated.
User Type [Operator]
User Name [demo2]
Type [help] for all commands

demo2:Command>lp
User Type [Operator]
Total Number Of Ports Accessible For This User Account = 4.
Port# PortName
-----
[01] [Port1-Loopback]
[02] [Port2-SUN]
[03] [Port3]
[04] [Port4]

demo2:Command>
```

Figure 71 Sample SSH Session Screen

## Port Sharing Using SSH

It is possible for SSH users to share ports with other authenticated and authorized users, regardless of whether they are SSH users or SSL (GUI) users. This capability is used for training or for troubleshooting applications.

SSH users are notified in real time if they have Write access or Read Only access at any point during the port-sharing session, and can request Write permission to a port by issuing the command:

**con 2 w** (or the full command **console\_cmd 2 w**)

or by using the **get\_write** command from the **console\_cmd** sub menu.

---

**Important: Only Administrators and Operators have capabilities to obtain write access**

---



## Chapter 6: Authentication and Authorization

If you selected LDAP as your remote authentication protocol, use the steps in the following section, **Implementing LDAP Remote Authentication**, to complete fields in the LDAP tab.

1. Before starting the configuration of the LDAP authentication section in the Dominion SX configuration, please gather all information for the required fields from the administrator of the directory server.
2. Log on as a user with Admin privileges. Click on the **Configuration** tab, and then select the **LDAP** tab.
3. Enter the IP Address of your primary and secondary remote authentication servers in the **Primary Server IP Address** and **Secondary Server IP Address** fields.
4. Enter the server secret/password needed to authenticate against your remote authentication servers in the **Secret Phrases** field. Re-type the server secret in the **Confirm Secret Phrase** field.
5. When finished, click **Update** and then click **Save** to save the changes made to the LDAP tab.

### Implementing LDAP Remote Authentication

---

**Important: Microsoft Active Directory functions natively as an LDAP authentication server.**

---

If you choose LDAP authentication protocol, complete the LDAP fields as follows:

- **Use Secure LDAP** – Apply this rule to enable LDAP(S), which ensures that all authentication requests and replies transmitted over the network are encrypted. Generally, LDAP uses TCP port 389, and LDAP(S) uses TCP port 636.
- **Secret** – This is the root password to access the directory server/manager. The name for this field depends on the Directory Server. The SUN iPlanet directory server uses *Secret*. Microsoft Windows Active Directory refers to it as the *password*.
- **Base DN** – This is the 'root' point to bind to the server; this is same as Directory Manager DN (e.g., BaseDn: cn=Directory Manager)
- **Base Search** – This 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. (e.g., BaseSearch: dc=raritan, dc=com).
- **Authorization Query String** – This can be any string. But, the same string needs to be added as an attribute under BaseSearch domain. For example, if the authorization query string is **DominionSX**, then an attribute named **DominionSX** needs to be added under the given domain specified by BaseSearch field. The values for this attribute are similar to as mentioned for RADIUS in Appendix C of the Dominion SX user manual.

***For example:***

o:\* gives access to all ports and the user type is Operator.  
o:1:2:3 gives access to ports 1,2,3 and user type is Operator  
ob:\* is for Observer  
a:\* is for Administrator

Consult your authentication server administrator for the appropriate values to type into these fields in order to process LDAP authentication queries from Dominion SX.

**If you have any questions at this point, please contact your LDAP server administrator or Raritan Customer Support.**

## TACACS+ Server Configuration

- 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 parameters are **port-list** and **user-type**.
- **port-list**: Specifies the ports that the user has access to. Currently, the only valid value is a space-separated list of port numbers. Multiple port-list parameters are allowed. All port-list values will be combined.
- **user-type**: A string representing the type of Dominion SX user. Currently: Administrator, Operator, and Observer.

For Dominion SX, both per port Authentication and Authorization are possible with TACACS+

### Cisco Freeware Daemon:

This daemon is freely available from Cisco at <http://www.cisco.com>.

Many other TACACS+ implementations are also based on the Cisco server.

No special steps are required to add the new service or parameters. Simply place them in the user database for each user that will be accessing a Dominion SX system. Below is an example of user and group usage:

```
group = anyone
{
  service = dominionsx {
    port-list = "1 2 3 4 5"
    user-type = observer
  }
}

user = tanaka
{
  login = cleartext "password"
  member = anyone
}

user = proctor
{
  login = cleartext "password"
  service = dominionsx {
    port-list = "1 2 3 4 5 15"
    user-type = administrator
  }
}
```

**Cisco Secure ACS:**

These instructions have been written for version 3.2.

Please refer also to the following URL:

[http://cisco.com/en/US/products/sw/secursw/ps2086/products\\_user\\_guide\\_chapter09186a008007cd49.html#12231](http://cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a008007cd49.html#12231)

1. Allow new services.
  - a. Select **Interface Configuration**.
  - b. Select **TACACS+ (Cisco IOS)**.
  - c. Add **dominionsx** service under the heading **New Services**.
2. When adding or editing a user or group, the **dominionsx** service will appear under the heading **TACACS+ Settings**. It can be enabled per user or per group by selecting the **dominionsx** and **Custom Attributes** check boxes. Add the attributes (port-list and user-type) and the appropriate values to the text box.



## Chapter 7: Logging

### NFS Per Port Logging Configuration Usage

#### Name

---

```
nfsportlog <enable/disable/status> [<PREFIX> <SIZE> <IP1> <DIR>
[<IP2> <DIR2>] ]
```

#### Description

---

Set the configuration parameters for logging all Port Activity to a NFS shared directory. All user activity and user port login/logouts are logged.

**nfsportlog status** will show the current configuration parameters.

**nfsportlog enable** will enable nfs per-port logging.

**nfsportlog disable** will disable nfs per-port logging.

[<PREFIX> <SIZE> <IP1> <DIR> [<IP2> <DIR2>]] are parameters that should be set once to ensure operation of the per-port logging.

<PREFIX> - the filename prefix prepended to each of the port log files.

<SIZE> - the maximum size for a log file, before a new file is created.

<IP1> - the IP address of the NFS shared directory

<DIR1> - the directory on the NFS server to write to.

<IP2> - Optional secondary NFS server to write to

<DIR2> - Optional secondary NFS server's directory to write to.

The Per-port log filename follows the following pattern:

<PREFIX>-<PortName>-<Timestamp>.

When the log file reaches <SIZE> it will create a new file with a new timestamp and start writing the port data into that file.

*Example:*

**nfsportlog status**

-display NFS port logging configuration parameters

**nfsportlog enable DomSX1 100000 192.168.111.11 /nfs/domlogging/**

-enable port logging into at the NFS server 192.168.111.11:/nfs/domlogging, with the filename starting with DomSX1.

**nfsportlog disable**

-disable the port logging facility

## NFS Server Setup

The NFS server must have the exported directory with write permission for the port logging to work. Because the per-port logging application runs at a privileged level, the NFS server used must also be set up to allow **root** access. To allow this kind of access you can do it one of two ways.

1. Set the **no\_root\_squash** option for the directory set up to receive the port log files. Example **/etc/exports** entry:  
**/nfs/domlogging 192.168.0.0/16** (rw, no\_root\_squash)
2. Force all accesses to a certain UID/GID. Example **/etc/exports** entry:  
**/nfs/domlogging 192.168.0.0/16** (rw, all\_squash, anonuid=700, anongid=700)

Make certain that the GID/UID pair has write permission to the particular directory.

Explaining these concepts or providing other information about NFS is beyond the scope of this document. Please provide your Systems Administrator with the above information, and ask them any additional questions about setting up the NFS server; should they have any additional questions, please contact Raritan support.



## Chapter 8: SNMP

### SNMP Trap Configuration

The Raritan Enterprise MIB can be accessed via the FAQ Support section on Raritan's Web site, [www.raritan.com](http://www.raritan.com).

#### Name

---

**snmp** [<enable|disable> [COMM\_NAME]]<add|del> RECIPIENT<>]

#### Description

---

Configure the SNMP feature.

##### **snmp**

With no parameters, the current SNMP configuration is displayed.

**snmp** <enable|disable> [COMM\_NAME]

Depending on the parameter, enable or disable SNMP traps. Specify the community name used to send traps using the optional COMM\_NAME parameter.

**snmp** <add|del> RECIPIENT

Add or delete 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.

**NOTE:** At this time, the Dominion SX system must be rebooted for configuration changes (other than disabling SNMP) to take effect.

*Example:( in this example, the username is TANAKA)*

TANAKA:Command>**snmp**

Enabled: N

Community: public

Trap Destinations:

10.0.0.125

6.6.6.6

TANAKA:Command>**snmp add 10.0.0.56 78**

Any SNMP configuration changes require rebooting to take effect.

TANAKA:Command>**snmp**

Enabled: N

Community: public

Trap Destinations:

10.0.0.125

6.6.6.6

10.0.0.56:78

TANAKA:Command>**snmp del 10.0.0.56**

Any SNMP configuration changes require rebooting to take effect.

TANAKA:Command>**snmp del 10.0.0.56 78**

Any SNMP configuration changes require rebooting to take effect.

TANAKA:Command>**snmp**

Enabled: N

Community: public

Trap Destinations:

10.0.0.125

6.6.6.6

TANAKA:Command>**snmp enable**

Any SNMP configuration changes require rebooting to take effect.

TANAKA:Command>**snmp**

Enabled: Y

Community: public

Trap Destinations:

10.0.0.125

6.6.6.6

# Chapter 9: System Configuration

## Local Port Access Configuration

### Name

---

**lpa** [<enable|disable> [BPS]]

### Description

---

Configure the Local Serial Port Access feature.

#### **lpa**

With no parameters, the current LPA configuration is displayed.

#### **lpa** <enable|disable>

Depending on the parameter, enable or disable usage of the serial port for LPA.

#### **lpa** <enable|disable> BPS

Enable or disable LPA as above, but the optional port speed is set.

---

*Note: On older SX 4 and SX 8, and other SX units with only **one** serial port, the serial port labeled MODEM has to be shared between modem and local port access usage. The modem must be **disabled** before LPA can be enabled and vice versa. Newer SX 4 and SX 8 units may have two serial ports; with firmware release 2.2 the port labeled MODEM has to be used for connecting a local VT100 terminal or PC/workstation/laptop with HyperTerminal or other VT100 terminal emulation program.*

---

Valid port speeds are:

- 4800
- 9600
- 19200
- 38400
- 57600
- 115200

*Example: ( in this example, the username is TANAKA)*

TANAKA:Command>**lpa**

Local Port Access Enabled: No

BPS: 9600

TANAKA:Command>**lpa enable**

Local Port Access Enabled: Yes

BPS: 9600

TANAKA:Command>**lpa enable 38400**

Local Port Access Enabled: Yes

BPS: 38400

TANAKA:Command>**lpa disable**

Local Port Access Enabled: No

BPS: 38400

---

*Note: If the user issues the command **lpa enable** AFTER changing the default port speed, the next time the command **lpa enable** is used without the optional port speed parameter, the port speed last set, e.g., 38400, will be used as a default; to override it, enter the **lpa enable** command with the new port speed explicitly specified, e.g., **lpa enable 9600***

---

## Name

---

reset

## Description

---

reboots unit, which may be required after some configuration changes, and may also be used to log-off all users

## Service (Telnet and SSH) Configuration

**IMPORTANT NOTE:** Telnet service should only be enabled when Dominion SX server's default TCP port is NOT set to 23, otherwise the unit will become unresponsive to **http** and **ssh** clients. If the unit is currently set to port 23, please **change** it to 2200-2400 range **BEFORE** enabling Telnet. **For Dominion SX units that are already running firmware version 2.2.4 or higher, the default port is 51000 and telnet can be enabled at any time.**

---

*Note: The Dominion SX system must be restarted for changes to the service configuration to take effect.*

---

To check what port the unit is currently installed on, please log into the unit using a browser, and click on the Configuration button on the left hand side of the screen. Sample output is shown below:

System Time: Fri Jul 16 16:25:41 2004  
 Ethernet Address: 00:60:e0:81:40:a8

Network Configuration:  
 Address IP: 192.168.51.227 (C0A833E3)  
 Subnet mask: 255.255.255.0 (FFFFFF00)  
 Gateway: 192.168.51.137 (C0A8337E)  
 Port Address: 2300                      ←*This is the port number*

## Name

---

service [<telnet|ssh> <enable|disable>]

## Description

---

Configure the SSH and Telnet access.

### service

With no parameters, the current service configuration is displayed.

### service telnet <enable|disable>

Depending on the parameter, enable or disable telnet access.

### service ssh <enable|disable>

Depending on the parameter, enable or disable SSH access.

*Example:*

TANAKA:Command>**service**

Telnet Enabled: No

SSH Enabled: Yes

TANAKA:Command>**service telnet enable**

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

TANAKA:Command>**service ssh disable**

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

TANAKA:Command>**service**

Telnet Enabled: Yes

SSH Enabled: No



## Appendix A: Specifications

ITEM	DIMENSIONS (W) x (D) x (H)	WEIGHT	POWER
SX4	11.34" x 10.7" x 1.75" 288 x 270 x 44mm	4.61 lbs (2.08 kg)	110/220V auto-switching: 50-60 Hz
DSXB-4-DC	11.34" x 10.7" x 1.75" 288 x 270 x 44mm	4.61 lbs (2.08 kg)	
DSXB-4-DCM	11.34" x 10.7" x 1.75" 288 x 270 x 44mm	4.81 lbs (2.17 kg)	
DSXB-4-M	11.34" x 10.7" x 1.75" 288 x 270 x 44mm	4.61 lbs (2.08 kg)	
SX8	11.34" x 10.7" x 1.75" 288 x 270 x 44mm	4.81 lbs (2.17 kg)	110/220V auto-switching: 50-60 Hz
DSXB-8-DC	11.34" x 10.7" x 1.75" 288 x 270 x 44mm	4.81 lbs (2.17 kg)	
DSXB-8-DCM	11.34" x 10.7" x 1.75" 288 x 270 x 44mm	5.0 lbs (2.17 kg)	
DSXB-8-M	11.34" x 10.7" x 1.75" 288 x 270 x 44mm	4.81 lbs (2.17kg)	
SX16	17.25" x 11.34" x 1.75" 438 x 288 x 44mm	9.57 lbs (4.35 kg)	110/220V auto-switching: 50-60 Hz
SX-16-DC	17.25" x 11.41" x 1.75" 438 x 290 x 44mm	8.2 lbs (3.75 kg)	
SX32	17.25" x 11.34" x 1.75" 438 x 288 x 44mm	10 lbs (4.53 kg)	110/220V auto-switching: 50-60 Hz
DSXA-32-AC	17.25" x 11.34" x 1.75" 438 x 288 x 44mm	10 lbs (4.53 kg)	
DSXA-32-DC	17.25" x 11.34" x 1.75" 438 x 288 x 44mm	10.0 lbs (4.53 kg)	
SX48	11.41" x 17.32" x 1.75" 290 x 440 x 44mm	8.77 lbs (3.98 kg)	110/220V auto-switching: 50-60 Hz
DSXA-48-DC	17.32" x 11.41" x 1.75" 440 x 290 x 44mm	8. lbs (4.04 kg)	
DSXA-48-AC	17.32" x 11.41" x 1.75" 440 x 290 x 44mm	8. lbs (4.04 kg)	

### General

Models: SX4, SX8, SX16, SX32, SX48

Power Requirements: 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

Network: One (1) or two (2) 10/100 Ethernet Base-T; RJ-45 connection

Modem: Dedicated Modem DB9M Port - many models; Integrated 56K V.92 (RJ11 port) many models

Protocols: TCP/IP, RADIUS, SNMP, SMTP, PAP, TACACS+, NFS, HTTP, HTTPS, SSL, SSH, PPP, NTP, LDAP, LDAP(S)

**Browser Requirements (Tested)**

PLATFORM	BROWSER
Netscape 7.0	Win 2K - SUN JRE 1.4.2
Netscape 7.1	Win 2K - SUN JRE 1.4.2
Mozilla 1.6	Win 2K - SUN JRE 1.4.2
IE 6.0	Win XP - MS VM
Netscape 7.0	Win XP - SUN JRE 1.4.2
Netscape 7.1	Win XP - SUN JRE 1.4.2
Mozilla 1.6	Win XP - SUN JRE 1.4.2
FireFox 1.0.4	Win XP - SUN JRE 1.4.2
Netscape 7.1	RedHat8
Mozilla 1.6	RedHat8
Netscape 7.1	RedHat9
Mozilla 1.6	RedHat9
IE 6.0, Netscape 7.0, Netscape 7.1, Mozilla 1.6	Win 2K - SUN JRE 1.4.3
IE 6.0, Netscape 7.0, Netscape 7.1, Mozilla 1.6	Win XP - SUN JRE 1.4.3

**Dominion SX Connectivity and Serial Pin-Out Guides****Connectivity Table**

This table lists the necessary Dominion SX hardware (adapters and/or cables) for connecting Dominion SX to common Vendor/Model combinations:

VENDOR	MODELS	CONSOLE CONNECTOR	SERIAL CONNECTION
Checkpoint	Firewall	DB9M	ASCSDB9F adapter and CAT5 cable
Cisco	PIX Firewall	DB9M	ASCSDB9F adapter and CAT5 cable
Cisco	Catalyst	RJ45	CRLVR-15 cable; or CRLVR-1 adapter cable
Cisco	Router	DB25F	ASCSDB25M adapter and CAT5 cable
Hewlett Packard	Unix Server	DB9M	ASCSDB9F adapter and CAT5 cable
Silicon Graphics	Origin	DB9M	ASCSDB9F adapter and CAT5 cable
Sun	SPARCStation	DB25F	ASCSDB25M adapter and CAT5 cable
Sun	Netra T1	RJ45	CRLVR-15 cable
Sun	Cobalt	DB9M	ASCSDB9F adapter and CAT5 cable
Various	Windows NT	DB9M	ASCSDB9F adapter and CAT5 cable
Raritan	RPCU	RJ45	CSCSPCS-10 cable or CSCSPCS-1 adapter cable



## Dominion SX Serial Pinouts

The RJ45 connector on the rear of the unit has the following pinout:

RJ45 PIN	SIGNAL
1	RTS
2	DTR
3	TxD
4	GND
5	Signal GND
6	RxD
7	DSR
8	CTS



## Appendix B: System Defaults

Dominion SX system defaults, as shipped from Raritan, are defined in the table below.

ITEM	DEFAULT
IP Address	192.168.0.192
Subnet Mask	255.255.255.0
Port Address	51000
Port address for CC discovery	5000
Factory default username	admin
Factory default password	raritan
GENERAL SETTINGS	
Modem	Disabled
RADIUS	Disabled
LDAP	Disabled
NTP	Disabled
Local Port Access	Enabled
Syslog	Disabled
TACACS+	Disabled
Event Notification	Disabled
Dialback	Disabled
IP-ACL	Disabled
Telnet	Disabled
SSH	Enabled
SNMP	Disabled
Logging to NFS	Disabled
SERIAL PORTS	
Baud Rate	9600
Parity	None
Flow Control	None

To initiate access using http, Ports 80, 443 and 51000 (can be configured) must be kept open in the firewall in order for the unit to be operational. When using https SSL(S) only, TCP port 443 needs to be open; port 80 can be closed. For SSH access, TCP port 22 needs to be open; for Telnet access, port 23 needs to be open.

Please note that you may need to open additional ports when using syslog, FTP (used in firmware upgrades from the GUI), NFS logging, LDAP servers, etc. These ports may vary from installation to installation, depending on network topologies, VLANs, and firewall configurations. Please contact your network administrator for site-specific information and settings.



## Appendix C: Certificates

### Certificate

A Certificate is an electronic document that is used to identify an individual, a server, or some other entity and to associate that identity with the public Key.

### Certificate Contents

This section discusses certificate contents and the differences between the CA (Certificate Authority) Certificate and the Server Certificate that are present on the Dominion SX unit.

A Certificate is an association of the public key with the real identity of an individual, server, or other entity. It contains information identifying data and a public key (a distinguishing name). The certificate also contains the identification and signature of the certificate authority that issued the certificate, and holds administrative information for the CA's use, such as version number, serial number, issuer name, etc.

#### To View the Certificate:

1. Click on **File** in the main menu.
2. Select *Properties* from the drop-down menu.
3. Click on the [**Certificates**] button.
4. Click on the **Details** tab.

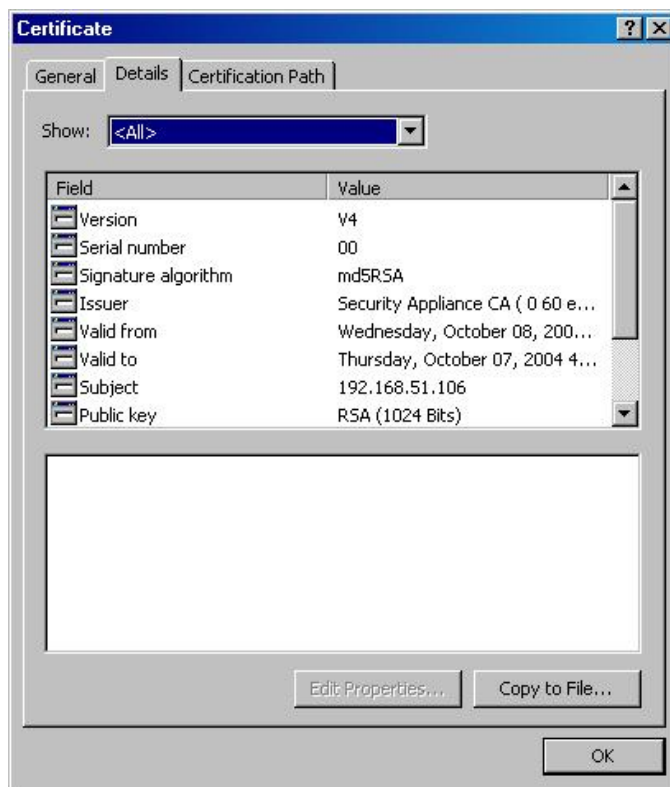


Figure 72 Administrative Information

---

**Note:** You can also click on the security icon on the browser to view the information.

---

## Certificate Authority

Certificates are issued by Certificate Authorities (CAs), such as Verisign, Thawte, Baltimore, and others. These certificate authorities validate the identity of the individual/entity before issuing the certificate. A Certificate Authority signs all certificates that it issues with its private key and the CA certificate contains the corresponding public key. A browser must contain this CA Certificate in its **Trusted Root Library** in order to “trust” certificates signed by the CA's private key. For additional information, please see <http://www.cren.net/ca/>.

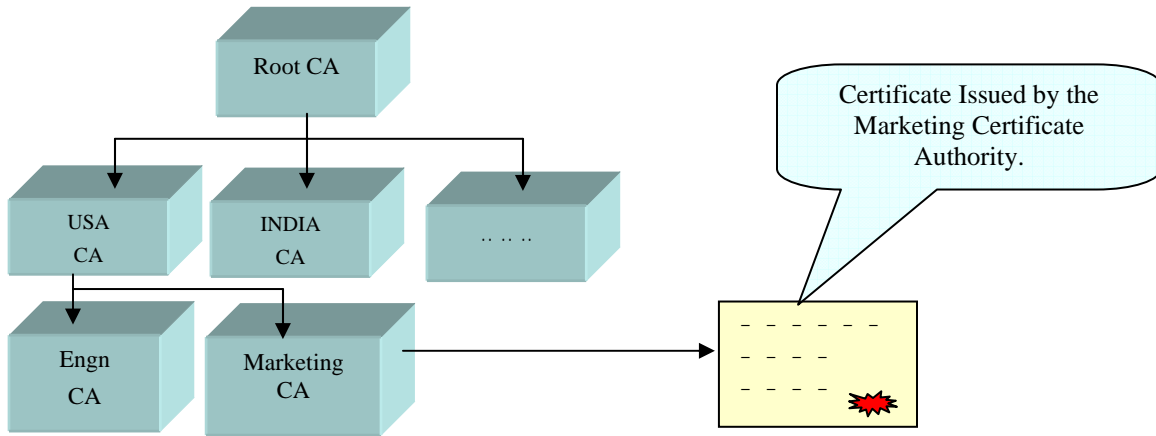


Figure 73 Hierarchies of Certificate Authorities

## Installing Dominion SX CA-Root Certificate to a Browser

The CA Root Certificate generated in the Dominion SX unit must be installed in the browser in order for the browser to trust the Server Certificate. When the user connects to the Dominion SX unit by entering the IP address in the browser, the Server Certificate is downloaded. The browser then checks if the Root Certificate is present in its CA list, which indicates signed Server Certificates. If the verification is successful, the Security Alert will not appear.

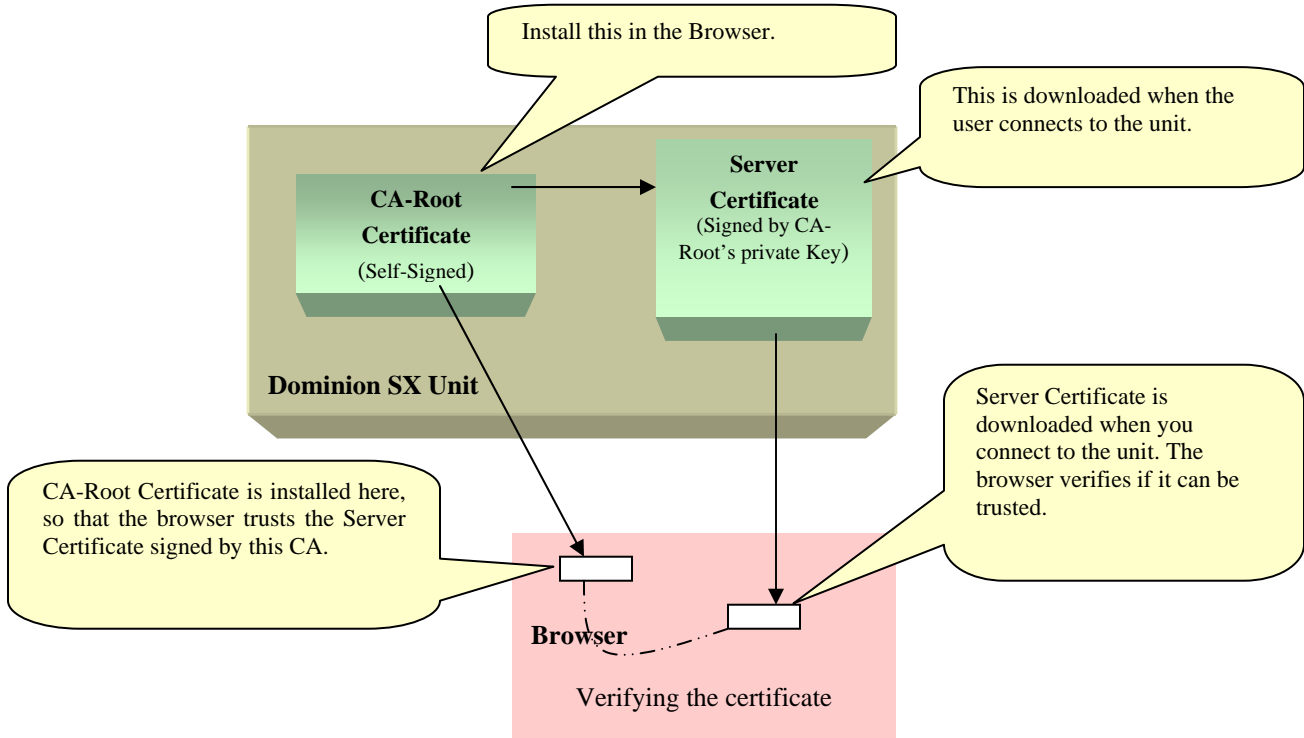


Figure 74 Schematic Diagram of Certificate Authentication Scheme

## Installing CA Root for IE Browsers

Each time you access an SSL-enabled Dominion SX unit, you will see a New Site Certificate window. Eliminate this window's appearance by either accepting a session certificate permanently or by installing the appropriate root certificate in your browser. These instructions apply if you use Internet Explorer. For Netscape Navigator instructions, please see the next section.

### Accept a Certificate (Session-Based)

Accepting a certificate from a particular unit means that the Security Alert window will not appear on your screen when accessing that particular unit. You will have to repeat the acceptance process for each Dominion SX unit you wish to access in order to eliminate the Security Alert window. To eliminate the appearance of this window for every Dominion SX unit with a particular certificate, you must install the root certificate in your browser, described in the *Install the Raritan Root Certificate* section that follows.

1. Open IE and connect to the Dominion SX unit's IP address. The Security Alert window will appear.
2. Click on the [View Certificate] button and the Certificate window will appear.



Figure 75 Install Session Based Certificate

3. Click on the [Install Certificate] button. This will install the certificate for the current session.

When the session closes, this certificate will expire and will have to be reloaded upon with the next connection.

### Install the Raritan Root Certificate

By installing the Raritan root certificate in IE, you can prevent the Security Alert window from appearing whenever you access any SSL-secured Dominion SX unit.

1. Open IE and connect to the Dominion SX unit. Enter **Username** and **Password** when prompted, and log on to the unit.
2. Click on **Configuration** button in the left panel and then click on the **Certificate** tab. The [Remove User Certificate] button should be inactive, indicating that a third-party certificate has not been installed and that the certificate in use is the Raritan default certificate.
3. Click on the [View Certificate] button. The code for the Raritan certificate should appear in the **Certificate** field.
4. Select the text in the **Certificate** field and copy it.
5. Paste the text into a text editor such as Notepad or WordPad, and save it as a **CA\_ROOT.cer** file on your desktop.



- Open the CA\_ROOT.cer file by double-clicking on it. This will open the certificate.

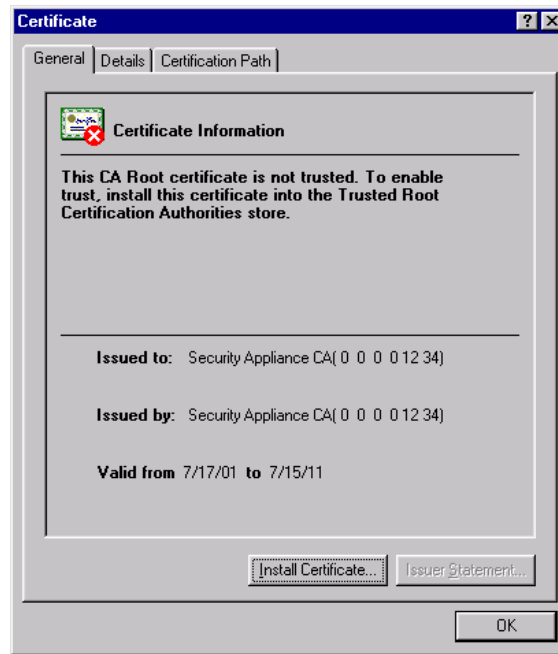


Figure 76 View of CA\_ROOT.cer

- Click on the [Install Certificate] button to start the Certificate Manager Import wizard.



Figure 77 Certificate Manager Import Wizard

- Click on the [Next] button.

9. Select the **Certificate store**, the system area where the certificates are stored. 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 on the **[Browse]** button to choose a file you prefer.



Figure 78 Import Wizard, Select a Certificate Page

10. Click on the **[Next]** button.
11. Click on the **[Finish]** button



Figure 79 Certificate Manager Import Wizard, Completion Page

12. After installing the certificate, close all IE Browsers and open 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

Removing a certificate that you have previously accepted from the unit is the same process whether removing an Raritan default certificate or a user-installed third-party certificate.

1. Open IE and select **Tools**→**Internet Options** from the main menu. The Internet Options window will appear.



Figure 80 Internet Options Display

2. Click on the **Content** tab and click on the [**Certificates**] button. The Certificates Manager window will appear

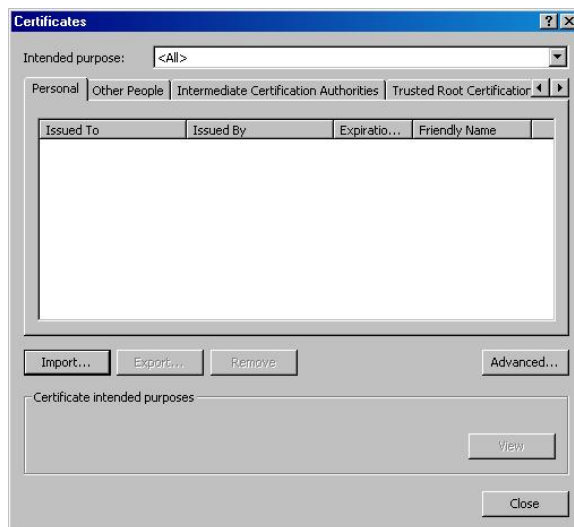


Figure 81 Certificate Manager Display

3. Scroll through the list of certificates and click on the certificate to be deleted.
4. Click on the [**Remove**] button.
5. Click on the [**Close**] button.
6. Click on the [**OK**] button.

## Install CA Root for Netscape Navigator

Each time you access an SSL-enabled Dominion SX unit, you will see a New Site Certificate window. Eliminate this window's appearance by either accepting a session certificate permanently or by installing the appropriate root certificate in your browser. These instructions apply if you use Netscape Navigator.

### Accept a Certificate (Session-Based)

Accepting a certificate from a particular unit means that the New Site Certificate will no longer appear on your screen when accessing that particular unit. You must repeat the acceptance process for each Dominion SX unit you wish to access. To eliminate the appearance of this window for every Dominion SX unit with a particular certificate, you must install the root certificate in your browser, described in the Install the Dominion SX Root Certificate section that follows.

1. Open Netscape Navigator and connect to the IP address of the Dominion SX unit. The New Site Certificate window will appear:



Figure 82 Netscape New Site Certificate Window

2. Click on the [Next] button, and then click on the [Next] button again.
3. Select the **Accept this certificate forever (until it expires)** radio button.



Figure 83 Netscape New Site Certificate Acceptance Window

4. Click on the [Next] button in this window, click on the [Next] button in the next window, and then click on the [Finish] button. The Raritan default certificate is now accepted on this computer.

## Install the Dominion SX Root Certificate

Install the Raritan root certificate in Netscape Navigator to eliminate the New Site Certificate window from appearing whenever you access any SSL-secured Dominion SX unit.

1. Open Netscape Navigator and connect to the unit. Enter **Username** and **Password** when prompted and log on to the unit.
2. Click on the [**Configuration**] button in the left panel and click on the **Certificate** tab. The [**Activate Default Certificate**] button should be inactive, indicating that a third-party certificate has not been installed and the Raritan default certificate is the certificate in use.

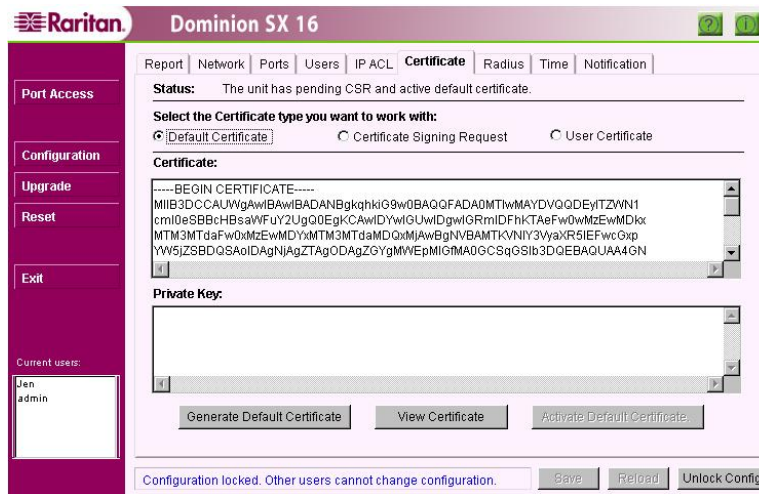


Figure 84 Viewing the Certificate

3. Click on the [**View Certificate**] button. The code for the Raritan certificate should appear in the **Certificate** text field.
4. Select the text in the **Base64 Certificate** field and copy it by selecting **Edit**→**Copy** from the main menu.
5. Open Notepad or another text editor and paste the text you have copied into the editor by selecting **Edit**→**Paste** from the main menu.
6. Save this file using the file name of your choice, onto your desktop, making certain to save it with the **cert** extension, for example, **root\_certificate.cert**
7. In Netscape Navigator, select **Edit**→**Preferences** from the main menu. On the left side of the Preferences window, click on the [**Navigator**] button and select *Applications*.
8. Scroll down to the bottom of the list of file types. Look for a file type with a name similar to **x509 Digital Certificate** - you should not find such a listing: if you do, please skip to Step 13.
9. Click on the [**New Type**] button. The New Type window will appear:

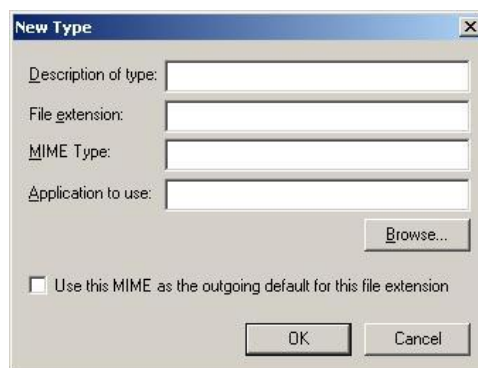


Figure 85 Netscape New Type Window

- a. **Description of type:** Enter x509 Digital Certificate
- b. **File extension:** Enter x509

- c. **MIME Type:** Enter application/x-x509-ca-cer
  - d. **Application to use:** Click on the [**Browse**] button and locate the Netscape Navigator executable, **netscape.exe**, on your hard drive. Select this executable and click on the [**Open**] button. The path to the Netscape executable, in quotes, will populate the Application to use field. After the end quotation mark, insert a space and type **%1**.
  - e. Click on the [**OK**] button and click on the [**Close**] button to close the Preferences window.
10. Click on the icon of the root certificate file you saved in Step 6 and drag it into an open Netscape Navigator window. The New Certificate Authority window should appear.
  11. Click on the [**Next**] button.
  12. Click on the [**Next**] button once more.
  13. The Certificate Fingerprint should be displayed. Next to **Signed by** should appear **Security Appliance CA**. Click on the [**Next**] button.
  14. Click on the first **Accept this Certificate Authority for Certifying network sites** checkbox. The second and third boxes are optional.



Figure 86 Netscape New Certificate Authority Window

15. Click on the [**Next**] button in this screen, and click on the [**Next**] button in the next screen. When prompted to enter a name for the Certificate Authority, type **Security Appliance CA**. Click on the [**Finish**] button. The Raritan default root certificate is now installed.

## 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. Open Netscape Navigator and click on either the [**Security**] button or on the lock icon in the lower left of the window. The Security Info window will appear.
2. On the left side of this window, locate Certificates and click on **Web Sites**.

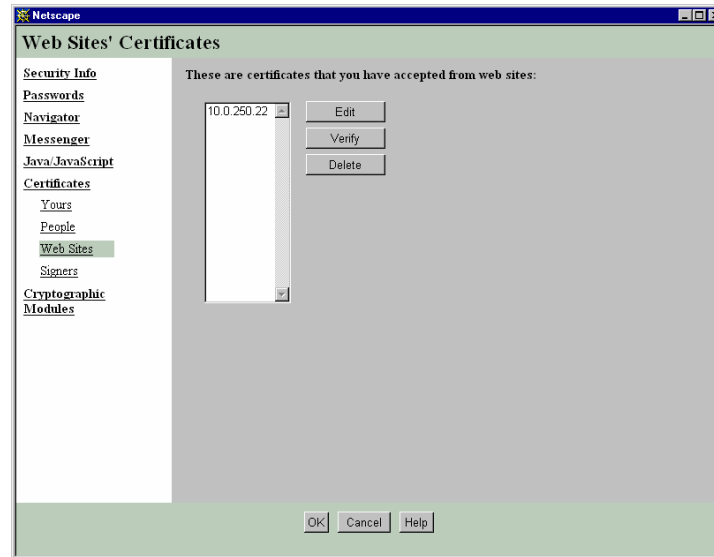


Figure 87 Netscape Web Site Certificates Window

3. In the displayed list, select the IP address of the Dominion SX unit from which the certificate was accepted.
4. Click on the [**Delete**] button.
5. Click on the [**OK**] button.
6. Close the Security 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	<a href="http://www.thawte.com/">http://www.thawte.com/</a>
VeriSign Incorporated	<a href="http://www.verisign.com/">http://www.verisign.com/</a>
Baltimore Technologies	<a href="http://www.baltimore.com/">http://www.baltimore.com/</a>

---

**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.

---

If the root certificate has already been installed, the following error will appear:

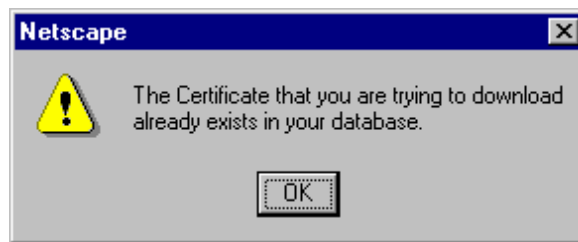


Figure 88 Certificate Already Exists Alert Window for Netscape.

If the error message **does not** appear, please skip ahead to Step 6.

If the error message **does** appear, you must uninstall the existing certificate.

1. Click on the [**Security**] button in Netscape, or on the lock icon in the lower left of the window to access the Security Information window.
2. Locate the **Certificates** section in the left panel and click on **Signers** to display a list of root certificates currently installed.

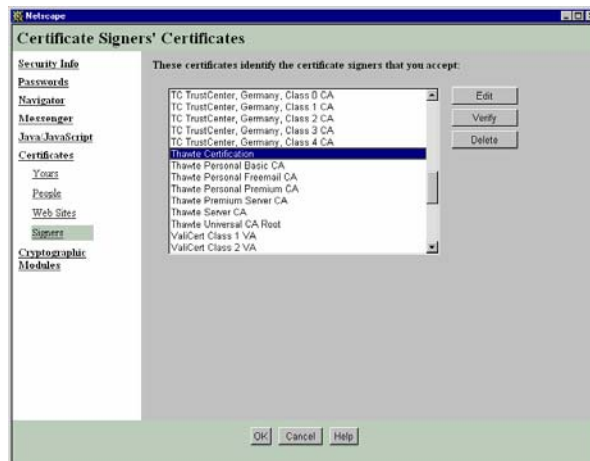


Figure 89 Certificate Signers' Certificates Window in Netscape

3. 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.
4. Click on the [**Delete**] button and then click on the [**OK**] button.



- Return to the CA's website and try to download the root certificate again.

---

*Note: If an error message appears, it indicates that the certificate deleted from the list in the Netscape security settings may not have been the correct one. Please go back to the list and double-check.*

---

- On the CA website, click on the root certificate link and the New Certificate Authority window will appear. Click on the **[Next]** button in this screen, and click on the **[Next]** button in the next screen.
- The Certificate Fingerprint will appear, providing information about the CA and the root certificate you are downloading. It will look similar to the window below. Record the **Signed by** information and click on the **[Next]** button.



Figure 90 New Certificate Authority Window in Netscape

- Check the **Accept this Certificate Authority for Certifying network sites** checkbox. The second and third boxes are optional.
- Click on the **[Next]** button, and then click on the **[Next]** button again. When prompted to enter a name for the Certificate Authority, enter the **Signed by** name that you recorded Step 7.
- Click on the **[Finish]** button. The root certificate for this Certificate Authority is now installed for this computer.



## Appendix D: RADIUS Server

*Note: This section has been provided for reference only. Please consult your local system administrator for exact implementation details.*

### Overview

The details of installing and configuring the RADIUS server software will depend on the Server you are using. This Appendix covers the installation and configuration of the **Windows 2000 RADIUS Server**, but regardless of the implementation, there are several items you must configure:

1. **A list of authorized clients and their shared secrets:** The RADIUS server must have the IP addresses of all authorized RADIUS clients. Along with each client's address is a secret. It is not critical what the secret is as long as this same secret is also configured into the client (**Dominion SX** unit). The RADIUS client and server use the secret to encrypt parts of the packets they send to each other and to guarantee that the messages and replies are authentic. In Windows 2000 implementations, this file is called *clients*. Please refer to **Step D**. in the *Install and Configure the RADIUS Server for Windows 2000* section that follows for more information.
2. **A list of authorized users and their configuration information:** The RADIUS server must know passwords, users, what these users are authorized to do after they log in. In Windows 2000 implementations, Administrators can use **Active Users** and **Directory or Local Authentication** to add users. Information about the user is stored as a list of RADIUS protocol attributes and associated values. These translate directly into the authentication reply the server will send back to the client.
3. **Reply items used by Dominion SX Products:** The following attributes are used by **Dominion SX** products:
  - **Vendor-Specific:** This Attribute is available to allow Raritan to support more detailed resource control. To control the number of ports being accessed by a particular user, a new Vendor code is added for Raritan Systems. The Vendor code takes a value of **8267** and the String to be entered should follow this format:
    - IP Address of the Dominion SX unit separated by a ‘:’
    - Privileges to be given to the user, separated by a ‘:’ Privileges should take one of the following values:

A for Administrator: has Read and Write access to the console window; can modify the configuration of the unit.

O for Operator: has Read and Write access to the console window; cannot modify the configuration of the unit.

OB for Observer: has Read-only access to the console window; cannot modify the configuration of the unit.

- Port number access, taking a value of:

‘\*’ indicating access to all the ports.

‘1:2:3’ indicating access to ports 1, 2 and 3 only.

*Note: For more information and examples, please see **Step E**. in the *Install and Configure the RADIUS Server for Windows 2000* section that follows.*

- **Service-Type:** You must specify characteristics of the service provided to the user by specifying the desired Service-Type in each user profile. The reply items in each user profile determine how the user's session is configured on the Dominion SX unit.

- If the RADIUS Server is not configured for Vendor-Specific type or it fails to follow the above specifications, the value specified for the Service-Type will determine the privileges to be given to the user. In this case, the user will be given access to all the ports. Our RADIUS clients build inside the Dominion SX unit the following attributes and maps them in the following order:

VALUE	ATTRIBUTE NAME	VALUE NAME /TYPE	DESCRIPTION
6	Service-Type	What type of Service the user receives?	
		1) Login	Maps to observer
		2) Framed	Maps to observer
		3) Callback Login	Maps to observer
		4) Callback Framed	Maps to observer
		5) Administrative	Maps to an administrator
		6) NAS prompt	Maps to an operator
		7)Callback NAS prompt	Maps to an observer

*Note: For more information and examples, please see **Step E.** in the Install and Configure the RADIUS Server for Windows 2000 section that follows.*

## Install and Configure the RADIUS Server for Windows 2000

### A. Install IAS (Internet Authorization Service)

1. Insert the Windows 2000 Server compact disc and start the Setup program.
2. Click **Install Add-On Components**, and then click **Add/Remove Windows Components**.
3. In Components, click **Networking Services** (but do not select or clear its check box), and then click **Details**.
4. Select the **Internet Authentication Service** check box and click on the **[OK]** button.
5. Click on the **[Next]** button.

### B. Configure IAS Port Information

1. To configure a remote IAS server, you must have administrative privileges on the remote server.
2. Open IAS: select **Start** → **Programs** → **Administrative Tools** → **Internet Authentication Service**.
3. Right-click on **Internet Authentication Service** and select *Properties* from the drop-down menu.
4. Click on the **RADIUS** tab, and examine the settings for ports. If your RADIUS authentication and RADIUS accounting UDP ports differ from the default values provided (1812,1645 for authentication and 1813,1646 for accounting), in **Authentication** and **Accounting**, type your port settings. The values of **1812** for authentication and **1813** for accounting are the RADIUS standards at this time. However, many network access servers use port **1645** for authentication requests and **1646** for accounting requests by default. To use multiple port settings for authentication or accounting requests, separate the ports by using commas.

### C. Configure Event Logging for IAS

1. Open IAS.
2. Right-click on **Internet Authentication Service** and select *Properties* from the drop-down menu.
3. Click on the **Service** tab and select each option that is appropriate.
4. Click on the **[OK]** button.

*Note: Selecting **Log successful authentication requests** can result in extremely large amounts of data being logged. Before selecting this option, verify that the Event Viewer is configured with a maximum log size that will accommodate this type of event logging.*

#### D. Register RADIUS Client

The client file installed in the RADIUS server must be modified. This flat file stores information about RADIUS clients, including IP addresses and shared secrets; the shared secrets must be protected from casual access. Every client trying to access the RADIUS server must be included in the list.

The following steps must be carried out for every new client trying to access the RADIUS server. As an example, imagine Dominion SX has an IP address of **10.0.3.60**. To add this IP address to the client list, perform these steps:

1. Open IAS.
2. Right-click on **Clients** and select *New Client* from the drop-down menu.
3. In **Friendly Name**, type a descriptive name.
4. In Protocol, click on **RADIUS**, then click on the **[Next]** button.
5. In **Client Address (IP or DNS)**, type the DNS or IP address for the client. If you are using a DNS name, click **Verify**. In the **Resolve DNS Name** dialog box, click **Resolve** and select the IP address you want to associate with that name from **Search Results**.
6. If the client is an NAS and you are planning to use NAS-specific remote access policies for configuration purposes (for example, a remote access policy that contains vendor-specific attributes), click on **Client Vendor**, and select the manufacturer's name. If you do not know the manufacturer's name, or if the name is not in the list, click on **RADIUS Standard**.
7. In **Shared Secret**, type the shared secret for the client, and then type it again in **Confirm Shared Secret**.
8. If your NAS supports using digital signatures for verification (with PAP, CHAP, or MS-CHAP), click on **Client must always send the signature attribute in the request**. If the NAS does not support digital signatures for PAP, CHAP, or MS-CHAP, do not click this option.

---

#### Notes:

→ If IAS receives an access request from a RADIUS proxy server, IAS cannot detect the manufacturer of the NAS that originated the request. This can cause problems if you plan to use authorization conditions based on the client vendor and have at least one client defined as a RADIUS proxy server.

→ Passwords (shared secrets) are case-sensitive. Be sure that the client's shared secret and the shared secret you enter in this field are identical to each other and conform to the password rules.

→ If the client address cannot be resolved when you click **Verify**, make sure the DNS name you entered is correct.

→ The friendly name that you provide for your RADIUS clients can be used in remote access policies to restrict access.

---

#### E. Add a Remote Access Policy

1. Open IAS and, if necessary, double-click on **Internet Authentication Service**.
2. In the console tree, right-click **Remote Access Policies** and select *New Remote Access Policy* from the drop-down menu.
3. In the **Properties** dialog box, type the name of the policy in the **Policy Friendly Name** field, and click on the **[Next]** button.
4. Click on the **[Add]** button to specify a new condition, then:
  - a. In the Select Attribute dialog box, click the attribute you want, and then click on the Add button. Please add Service-Type for Raritan.
  - b. Select **Authenticate only** and click on the **[OK]** button.
    - i. To change the configuration of an existing condition:
      - (1) Click the condition, and then click on the **[Edit]** button.
      - (2) In the attribute dialog box, specify the settings you want, and then click on the **[OK]** button.
    - ii. Click on the **[Next]** button. Under **If a user matches the specified conditions**:
      - (1) To grant dial-up permission to these users, select **Grant remote access permission**.
      - (2) To deny dial-up permission to these users, select **Deny remote access permission**.
    - iii. Click on the **[Next]** button. You can now make changes to the profile by selecting **Edit Profile**.

- (1) Click on the [**Advanced**] button and add **Vendor-Specific for Raritan**. Please use Vendor Code = **8267** and enter String in the following format:
  - (a) IP Address of the Dominion SX unit separated by a ‘.’.
  - (b) Privileges to be given to the user separated by a ‘:’ Privileges takes a value of:
    - (i) **A for Administrator**
    - (ii) **O for Operator**
    - (iii) **OB for Observer**
  - (c) Port numbers should follow, with a value of:
    - (i) ‘\*’ indicating access to all the ports.
    - (ii) ‘1:2:3’ indicating access to ports 1, 2 and 3 only.
- c. 2:4:6:8:10:12:14:1 gives access to only these specified ports.

*Configuration examples:*

- **10.0.3.60:A:3:6:9:12:15**
  - **10.0.3.60** is the IP address of the Dominion SX unit. The privileges and port numbers will apply **only** to this IP address.
  - **A** indicates Administrative privileges are given to the user.
  - **3:6:9:12:15** gives access to only ports 3, 6, 9, 12 and 15.
- **10.0.3.201:O:\***
  - **10.0.3.201** is the IP address of the Dominion SX unit. The privileges and port numbers will apply **only** to this IP address.
  - **O** maps to an Operator – this user has only limited privileges.
  - **‘\*’** Gives access to all ports.
- **10.0.3.61:OB:2:4:6:8:10:12:14:16**
  - **10.0.3.61** is the IP address of the Dominion SX unit. The privileges and port numbers will apply **only** to this IP address.
  - **OB** maps to an Observer – no Dominion SX console-write permission will be given to this user.

---

***Note:** A string following the format outlined above must be provided for every Dominion SX box contacting the RADIUS server, or else the box will take a default value. If the RADIUS Server is not configured for Vendor-Specific type, or if it fails to follow the above specifications, the value specified for the Service-Type will determine the privileges to be given to the user. In this case, the user will be given total access. In order to change the Service-Type, edit the **Service-Type** in the **Edit Dial-in Profile** menu and modify the **Attribute Value** to take any one of the following values:*

→ Login  
 → Framed  
 → Callback Login  
 → Callback Framed  
 → Outbound  
 → Administrative  
 → NAS Prompt  
 → Authenticate Only  
 → Callback NAS Prompt

---

For **Raritan**, the above has been mapped as follows:

- In order to assign *Administrative Privileges* to a user, change the **Service-Type** to **Administrative**. In such a situation, a user is granted all the permissions as if the user had logged in using !root. The user has full configuration ability and access to the port.
- In order to give *Limited Administrative Access* to the unit, change the **Service-Type** to **NAS Prompt**. In such a situation, the user becomes an **Operator** and can access all ports.
- For a **Service-Type** of **Login, Framed, Callback Login, Callback Framed, Outbound, or Callback NAS Prompt**, the user is mapped only to an **Observer-type** user and has *read-only* access to all ports.

---

***Note:** The setting of Remote Access Permission on the user object will override this setting if set to either Grant remote access permission or Deny remote access permission.*

---

## F. Select Requests to be Logged

1. Open IAS.
2. In the Console Tree, click on **Remote Access Logging**.
3. In the Details pane, right-click on **Local File** and select *Properties*.
4. Click on the **Settings** tab and select one or more check boxes for recording authentication and accounting requests in the IAS log files:
  - a. Click in the **Log accounting requests** check box to capture accounting requests and responses.
  - b. Click in the **Log authentication requests** check box to capture authentication requests, access-accept packets, and access-reject packets.
  - c. Click in the **Log periodic status** check box to capture periodic status updates such as interim accounting packets.

---

### Notes:

→ It is suggested that you initially select the first two options. You can change the selections if needed to fit your requirements.

→ The Log authentication requests option can help by alerting you to problems with transaction volume and unauthorized attempts to access resources.

→ If you select Log periodic status, attributes are logged only if you have configured the Acct-Interim-Interval attribute to generate the interim accounting requests.

→ To configure this attribute for remote access policies in IAS, do the following:

- In the IAS console tree, click *Remote Access Policies*.

- Right-click the policy for which interim accounting requests are to be generated and select *Properties* from the drop-down menu.

- On the **Settings** tab, click **Edit profile**.

- On the **Advanced** tab, click **Add**.

- In the Add Attributes dialog box, select **Acct-Interim-Interval** and click on the **[Add]** button.

- In the Attribute Information dialog box, type the interval for generating interim accounting requests in the Attribute value field, for example, type 600 to generate requests every 600 seconds (600 is the recommended value).

---

## G. Configure Log File Properties

1. Open IAS.
2. In the Console Tree, click **Remote Access Logging**.
3. In the Details pane, right-click on **Local File** and select *Properties* from the drop-down menu.
4. Click on the **Local File** tab and select **Database-import Format**. To keep your log files in IAS format, click **IAS format**.
5. To open a new log file at specific intervals, select the interval you want to use:
  - a. To handle heavy transaction volume and logging activity, select **Daily**.
  - b. To handle lesser transaction volumes and logging activity, select **Weekly** or **Monthly**.
  - c. To store all transactions in one log file, select **unlimited file size**.
  - d. If you are unsure of the transaction volume, select **when log file size reaches**, then type a log size at which a new log should be opened. The default is **10 MB**.
6. In Log file directory, enter the location where log files are to be stored. The default location is the system root `\system32\LogFiles` folder.
7. Click on the **[OK]** button.

## H. Enable the Routing and Remote Access Service

If this server is a member of a Windows 2000 Active Directory domain and you are not a domain administrator, your domain administrator must add the computer account of this server to the **RAS and IAS Servers security group** in the domain of which this server is a member. The domain administrator can add the computer account to the **RAS and IAS Servers security group** by using Active Directory Users and Computers or with the **netsh ras add registered server** command.

1. Open Routing and Remote Access.
2. By default, the local computer is listed as a server.
3. To add another server, in the console tree, right-click on **Server Status** and select *Add Server* from the drop-down menu.
4. In the Add Server dialog box, click the applicable option, and then click on the [OK] button.
5. If the server you want is already added, enable the server.
  - a. In the console tree, right-click the server you want to enable and select *Configure and Enable Routing and Remote Access* from the drop-down menu.
  - b. Follow the instructions in the **Routing and Remote Access** wizard.

---

*Note:* To open Routing and Remote Access, select **Start** → **Programs** → **Administrative Tools** → **Routing and Remote Access**.

---

## I. Use RADIUS Authentication

1. Open Routing and Remote Access.
2. Right-click on the server name for which you want to configure RADIUS authentication and select *Properties* from the drop-down menu.
3. Click on the **Security** tab and under **Authentication Provider**, select **RADIUS Authentication**.
4. Click on the [Apply] button.
5. Click on the [OK] button.

## J. Enable the IAS Server to Read User Objects in Active Directory

1. Log on to the IAS server with an account that has domain administrator credentials.
2. Open **Internet Authentication Service**.
3. Right-click on **Internet Authentication Service** and select *Register Service in Active Directory* from the drop-down menu.
4. When the Register Internet Authentication Service in Active Directory dialog box appears, click on the [OK] button.

---

### Notes:

→ To open IAS, click **Start**, select **Programs**, select **Administrative Tools**, and click on **Internet Authentication Service**.

→ This procedure adds the IAS server only to the default domain. To add the IAS server to other domains, you must add the servers manually. To do this:

- Log onto the server using domain administrator credentials.

- Select **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**.

- In the **Console Tree**, select **Users**.

- In the **Details** pane, right-click on **RAS and IAS Servers** and select *Properties* from the drop-down menu.

- In the **RAS and IAS Servers Properties** dialog box, click on the **Members** tab and add each of the IAS servers.

→ After you register the service in Active Directory, it is a good idea to verify the security settings.

---




### K. Add a User Account

1. Open Active Directory Users and Computers.
2. In the Console Tree, double-click on the domain node.
3. In the Details pane, right-click on the organizational unit to which you want to add the user, point to **New** and select *User*.
4. In the **First Name** field, type the user's first name.
5. In the **Initials** field, type the user's initials.
6. In the **Last Name** field, type the user's last name.
7. Modify **Full Name** as desired.
8. In the **User Logon Name** field, type the name that will be used to log on and select the UPN suffix that must be appended to the user logon name (following the @ symbol) from the drop-down list. If the user will use a different name to log on from computers running Windows NT, Windows 98, or Windows 95, change the user logon name as it appears in **User Logon Name (pre-Windows 2000)** to the different name.
  - a. In **Password** and **Confirm password** fields, type the user's password.
  - b. Select the appropriate password options.

---

#### Notes:

→ To open Active Directory Users and Computers, select **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**.

→ To add a user, you can click on the new user shortcut icon  in the toolbar.

→ After creating a user account, edit the user account properties to enter additional user account information.

→ To add a user, you can copy any previously created user account.

→ A new user account with the same name as a previously deleted user account does not automatically assume the permissions and memberships of the previously deleted account, because the security descriptor for each account is unique. All permissions and memberships must be manually recreated to duplicate a deleted user account.

---

### L. Create Groups in Active Directory and Add User Accounts

This procedure provides guidelines to assign different roles (Administrative, Operator and Observer) to domain users and add respective groups to the corresponding IAS policy. For instance, create the following groups: RASAdmin, RASOperator, RASObserver. Then assign the appropriate users to these groups.

1. Open Active Directory Users and Computers.
2. In the console tree, click on the domain node.
3. In the details pane, right-click the organizational unit to which you want to add the group, point to **New** and select *Group*.
4. In **Group name**, type the group name, for example, RASAdmin.
5. Under **Group scope**, select **Global**.
6. Under **Group type**, select **Security**.
7. Click on the **[OK]** button.
8. Create two other types of groups, for example, RASOperators and RASObserver.
9. Add users to these groups depending upon types of access to be given.
  - a. Right-click on the group and select *Properties* from the drop-down menu.
  - b. Click on the **Members** tab.
  - c. Click on **Add** and select the users to add to this group.
10. Add these groups in respective IAS policies to assign appropriate user roles to domain users.
  - a. Open IAS.
  - b. Right-click on **Policy** and select *Properties* from the drop-down menu.
  - c. Click **Add** under **Specify the conditions to match**.
  - d. From the **Attribute types** pop-up menu, click on *Windows-Groups*
  - e. Click on the **[Add]** button.
  - f. Click on **Groups** menu.

- g. Click on the [**Add**] button.
- h. Click on the appropriate group and click on the [**OK**] button.

After these steps are executed, a new user can connect to the NAS device and IAS will look at the user name, find the group in which it is a member, and use the policy associated with that group.

## Appendix E: Configuring Cisco ACS RADIUS Server

Use the following procedure to configure the Cisco RADIUS server so that you can work with Dominion SX. It is assumed here that Administrators are familiar with setting up and configuring the RADIUS server. In order for Dominion SX to support RADIUS, both the unit and the user information must be added into the RADIUS configuration.

Only Version 3.0 has been validated; however, other versions of the RADIUS server should operate with the unit. Only the user's role can be controlled on the unit using the RADIUS (IETF) option.

*Note: Access restrictions to specific ports on the unit cannot be controlled.*

1. Log on to Cisco ACS Server using the browser.



Figure 91 Cisco ACS Main Display

2. Click on the [Network Configuration] button in the left panel of the screen and select **Add Entry** to add/edit AAA Client. This must be done for each unit that is going to be accessed via RADIUS. Click on the **Authenticate Using** drop-down menu and select **RADIUS (IETF)** from this list. Click on the [Submit] button.

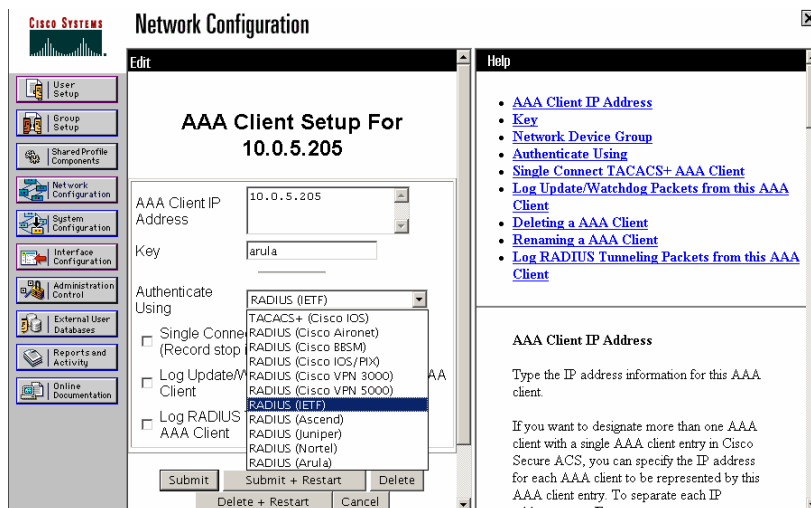


Figure 92 Unit Configuration Display

- Click on the **[Interface Configuration]** button in the left panel of the screen.

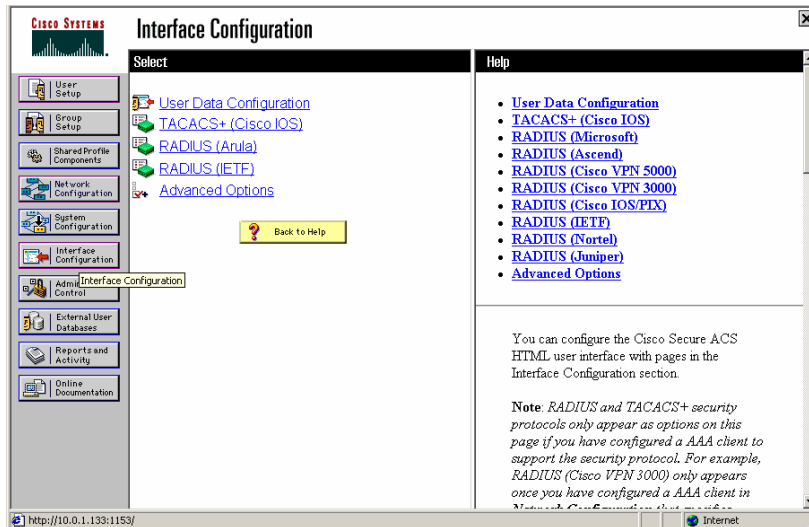


Figure 93 Interface Configuration Display

- Click on the **RADIUS (IETF)** link to edit properties. Under the **User** heading, click on the check boxes before **Service-Type** and **Framed Protocol**. Click on the **[Submit]** button.

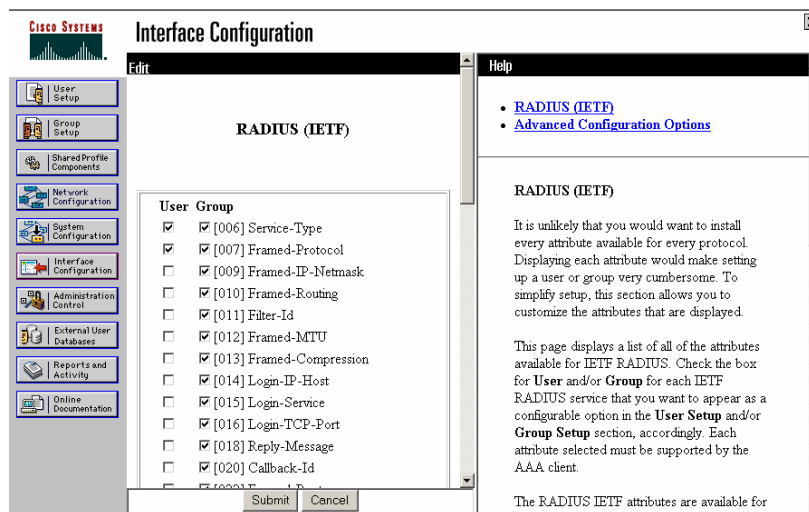


Figure 94 RADIUS Properties Display

- To add new users and configure RADIUS (IETF) attributes, click on the **[User Setup]** button in the left panel of the screen. Enter the user's name and click on the **[Add/Edit]** button.

6. To edit existing users, click on the [User Setup] button in the left panel of the screen. Click on the [List All Users] button and select a user from the list.

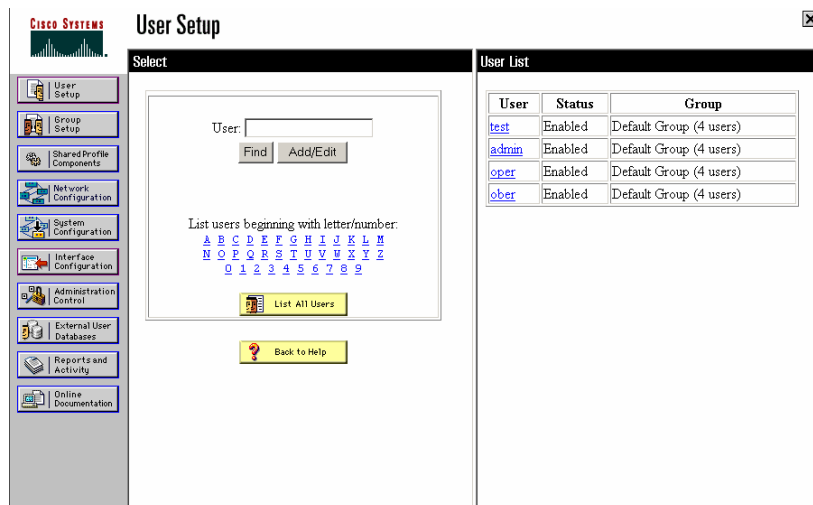


Figure 95 New User Display

7. Once you have selected a user, on the user properties page, scroll down to the **RADIUS (IETF)** section.

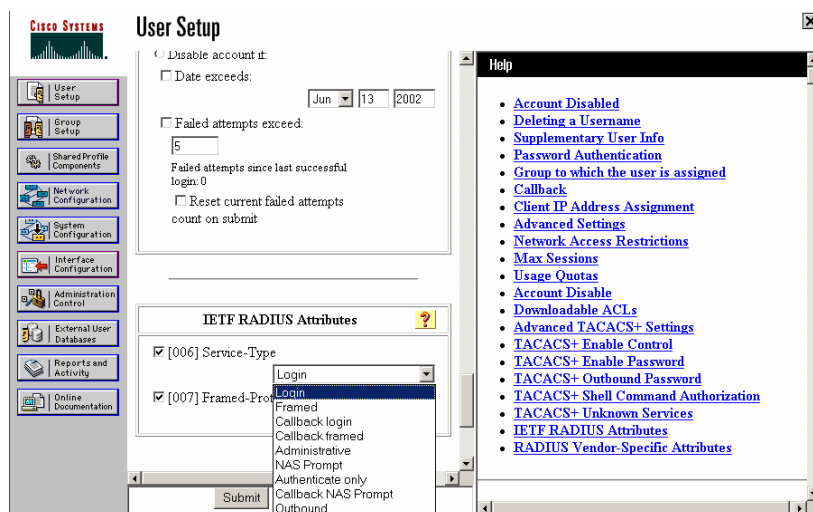


Figure 96 User Properties Display

8. Click on the **Service-Type** check box and select the appropriate service-type from the drop-down menu:
- **Administrative:** User with this Service-type will have Administrative privileges on the unit and access to all the ports.
  - **NAS Prompt:** User with this Service-Type will have Operator privileges on the unit and access to all the ports.
  - **Login:** User with this Service-Type will have Observer privileges on the unit and access to all ports.
9. Click on the [Submit] button.



## Appendix F: RSA ACE/Server Configuration

This section provides guidelines for configuring the RSA ACE/Server 5.0 so that SecureID can be used as the authentication mechanism. Users in an ACE server native database can log on to Dominion SX units installed in the network using SecureID token authentication.

It is assumed that RSA ACE/Server is running RADIUS services and able to authenticate users from its native database. This guide does not provide initial configuration procedures for the ACE server but assumes that the administrator is familiar with the ACE server and has the ability to set up and configure the application. Guidelines are provided to allow SecureID to be used with the Dominion SX units.

These steps must be performed on the RADIUS server in order to use SecureID:

1. Configure all the units (define them in the RADIUS server database)
2. Establish profiles
3. Configure users and associate profiles to each

**Please follow the steps below:**

1. Select **Start** → **Programs** → **RSA ACE Server** → **Database Administration-Host Mode**.

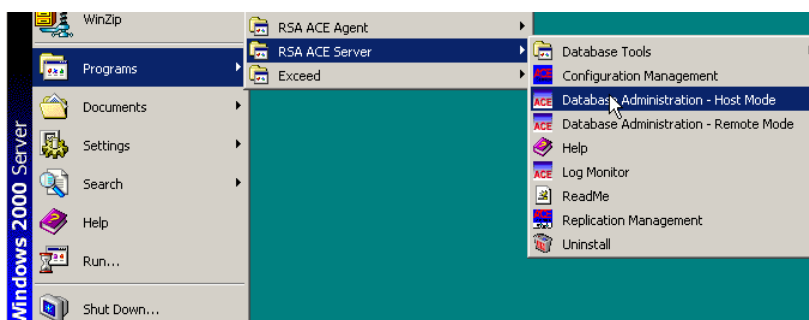


Figure 97 Launching RSA Administration Application

2. Select **Agent Host** → **Add Agent Host** from the main menu to launch the configuration menu.

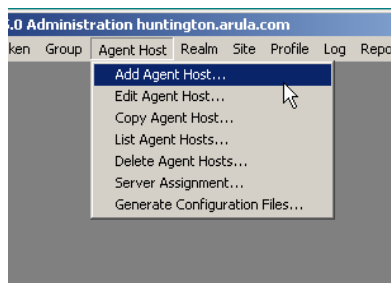


Figure 98 Add Agent Host Selection

## 3. Define and configure all Dominion SX units.

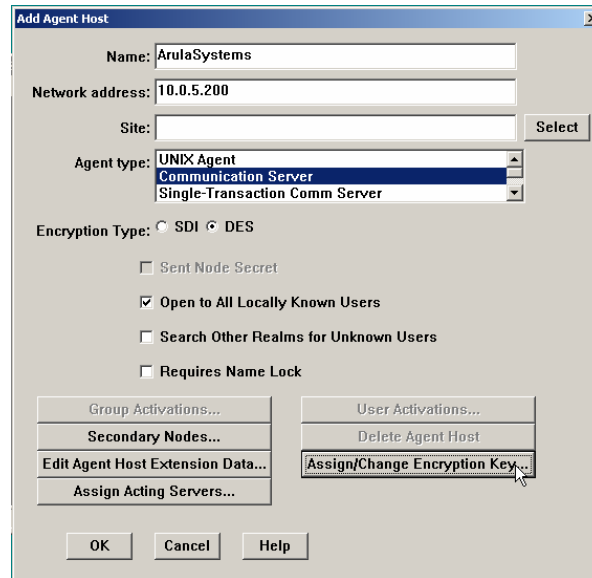


Figure 99 Add Agent Host Display

- a. **Name:** Name of the Agent Host; must be a primary name or alias listed in the local host file or DNS server. If an alias is entered, the primary name of the Agent Host appears upon clicking on the [OK] button. If the name entered is not listed in the local host file or DNS server, and error message will appear.
- b. **Network Address:** IP address of Dominion SX unit in the network.
- c. **Site:** Optional entry.
- d. **Agent Types:** Communication Server: Select this option for Dominion SX units.
- e. **Encryption Type:** Select **DES** radio button for Dominion SX units
- f. **Open to All Locally Known Users:** Checking this box makes the Agent Host an “open” Agent Host, which needs no specific user or group activations. Any valid user in the local Server database can authenticate on an open Agent Host.
- g. **Assign/Change Encryption Key:** If RADIUS is installed and enabled on your system, use this command to enter the secret Key (up to 48 characters) shared between this Agent Host and the RADIUS server with which it will communicate (this Key must also be entered in the unit’s RADIUS configuration tab).

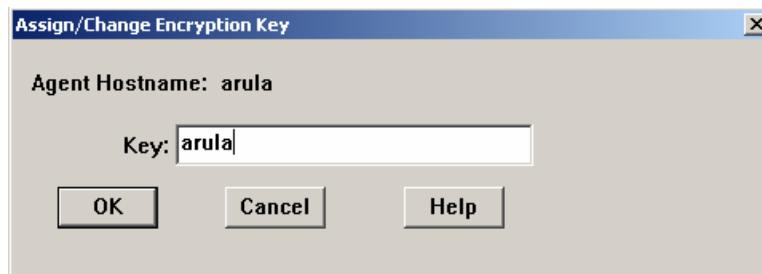


Figure 100 RADIUS Secret Key Display

- h. Click on the [OK] button to save all changes, or click on the [Cancel] button to exit the window without saving changes.



4. Select **Profile** → **Add Profile** in the main menu.

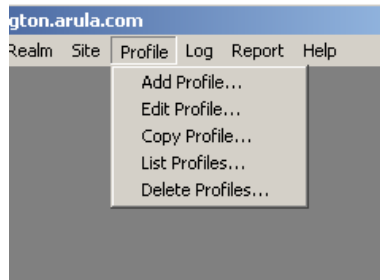


Figure 101 Add Profile Selection

5. In the Add Profile window, assign an appropriate name to identify the desired profile, such as Raritan-Administrator.

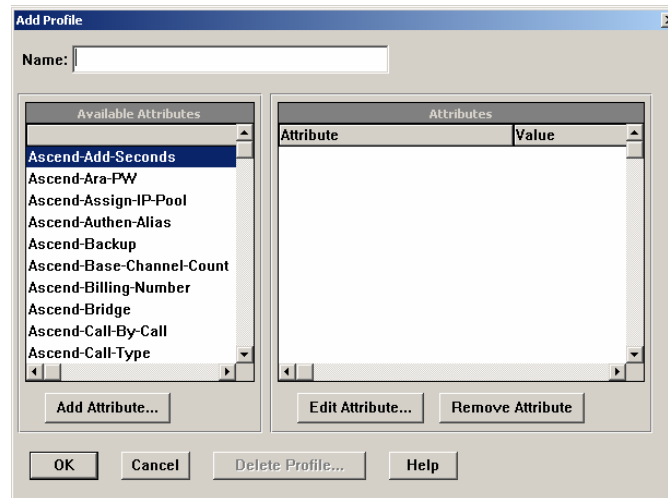


Figure 102 Add Profile Display

6. Scroll through the list in the **Available Attributes** frame and select **Service-Type**. Click on the [**Add Attribute**] button. The Service-Type Profiles and corresponding user roles are as follows:
- **Administrative-User:** Users with this profile will have Administrator privileges on the unit; they will have read/write access to all ports and will be able to edit the unit's configuration.
  - **NAS Prompt:** Users with this profile will have Operator privileges on the unit; they will have read/write access to all ports, but will not be able to edit the unit's configuration.
  - **Login:** Users with this profile will have Observer privileges on the unit; they will have only read access to all ports, and will not be able to edit the unit's configuration.

- Click on the [OK] button to save the changes, then click on the [OK] button in the Add Profile window to return to the main menu.

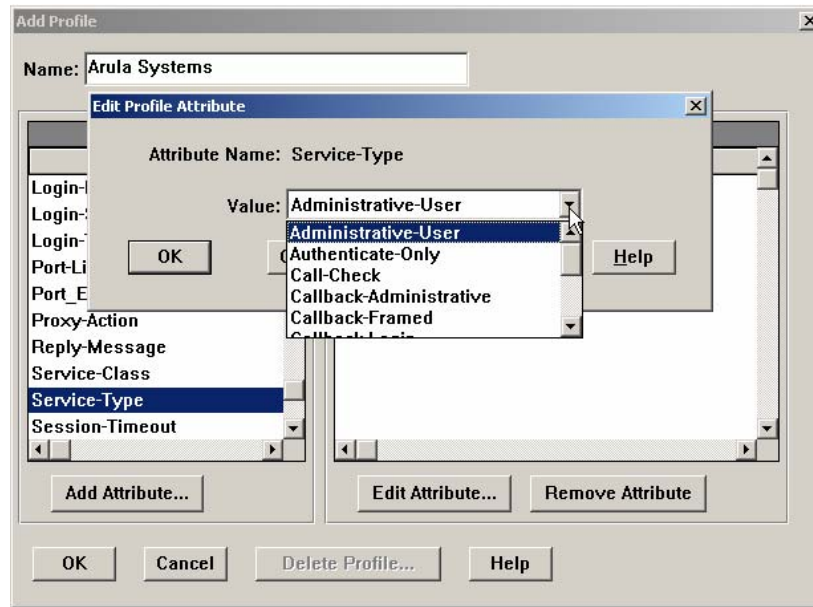


Figure 103 Add Attribute Display

**Note:** Only the user's Role can be controlled on the Dominion SX units using specific Service-Type profiles. Access restriction to specific ports on cannot be controlled.

- Select **User** → **Add User/Edit User** in the main menu to add a user and assign the appropriate profile.

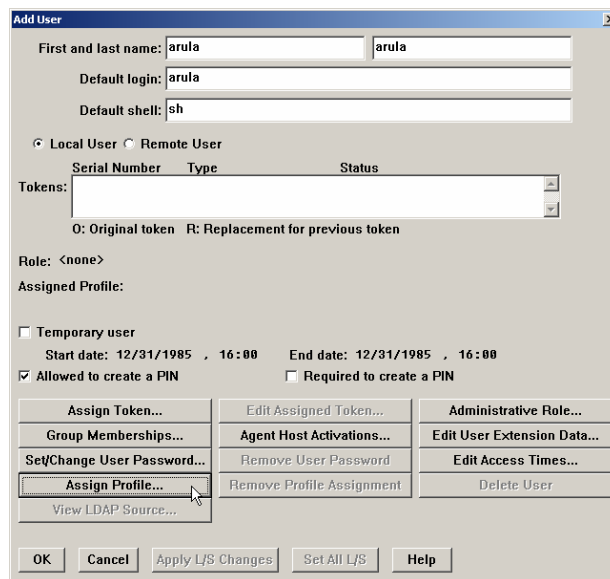


Figure 104 Add User Display

9. Click on the **[Assign Profile]** button and select the appropriate profile from the Select Profile window. Only one profile can be assigned to each user. Click on the **[OK]** button.

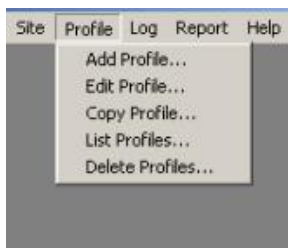


Figure 105 Profile Selection Display

10. To control access to specific units, click on the **[Agent Host Activations]** button. Select the appropriate units from the **Available Agent Host Activation** list and click on the **[Activate On Agent Hosts]** button.

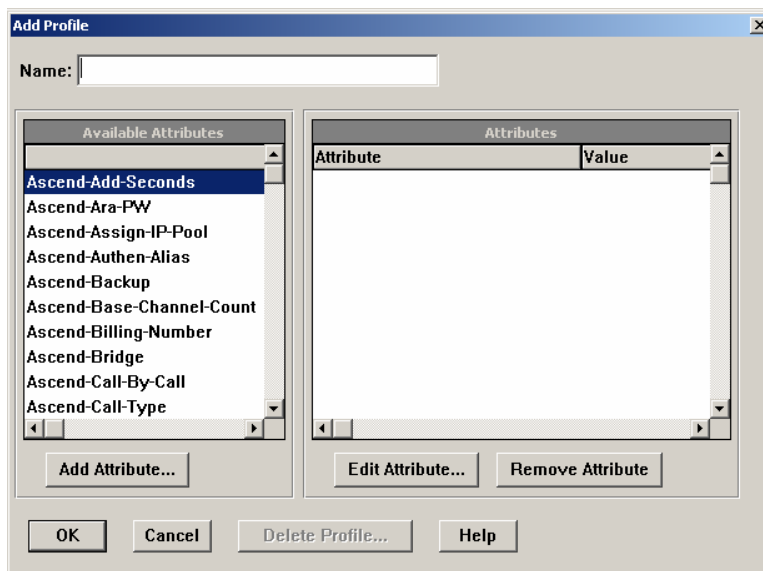


Figure 106 Unit Selection Display per User

11. To configure the Dominion SX device to use RSA/ACE Server as the RADIUS authentication server, log on to the unit with the local administrative account, click on the **[Configuration]** button in the left panel, and select the **RADIUS** tab. Configure the appropriate RADIUS Server IP address, Shared Secret (encryption key), and Port. The unit is now ready to authenticate the user using the ACE RADIUS server.
12. At the login screen for the Dominion SX unit, enter the **Username** and **Passcode** (a combination of the PIN and a number generated on the SecureID token). Authentication will be made using the RADIUS server and access granted based upon user profile.

## Lightweight Directory Access Protocol (LDAP)

Using Dominion SX software revision 2.1 or higher, your Dominion SX unit can authenticate users via LDAP/S (LDAP Secure). If your Dominion SX unit does not have revision 2.1, upgrade via the upgrade feature and download the appropriate software from <http://www.raritan.com/support> to gain access to the LDAP feature.

The screenshot displays the LDAP configuration interface for Dominion SX 16. The interface is divided into a left-hand navigation pane and a main configuration area. The navigation pane includes links for Port Access, Configuration, Upgrade, Reset, and Exit, along with a 'Current users:' section showing 'admin'. The main configuration area has tabs for Report, Network, Ports, Users, IP ACL, Certificate, RADIUS, Time, Notification, and LDAP. The LDAP tab is active, showing an 'Enable LDAP' checkbox. Below this, there are two server configuration sections: 'Primary Server' and 'Secondary Server (Optional)'. Each section includes fields for IP, Port, Secret, Confirm Secret, Base DN, Base Search, and Authorization Query String. The 'Update' button is visible at the bottom right of the configuration area. A status bar at the very bottom indicates 'Configuration locked. Other users cannot change configuration.' and contains 'Save', 'Reload', and 'Unlock Config' buttons.

Figure 107 LDAP Configuration Screen

1. Click on the **LDAP** tab.
2. Verify that the LDAP or LDAP(S) server is running, and confirm its IP Address and TCP port number, and other information required to communicate with it (check with your LDAP server administrator). We recommend you obtain this information before you start configuring LDAP on the Dominion SX.
3. Click on the **Enable LDAP** check box to enable LDAP.
4. Type a valid IP address in the **Primary Server** field.
5. The default TCP **Port** is 389 for LDAP. (For LDAP(S), type 636 in the **Port** field).
6. Type the secret password in the **Secret** field.
7. Re-type the secret password in the **Confirm Secret** field.
8. Type the base directory name in the **Base DN** field.
9. Type search information in the **Base Search** field.
10. Type a valid authorization query string in the **Authorization Query String** field.
11. If you use a secondary server, click on the **Enable Secondary Server** check box, and fill in all data for the secondary server, as outlined above.
12. Click [**Update**].
13. Click [**Save**].

## Appendix G: Modem Configuration

### Client Dialup Networking Configuration

Configuring Microsoft Windows Dialup Networking for use with Dominion SX allows configuration of a PC to reside on the same 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 98
- Windows 2000

### Windows NT Dialup Networking Configuration

1. Select **Start** → **Programs** → **Accessories** → **Dial-Up Networking**.
2. Click on the [New] button.

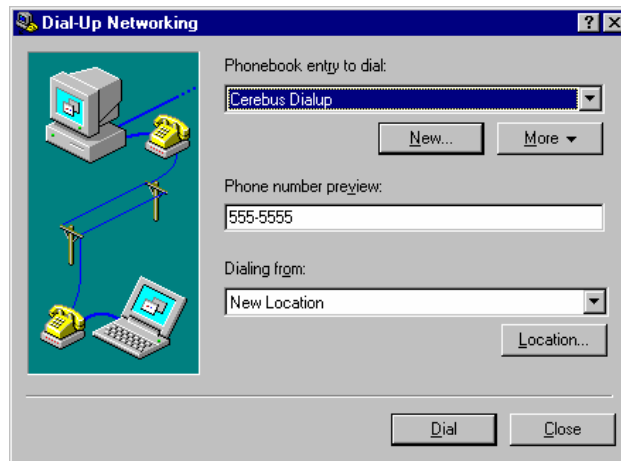


Figure 108 Dial-Up Networking Display

3. The New Phonebook Entry window allows you to configure the details of this connection. Click on the Basic tab and complete the following fields:
  - a. **Entry name:** Name of the Dominion SX connection
  - b. **Phone number:** Phone number of the line attached to the Dominion SX unit
  - c. **Dial using:** Modem being used to connect to Dominion SX; if there is no entry here, there is no modem installed in your workstation

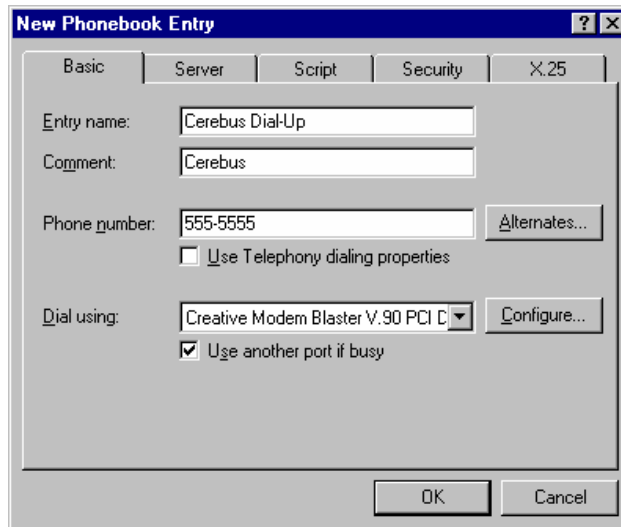


Figure 109 New Phone Entry Display

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.
  - a. Click on the **Accept any authentication including clear text** radio button.
  - b. Click on the [OK] button to return to the main Dial screen.

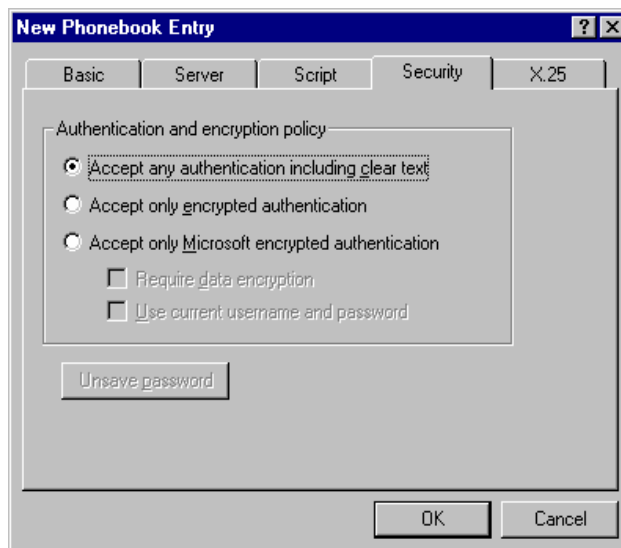


Figure 110 Dial-Up Security Display

5. Click on the [Dial] button.
6. In the event of connection error messages, please refer to your Windows NT Users Guide.

## Windows 98 Dialup Networking Configuration

1. Select **Start** → **Programs** → **Accessories** → **Communications** → **Dialup Networking**.
2. Double-click on the **Make New Connection** icon in the Dialup Networking window to launch it.

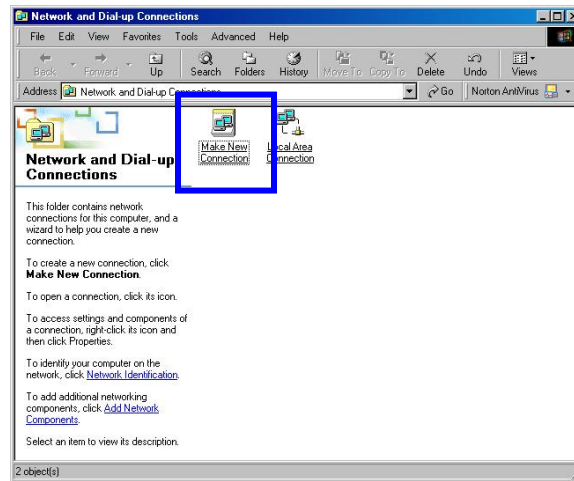


Figure 111 Configuring Windows 98 Dialup Networking

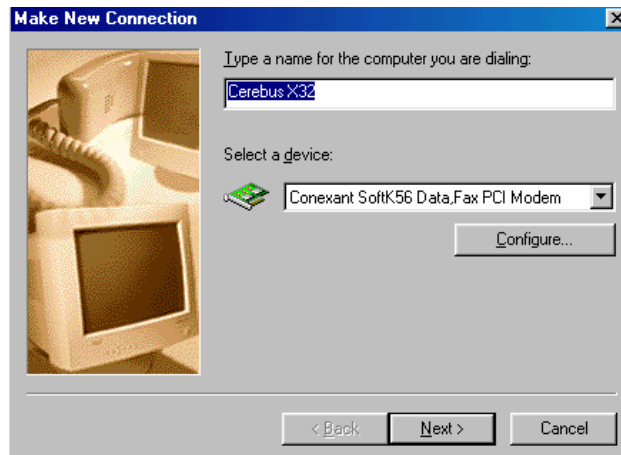


Figure 112 Make New Connection – Connection Name

3. In the Make New Connection window, enter:
  - a. **Name:** Name for the Dominion SX unit you are dialing.
  - b. **Device:** Device you wish to use to connect to the Dominion SX unit from the drop-down list (this will be the Modem).
  - c. Click on the **[Next]** button.
  - d. **Area code and phone number:** The full number of the phone line connected to the Dominion SX unit.
  - e. Click on the **[Next]** button.

- f. The next window will inform you that you have successfully created the Dialup Networking Connection.



Figure 113 Make New Connection – Complete

- g. Click on the [**Finish**] button and an icon will appear in the Dialup Networking window.
4. Double-click on the new icon, and in the Connect To window that appears, click on the [**Connect**] button to establish the connection with the Dominion SX unit. No username or password is required for connection, as the security is provided by the Dominion SX unit authentication protocol.

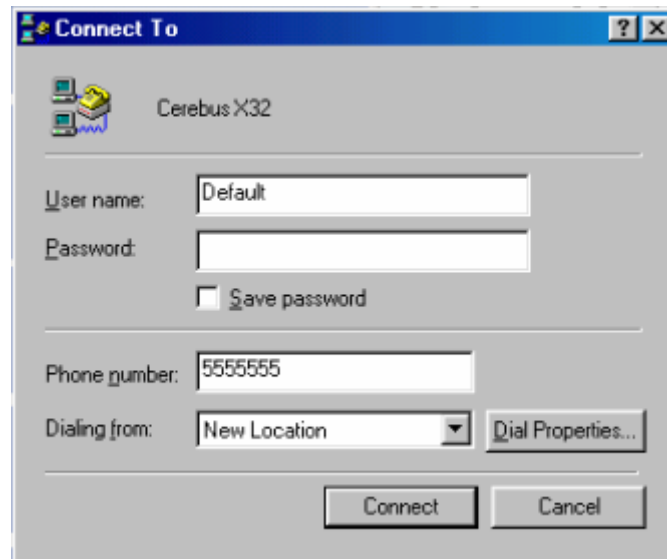


Figure 114 Connect to Window

5. Once logged in, you may connect to the Dominion SX unit with a supported Java-enabled browser. Or, for getting access to target ports, launch SSH or Telnet (if enabled). Because SSH and Telnet are CLI-based, access is very fast.



## Windows 2000 Dialup Networking Configuration

1. Select **Start** → **Programs** → **Accessories** → **Communications** → **Network and Dial-Up Connections**.
2. When the Network and Dial-Up Connections window appears, double-click on the **Make New Connection** icon.

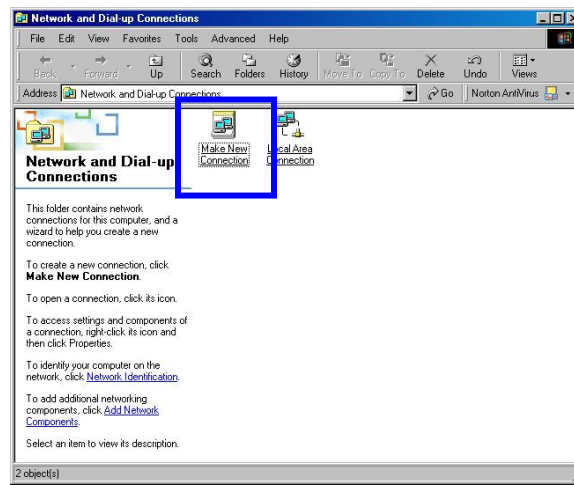


Figure 115 Windows 2000 Network and Dialup Connections

3. Follow the steps in the **Network Connection Wizard** window to create custom dialup network profiles. Click on the **[Next]** button.



Figure 116 Welcome to the Network Connection Wizard

- Click on the **Dial-up to private network** radio button and click on the **[Next]** button.

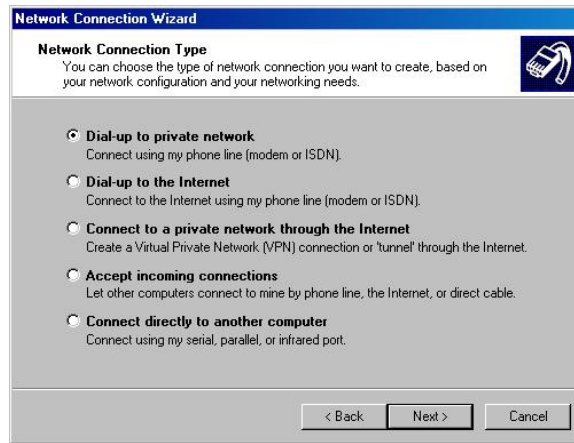


Figure 117 Network Connection Type

- Click on the check box before the modem that you want to use to connect to the Dominion SX unit and then click on the **[Next]** button.

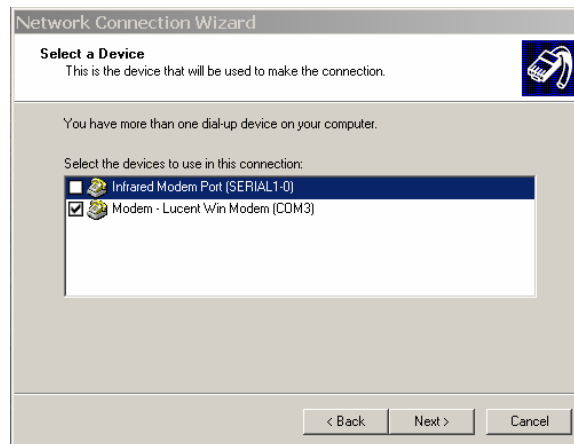
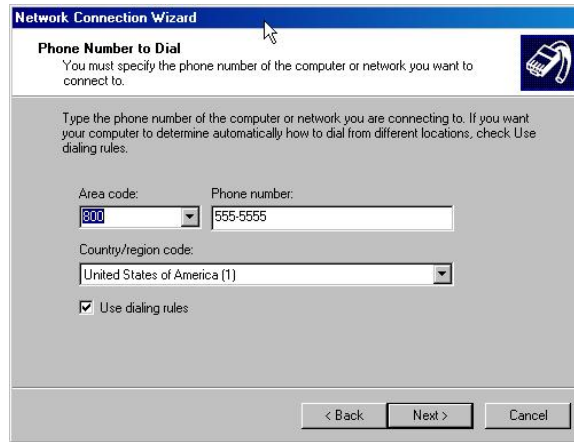


Figure 118 Device Selection

- Click in the **Use dialing rules** check box and enter the **Area code** and **Phone number** you wish to dial in the fields. Click on the **[Next]** button.



The screenshot shows the 'Network Connection Wizard' window with the 'Phone Number to Dial' step. The window title is 'Network Connection Wizard'. Below the title bar, there is a sub-header 'Phone Number to Dial' and a small icon of a telephone handset. The main text reads: 'You must specify the phone number of the computer or network you want to connect to.' Below this, there is a paragraph: 'Type the phone number of the computer or network you are connecting to. If you want your computer to determine automatically how to dial from different locations, check Use dialing rules.' There are three input fields: 'Area code:' with a dropdown menu showing '800', 'Phone number:' with a text box containing '555-5555', and 'Country/region code:' with a dropdown menu showing 'United States of America (1)'. Below these fields is a checked checkbox labeled 'Use dialing rules'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 119 Phone Number to Dial

- In the Connection Availability screen, click on the **Only for myself** radio button. Click on the **[Next]** button.



The screenshot shows the 'Network Connection Wizard' window with the 'Connection Availability' step. The window title is 'Network Connection Wizard'. Below the title bar, there is a sub-header 'Connection Availability' and a small icon of a telephone handset. The main text reads: 'You may make the new connection available to all users, or just yourself.' Below this, there is a paragraph: 'You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.' There are two radio buttons under the heading 'Create this connection:': 'For all users' (which is selected) and 'Only for myself'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 120 Connection Availability

- The Network Connection has been created, and you can complete set-up of the dial-up connection by entering the name of the Dial-up connection.



Figure 121 Network Connection Wizard Completion

- Click on the **[Finish]** button.
- To connect to the remote machine, when the Dial Window appears, click on the **[Dial]** button. A window indicating that a successful connection has been established will appear. If you get any errors during this phase, please consult your Windows 2000 Dial-up Networking Help.

# Appendix H: TCL Programming Guide

**Disclaimer: The information contained in this section is subject to change without notice. Raritan shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material. Raritan assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Raritan.**

## Overview

Dominion SX supports TCL (version 7.0), an industry standard scripting engine. Using TCL scripting capabilities, you can create customized conditions for event detection, and can generate customer-specific notifications and alerts. Dominion SX features a TCL engine and a flash file system for the development and storage of TCL scripts.

Dominion SX is pre-configured with a set of User Definable Events that can be generated by TCL scripts. Raritan has introduced an extension library to provide an API to Dominion SX's functions. In addition, Dominion SX includes an extensive list of notification events that can be used to audit, track, and trace the conditions of and modifications to the unit itself.

This appendix describes the architecture and features of the TCL script engine, and provides information to help you develop scripts to manage multiple remote target devices.

## TCL Architecture with Target System

The following diagram illustrates the TCL Engine architecture:

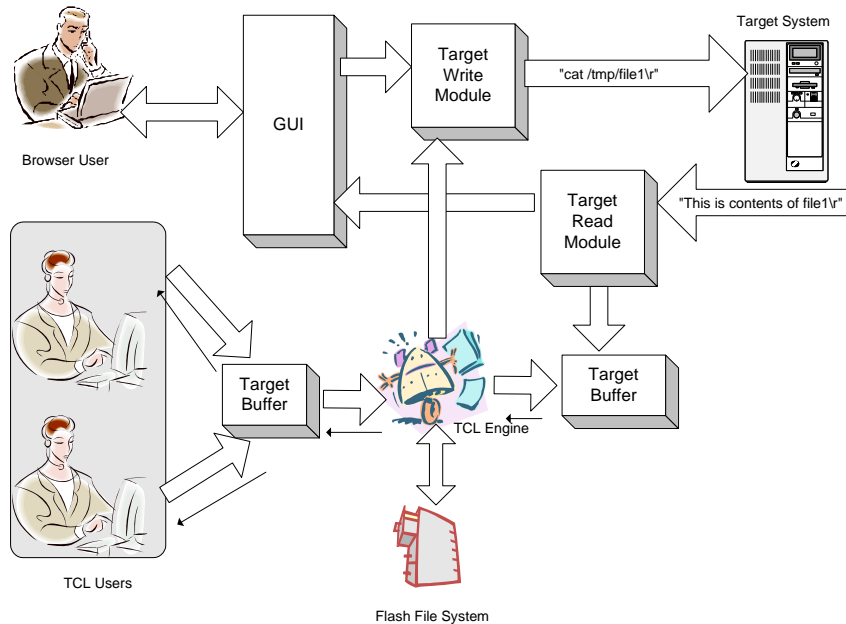


Figure 124 TCL Architecture

Key aspects of TCL architecture:

- The TCL Engine is single-threaded and shared across multiple users and target devices.
- A browser user (standard GUI) does not interact with the TCL Engine.
- The TCL Engine shares the same function blocks for accessing the console via the RS-232 port.
- The TCL Engine does not interfere with normal console access function.
- Only Administrators may operate TCL.
- Data received from each target system on the RS-232 port is sent to all connected Java user consoles and also stored in an internal TCL buffer. Each internal buffer has the following properties:
  - Data received on an RS-232 port from a target device is stored in this buffer.
  - The TCL Engine is the only reader of this data.

- Internal buffers are circular buffers; 64Kbytes.
- The buffer uses the FIFO storage method.
- A data stream methodology for data retrieval is used and there is no random access capability.

Extensions have been made to the TCL framework to enable retrieving data from the TCL internal buffer and to send commands to the target systems. A single script can include instructions to access any RS-232 port. The script has the ability to take away the write access to an RS-232 port from other users, which is communicated to each user through the GUI. Once the script acquires the write access, other users will not be allowed to take the write access until the script releases it. There are several requirements to be considered

- If the script has write access and the user resets TCL through the GUI, the TCL interpreter will release write access before resetting.
- If the script has write access and the user logs out without releasing the write access, access will be held by the TCL interpreter until a user connects to the interpreter and instructs the interpreter to release it or resets the interpreter.
- It is important for the scriptwriter to release the write access, if acquired, in the boot script.
- The write access lock is always associated with a port number. The user is responsible for releasing any locks acquired during script execution.

With the following commands (which may be used interactively by a TCL user or in a TCL script), the user can access the RS-232 ports. Each command takes a number as the final argument to indicate which serial port should be affected:

- *amplock/ampunlock <port>*
  - TCL engine locks the write access for this port. GUI users using the Java Console cannot supersede TCL and force TCL unlock by the issuing the Get Write Access or F8 key. An administrator may only force a TCL unlock by issuing a Reset from the Script Shell window or main GUI.
  - The TCL user must lock the write access in order for the TCL Engine to write to the Console.
- *ampclear <port>*
  - Mark all data in the TCL internal buffer associated with the port as having been READ. Essentially, this command flushes all data in the TCL internal buffers.
- *ampread <timeout> <termination string> <port>*
  - TCL will start examining the unread data in a TCL internal buffer and return the result until:
    - A timeout has occurred or
    - A termination string is found in the data stream.
  - If zero is given as the timeout, no timeout limit will be checked.
- *ampwrite <output string> <port>*
  - The string is written to Console port.
- *ampexec <output string> <timeout> <termination string> <port>*
  - This command is simply an ampwrite follow by an ampread.

The above extensions to TCL, along with the standard TCL commands, provide a development platform for powerful scripts for managing the target devices. This guide provides details on all of the extensions provided in the Dominion SX product. A few sample scripts are also provided.

The TCL command queuer provides the following features:

- Serialize multiple TCL Command Requests.
- Process one command with one response.
- Multi-lined single command (multiple commands issued by user as a single task by using “;” between commands) is processed as a single request and single response is returned.
- Execution result returned to the command issuer.
- Access control for TCL.
- By default, administrators are the only users that can access TCL. However, administrators may disable the check.

`amppermission`, `amplisten` and `ampresponse` are commands to enable a TCL script to interact with other TCL users.

- `amppermission <on/off>`
  - On will enforce permission checking.
  - Off will allow observers and operators to access TCL.
- `amplisten`
  - Remember who sent the command and respond to the sender instead of the executer of the script.
  - If no command is present, `amplisten` returns a null.
- `ampresponse`.
  - Flush the data in current result buffer (stdout) to the user.

The extensions enable a TCL script/user to send notifications (SMTP) to subscribed users when an event occurs. The creator of the script is required to generate an event and users are given the option to subscribe to the event. Commands are provided for a script to send notifications to subscribed users when an event occurs. This appendix provides information on how to create and subscribe to an event.

---

## Boot Script Support

A mechanism is available to write scripts that will be executed when the system boots. The boot script is a normal script except that it should be named “boot.scr” (case insensitive). On factory reset, the boot.scr script will be renamed to boot.bak automatically. After the factory reset, the user can make necessary changes in the boot script (“boot.bak”) and rename it back to boot.scr.

The boot script can access the RS-232 ports, but the user must insure that the write locks are released otherwise no user will be able to get write access to the console of the remote target device. In case a write lock is not released, the user has to change the boot script appropriately and perform a soft reset.

---

## File System

Dominion SX includes a general-purpose flash file system, which can be accessed by both the internal web server and the TCL interpreter. The file system is MSDOS 3.3 compatible with 8.3 (xxxxxxx.xxx) file name constraints and can be used to store TCL data and scripts. A total of 10MB is available for storage of user data. There is no specific limit on the size of a particular script or the number of scripts a user may save.

The file system is accessible only by the TCL engine and hence only Administrator users can modify the filesystem (e.g. create, delete files etc). Operator and Observer users can be granted access to the TCL engine and hence to the filesystem by administrators through the use of the `amppermission` command.

---

## File Directory Structure

All user scripts and data are stored in `/ata/usr`. Access to all other directories in the system are restricted to the user.

---

## File System API through TCL

### **`pwd`**

Display current path.

### **`dir <directory name>`**

List directory contents.

### **`mkdir <directory name>`**

If absolute path is not provided, then the new directory is created in the present working directory.

### **`rmdir <directory name>`**

Remove the specified directory.

**cd <directory name>**

Change the current directory to the new directory specified. This command will take a relative path or an absolute path. /ata and system related directories are not accessible.

**del <filename>**

Delete specified file name

**TCL Commands**

The TCL interpreter incorporated supports TCL 7.0. All built-in TCL commands for TCL 7.0 are supported *except* **exec**, **interp**, **library**, and **TCLvars**.

The following TCL commands are supported:

append	glob	pwd
array	global	read
break	history	regexp
case	if	regsub
catch	incr	rename
cd	info	return
close	join	scan
concat	lappend	seek
continue	lindex	set
eof	linsert	source
error	list	split
eval	llength	string
exit	lrange	switch
expr	lreplace	tell
file	lsearch	time
flush	lsort	trace
for	open	unknown
foreach	pid	unset
format	proc	uplevel
gets	puts	upvar
		while



## Accessing TCL Window

The TCL Interpreter can be accessed through RaritanConsole using the **Script** menu selection, as described in **Chapter 4: Console Features**.

The TCL prompt is “%”. The command(s) to be executed must be entered AFTER the prompt. The result will be echoed on the next new line. The user may execute multiple-line commands using the Copy and Paste features from the Windows/Unix operating system.

*Note: Any response that is larger than 4K will not be echoed back to the user, but the command's output may be stored in a variable.*

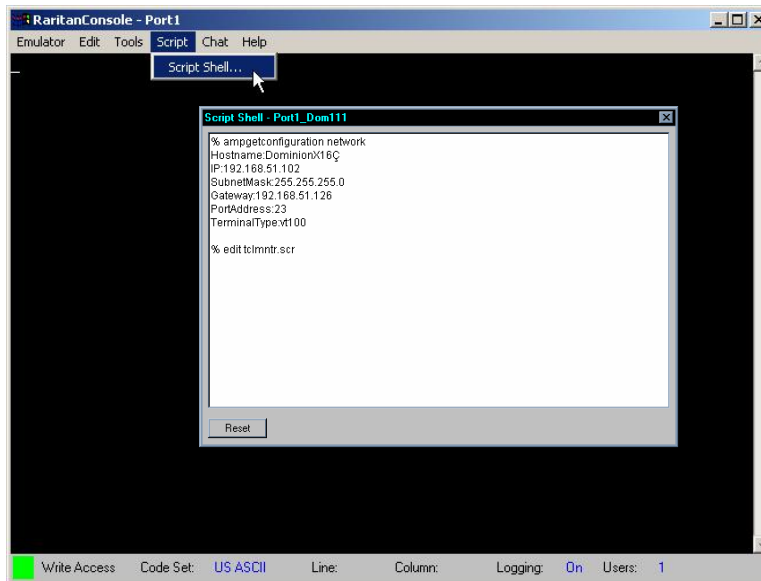


Figure 125 Activating TCL Scripting Window

## Resetting TCL Interpreter

TCL scripts may have forever-loops due to programming errors, unknown conditions, or by design. When this condition occurs, click on the **[Reset]** button in the scripting window to halt the execution of the TCL script. However, not all conditions are recoverable by clicking on the **[Reset]** button. Therefore, full software reset from the GUI may be necessary to restart the interpreter.

When a *Reset* has been issued to the TCL Interpreter, the **BOOT.SCR** will **NOT** be executed. This will prevent errors in the boot script from incapacitating the interpreter. Not all conditions are recoverable by *Reset*. The user may have to execute a factory reset to remove the error condition. When factory reset occurs, **boot.scr** is renamed **boot.bak**. Administrations will need to rename **boot.bak** to **boot.scr** once the factory reset is complete.

## Editing TCL Scripts

The TCL Shell includes a built-in editor, activated by typing *edit <filename>* at the % prompt. The file will be saved to the directory in which the TCL interpreter is currently operating. Administrators, Operators, and TCL script developers should understand the mechanisms by which Write Access is obtained and released in order to develop applications to manage target devices.

*Note: The TCL engine owns files created by the users. Removing a user account does not delete any created files.*

## Executing TCL Scripts

A stored TCL Script may be executed as follows.

```
% source <filename>
```

The prompt does not return if the script contains forever-loops, but the shell is active (listening) and will take input if the script is designed to accept them.

## **Automatic Execution of a TCL Script upon Power Up**

---

For a TCL script to be executed automatically upon each reboot or power cycle of the unit, the script needs to be named *boot.scr* and placed in the */ata/usr* directory.

---

**Important! Using *ampreset*, *ampformatfs* or *ampupgrade* in a boot script may lead to unknown state.**

---

## Generating a User Event

TCL scripts are a powerful tool for performing true device management, in the form of customer-defined monitoring and notification of events. A sample script is shown below:

```
#This script performs the monitoring of HTTP servers.
proc pstat {procname port_num} {
    set psef [concat "ps -ef | grep " $procname | grep -v "grep" | wc -l]
    ampexec "stty -echo\r" 5 "#" $port_num
    set output [ampexec "$psef\r" 10 "#" $port_num]
    ampexec "stty echo\r" 5 "#" $port_num
    return [lindex $output 0]
}

# add subscription to an event here.
ampaddsubscription event.user.httpProcess "xyz@xyz.com"

# Run through 4 different servers to find out if HTTP service is running
# on each one of them and trigger an event appropriately.
for {set port_num 0} {$port_num < 4} {incr port_num +1} {
    ampclear $port_num
    amplock $port_num

    set output [pstat httpd $port_num]
    ampunlock $port_num

    if {$output > 0} {
        puts "HTTP_SERVER_OK $port_num"
        amptriggerevent event.user.httpProcess "HTTP service is up and running on
$port_num"
    } else {
        puts " HTTP_SERVER_ERROR $port_num"
        amptriggerevent event.user.httpProcess "HTTP service down on $port_num"
    }
}
}
```

In the Notification tab of the unit, the user can subscribe to either of the following:

*event.user* or *event.user.httpProcess* to get this message: "HTTP service is up and running on 1". To subscribe to user-defined events (defined in the TCL script), the event name must be specified.

---

**Note:** This Event Name must match **EXACTLY** with the event name the user generated using the TCL script. *event.user* will send out a notification whenever this event is triggered. *event.user.httpProcess* will be sent out only when this specific event occurs. The entry must be entered in the notification tab exactly as it appears in the script.

---

## Extensions to TCL

Various extensions have been incorporated into TCL to support functions to interact with the RaritanConsole unit. The command *info comm amp* (executed in a Script Shell Window) lists all the commands that are supported.

*ampsetconfiguration*, *ampaddsubscription*, *amprmsubscription*, *ampsetipacl*, *ampmipacl*, *ampadduser*, *ampmuser* are commands that make configuration changes to the Raritan unit. *ampsave* must be executed in order for the changes to become effective, and may be executed at the end of executing a set of these commands or after each command. Please note that in some cases (network), *ampsave* causes the unit to reboot. Use *ampreload* to revert changes before a save is executed.

### **ampgetconfiguration**

Returns a list of categories that can be displayed

#### **Usage: ampgetconfiguration**

```
% ampgetconfiguration
network
modem
datacom
smtp
radius
```

If a specific category is specified, then the data for that category will be displayed.

#### **Usage: ampgetconfiguration <category><port number>**

- **Category:** can be network, datacom, smtp, and radius
- **Port\_number:** valid port number, applies only to datacom category; otherwise not used

```
% ampgetconfiguration network
Hostname: RaritanConsole_C3200
IP:10.0.1.41
SubnetMask:255.0.0.0
Gateway:10.0.1.41
PortAddress:2398
TerminalType:VT100
```

### **ampsetconfiguration**

Sets the specified field to the value passed. Returns an error if the interpreter cannot get the config lock.

#### **Usage: ampsetconfiguration <category> <field name> <value>**

- **Category:** network, datacom, smtp, radius
- **Field\_name:** field to be altered in a particular category
- **Value:** new value

Setting a specific parameter is done as follows (changing a port configuration):

```
% ampsetconfiguration network portaddress 2398
configuration successful
% ampsave
```

---

**Important! An ampsave command must be executed in order for any changes to take effect. In the instance above, a reboot occurs.**

---

Possible error condition:

```
% ampsetconfiguration network portaddress 2398
TCL cannot write to the configuration: locked by John Smith
```

This denotes that there is a user that is viewing/modifying the configuration of the unit and the command cannot modify the configuration parameters.

### **ampgetuser**

Returns a string listing all the currently configured users and their user account parameters.

#### **Usage: ampgetuser**

```
% ampgetuser
Users: Steve Gaumer John Smith Michael White Fredrick Jones
```

---

*Note: The names are not shown with any delimiters.*

---

If a specific user is specified, only that user's account information is listed. If the user name contains spaces, the name needs to be entered in quotes.

#### **Usage: ampgetuser <user name>**

```
% ampgetuser "Steve Gaumer"
userid:5
loginname:wgaumer
capability:observer
username:Steve Gaumer
userinfo:Network Engineer in Training
Ports:1:2:3:4:5:6:7:8
```

**ampadduser**

Creates a new user account or edit an existing user account. The last argument is optional.

**Usage: ampadduser <loginname> <function> <user name> <password> <portpermission> [information]**

- **Loginname:** user login name
- **Function:** type of user (administrator, operator, observer)
- **User\_name:** name of user; if there are spaces in the name, the name must be entered in quotes
- **Password:** password
- **Port permission:** ports the person will have access to. **For administrator type, use “” for port permission parameter.**
- **Information** (optional): information field; if there are spaces the content must be in quotes

```
% ampadduser pwright observer "Patrick Wright" pass1285 1:2:3:4 "Unix System
Administrator in Training"
user pwright set
% ampsave
save complete

%ampgetuser
Users: Steve Gaumer John Smith Michael White Fredrick Jones Patrick Wright
% ampgetuser "Patrick Wright"
userid:1
loginname:pwright
capability:observer
username:Patrick Wright
userinfo:Unix System Administrator in Training
Ports:1:2:3:4

%
```

ampsave command  
required for changes  
to take effect.

**amprmuser**

Deletes the named user account.

**Usage: amprmuser <user name>**

- **User\_name:** user name to be removed. If there are spaces in the name then the name should appear in quotes i.e. “John Doe”

```
% amprmuser "Patrick Wright"
user deleted

% ampgetuser
Users: Steve Gaumer John Smith Michael White Fredrick Jones Patrick Wright
% ampsave
save complete

% ampgetuser
Users: Steve Gaumer John Smith Michael White Fredrick Jones
%
```

User not removed  
because ampsave  
command has not  
been executed.

**ampreset**

Reboots the unit. All users are disconnected.

**Usage: ampreset****ampupgrade**

Upgrades the unit. `ip_address` specifies the server to obtain the file specified by `file_path`. If the login and password are specified they are used by FTP. If they are not specified, anonymous FTP is used.

**Usage: amppupgrade <ip address> <file path> [login] [password] <port number>**

- **Ip\_address**: location of the files that are to be used in the upgrade
- **File\_path**: location where the files are stored
- **Login** (optional)

**ampgetversion**

Returns a string containing a version report.

**Usage: ampgetversion**

```
% ampgetversion  
  
Kernel version: K.02.00.000  
Software version: K.02.00.000  
GUI version: K.02.00.000
```

**ampgetipacl**

Returns a string containing a list of IP addresses configured to have access to the unit.

**Usage: ampgetipacl**

```
% ampgetipacl  
IP acl: disabled  
acl entries:0  
  
%
```

**ampsetipacl add**

Adds an IP address to the IP ACL list.

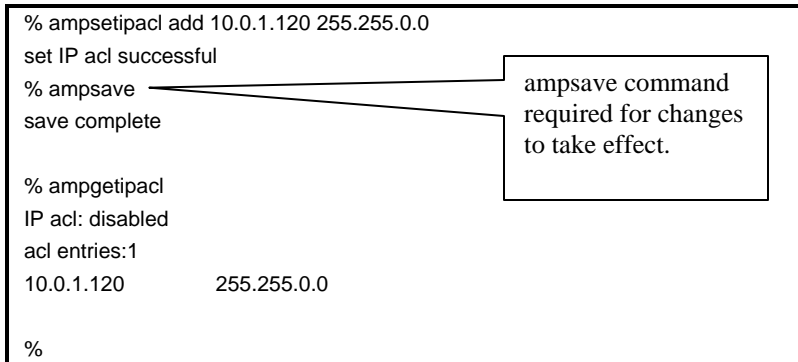
**Usage: ampsetipacl add <ip address> <subnet mask>**

- **Ip\_address:** ip address to be added to the list
- **Subnet\_mask:** subnet mask

```
% ampsetipacl add 10.0.1.120 255.255.0.0
set IP acl successful
% ampsave
save complete

% ampgetipacl
IP acl: disabled
acl entries:1
10.0.1.120      255.255.0.0

%
```


**ampsetipacl**

Either turns on or turns off access-based on-source IP address.

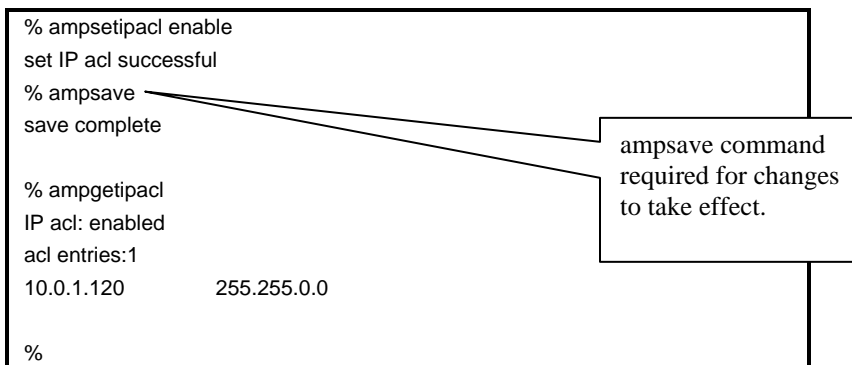
**Usage: ampsetipacl <enable/disable>**

- **Enable:** turns on ip acl
- **Disable:** turns off ip acl

```
% ampsetipacl enable
set IP acl successful
% ampsave
save complete

% ampgetipacl
IP acl: enabled
acl entries:1
10.0.1.120      255.255.0.0

%
```


**amprmipacl**

Removes an IP address from the IP ACL list.

**Usage: amprmipacl <ip address> or amprmipacl <all>**

- **ip\_address:** ip address to be removed from the list
- **All:** remove all the ip addresses from the list

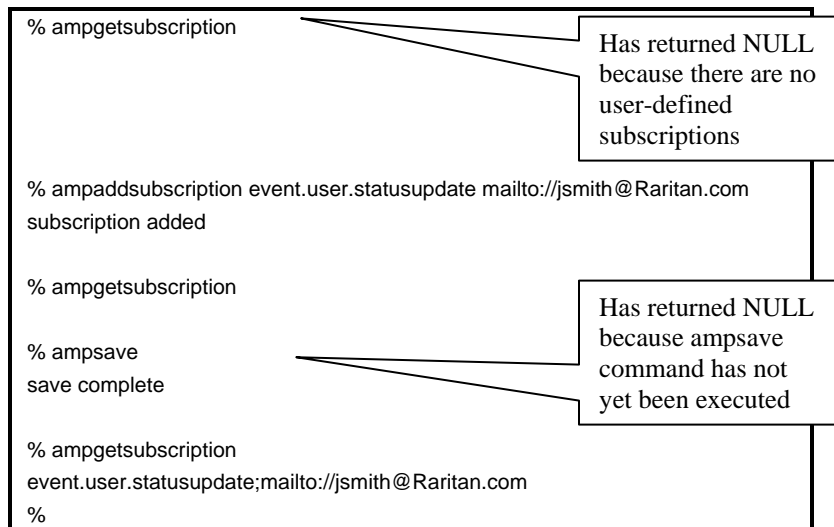


**ampgetsubscription**

Returns a string listing all user-defined subscriptions.

**ampaddsubscription <event> <url>**

Creates a subscription for the URL to the event specified. The URL encapsulates the service to be used for notification, and any parameters required by that service.

**ampunsubscribe <event> <url>**

Deletes the subscription.

**amping <ip address>**

Returns true (1) if a response from the IP address is received within the ping timeout, false (0) if not.

**ampread <timeout> <terminator> <port>**

Returns a string representing the next chunk of console data up to and including the terminator or the end of the data stream when a timeout occurs (in seconds), whichever comes first.

---

*Note: Issue an `ampclear` command to clear old data before starting any new operations. The terminator can be a multi-character (up to 32) string specified in quotes.*

---

**ampwrite <string> <port>**

Writes the string to the console (the script must first lock the write access using `amplock`).

**ampclear <port>**

Clears the buffer from which `ampread` and `ampexec` read.

**ampexec <string> <timeout> <terminator> <port> <number>**

A convenience routine: writes the string to the console and then reads the response until the terminator OR timeout occurs. A typical terminator can be the system prompt to indicate the completion of an execution. The response is returned as a string.

**ampdelay <seconds>**

Pauses the TCL script a number of seconds equal to the integer argument.

**amptriggerevent <event> <message>**

Generates an event with the appropriate associated message. The event may not begin with the amp prefix. Events that begin with the amp prefix may only be generated by the AMP and not by a user created script or interactively.

**amplock <port>**

Gets write access to the console and locks it.

**ampunlock <port>**

Unlocks the console regardless of who has write access to the console. The script must be running as an Administrator to succeed.

**amplisten**

Reads the client input waiting to be read by the interpreter, calls *exec* on the input, and returns the resulting string to the client.

**ampsave**

Saves any changes to the system configuration. In order for changes (network) to take effect, the system will be rebooted.

**ampreload**

Reloads the previous configuration before changes were made.

**amppermission [on/off]**

In order for observers and operators to access a user programmed TCL Script Server, the script must issue *amppermission* off to allow the access.

---

*Note: if the permission is left off without restoring security, non-administrator users may gain privilege access through TCL scripting shell. A reset to the TCL interpreter or the device will reset the permission to on and prevent observer and operator type users from accessing TCL interpreter.*

---

**ampresponse**

Flushes the output buffer to the client who has last requested the data.

**ampopensocket [ip address port number]**

Opens a socket to a specific port on a device with a given IP address. The command returns a unique socket ID. If the command fails or the arguments are improperly formatted, the command will return an error message. The IP address must be specified in “dot notation.” (i.e., 207.25.71.20)

Command Return	Messages
0 (TCL_OK)	Unique socket ID returned
1 (TCL_ERROR)	wrong # args: should be ampopensocket ipAddress port invalid IP address %s Invalid Port Number %s, values allowed between [0-65535] Invalid Port Number %s, only 16 bits digit allowed open socket failed

**ampwritesocket [socket id message]**

Sends a string to the socket represented by the socket ID. If the write fails or the arguments are invalid, the command will return an error with an error message.

Command Return	Messages
0 (TCL_OK)	No message returned
1 (TCL_ERROR)	wrong # args: should be ampwritesocket socketDescriptor message. Command failed Invalid Socket Descriptor %s write socket failed

**ampclosesocket [socket id]**

Closes the socket represented by the socket ID. If the command fails or the arguments are invalid, the command will return an error with an error message.

Command Return	Messages
0 (TCL_OK)	No message returned
1 (TCL_ERROR)	wrong # args: should be ampclosesocket socketDescriptor Invalid Socket Descriptor %s close socket failed

**ampreadsocket [socket\_id length timeout]**

A non-blocking call: reads from the socket represented by the socket ID until either the length or timeout is reached. Timeout is specified in microseconds; a timeout of zero indicates the socket will be polled and the results returned immediately. The command returns a buffer with the data read, and if the data available to read is less than the length requested, the command returns a buffer with the data read. If there is no data read or timeout occurs, the command returns an “OK” with an empty buffer. If the command fails or the arguments are invalid, the command will return an error with an error message.

Command Return	Messages
0 (TCL_OK)	No data read Actual data read Timeout occurred
1 (TCL_ERROR)	Command failed: "not enough memory" Command failed: "Invalid Socket Descriptor OR read socket failed" Arguments invalid: "wrong # args: should be ampreadsocket socketDescriptor messagelength timeout" Arguments invalid: "Invalid Socket Descriptor %s" Arguments invalid: "invalid length %s, only digits allowed" Arguments invalid: "invalid timeout %s, only digits allowed"

---

**Note:** Issue an *ampclear* command to clear old data before starting any new operations.

---

**ampgetmacaddress**

Returns the Ethernet MAC address of the unit.

**ampsetconfig datacom checkparity <value>**

Enables the parity bit if value is 1; disables the parity bit if value is 0.

An administrator/operator user will not have write access in a console window when a TCL script is running and has executed *amplock* for that port. Issuing an F8 or “Get Write Access” will **not** result in getting writing access.

In order for the administrator/operator user to get write access, one of the following methods must be used.

1. Administrator issues a *Reset* to the TCL interpreter by pressing the [**Reset**] button in the Script shell window.
2. Operator/Observers execute the [**Reset**] button in the script shell window if the TCL script running has the *amppermission* off command built into the script.
3. A TCL script may be designed to accept input from users (administrators and operator/observers if *amppermission* off has been performed by the script) and based on the input, may either exit the execution of the script or release the lock and wait for further input before getting the lock and continuing execution of the script. In this case, the Administrator/Operator must be aware of the inputs that may be sent to the running TCL script and type the appropriate word/number in the Script shell window to gain write access to the console and relinquish write access if appropriate.

## Basic TCL Server Example

```
while (1) {
    amppermision off
    set s ""
    set s [amplisten]
    if {[string length $s] !=0} {
        puts $s
        amppresponse
    }
    if {[string length $s] == 5} {
        amppermision on
        break
    }
}
```

### **Script Function Description:**

This TCL Server will echo back any strings from any client who connects to the TCL interpreter through the TCL Scripting Window.

### **Key programming points:**

*amplisten* checks to see if there is a new command from any client.

*Puts* will push back the response to the output buffer.

*amppresponse* will push the previous response back to the EXACT client who sent the command.

Due to security, the TCL scripting feature is not normally accessible by Operators or Observers. However, for the TCL Server to be general, Operators and Observers need access to the TCL scripting feature. *amppermision* allows such communication. Also, when reset, *amppersmission* will, by default, be on. (Hence, only explicit “unlocks” by the Administrator are allowed.)

## Basic CPU Utilization Monitoring Example

```
#Description: This TCL script checks the CPU utilization for each port connected
#             to a HP-UX server. It alerts the subscribed user that the threshold
#             limit has reached through e-mail notification. This TCL script uses
#             vmstat to find out the CPU usage of the user process and checks with
#             given threshold limit. During the process user can input the threshold
#             limit or the interval through the following commands:
#             THR <threshold> - Input of threshold
#             INTR <interval> - Interval at which the TCL script has to do checking.
#             To quit out of the script type QUIT and hit enter

#Default threshold is 2 %
set thr 2
#Default interval is 10 seconds
set intr 10

#change this mail id to your own
set mailid "mailto://xyz@xyz.com"

#initialize events
proc initEvents { } {
    global mailid
    #add subscriptions to events.
    ampaddsubscription event.alarm.cpu $mailid
    #save subscription
    ampsave
}

#delete events. Called during QUIT
proc delEvents { } {
    global mailid
    #delete subscriptions to events
    amprmsubscription event.alarm.cpu $mailid
    #save configuration
    ampsave
}

#Retrive cpu utilization for user process,
#check if it has reached the threshold and trigger an event

proc cpuUtil { port } {
    global thr

    set us 0
    set sy 0
    set id 0

    #lock the console
    amlock $port
```

```

#clear any previous data in the read buffer
ampclear $port

#write to the console
ampwrite "vmstat -n\n" $port

#ignore the first 8 lines to read the cpu usage params.
for {set i 0} {$i < 9} {incr i +1} {
    set cpu [ampread 1 "\n" $port]
}

#unlock the console
ampunlock $port

#set the user's cpu usage
scan $cpu "%d %d %d" us sy id

#Trigger event if user process utilization has gone beyond threshold
if { $us > $thr } {
    amptriggerevent event.alarm.cpu "User Process CPU utilization goes beyond threshold
$thr on port$port"
}
}

#listen to command inputs from user - QUIT/THR/INTR
proc ListenCmds { } {

    global thr incr

    set cmd [amplisten]
    if { [string compare $cmd "QUIT"] == 0 } {
        puts "Quitting"
        ampresponse
        return 1
    } elseif [string match THR* $cmd] {
        scan $cmd "%s %d" c thr
        puts "Threshold is $thr"
        ampresponse
    } elseif [string match INTR* $cmd] {
        scan $cmd "%s %d" c intr
        puts "Interval now is $intr"
        ampresponse
    }
    ampresponse
}

set ports 1
set noOfPorts 2

```

```
initEvents
```

```
#Main loop starts here...
```

```
while { 1>0 } {
    cpuUtil $ports
    ampdelay $intr
    set rval [ListenCmds]
    if { $rval == 1 } {
        delEvents
        unset $ports
        unset $noOfPorts
        unset $thr
        unset $intr
        unset $mailid
        break
    }
    incr ports 1
    if { $ports > $noOfPorts } {
        set ports 1
    }
}
```

#### **Script Function Description:**

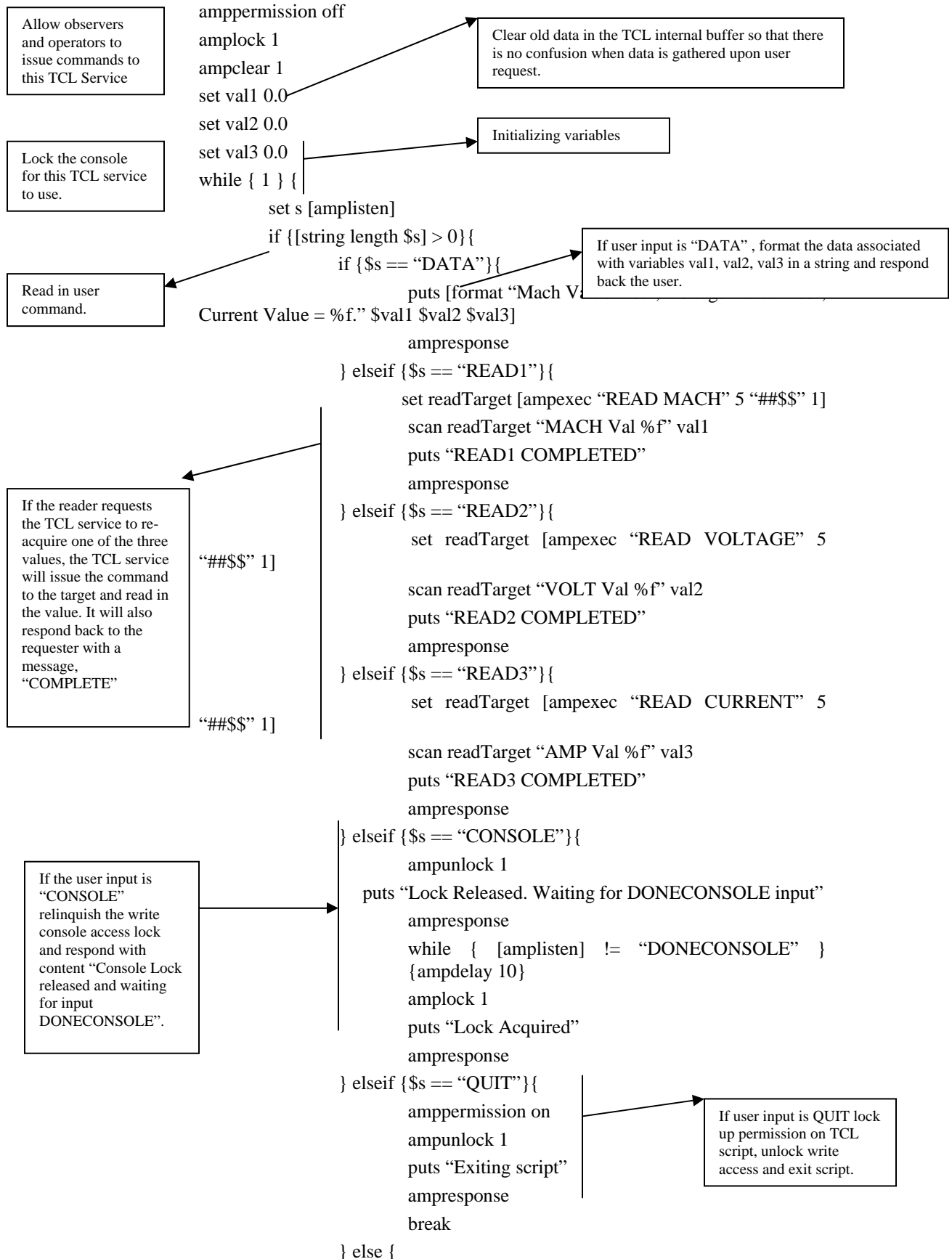
It is required to monitor CPU usage of user process running on several HP-UX machines through RS232 console connections. This TCL script will monitor the use through the well-known *vmstat* functionality given by HP-UX. When CPU utilization has surpassed the given limit, this script will trigger an event that notifies the subscribed users via e-mail. The user is allowed to input the threshold limit or the frequency through his/her own commands (This example use THR and INTR respectively).

#### **Key programming points:**

- Use *ampclear* to remove all history information for a port
- Use *ampread* with “\n” as terminator since the script has to read each line to find out the user process utilization that is on the 10<sup>th</sup> line.
- Use *amptriggerevent* to trigger a user-defined event *event.alarm.cpu*. The event may not begin with “amp,” as that namespace is reserved for system-generated events. A user may subscribe to events related only to one server by designating which server they are interested in. For example, a user may subscribe to *event.alarm.cpu.2* to receive a notification when cpu utilization on server 2 is measuring above 10 %.
- The event will be sent only if the user who requests the notification is properly subscribed in the Notification subscription list.
- In the subscription option, the User must type in the EXACT event shown previously: *event.alarm.cpu*.
- Delay 10 seconds so the script does not overflow the e-mail system. This is configurable using the command **INTR** while this script is running using the *amplisten* facility.



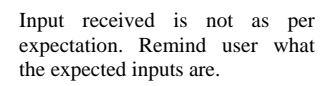
## TCL Server designed to interact with a TCL user



puts "A TCL script is running.\rInputs accepted are DATA/READ1/READ2/READ3/CONSOLE/QUIT"

ampresponse

```
}  
}  
}
```



Input received is not as per expectation. Remind user what the expected inputs are.

# Appendix I: Troubleshooting

## Problems and Suggested Solutions

### Page Access

PROBLEM	SOLUTION
Cannot login – what are factory defaults? (only for Dominion SX units running firmware version 2.5 or higher)	username: <b>admin</b> (all lower case) password: <b>raritan</b> (all lower case)
Server Unreachable	<p>If a unit appears to be unreachable by a given browser, please run through the following troubleshooting list:</p> <p>Verify that the unit is powered on.</p> <p>Verify that the unit is properly connected to a network.</p> <p>Ping the unit from a computer on the same network to ensure that network communication with the unit occurs.</p> <p>Should the <i>ping</i> fail, contact your network administrator. There may be a problem with your network configuration that is preventing communication with the unit.</p> <p>Should the <i>ping</i> succeed, consult the following topics.</p>
DNS Error/Server Unreachable	<p>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.</p> <p>Remove any installed Dominion SX certificates and restart the browser.</p>
Unsupported Encryption	<p>The unit supports only 128-bit SSL encryption.</p> <p>In Internet Explorer, view <b>Help→About Internet Explorer</b> and determine the maximum SSL bit strength for the browser. If it is not at the desired strength, it is recommended that the browser be upgraded.</p> <p>In Netscape, view <b>Communicator→Tools→Security Info→SSL v3.0 Configuration</b> and ensure that 128-bit SSL is supported</p>
Number of Users Exceeded	<p>The unit has a security measure that allows only a specific number of login pages to be authenticated at any given time. Should this number be reached when attempting to login to the unit, a pop-up window will be displayed indicating that the maximum number of users is exceeded. This is normal behavior for the unit.</p> <p>Wait for a few minutes and attempt to login again. Note that you may need to refresh or &lt;<b>Shift+Refresh</b>&gt; your browser to successfully log on.</p>

## Firewall

PROBLEM	SOLUTION
Unable to Access the Web Page	Firewalls must allow access on port 80 and 443 in order for the unit to operate through a firewall. Contact your system administrator and request port 80 and 443 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 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

PROBLEM	SOLUTION
Login Failure	To provide additional security, the unit login screen expires after 20 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 on the <b>[Reload]</b> button 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 to be a local user is considered to be a RADIUS user when RADIUS is enabled. Should the RADIUS server not be 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. Please be patient and wait until either the user successfully logs in, or the Authentication Denied message is displayed.

## Port Access

PROBLEM	SOLUTION
Port Access Refresh	<p>The unit does not automatically refresh the Port Access List. It is refreshed only when the user clicks on the <b>[Port Access]</b> button, 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 <b>[Port Access]</b> button is activated.</p> <p>A window will appear indicating that permission is no longer allowed to this port.</p> <p>Whenever possible, it is recommended that Administrators not change port access rights to a user who is already logged in to the unit.</p>

## Upgrade

PROBLEM	SOLUTION
FTP - Server Unreachable	<p>Should the FTP server specified in the upgrade panel be unreachable or incorrect, the upgrade process will halt until a response is received from the FTP server or until a timeout occurs.</p> <p>Please wait and allow the FTP Server Unreachable message to appear.</p>
FTP - File Not Found	<p>The unit requires a package of upgrade files to be in the directory specified by the upgrade path. This package must have all included files and an <b>upgrade.cnf</b> file. Should this file not exist, or if the contents of the file are not in the indicated places, the File Not Found message will appear.</p> <p>Verify that the upgrade package is in the correct directory and confirm the upgrade path and IP address of the FTP server.</p> <p>If the upgrade still fails, reinstall the upgrade package and begin again.</p>

## Modem

PROBLEM	SOLUTION
Login Failure	<p>The unit supports Web-browser access through the modem at connection speeds of 28.8K bps or greater. Should the baud rate be insufficient, the user will be unable to log on to the unit via the modem.</p> <p>28.8K bps minimum connection speed is recommended for browser-based modem authentications (login). For CLI-based access, using SSH or Telnet, speed as low as 9600bps is adequate.</p>



## Appendix J: Technical FAQs

QUESTION	ANSWER
What are the browsers (and versions) supported?	Netscape 7.0 or greater (but not 6.0), Mozilla Firefox 1.0 or higher, or Internet Explorer 6.0 with Java Microsoft VM or SUN JRE 1.4.2 or higher.
Is the status of the unit limited by the status of the device or equipment to which it is attached (i.e. Server, router, firewall, load balancer, or other network device)?	No, because the unit is a totally “out of band” solution that runs on its own dedicated microprocessor. Even if the target devices to which the Dominion SX is attached are turned off, you will still be able to access the unit.
Can I reset the unit without losing my settings?	<p>There are two ways to perform a basic reset without losing your user-defined settings: (1) Click on the <b>[Reset]</b> button in the left panel of the Main Menu screen, or (2) Switch off power from the unit, and then switch the power back on. Using either of these two methods, the previously established IP address and all other user-defined settings will be preserved.</p> <p><b>Important:</b> Performing a “soft” reset as described above will log all users off the unit. Users will be able to access the unit again once the unit’s boot sequence is complete.</p>
How do I reset the unit back to its factory-default settings?	<p>To perform a factory default reset, which will erase all custom settings and re-establish the factory default settings, attach the “factory reset fixture” to the unit’s 9-pin serial port (located on the back of the chassis), turn the unit off, wait a few seconds, turn the unit back on, and allow the unit to complete the factory default reset sequence. This will take about 60 seconds. The factory default reset sequence consists of the following: A solid green light for about 5 seconds, then no light for about 15-20 seconds, then another solid green light for about 5 seconds and then 3 green flashes (about 1 second each). The total time for this sequence is generally <u>about 40 seconds</u>. The IP address for the unit will be reset to <b>192.168.0.192</b>.</p> <p><b>Important:</b> Performing a “hard” reset as described above will log all users off the unit. Users will not be able to access the unit again until the unit is re-configured.</p> <p>For SX4, SX8, and all other models with a RESET switch on the rear panel, using a ball-point pen (please do not use a graphite pencil), while the unit is powered ON, push in and hold the switch for about 30 seconds (or until the blue LED on the front of the unit goes off), and then release the switch. Only gentle pressure is required. The SX unit will detect the RESET switch and reset the unit to factory default. It will take about 60 seconds for the unit to reboot. On these units, a reset to factory defaults can be performed with the unit powered ON.</p>
Does the unit need to be on the same physical LAN as the client_host during installation and setup?	Yes, the unit must be on the same physical LAN as the client_host during installation and setup. There should be no intermediate IP routers between the unit and the client_host during this stage.
Once the physical installation is complete and my ping query elicits a response from the unit, how do I initially access the unit and begin the process to customize the unit?	Open a supported network-enabled web browser, type “ <b>192.168.0.192</b> ” in the address line, and press the <Enter> key. You will be presented with the start-up screen for the unit, and prompted through the entire set-up process. Once setup is complete, you will log off the console, and use the IP address you assigned during set-up to re-access the unit.

QUESTION	ANSWER
Once I have assigned the unit a unique IP address, how do I access the unit in the future?	Open your supported Web browser, enter the IP address you have assigned to that unit into the Address field, and press the <Enter> key. The login/password screen for the unit will appear.
Can I assign specific port access to a specific user?	Yes, but only if the user is NOT an Administrator. Administrator will always have access to all the ports.
Sometimes when I try to log on, I see a message that states my “login is incorrect” even though I am sure I am entering the correct User Name and Password. Why is this?	There is a session-specific ID that is sent out each time you login to the unit. This ID has a time-out feature, so if you do not login to the unit before the time-out occurs, then the session ID becomes invalid. Performing a <Shift-Reload> refreshes the page from the unit, and not from the now-expired cache. Similarly, you may close the current browser, open a new browser, and login again. This provides an additional security feature so that no one can recall information stored in cache to access the unit.
What should I do if the browser returns with the message that the device timed out?	Try reloading using <Shift-Reload>. If this does not work, check your network connections and network status. You may also want to <b>ping</b> the console or perform a <b>route print</b> (as described in other FAQs) to ensure that proper network communication is occurring. If a web page does not load to your browser, there are probably network difficulties that are preventing the page from loading.
How do I upgrade the Dominion SX software?	Software upgrades are easy to perform on the unit. In the Main Menu screen, click “ <b>Upgrade</b> ” and then follow the prompts. You will need to enter the “ <b>IP Address</b> ” and “ <b>File Path</b> ” to perform the upgrade.
What if I forget or lose my password?	Any Administrator can assign any user (Administrator, Operator, or Observer) a new password if it is forgotten or lost. <b>Important:</b> If there is only one Administrator, and he/she forgets his/her password, then the unit must be factory-reset and re-configured from the initial set-up screen. In this case, all saved values would be lost.
Is there any way for me to optimize the performance of Microsoft Internet Explorer if it is my preferred Web browser?	To improve the performance of Microsoft Internet Explorer when accessing the console, disable <b>JIT compiler for virtual machine enabled, Java logging enabled, and Java console enabled</b> . Select <b>Tools→Internet Options→Advanced</b> from the main menu. Scroll through the list until you see the above items and make sure that they are disabled.
I am having trouble using the 128-bit SSL on the unit. Do you know what might be causing this?	It is likely that the browser you are using does not support 128-bit SSL encryption. Depending on the version of browser installed on your workstation, you may need to either (1) install a 128-bit SSL compatible version of your browser, or (2) upgrade your current browser to be 128-bit SSL compatible. Refer to the browser manufacturer’s web site for instructions.
Sometimes when I am trying to dial-in to the unit or when I am connected to the unit via the modem and I lose my connection, if I immediately try to dial-in again, I can’t get connected. However, if I wait for a few minutes, the dial-in is successful. Why is this?	In this case, “a few minutes” is the key: The modem has a pre-defined “clean up time” after every connection ends. It does not matter whether the connection is dropped, severed, or intentionally closed by the user. The modem will take about one minute to re-cycle itself to be ready for the next incoming call.





255-60-2000