SLC™ Console Manager User Guide

- SLC8
- SLC16
- SLC32
- SLC48

Part Number 900-449
Revision I November 2013

Copyright and Trademark

Warranty

For details on the Lantronix warranty replacement policy, please go to our web site at http://www.lantronix.com/support/warranty.

Open Source Software

Some applications are Open Source software licensed under the Berkeley Software Distribution (BSD) license or the GNU General Public License (GPL) as published by the Free Software Foundation (FSF). Redistribution or incorporation of BSD or GPL licensed software into hosts other than this product must be done under their terms. A machine readable copy of the corresponding portions of GPL licensed source code is available at the cost of distribution.

Such Open Source Software is distributed WITHOUT ANY WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. See the GPL and BSD for details.

A copy of the licenses is available from Lantronix. The GNU General Public License is available at http://www.gnu.org/licenses/.

Contacts

Lantronix, Inc.
Corporate Headquarters
167 Technology Drive
Irvine, CA 92618, USA

Toll Free:	800-526-8766
Phone:	949-453-3990
Fax:	949-453-3995

Technical Support
Online: www.lantronix.com/support

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.

Disclaimer and Revisions

Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Notes:

- *This equipment has been tested and found to comply with the limits for Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.*
- *This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user guide, may clause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.*
- *The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.*
- *Changes or modifications to this device not explicitly approved by Lantronix will void the user's authority to operate this device.*
- *The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide. For the latest revision of product documents, please check our online documentation at www.lantronix.com/support/documentation.*

Revision History

Date	Rev.	Comments
June 2006	A	Initial Release
August 2006	B	Added event configuration, local/remote user authentication precedence, firmware update via HTTPS, complex passwords, and port permissions for remote users.
January 2007	C	Added dial-in & dial-on-demand modem state, IP filters, active directory to LDAP section, and additional TACACS+ servers.
April 2007	D	Added ability to import site-specific SSL certificates and SSH host keys, to display a list of web sessions, to set an IP filter timer, and to save system logs across reboots. Enabled dual boot-up.
August 2007	E	Added gateway page, phone home; alarm delay; SSH v1 logins; trap community; configuration manage option; system logs beginning and end dates, device port logging to syslog.
April 2008	F	New web page design with tabbed menus. Added support for the following: Sensorsoft devices; SecureID over Radius; command and status of the SLP expansion chassis; escape and break sequences for remote users; password aging, iGoogle Gadget; SNMP v3 encryption; ability to copy boot bank; host lists for outgoing modem and direct connection at the CLI; new option for local users to display a custom menu at login.
January 2010	G	Added support for Interface and Batch Scripting, Ethernet Bonding, configurable LCD screens and scrolling, redesigned SLC Network web page, Email Log, Firmware Update vi PC Card and NFS, SLC Temperature, and PPP dialback (including CallBack Control Protocol).
March 2010	H	Updated for USB support that was added in firmware 5.5.
November 2013	I	Updated product name and trademark information.

Table of Contents

List of Figures

List of Tables

1: About This Guide

This guide provides the information needed to install, configure, and use the products in the Lantronix® SLC™ Console Manager family. It is for IT professionals who must remotely and securely configure and administer servers, routers, switches, telephone equipment, or other devices equipped with a serial port.

Note: *The features and functionality described in this document specific to PC Card use are supported on SLC-02 part numbers. The features and functionality specific to USB port use are supported on SLC-03 part numbers.*

This chapter contains the following sections:

- *Chapter Summaries*
- *Conventions*
- *Additional Documentation*

Chapter Summaries

Table 1-1 lists and summarizes each chapter and appendix.

Table 1-1Chapter/Appendix and Summary

Chapter/Appendix	Summary
Chapter 2: Overview	Describes the SLC models, main features, and supported protocols.
Chapter 3: Installation	Provides technical specifications; describes connection formats and power supplies; provides instructions for installing the unit in a rack.
Chapter 4: Quick Setup	Provides instructions for getting your unit up and running and for configuring required settings.
Chapter 5: Web and Command Line Interfaces	Describes the web and command line interfaces available for configuring the unit. ***Note:*** *Chapters 7: Services, 8: Devices, 9: PC Cards, 10: USB Port, 11: Connections, and 12: User Authentication provide detailed instructions for using the web interface and include command line interface commands.*
Chapter 6: Basic Parameters	Provides instructions for configuring network ports, firewall and routing settings, and date and time.
Chapter 7: Services	Provides instructions for enabling and disabling system logging, SSH and Telnet logins, SNMP, SMTP, and the date and time.
Chapter 8: Devices	Provides instructions for configuring global device port settings, individual device port settings, and console port settings.
Chapter 9: PC Cards	Provides instructions for configuring storage (Compact Flash) and modem/ISDN PC cards.

Table 1-1Chapter/Appendix and Summary (continued)

Chapter/Appendix	Summary
Chapter 10: USB Port	Provides instructions for configuring USB storage devices (thumb drive) or USB modems.
Chapter 11: Connections	Provides instructions for configuring connections and viewing, updating, or disconnecting a connection.
Chapter 12: User Authentication	Provides instructions for enabling or disabling methods that authenticate users who attempt to log in via SSH, Telnet, or the console port. Provides instructions for creating custom menus.
Chapter 13: Maintenance	Provides instructions for upgrading firmware, viewing system logs and diagnostics, generating reports, and defining events. Includes information about web pages and commands used to shut down and reboot the SLC console manager.
Chapter 14: Application Examples	Shows how to set up and use the SLC device in three different configurations.
Chapter 15: Command Reference	Lists and describes all of the commands available on the SLC command line interface
Appendix A: Bootloader	Lists and describes the commands available for the bootloader command line interface.
Appendix B: Security Considerations	Provides tips for enhancing SLC security.
Appendix C: Safety Information	Lists safety precautions for using the SLC console manager.
Appendix D: Sicherheitshinweise	Lists safety precautions for using the SLC device in German.
Appendix E: Adapters and Pinouts	Includes adapter pinout diagrams.
Appendix F: Protocol Glossary	Lists the protocols supported by the SLC console manager with brief descriptions.
Appendix G: Compliance Information	Provides information about the SLC compliance with industry standards.
Appendix H: DC Connector Instructions	Provides -48VDC plug connector instructions for the SLC console manager.
Appendix I: LDAP Schemas	Provides information about configuring LDAP schemas in Windows active directory.

Conventions

Table 1-2 lists and describes the conventions used in this book.

Table 1-2 Conventions Used in This Book

Convention	Description
Bold text	Default parameters.
Brackets [ ]	Optional parameters.
Angle Brackets < >	Possible values for parameters.
Pipe |	Choice of parameters.
Warning	***Warning:*** ***Means that you are in a situation that could cause equipment damage or bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.***
Note	***Note:*** *Means take notice. Notes contain helpful suggestions, information, or references to material not covered in the publication.*
Caution	***Caution:*** ***Means you might do something that could result in faulty equipment operation, or loss of data.***
Screen Font (Courier New)	CLI terminal sessions and examples of CLI input.

Additional Documentation

Visit the Lantronix web site at www.lantronix.com/support/documentation for the latest documentation and the following additional documentation:

- ***SLC Console Manager Quick Start***—Describes the steps for getting the SLC console manager up and running.
- ***SLC Console Manager Online Help for the Command Line Interface***—Provides online help for configuring the SLC console manager using commands.
- ***SLC Console Manager Online Help for the Web Interface***—Provides online help for configuring the SLC console manager using the web page.
- ***Detector™ Online Help***—Provides online help for assigning a static IP address to the SLC console manager using the Lantronix® Detector™ tool.

2: Overview

SLC console managers are members of a secure IT management family of products. These products offer systems administrators and other IT professionals a variety of tools to securely access and manage their resources. Lantronix has been an innovator in this market with terminal servers and secure console servers, as well as other remote access devices. The SLC console managers build on that foundation and offer new features and capabilities.

IT equipment can be configured, administered, and managed in a variety of ways, but most devices have one method in common: an RS-232 serial port, sometimes called a console, auxiliary, or management port. These ports are often accessed directly by connecting a terminal or laptop to them, meaning that the administrator must be in the same physical location as the equipment. SLC console managers give the administrator a way to access them remotely from anywhere there is a network or modem connection.

Many types of equipment can be accessed and administered using Console Managers including:

- **Servers:** Unix, Linux, Windows 2003, and others.
- **Networking equipment:** Routers, switches, storage networking.
- **Telecom:** PBX, voice switches.
- **Other systems with serial interfaces:** Heating/cooling systems, security/building access systems, UPS, medial devices.

The key benefits of using Console Managers:

- **Saves money:** Enables remote management and troubleshooting without sending a technician onsite. Reduces travel costs and downtime costs.
- **Saves time:** Provides instant access and reduces response time, improving efficiency.
- **Simplifies access:** Enables you to access equipment securely and remotely after hours and on weekends and holidays—without having to schedule visits or arrange for off-hour access.
- **Protects assets:** Security features provide encryption, authentication, authorization, and firewall features to protect your IT infrastructure while providing flexible remote access.

SLC console servers provide features such as convenient text menu systems, break-safe operation, port buffering (logging), remote authentication, and Secure Shell (SSH) access. Dial-up modem support ensures access when the network is not available.

This chapter contains the following sections:

SLC Models and Part Numbers

The SLC models offer a compact solution for remote and local management of up to 48 devices, for example, servers, routers, and switches with RS-232C (now EIA-232) compatible serial consoles in a 1U-tall rack space. All models have two Ethernet ports called Eth1 and Eth2 in this document. There are two groups of models with different part numbers - one group of models with a USB port (part number -03) and one group of models with PC Card slots (part number -02).

Two Ethernet ports are useful when you want to use one port on a private, secure network and the other on a public, unsecured network.

Table 2-1 lists the part numbers, models, and descriptions.

Table 2-1 SLC Part Numbers, Models, and Descriptions

Part Number USB	Part Number PC Card Slots	Model and Description
SLC00812N-03	**SLC00812N-02**	**SLC8:** 8 port, Single AC Supply Secure Console Manager
SLC01612N-03	**SLC01612N-02**	**SLC16:** 16 Port, Single AC Supply Secure Console Manager
SLC03212N-03	**SLC03212N-02**	**SLC32:** 32 Port, Single AC Supply Secure Console Manager
SLC04812N-03	**SLC04812N-02**	**SLC48:** 48 Port, Single AC Supply Secure Console Manager
SLC00822N-03	**SLC00822N-02**	**SLC8**: 8 Port, Dual AC Supply Secure Console Manager
SLC01622N-03	**SLC01622N-02**	**SLC16:** 16 Port, Dual AC Supply Secure Console Manager
SLC03222N-03	**SLC03222N-02**	**SLC32:** 32 Port, Dual AC Supply Secure Console Manager
SLC04822N-03	**SLC04822N-02**	**SLC48:** 48 Port, Dual AC Supply Secure Console Manager
SLC00824N-03	**SLC00824N-02**	**SLC8:** 8 Port, Dual DC Supply Secure Console Manager
SLC01624N-03	**SLC01624N-02**	**SLC16:** 16 Port, Dual DC Supply Secure Console Manager
SLC03224N-03	**SLC03224N-02**	**SLC32:** 32 Port, Dual DC Supply Secure Console Manager
SLC04824N-03	**SLC04824N-02**	**SLC48:** 48 Port, Dual DC Supply Secure Console Manager

The products differ in the number of device ports provided, USB port or PC Card slots, and AC or DC power availability. Some models have dual entry redundant power supplies for mission critical applications. These models are available in AC or DC powered versions. *Figure 2-2* depicts the SLC48 console manager with PC Card slot (a part number -02) and *Figure 2-3* depicts the SLC48 console manager with USB port (a part number -03).

Figure 2-2 Lantronix SLC48 Console Manager with PC Card Slots

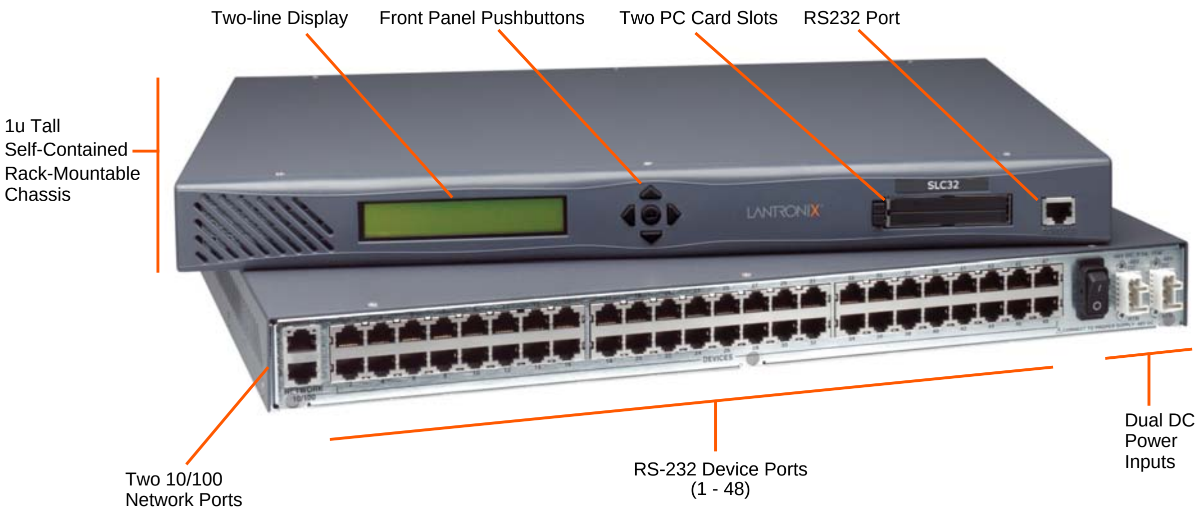
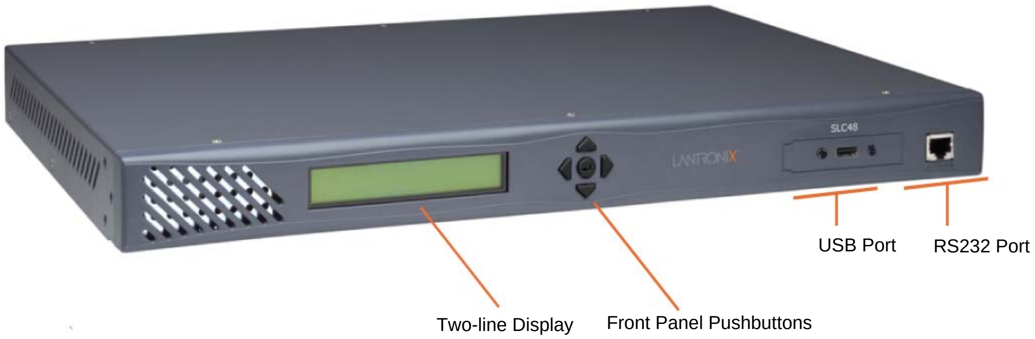


Figure 2-3 Lantronix SLC48 Console Manager with USB Port



System Features

The SLC console manager has the following capabilities:

- Connects up to 48 RS-232 serial consoles
- 10Base-T/100Base-TX Ethernet network compatibility
- Buffer logging to file
- Email and SNMP notification
- ID/Password security, configurable access rights
- Secure shell (SSH) security; supports numerous other security protocols
- Network File System (NFS) and Common Internet File System (CIFS) support
- Telnet or SSH to a serial port by IP address per port or by IP address and TCP port number

- Configurable user rights for local and remotely authenticated users
- Supports an internal PC Card modem, USB modem, or an external modem
- No unintentional break ever sent to attached servers (Solaris Ready)
- Simultaneous access on the same port - “listen” and “direct” connect mode
- Local access through a console port
- Web administration (using most browsers)

Protocols Supported

The SLC console manager supports the TCP/IP network protocol as well as:

- SSH, Telnet, PPP, NFS, and CIFS for connections in and out of the SLC console manager
- SMTP for mail transfer
- DNS for text-to-IP address name resolution
- SNMP for remote monitoring and management
- FTP and SFTP for file transfers and firmware upgrades
- TFTP for firmware upgrades
- DHCP and BOOTP for IP address assignment
- HTTPS (SSL) for secure browser-based configuration
- NTP for time synchronization
- LDAP, NIS, RADIUS, CHAP, PAP, Kerberos, TACACS+, and SecurID (via RADIUS) for user authentication
- Callback Control Protocol (CBCP)

For descriptions of the protocols, see *Chapter 6: Protocol Glossary* .

Access Control

The system administrator controls access to attached servers or devices by assigning access rights to up to 128 user profiles. Each user has an assigned ID, password, and access rights. Other user profile access options may include externally configured authentication methods such as NIS and LDAP.

Device Port Buffer

The SLC console manager supports real-time data logging for each device port. The port can save the data log to a file, send an email notification of an issue, or take no action.

You can define the path for logged data on a port-by-port basis, configure file size and number of files per port for each logging event, and configure the device log to send an email alert message automatically to the appropriate parties indicating a particular error.

Configuration Options

You may use the backlit front-panel LCD display for initial setup and later to view and configure current network, console, and date/time settings.

Both a web interface viewed through a standard browser and a command line interface (CLI) are available for configuring the SLC console manager settings and monitoring performance.

Hardware Features

The SLC hardware includes the following:

- 1U-tall (1.75 inches) rack-mountable secure console server
- Two 10Base-T/100Base-TX network ports
- Up to 48 RS-232 serial device ports connected via Category 5 (RJ45) wiring
- One serial console port for VT100 terminal or PC with emulation
- Two PC Card slots or one USB port
- 256 Kbytes-per-port buffer memory for device ports
- LCD display and keypad on the front
- Universal AC power input (100-240V, 50/60 Hz); options include single input, single supply or dual input, redundant supplies
- -48 VDC power input, dual input, redundant power supplies
- Convection cooled, silent operation, low power consumption

Note: *For more detailed information, see Technical Specifications on page 26.*

All physical connections use industry-standard cabling and connectors. The network and serial ports are on the rear panel of the SLC console manager, and the console port is on the front. Required cables and adapters for certain servers, switches, and other products are available from Lantronix at www.lantronix.com.

Serial Connections

All devices attached to the device ports and the console port must support the RS-232C (EIA-232) standard. Category 5 cabling with RJ45 connections is used for the device port connections and for the console port. For pinout information, see 5: Adapters and Pinouts on page 272.

Note: *RJ45 to DB9/DB25 adapters are available from Lantronix.*

Device ports and the console port support eight baud-rate options: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The ports are shown in *Figure 2-4* and *Figure 2-5*.

Figure 2-4 Device Port Connections

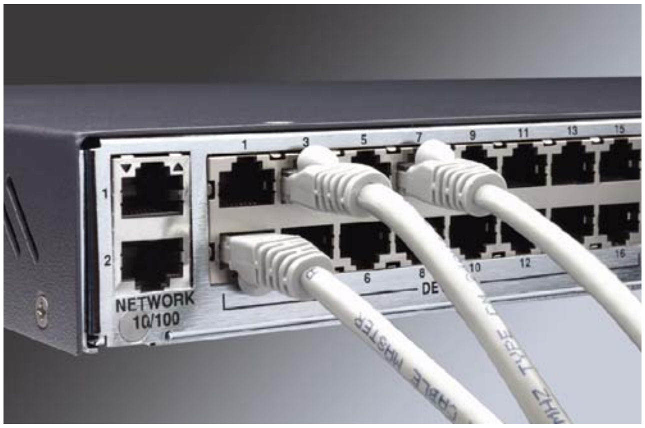
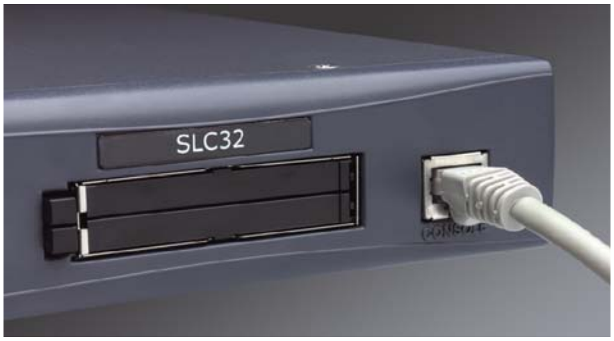


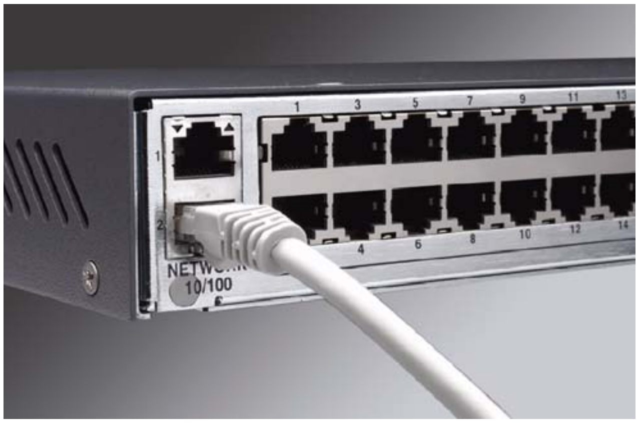
Figure 2-5 Console Port Connection



Network Connections

The SLC network interfaces are 10Base-T/100Base-TX connectors for use with a conventional Ethernet network as shown in *Figure 2-6*. Use standard RJ45-terminated Category 5 cables. Network parameters must be configured before the SLC console manager can be accessed over the network.

Figure 2-6 Network Connection

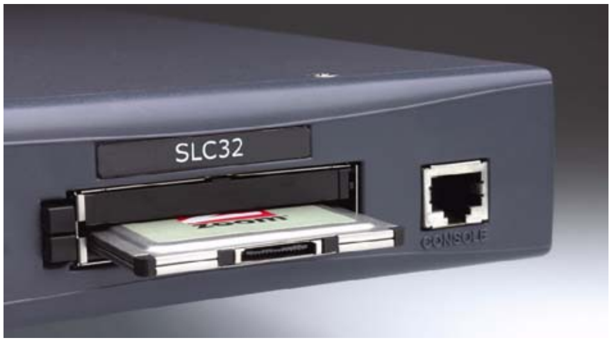


PC Card Interface

Note: *This PC Card interface is only supported on SLC -02 part numbers.*

The SLC console manager has two PC Card slots as shown in *Figure 2-7*. Lantronix qualifies cards continuously and publishes a list of qualified cards on the Lantronix web site.

Figure 2-7 PC Card Interface

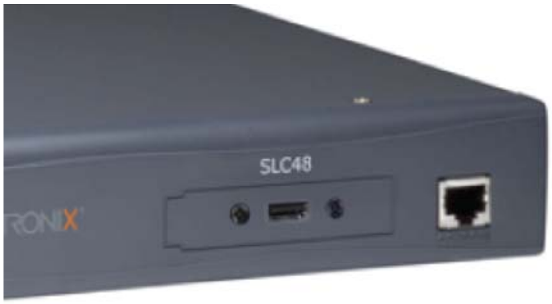


USB Port

Note: *This USB port is only supported on SLC -03 part numbers.*

The SLC console manager has a USB port as shown in *Figure 2-8*.

Figure 2-8 SLC Console Manager with USB Interface



3: Installation

This chapter provides a high-level procedure for installing the SLC console manager followed by more detailed information about the SLC connections and power supplies.

Caution: ***To avoid physical and electrical hazards, please be sure to read Appendix C: Safety Information on page 266 before installing the SLC device.***

It contains the following sections:

- *What's in the Box*
- *Technical Specifications*
- *Physical Installation*

What's in the Box

In addition to the SLC console manager, *Table 3-1* lists the components in the box and part numbers.

Table 3-1 Component Part Numbers and Descriptions

Component Part #	Description
Adapters	
200.2066A	Adapter: DB25M (DCE), Sun w/DB25 female
200.2067A	Adapter: DB25F (DCE) to RJ45, Sun w/DB25 male and some HP9000s
200.2069A	Adapter: DB9M (DCE) to RJ45, SGI Onyx
200.2070A	Adapter: DB9F (DCE) to RJ45, HP9000, SGI Origin, IBM RS6000, and PC-based Linux servers
ADP010104-01	Adapter: RJ45 rolled serial, Cisco, and Sun Netra
Note: *An optional adapter for an external modem is available from Lantronix. The part number is 200.2073 and description is DB25M (DCE) to RJ45.*	
Cables	
200.0063	Cable: RJ45 to RJ45, 6.6 ft (2 m)
500-153	Cable: Loopback
Power Cords	
500-041	For single AC models: one AC power cord For dual AC models: two AC power cords
083-011	For dual DC models: one accessory kit, containing DC plug connectors and instructions
Documentation	
	Quick Start Guide and SLC Console Manager User Guide available at http://www.lantronix.com/support/downloads/.

Verify and inspect the contents of the SLC package using the enclosed packing slip or the table above. If any item is missing or damaged, contact your place of purchase immediately.

Product Information Label

The product information label on the underside of the unit contains the following information about each specific unit:

- Part Number
- Serial Number Bar Code
- Serial Number and Date Code
- Regulatory Certifications and Statements

Technical Specifications

Table 3-2 lists the SLC technical specifications.

Table 3-2 Components and Descriptions

Component	Description
Serial Interface (Device)	RJ45-type 8-conductor connector (DTE) Speed software selectable (300 to 115,200 baud)
Serial Interface (Console)	RJ45-type 8-pin connector (DTE) Speed software selectable (300 to 115,200 baud)
Network Interface	10Base-T/100Base-TX RJ45 Ethernet
Power Supply	Universal AC power input: 100-240 VAC, 50 or 60 Hz IEC-type regional cord set included DC power input: -24 to -60 VDC
Power Consumption	Less than 20 watts
Dimensions	1U, 1.75 in x 17.25 in x 12 in
Weight	10 lbs or less, depending on the options
Temperature	Operating: 0 to 50 °C (32 to 122 °F), 30 to 90% RH, non-condensing Storage: -20 to 70 °C (-4 to 158 °F), 10 to 90% RH, non-condensing
Relative Humidity	Operating: 10% to 90% non-condensing; 40% to 60% recommended Storage: 10% to 90% non-condensing
Heat Flow Rate	68 BTU per hour

Install the SLC console manager in an EIA-standard 19-inch rack (1U tall) or as a desktop unit. The SLC device uses convection cooling to dissipate excess heat.

Physical Installation

To install the unit in a rack:

1. Place the unit in a 19-inch rack.

Warning: ***Be careful not to block the air vents on the sides of the unit. If you mount the SLC console manager in an enclosed rack, we recommended that the rack have a ventilation fan to provide adequate airflow through the unit.***

2. Connect serial devices to the SLC device ports. See *Connecting to Device Ports on page 27.*
3. Install any PC Cards or USB devices that you intend to use. If you install a modem card, connect to the phone line. See *Chapter 9: PC Cards* or *10: USB Port*. You have the following options:
    a. To configure the SLC console manager using the network, or to monitor serial devices on the network, connect at least one SLC network port to a network. See *Connecting to Network Ports on page 28.*

    b. To configure the SLC console manager using a dumb terminal or a computer with terminal emulation, connect the terminal or PC to the SLC console port. See *Connecting to Terminals on page 28*.
4. Connect the power cord, and apply power. See *Power on page 28.*
5. Wait approximately a minute and a half for the boot process to complete. When the boot process ends, the SLC host name and the clock appear on the LCD display.

   Now you are ready to configure the network settings as described in *Chapter 4: Quick Setup .*

Connecting to Device Ports

You can connect any device that has a serial console port to a device port on the SLC console manager for remote administration. The console port must support the RS-232C interface.

Note: Many servers must have the serial port enabled as a console or the keyboard and mouse detached. Consult the server hardware and/or software documentation for more information.

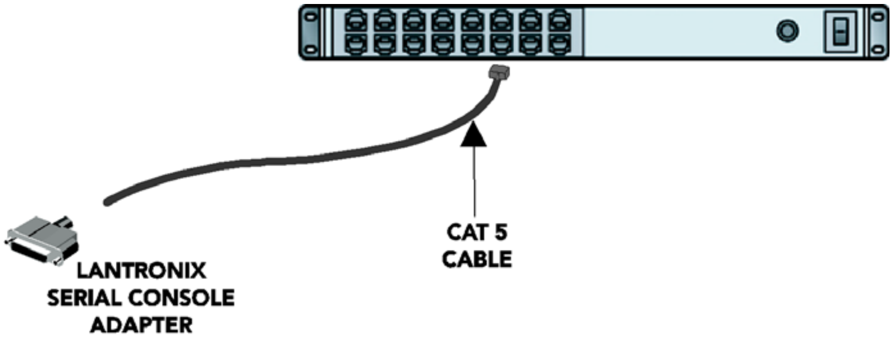
To connect to a device port:

1. Connect one end of the Cat 5 cable to the device port.
2. Connect the other end of the Cat 5 cable to a Lantronix serial console adapter.

Note: To connect a device port to a Lantronix SLP™ power manager, use the rolled serial cable provided with the unit, a 200.2225 adapter and Cat 5 cabling, or the ADP010104 adapter that eliminates the need for an additional Cat 5 patch cable between the adapter and the connected equipment. See Chapter 5: Adapters and Pinouts on page 272 for more information about Lantronix adapters.

3. Connect the adapter to the serial console of the serial device as shown in *Figure 3-3*.

Figure 3-3 CAT 5 Cable Connection



Connecting to Network Ports

The SLC network ports, 10Base-T/100Base-TX, allow remote access to the attached devices and the system administrative functions. Use a standard RJ45-terminated Category 5 cable to connect to the network port.

Note: *One possible use for the two Ethernet ports is to have one port on a private, secure network, and the other on an unsecured network.*

Connecting to Terminals

The console port is for local access to the SLC console manager and the attached devices. You may attach a dumb terminal or a computer with terminal emulation to the console port. The SLC console port uses RS-232C protocol and supports VT100 emulation. The default baud rate is 9600.

To connect the console port to a terminal or computer with terminal emulation, Lantronix offers optional adapters that provide a connection between an RJ45 jack and a DB9 or DB25 connector. The console port is configured as DTE. For more information, see *Appendix E: Adapters and Pinouts on page 272* and go to the Lantronix web site at www.lantronix.com/support and click Cable/Adapter Lookup on the **Support** menu.

To connect a terminal:

1. Attach the Lantronix adapter to your terminal (use **PN 200.2066A** adapter) or your PC's serial port (use **PN 200.2070A** adapter).
2. Connect the Cat 5 cable to the adapter, and connect the other end to the SLC console port.
3. Turn on the terminal or start your computer’s communication program (e.g., HyperTerminal for Windows).
4. Once the SLC console manager is running, press **Enter** to establish connection. You should see the model name and a **login** prompt on your terminal. You are connected.

Power

The SLC device consumes less than 20W of electrical power.

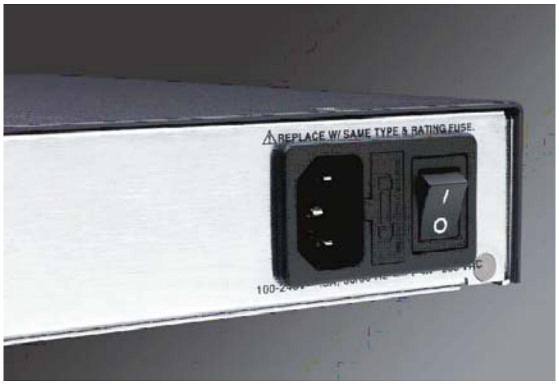
AC Input

The SLC console manager has a universal auto-switching AC power supply. The power supply accepts AC input voltage between 100 and 240 VAC with a frequency of 50 or 60 Hz. Rear-mounted IEC-type AC power connector(s) are provided for universal AC power input (North American cord provided).

The SLC0xx12N models have a single supply/input, while the SLC0xx22N models have dual inputs and dual supplies. The power connector also houses a replaceable protective fuse (fast-blow 4.0A, maximum 250V AC) and the on/off switch. In addition, we provide the SLC0xx22N with a “Y” cord. See the SLC models listed in Table 3-2 on page 26.

Figure 3-4 shows the AC power inputs and power switch.

Figure 3-4 AC Power Input and Power Switch (SLCxxxx2N)

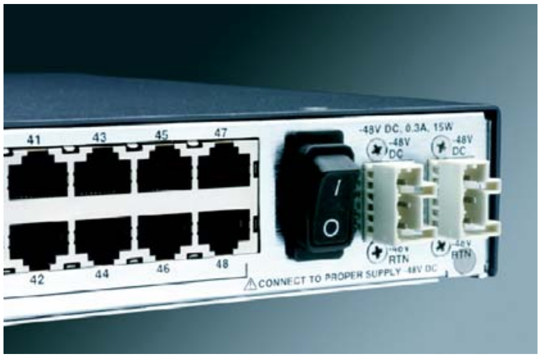


Note: *The SLC48 console manager with dual AC does not have an on/off switch.*

DC Input

The DC version of the SLC console manager accepts standard –48 VDC power. The SLC0xx24T models accept two DC power inputs for supply redundancy. Lantronix provides the DC power connections using industry standard Wago connectors. One set of connectors is included with the SLC console manager. You can order additional connectors (part number 721-103/031-000) from the Wago catalog at http://www.wagocatalog.com/okv3/index.asp?lid=1&cid=1&str_from_home=first. *Figure 3-5* shows the DC power inputs and power switch.

Figure 3-5 DC Power Inputs and Power Switch (SLCxxx24T)



4: Quick Setup

This chapter helps get the IP network port up and running quickly, so you can administer the SLC console manager using your network. It contains the following sections:

- *Recommendations*
- *IP Address*
- *Next Step*

Recommendations

To set up the network connections quickly, we suggest you do one of the following:

- Use the front panel LCD display and pushbuttons.
- Complete the Quick Setup web page on the web interface.
- SSH to the command line interface and follow the Quick Setup script on the command line interface.
- Connect to the console port and follow the Quick Setup script on the command line interface.

Note: *The first time you power up the SLC console manager, Eth1 tries to obtain its IP address via DHCP. If you have connected Eth1 to the network, and Eth1 is able to acquire an IP address, you can view this IP address on the LCD or by running the Detector tool available for download at http://www.lantronix.com/support/downloads/. If Eth1 cannot acquire an IP address, you cannot use Telnet, SSH, or the web interface to run Quick Setup.*

IP Address

Your SLC console manager must have a unique IP address on your network. The system administrator generally provides the IP address and corresponding subnet mask and gateway. The IP address must be within a valid range, unique to your network, and in the same subnet as your PC. *Table 4-1* lists the options for assigning an IP address to your unit.

Table 4-1 Methods of Assigning an IP Address

Method	Description
DHCP	A DHCP server automatically assigns the IP address and network settings. The SLC console manager is DHCP-enabled by default. With the Eth1 network port connected to the network, and the SLC device powered up, Eth1 acquires an IP address, viewable on the LCD. At this point, you can Telnet into the SLC console manager, or use the web interface.
BOOTP	Similar to DHCP but for smaller networks.

Table 4-1 Methods of Assigning an IP Address (continued)

Method	Description
Detector™	A Windows-based application available for download at http://www.lantronix.com/support/downloads/ for viewing a DHCP-provided IP address or for assigning a static IP address to the SLC console manager. You can use Detector only if you have not already assigned a static IP address by another method. For more information, see Detector's online help.
Front panel LCD display and pushbuttons	You manually assign the IP address and other basic network, console, and date/time settings. If desired, you can restore the factory defaults.
Serial port login to command line interface	You assign an IP address and configure the SLC console manager using a terminal or a PC running a terminal emulation program to the unit's serial console port connection.

Method # 1 Using the Front Panel Display

Before you begin, ensure that you have:

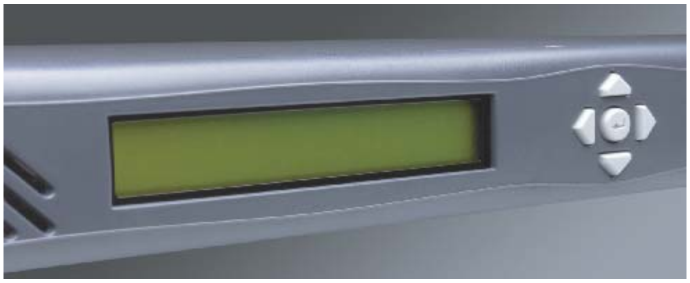
- Unique IP address that is valid on your network (unless automatically assigned)
- Subnet mask (unless automatically assigned)
- Gateway
- DNS settings
- Date, time, and time zone
- Console port settings: baud rate, data bits, stop bits, parity, and flow control

Make sure the SLC console manager is plugged into power and turned on.

Front Panel LCD Display and Pushbuttons

With the SLC console manager powered up, you can use the front panel display and pushbuttons to set up the basic parameters. *Figure 4-2* shows the front panel.

Figure 4-2 Front Panel LCD Display and Arrow Pushbuttons



The front panel display initially shows the host name and the date and time. Using the five pushbuttons, you can change the network, console port, and date/time settings and view the firmware release version. If desired, you can restore the factory defaults.

Note: *Have your information handy as the display times out without accepting any unsaved changes if you take more than 30 seconds between entries.*

Any changes made to the network, console port, and date/time settings take effect immediately.

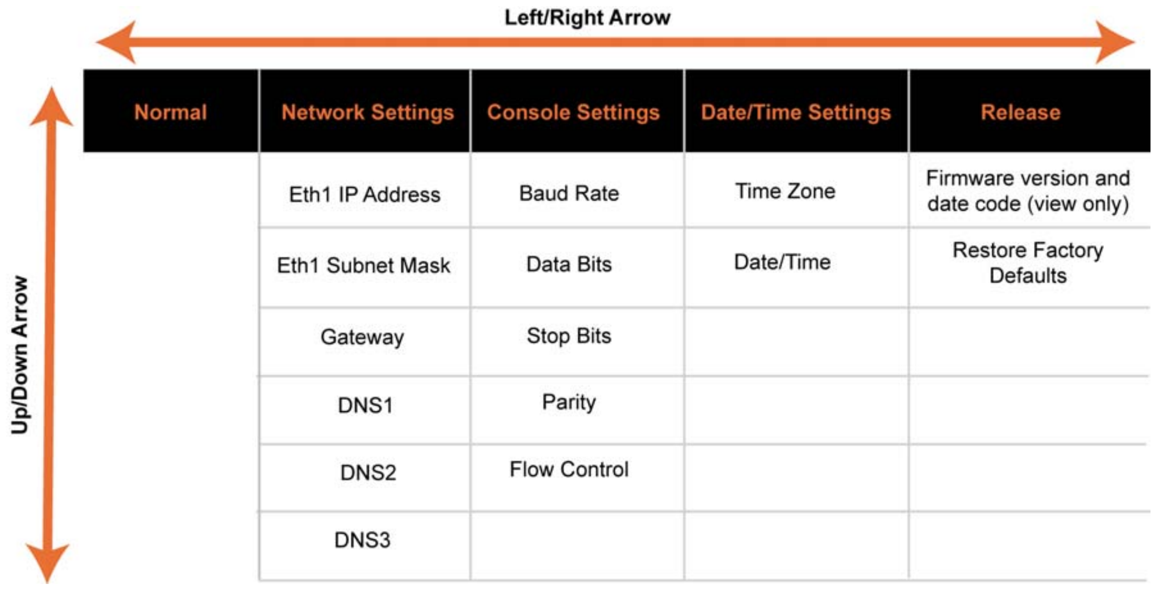
Navigating

The front panel has one **Enter** button (in the center) and four arrow buttons (**up, left, right,** and **down**). Press the arrow buttons to navigate from one option to another, or to increment or decrement a numerical entry of the selected option. Use the **Enter** button to select an option to change or to save your settings. *Table 4-3* and *Table 4-4* list the actions, buttons, and options.

Table 4-3 LCD Arrow Pushbutton Actions

Action	Button
To move to the next option (e.g., from Network Settings to Console Settings)	Right arrow
To return to the previous option	Left arrow
To enter edit mode	Enter (center button)
Within edit mode, to increase or decrease a numerical entry	Up and down arrows
Within edit mode, to move the cursor right or left	Right or left arrows
To exit edit mode	Enter
To scroll up or down the list of parameters within an option (e.g., from IP Address to Mask)	Up and down arrows

Table 4-4 Front Panel Setup Options with Associated Parameters


Left/Right Arrow
Up/Down Arrow

Normal	Network Settings	Console Settings	Date/Time Settings	Release
	Eth1 IP Address	Baud Rate	Time Zone	Firmware version and date code (view only)
	Eth1 Subnet Mask	Data Bits	Date/Time	Restore Factory Defaults
	Gateway	Stop Bits		
	DNS1	Parity		
	DNS2	Flow Control		
	DNS3			

Entering the Settings

To enter setup information:

1. From the normal display (host name, date and time), press the **right arrow** button to display **Network Settings**. The IP address for Eth1 displays.

Note: If you have connected Eth1 to the network, and Eth1 is able to acquire an IP address through DHCP, this IP address displays, followed by the letter [D]. Otherwise, the IP address displays as all zeros (000.000.000.000).

2. Press the **Enter** button on the keypad to enter edit mode. A cursor displays below one character of the existing IP address setting.
3. To enter values:

- Use the **left** or **right arrow** to move the cursor to the left or to the right position.
- Use the **up** or **down arrow** to increment or decrement the numerical value.

4. To toggle between a DHCP and static IP address, place the cursor over the [D] or [N] and press the **up** and **down arrows**.
5. When you have the IP address as you want it, press **Enter** to exit edit mode, and then press the **down arrow** button. The Subnet Mask parameter displays.

Note: You must edit the IP address and the Subnet Mask together for a valid IP address combination.

6. To save your entries for one or more parameters in the group, press the **right arrow** button. The **Save Settings? Yes/No** prompt displays.

Note: If the prompt does not display, make sure you are no longer in edit mode.

7. Use the **left/right arrow** buttons to select **Yes**, and press the **Enter** button.
8. Press the **right arrow** button to move to the next option, **Console Settings**.
9. Repeat steps 2-7 for each setting.
10. Press the **right arrow** button to move to the next option, **Date/Time Settings**, and click **Enter** to edit the time zone.

    a. To enter a US time zone, use the **up/down arrow** buttons to scroll through the US time zones, and then press **Enter** to select the correct one.

    b. To enter a time zone outside the US, press the **left arrow** button to move up to the top level of time zones. Press the **up/down arrow** button to scroll through the top level.

    A time zone with a trailing slash (such as Africa/) has sub-time zones. Use the **right arrow** button to select the Africa time zones, and then the **up/down arrows** to scroll through them.

    Press **Enter** to select the correct time zone. To move back to the top-level time zone at any time, press the **left arrow**.

11. To save your entries, press the **right arrow** button. The **Save Settings? Yes/No** prompt displays.

Note: If the prompt does not display, make sure you are no longer in edit mode.

12. Use the **left/right arrow** buttons to select **Yes**, and press the **Enter** button.
13. To review the saved settings, press the **up** or **down arrows** to step through the current settings.

    When you are done, the front panel returns to the clock display. The network port resets to the new settings, and you can connect to your IP network for further administration. You should be able to Telnet or SSH to the SLC console manager through your network connection, or access the web interface through a web browser.

Restoring Factory Defaults

To use the LCD display to restore factory default settings:

1. Press the **right arrow** button to move to the last option, **Release**.
2. Use the **down arrow** to move to the **Restore Factory Defaults** option. A prompt for the 6-digit **Restore Factory Defaults** password displays.
3. Press **Enter** to enter edit mode.
4. Using the **left** and **right arrows** to move between digits and the **up** and **down** arrows to change digits, enter the password (the default password is 999999).

Note: *The **Restore Factory Defaults** password is only for the LCD. You can change it at the command line interface using the `admin keypad password` command.*

5. Press **Enter** to exit edit mode. If the password is valid, a **Save Settings? Yes/No** prompt displays.
6. To initiate the process for restoring factory defaults, select **Yes**. When the process is complete, the SLC device reboots.

Method # 2 Quick Setup Using the Web

After the unit has an IP address, you can use the Quick Setup tab to configure the remaining network settings. This page displays the first time you log into the SLC console manager only. Otherwise, the SLC Home Page displays. For information about the web interface, see 5: Web and Command Line Interfaces.

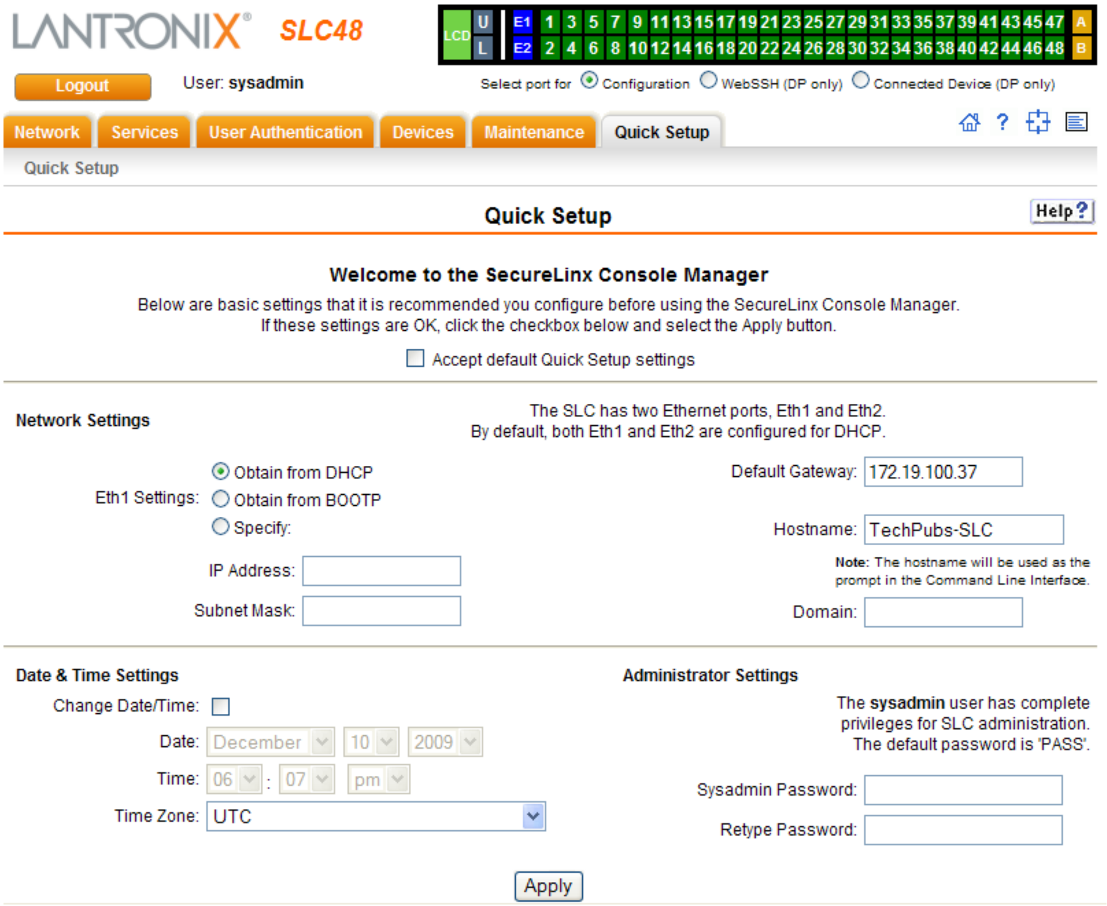
To complete the Quick Setup tab:

1. Open a web browser (Netscape Navigator 6.x and above or Internet Explorer 5.5. and above, with JavaScript enabled).
2. In the URL field, type **https://** followed by the IP address of your SLC console manager.

Note: *The web server listens for requests on the unencrypted (HTTP) port (port 80) and redirects all requests to the encrypted (HTTPS) port (port 443).*

3. Log in using **sysadmin** as the user name and **PASS** as the password. The first time you log in to the SLC console manager, the **Quick Setup** tab automatically displays as shown in *Figure 4-5*. Otherwise, the **Home** page displays.

Figure 4-5 Quick Setup Tab


LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network
Services
User Authentication
Devices
Maintenance
Quick Setup
Help?
Apply

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Quick Setup

Quick Setup

Welcome to the SecureLinx Console Manager

Below are basic settings that it is recommended you configure before using the SecureLinx Console Manager.
If these settings are OK, click the checkbox below and select the Apply button.

□ Accept default Quick Setup settings

Network Settings

The SLC has two Ethernet ports, Eth1 and Eth2.
By default, both Eth1 and Eth2 are configured for DHCP.

Eth1 Settings: ● Obtain from DHCP ○ Obtain from BOOTP ○ Specify:

IP Address:

Subnet Mask:

Default Gateway: 172.19.100.37

Hostname: TechPubs-SLC

Note: The hostname will be used as the prompt in the Command Line Interface.

Domain:

Date & Time Settings

Change Date/Time: □

Date: December 10 2009

Time: 06 : 07 pm

Time Zone: UTC

Administrator Settings

The **sysadmin** user has complete privileges for SLC administration. The default password is 'PASS'.

Sysadmin Password:

Retype Password:

4. To accept the defaults, select the **Accept default Quick Setup settings** checkbox in the top portion of the page and click the **Apply** button at the bottom of the page. Otherwise, continue with step 5.

Note: *Once you click **Apply** on the Quick Setup page, you can continue using the web interface to configure the SLC console manager.*

5. Enter the following fields.

Note: *Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.*

Network Settings

Eth1 Settings	**Obtain from DHCP**: Acquires IP address, subnet mask, hostname and gateway from the DHCP server. (The DHCP server may not provide the hostname gateway, depending on its setup.) This is the default setting. If you select this option, skip to Gateway. **Obtain from BOOTP**: Lets a network node request configuration information from a BOOTP “server” node. If you select this option, skip to Gateway. **Specify**: Lets you manually assign a static IP address, generally provided by the system administrator.

IP Address	If specifying an IP address, enter an IP address that will be unique and valid on your network. There is no default. Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last segment. ***Note:*** *Currently, the SLC console manager does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).*
Subnet Mask	If specifying an IP address, enter the network segment on which the SLC device resides. There is no default.
Default Gateway	The IP address of the router for this network. There is no default.
Hostname	The default host name is slcXXXX, where XXXX is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). The host name becomes the prompt in the command line interface.
Domain	If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLC console manager. For example, if abcd is specified for the SMTP server, and mydomain.com is specified for the domain, if abcd cannot be resolved, the SLC device attempts to resolve abcd.mydomain.com for the SMTP server.

Date & Time Settings

Change Date/ Time	Select the checkbox to manually enter the date and time at the SLC location.
Date	From the drop-down lists, select the current month, day, and year.
Time	From the drop-down lists, select the current hour and minute.
Time Zone	From the drop-down list, select the appropriate time zone.

Administrator Settings

Sysadmin Password/ Retype Password	To change the password (e.g., from the default), enter a password of up to 64 characters.

6. To save your entries, click the **Apply** button.

Method # 3 Quick Setup on the Command Line Interface

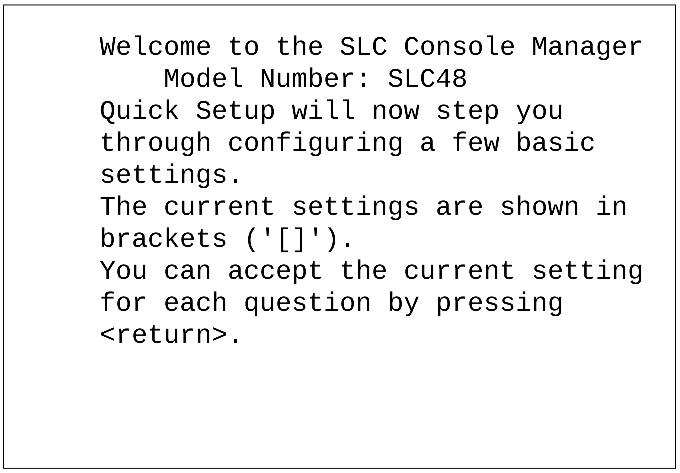
If the SLC console manager does not have an IP address, you can connect a dumb terminal or a PC running a terminal emulation program (VT100) to access the command line interface (CLI). See *Connecting to Terminals on page 28* If the unit has an IP address, you can use SSH or Telnet to connect to the SLC device.

Note: *By default, Telnet is disabled and SSH is enabled. To enable Telnet, use the Services web page (see Chapter 7: Services), a serial terminal connection, or an SSH connection.*

To complete the quick setup:

1. Do one of the following:
    - With a serial terminal connection, power up, and when the command line displays, press **Enter**.
    - With a network connection, use an SSH program or Telnet program (if Telnet has been enabled) to connect to **xx.xx.xx.xx** (the IP address in dot quad notation), and press **Enter**. You should be at the **login** prompt.
2. Enter **sysadmin** as the user name and press **Enter**.
3. Enter **PASS** as the password and press **Enter**. The first time you log in, the Quick Setup script runs automatically. Normally, the command prompt displays.

Figure 4-6 Quick Setup Screen Using CLI



```
Welcome to the SLC Console Manager
    Model Number: SLC48
Quick Setup will now step you
through configuring a few basic
settings.
The current settings are shown in
brackets ('[]').
You can accept the current setting
for each question by pressing
<return>.
```

4. Enter the following fields.

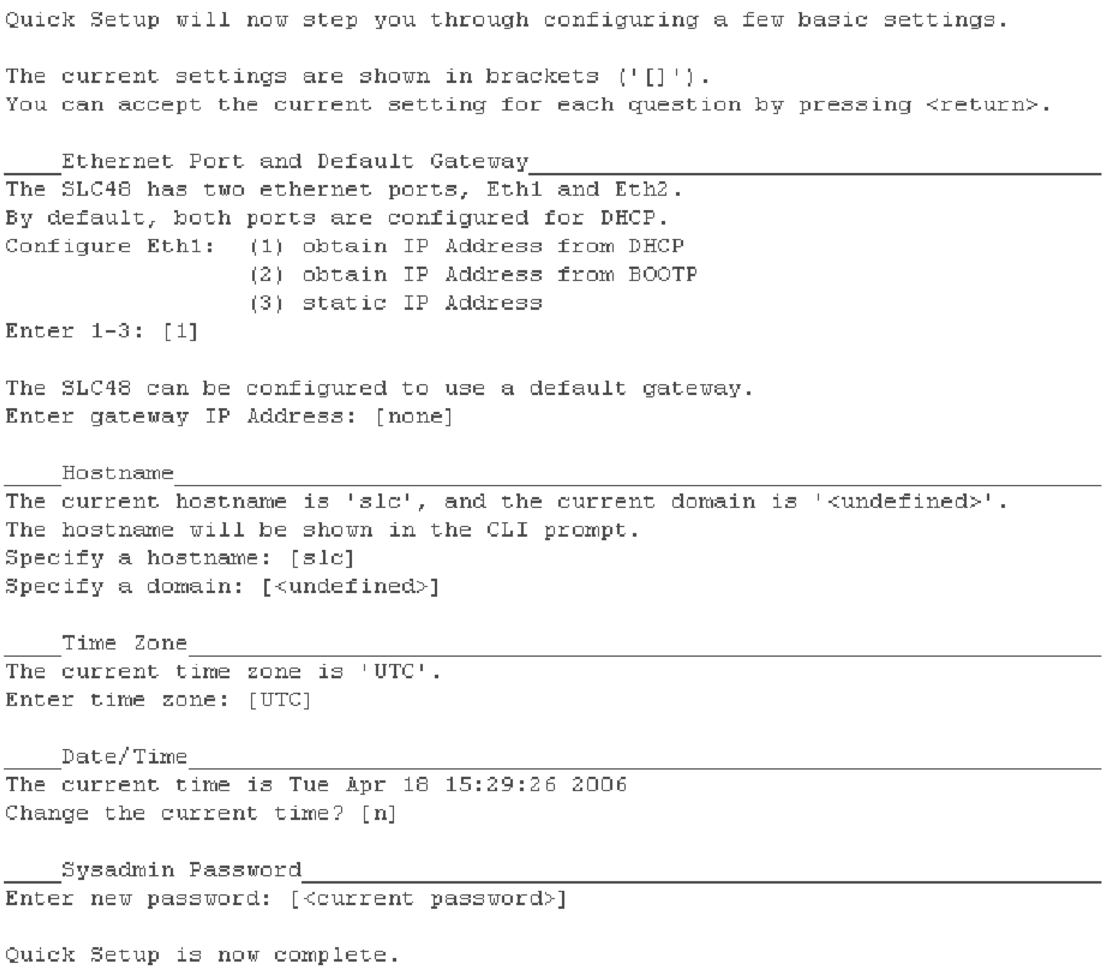
Note: *To accept a default or to skip an entry that is not required, press* ***Enter****.*

Configure Eth1	Select one of the following: **<1>** obtain IP Address from DHCP: The unit will acquire the IP address, subnet mask, hostname and gateway from the DHCP server. (The DHCP server may or may not provide the hostname and gateway, depending on its setup.) This is the default setting. **<2>** obtain IP Address from BOOTP: Permits a network node to request configuration information from a BOOTP “server” node. **<3>** static IP Address: Allows you to assign a static IP address manually. The IP address is generally provided by the system administrator.
IP Address (if specifying)	An IP address that will be unique and valid on your network and in the same subnet as your PC. There is no default. If you selected DHCP or BOOTP, this prompt does not display. Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last segment. ***Note:*** *Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.*

Subnet Mask	The subnet mask specifies the network segment on which the SLC console manager resides. There is no default. If you selected DHCP or BOOTP, this prompt does not display.
Default Gateway	IP address of the router for this network. There is no default.
Hostname	The default host name is slcXXXX, where XXXX is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). ***Note:*** *The host name becomes the prompt in the command line interface.*
Domain	If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLC console manager. For example, if abcd is specified for the SMTP server, and mydomain.com is specified for the domain, if abcd cannot be resolved, the SLC device attempts to resolve abcd.mydomain.com for the SMTP server.
Time Zone	If the time zone displayed is incorrect, enter the correct time zone and press Enter. If the entry is not a valid time zone, the system guides you through selecting a time zone. A list of valid regions and countries displays. At the prompts, enter the correct region and country.
Date/Time	If the date and time displayed are correct, type n and continue. If the date and time are incorrect, type y and enter the correct date and time in the formats shown at the prompts.
Sysadmin password	Enter a new sysadmin password.

After you complete the Quick Setup script, the changes take effect immediately as shown in *Figure 4-7*.

Figure 4-7 Completed Quick Setup



```
Quick Setup will now step you through configuring a few basic settings.

The current settings are shown in brackets ('[]').
You can accept the current setting for each question by pressing <return>.

____Ethernet Port and Default Gateway_______________________________________
The SLC48 has two ethernet ports, Eth1 and Eth2.
By default, both ports are configured for DHCP.
Configure Eth1:   (1) obtain IP Address from DHCP
                  (2) obtain IP Address from BOOTP
                  (3) static IP Address
Enter 1-3: [1]

The SLC48 can be configured to use a default gateway.
Enter gateway IP Address: [none]

____Hostname________________________________________________________________
The current hostname is 'slc', and the current domain is '<undefined>'.
The hostname will be shown in the CLI prompt.
Specify a hostname: [slc]
Specify a domain: [<undefined>]

____Time Zone_______________________________________________________________
The current time zone is 'UTC'.
Enter time zone: [UTC]

____Date/Time_______________________________________________________________
The current time is Tue Apr 18 15:29:26 2006
Change the current time? [n]

____Sysadmin Password_______________________________________________________
Enter new password: [<current password>]

Quick Setup is now complete.
```

5. To logout, type **logout** at the prompt and press **Enter**.

Next Step

After quick starting the SLC console manager, you may want to configure other settings. You can use the web page or the command line interface for configuration.

- For information about the web and the command line interfaces, go to 5: Web and Command Line Interfaces.
- To continue configuring the SLC console manager, go to 6: Basic Parameters.

5: Web and Command Line Interfaces

This chapter describes the interfaces for configuring the SLC console manager that are: command line interface (CLI) and the Web Manager. You can also use the Front Panel LCD which is described in *Chapter 4: Quick Setup*.

This chapter contains the following sections:

- *Web Interface*
- *Command Line Interface*

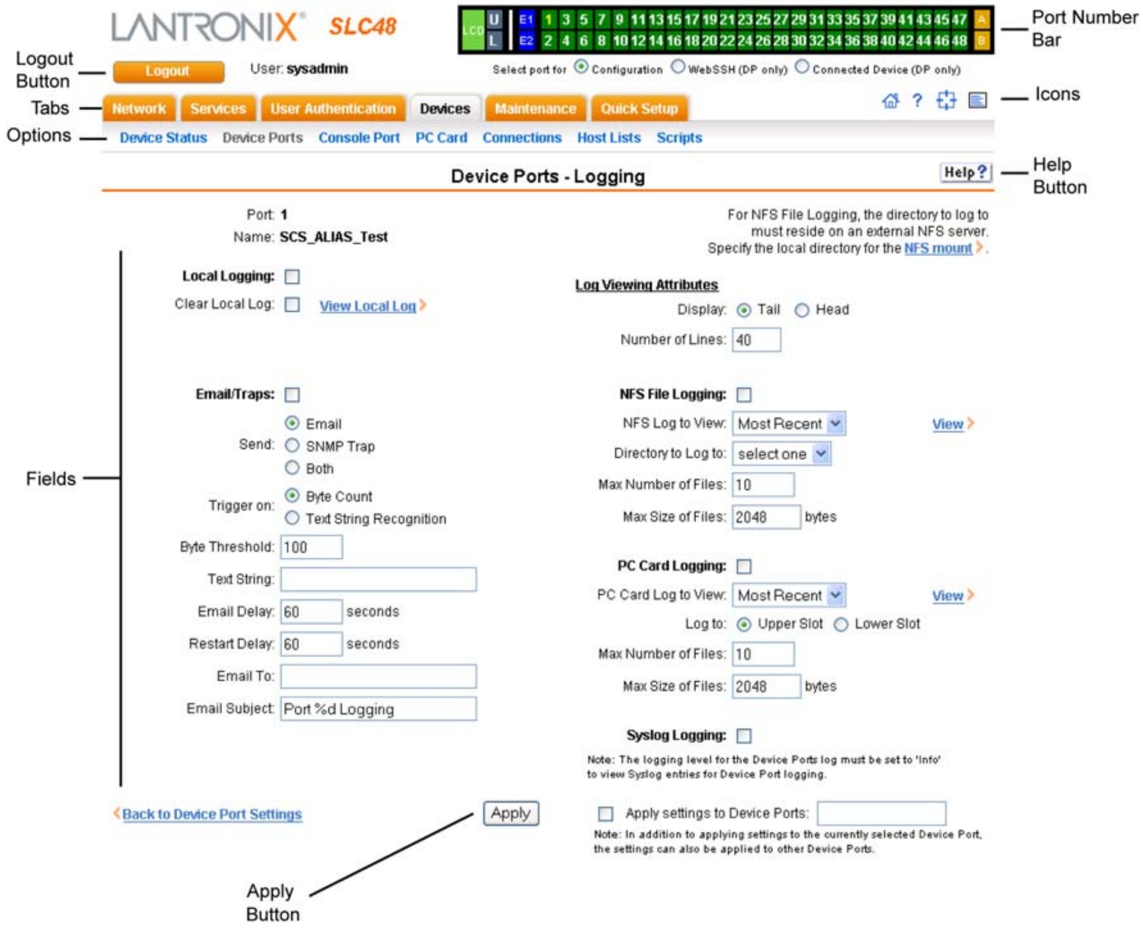
Note: *The features and functionality described in this chapter specific to PC Card use are supported on SLC -02 part numbers. The features and functionality specific to USB port use are supported on SLC -03 part numbers.*

Web Interface

A web interface shown in *Figure 5-1* allows the system administrator and other authorized users to configure and manage the SLC console manager using most web browsers (Netscape Navigator 6.x and above or Internet Explorer 5.5. and above, with JavaScript enabled). The Web Telnet and Web SSH features require Java 1.1 (or later) support in the browser. The SLC device provides a secure, encrypted web interface over SSL (secure sockets layer).

Note: *The web server listens for requests on the unencrypted (HTTP) port (port 80) and redirects all requests to the encrypted (HTTPS) port (port 443).*

Figure 5-1 Web Page Layout



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Device Ports - Logging

Port: 1
Name: SCS_ALIAS_Test

For NFS File Logging, the directory to log to must reside on an external NFS server. Specify the local directory for the NFS mount.

Local Logging: □
Clear Local Log: □ View Local Log

Log Viewing Attributes
Display: ● Tail ○ Head
Number of Lines: 40

Email/Traps: □
Send: ● Email ○ SNMP Trap ○ Both
Trigger on: ● Byte Count ○ Text String Recognition
Byte Threshold: 100
Text String:
Email Delay: 60 seconds
Restart Delay: 60 seconds
Email To:
Email Subject: Port %d Logging

NFS File Logging: □
NFS Log to View: Most Recent View
Directory to Log to: select one
Max Number of Files: 10
Max Size of Files: 2048 bytes

PC Card Logging: □
PC Card Log to View: Most Recent View
Log to: ● Upper Slot ○ Lower Slot
Max Number of Files: 10
Max Size of Files: 2048 bytes

Syslog Logging: □
Note: The logging level for the Device Ports log must be set to 'Info' to view Syslog entries for Device Port logging.

□ Apply settings to Device Ports:
Note: In addition to applying settings to the currently selected Device Port, the settings can also be applied to other Device Ports.

The web page has the following components:

- **Tabs:** Groups of settings to configure.
- **Options:** Below each tab are options for specific types of settings. Only those options for which the currently logged-in user has rights display.
- **Port Number Bar:** Allows you to select a port and display its settings. The **E1** and **E2** buttons display the Network – Settings page. The **A** and **B** buttons display the status of the power supplies. Only ports to which the currently logged-in user has rights are enabled.
- **Entry Fields and Options:** Allow you to enter data and select options for the settings.

Note: For specific instructions on completing the fields on the web pages, see Chapters Chapter 6: Basic Parameters, Chapter 7: Services, Chapter 8: Devices, Chapter 9: PC Cards, Chapter 10: USB Port, Chapter 11: Connections, and Chapter 12: User Authentication.

- **Apply Button: Apply** on each web page makes the changes immediately and saves them so they will be there when the SLC console manager is rebooted.
- **Icons:** The icons in the icon bar above the Main Menu ⌂ ? ✜ ▤ are (from left to right):
  - Home page.

  - Information about the SLC device and Lantronix contact information.
  - Configuration site map.
  - Status of the SLC console manager.

- **Help Button:** Provides online Help for the specific web page.
- **Logout Button:** Closes SLC device.

Logging In

Only the system administrator or users with web access rights can log into the web page. More than one user at a time can log in, but the same user cannot login more than once unless configured for multiple logins. See 15: Command Reference for more information.

To log into the SLC web interface:

1. Open a web browser (Netscape Navigator 6.x and above or Internet Explorer 5.5. and above).
2. In the URL field, type **https://** followed by the IP address of your SLC console manager.
3. To configure the SLC device, use **sysadmin** as the user name and **PASS** as the password. These values are the defaults.

Notes:

The administrator may have changed the password using the method described in the previous chapter.

When SecurID over RADIUS is used, the user must enter the passcode corresponding to their RSA token. Depending on the state of the user, the login pages may also require a new PIN number, the next passcode, or the next tokencode.

The Lantronix SLC Quick Setup page displays automatically the first time you log in. Subsequently, the Lantronix SLC Home page displays. (If you want to display the Quick Setup page again, click **Quick Setup** on the main menu.)

Logging Off

To logoff the SLC web interface:

Click the **Logoff** button. The “Logging out” message, followed by the login page displays.

Web Page Help

To view detailed information about an SLC web page:

Click the **Help** button to the right of the web page title.

Command Line Interface

A command line interface (CLI) is available using Telnet, SSH, or a serial terminal connection to enter SLC commands. Each command that corresponds to the web interface description in each chapter gets listed as a cross-reference to the complete command syntax and description contained in 15: Command Reference.

Note: *By default, Telnet is disabled and SSH is enabled. To enable Telnet, use the SSH/Telnet/Logging tab, a serial terminal connection, or an SSH connection. See Chapter 7: Services for more information.*

The sysadmin user and users with who have full administrative rights have access to the complete command set, while all other users have access to a reduced command set based on their permissions.

Logging In

To log into the SLC command line interface:

1. Do one of the following:
   - With a serial terminal connection, power up, and when the command line displays, press **Enter**.
   - If the SLC console manager already has an IP address (assigned previously or assigned by DHCP), Telnet (if Telnet has been enabled) or SSH to **xx.xx.xx.xx** (the IP address in dot quad notation) and press **Enter**. The login prompt displays.
2. To login as the system administrator for setup and configuration:

   a. Enter **sysadmin** as the user name and press **Enter**.

   b. Enter **PASS** as the password and press **Enter**. The first time you log in, the Quick Setup script runs automatically. Normally, the command prompt displays. (If you want to display the Quick Setup script again, use the `admin quicksetup` command.)

   Note: The system administrator may have changed the password using one of the Quick Setup methods in the previous chapter.
3. To login any other user:

   a. Enter your SLC user name and press **Enter**.

   b. Enter your SLC password and press **Enter**.

Logging Out

To logout of the SLC command line interface:

Type **logout** and press **Enter**.

Command Syntax

Commands have the following syntax: <action> <category> <parameters>.

Action commands are: set, show, connect, admin, diag, pccard, or logout. Category commands are groups of related parameters whose settings you want to configure or view. Examples are ntp, deviceport, and network. Parameters are one or more name-value pairs in one of the following formats:

- <aa|bb>—Specify one of the values (aa or bb) separated by a vertical line (|). The values are in all lowercase and must be entered exactly as shown. Bold indicates a default value.
- <Value>—Specify an appropriate value, for example, an IP address. The parameter values are in mixed case. Square brackets [ ] indicate optional parameters.

Table 5-2 Actions and Category Options

Action	Category
set	auth | cifs | cli | command | consoleport | datetime | deviceport | history | hostlist | ipfilter | kerberos | ldap | localusers | log | menu | network | nfs | nis | ntp | password | radius | remoteusers | routing | script | services | slcnetwork | sshkey | tacacs+ | temperature | usb[1]
show	auth | auditlog | cifs | cli | connections | consoleport | datetime | deviceport | emaillog | history | hostlist | ipfilter | kerberos | ldap | localusers | log | menu | network | nfs | nis | ntp | pccard | portcounters | portstatus | radius | remoteusers | routing | script | services | slcnetwork | sshkey | sysconfig | syslog | sysstatus | tacacs+ | temperature | user | usb[1]
connect	bidirection | direct | global | listen | script | terminate | unidirection
diag	arp | internals | lookup | loopback | netstat | nettrace | perfstat | ping | ping6| sendpacket | traceroute
pccard	modem | storage
admin	banner | clear | config | events | firmware | ftp | keypad | lcd | quicksetup | reboot| shutdown | site | version | web
logout	Terminates CLI session.

[1] USB commands are only accessible on SLC USB part number -03.

Command Line Help

For general Help and to display the commands to which you have rights, type “help.” For general CLI help, type “help command line”.

For more information about a specific command, type `help` followed by the command, for example, “help set network **or** help admin firmware.”

Tips

- Type enough characters to uniquely identify the action, category, or parameter name. For parameter values, type the entire value. For example, you can shorten:

```
set network port 1 state static ipaddr 122.3.10.1 mask 255.255.0.0
```

- to:

```
se net po 1 st static ip 122.3.10.1 ma 255.255.0.0
```

- Use the **Tab** key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** either to complete the name if only one is possible, or to display the possible names if more than one is possible. Following a space after the preceding name, **Tab** displays all possible names.
- Should you make a mistake while typing, backspace by pressing the **Backspace** key and/or the **Delete** key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the **left** and **right** arrow keys to move within a command.
- Use the **up** and **down arrows** to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.

- To clear an IP address, type **`0.0.0.0`**, or to clear a non-IP address value, type **`CLEAR`**.

  When the number of lines displayed by a command exceeds the size of the window (the default is 25), the command output is halted until the user is ready to continue. To display the next line, press **Enter**, and to display the page, press the space bar. You can override the number of lines (or disable the feature altogether) with the `set cli` command.

General CLI Commands

The following commands relate to the CLI itself.

To configure the current command line session:

```
set cli scscommands <enable|disable>
```

Allows you to use SCS-compatible commands as shortcuts for executing commands.

Note: *Settings are retained between CLI sessions for local and remote users.*

Table 5-1 SCS and SLC Commands

SCS Commands	SLC Commands
info	show sysstatus
version	admin version
reboot	admin reboot
poweroff	admin shutdown
listdev	show deviceport names
direct	connect direct deviceport
listen	connect listen deviceport
clear	set locallog clear
telnet	connect direct telnet
ssh	connect direct ssh

To start a menu if a menu is associated with the current user and was not displayed at login:

```
set cli menu start
```

To set the number of lines displayed by a command:

```
set cli terminallines <disable | Number of lines>
```

Sets the number of lines in the terminal emulation screen for paging through text one screen at a time, if the SLC console manager cannot detect the size of the terminal automatically.

To show current CLI settings:

```
show cli
```

To view the last 100 commands entered in the session:

```
show history
```

To clear the command history:

```
set history clear
```

To view the rights of the currently logged-in user:

```
show user
```

Note: *For information about user rights, see Chapter 12: User Authentication.*

6: Basic Parameters

This chapter describes how to set the following basic configuration settings for the SLC console manager using the SLC web interface or CLI:

- Network parameters that determine how the SLC console manager interacts with the attached network
- Firewall and routing
- Date and time

Note: *If you entered some of these settings using a Quick Setup procedure, you may update them here.*

This chapter contains the following sections:

Note: *The features and functionality described in this chapter specific to PC Card use are supported on SLC -02 part numbers. The features and functionality specific to USB port use are supported on SLC -03 part numbers.*

Requirements for IP Address Assignment

If you assign a different IP address from the current one, it must be within a valid range, unique to your network, and with the same subnet mask as your workstation.

To configure the unit, you need the following information:

Eth1

IP address: ________. ________ . ________ .________

Subnet mask: ________. ________ . ________ .________

Eth2

IP address (optional): ________. ________ . ________ .________

Subnet mask (optional): ________. ________ . ________ .________

Gateway: ________. ________ . ________ .________

DNS: ________. ________ . ________ .________

Network Settings

Network parameters determine how the SLC console manager interacts with the attached network. Use this page to set the basic configuration settings for the network ports (Eth1 and Eth2). If you entered some of these settings using a Quick Setup procedure, you may update them here.

Ethernet Bonding

The SLC console manager supports dual Ethernet interfaces. Typically both Ethernet interfaces are configured to work as independent network interfaces and given unique IP addresses and fixed MAC addresses. The Ethernet Bonding feature “bonds” the interfaces together to create a single virtual Network interface to SLC network applications.

All network parameters get configured on the primary Ethernet interface (1). The network application only registers with the Virtual interface (Bond0). In the case of a Ethernet link fault, the Virtual Interface (Bond 0) remains up, the application is completely unaware of the network fault and continues as if there was no fault. During Ethernet link faults an alert (interface trap) could be generated to the System Administrator if SNMP is configured and enabled.

Note: *You must configure Static IP addresses.*

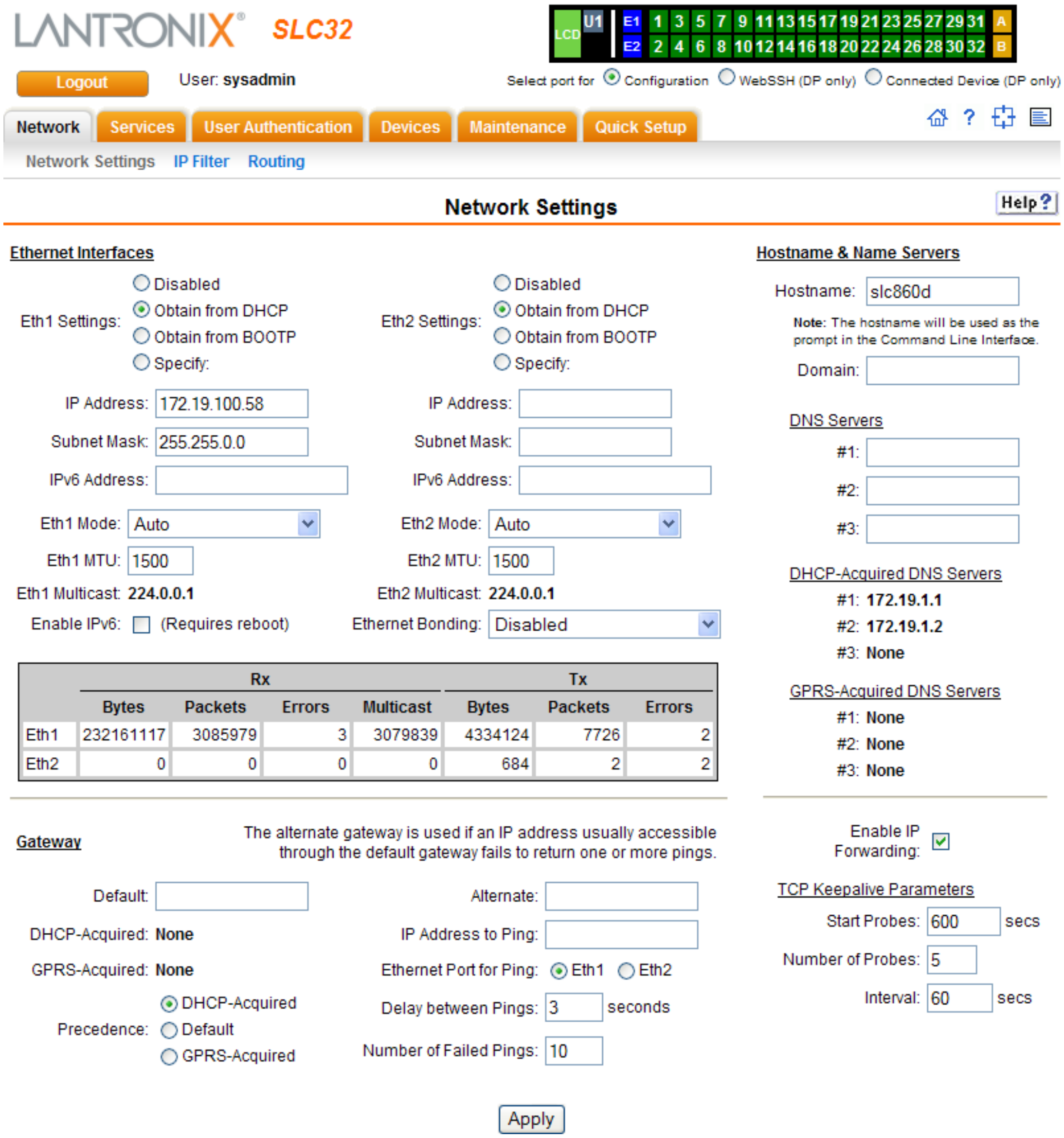
The virtual interface can be configured to run in one of three modes, and they are:

- Active Backup—Uses Ethernet 2 as a backup to Ethernet 1. All network parameters get configured on Ethernet 1. Both ports are connected to the network (preferably different switches for increased network connection reliability), but the Virtual Interface Manager only uses one interface. When the Virtual Interface Manager detects a link-down status on the active port, it switches over to the backup interface making it the primary. When the switch occurs to the backup interface, all Physical Layer communications with the SLC console manager continue using the MAC address of the active interface. The IP stack sees one interface (Virtual Interface bond0) only.
- 802.3ad Dynamic Link Aggregation (load-balancing protocol)—Uses both Ethernet interfaces for transmission. The Virtual Interface (Bond0) Manager uses the protocol to determine which Ethernet interface to use for transmission, based on the Source and Destination MAC address pair and Ethernet interface number. All data continues to get received on the primary Ethernet Interface (1). Both interfaces are connected to the switch. When the Virtual Interface Manager detectes a link-down status on any active interface, it disables the 802.3ad Dynamic Link Aggregation making the active interface the primary.
- Load Balancing (Transmit Load Balancing)—Uses both Ethernet interfaces for transmission load balancing. The Virtual Interface Manager determines which Ethernet interface to use based on the transmit load of the Ethernet interfaces (typically alternating). All data continues to get received on primary Ethernet Interface (1). Both interfaces are connected to the switch. When the Virtual Interface Manager detects a
link-down status on any active interface it disables Load Balancing making the active interface the primary.

To enter settings for one or both network ports:

1. Click the **Network** tab and the **Network Settings** option. *Figure 6-1* shows the page that displays.

Figure 6-1 Network Web Page



User: **sysadmin**

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Network Settings

Ethernet Interfaces

Eth1 Settings: ○ Disabled ● Obtain from DHCP ○ Obtain from BOOTP ○ Specify:

IP Address: 172.19.100.58

Subnet Mask: 255.255.0.0

IPv6 Address:

Eth1 Mode: Auto

Eth1 MTU: 1500

Eth1 Multicast: **224.0.0.1**

Enable IPv6: □ (Requires reboot)

Eth2 Settings: ○ Disabled ● Obtain from DHCP ○ Obtain from BOOTP ○ Specify:

IP Address:

Subnet Mask:

IPv6 Address:

Eth2 Mode: Auto

Eth2 MTU: 1500

Eth2 Multicast: **224.0.0.1**

Ethernet Bonding: Disabled

	Rx				Tx		
	Bytes	**Packets**	**Errors**	**Multicast**	**Bytes**	**Packets**	**Errors**
Eth1	232161117	3085979	3	3079839	4334124	7726	2
Eth2	0	0	0	0	684	2	2

Hostname & Name Servers

Hostname: slc860d

Note: The hostname will be used as the prompt in the Command Line Interface.

Domain:

DNS Servers

#1:

#2:

#3:

DHCP-Acquired DNS Servers

#1: **172.19.1.1**

#2: **172.19.1.2**

#3: **None**

GPRS-Acquired DNS Servers

#1: **None**

#2: **None**

#3: **None**

Gateway

The alternate gateway is used if an IP address usually accessible through the default gateway fails to return one or more pings.

Default:

DHCP-Acquired: **None**

GPRS-Acquired: **None**

Precedence: ● DHCP-Acquired ○ Default ○ GPRS-Acquired

Alternate:

IP Address to Ping:

Ethernet Port for Ping: ● Eth1 ○ Eth2

Delay between Pings: 3 seconds

Number of Failed Pings: 10

Enable IP Forwarding: ☑

TCP Keepalive Parameters

Start Probes: 600 secs

Number of Probes: 5

Interval: 60 secs

2. Enter the following fields.

Ethernet Interfaces

Note: *Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.*

Eth1/Eth2 Settings	**Disabled:** If selected, disables the network port. Defaults are Eth1 and Eth2 enabled. **Obtain from DHCP:** Acquires IP address, subnet mask, hostname and gateway from the DHCP server. (The DHCP server may not provide the hostname gateway, depending on its setup.) This is the default setting. If you select this option, skip to **Gateway**. **Obtain from BOOTP:** Lets a network node request configuration information from a BOOTP “server” node. If you select this option, skip to **Gateway**. **Specify:** Lets you manually assign a static IP address, generally provided by the system administrator.
IP Address (if specifying)	Enter an IP address that will be unique and valid on your network. There is no default. Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last segment. ***Note:*** *Currently, the SLC console manager does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).*
Subnet Mask (if specifying)	If specifying an IP address, enter the network segment on which the SLC console manager resides. There is no default.
Eth1/Eth2 IPv6 Address	Address of the port in IPv6 format. ***Note:*** *The SLC console manager supports IPv6 connections for a limited set of services: the web, ssh, and Telnet.* IPv6 addresses are written as 8 sets of 4-digit hexadecimal numbers separated by colons. There are several rules for modifying the address. For example, 1234:0BCD:1D67:0000:0000:8375:BADD:0057 may be shortened to 1234:BCD:1D67::8375:BADD:57.
Eth1/Eth2 Mode	Select the direction (full duplex or half-duplex) and speed (10 or 100Mbit) of data transmission. The default is **Auto**, which allows the Ethernet port to auto-negotiate the speed and duplex with the hardware endpoint to which it is connected.
Eth1/Eth2 MTU	Specifies the Maximum Transmission Unit (MTU) or Maximum Packet Size of packets at the IP layer (OSI layer 3) for the Ethernet port. When fragmenting a datagram, this is the largest number of bytes that can be used in a packet.
Eth1/Eth2 Multicast	Displays the multicast address of the Ethernet port.
Enable IPv6	Check this box to enable IPv6. You must reboot the SLC console manager to enable IPv6.

Ethernet Bonding	Use the pull-down menu to select and configure one of the following: ◆ Disabled ◆ Active Backup ◆ 802.3 ◆ Transmit Load Balancing **Note:** *Bonding requires a static IP address.*

Gateway

Default	IP address of the router for this network. If this has not been set manually, any gateway acquired by DHCP for Eth1 or Eth2 displays. All network traffic that matches the Eth1 IP address and subnet mask is sent out Eth1. All network traffic that matches the Eth2 IP address and subnet mask is sent out Eth 2. If you set a default gateway, any network traffic that does not match Eth1 or Eth2 is sent to the default gateway for routing.
DHCP-Acquired (view only)	Gateway acquired by DHCP for Eth1 or Eth2.
GPRS-Acquired (view only)	Displays the IP address of the router if it has been automatically assigned by General Packet Radio Service (GPRS).
Precedence	Indicates whether the gateway acquired by DHCP or the default gateway takes precedence. The default is DHCP Gateway. If the DHCP Gateway is selected and both Eth1 and Eth2 are configured for DHCP, the SLC console manager gives precedence to the Eth1 gateway.
Alternate	An alternate IP address of the router for this network, to be used if an IP address usually accessible through the default gateway fails to return one or more pings.
IP Address to Ping	IP address to ping to determine whether to use the alternate gateway.
Ethernet Port to Ping	Ethernet port to use for the ping.
Delay between Pings	Number of seconds between pings
Number of Failed Pings	Number of pings that fail before the Lantronix SLP™ power manager uses the alternate gateway.
Enable IP Forwarding	IP forwarding enables network traffic received on one interface (Eth1, Eth2, or an external/PC Card/USB modem attached to the SLC console manager with an active PPP connection) to be transferred out another interface (any of the above). The default behavior (if IP forwarding is disabled) is for network traffic to be received but not routed to another destination. Enabling IP forwarding is required if you enable Network Address Translation (NAT) for any device port modem or PC Card/USB/ISDN modem. IP forwarding allows a user accessing the SLC console manager over a modem to access the network connected to Eth1 or Eth2.

Hostname & Name Servers

Hostname	The default host name is slcXXXX, where XXXX is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). The host name becomes the prompt in the command line interface.
Domain	If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLC console manager. For example, if **abcd** is specified for the SMTP server, and **mydomain.com** is specified for the domain, if **abcd** cannot be resolved, the SLC device attempts to resolve **abcd.mydomain.com** for the SMTP server.
DNS Servers	Configure up to three name servers. #1 is required if you choose to configure DNS (Domain Name Server) servers. The first three DNS servers acquired via DHCP through Eth1 and/or Eth2 display automatically.
DHCP-Acquired DNS Servers	Displays the IP address of the name servers if automatically assigned by DHCP.
GPRS-Acquired DNS Servers	Displays the IP address of the name servers if automatically assigned by General Packet Radio Service (GPRS).
TCP Keepalive Parameters	**Start Probes**—Number of seconds the SLC console manager waits after the last transmission before sending the first probe to determine whether a TCP session is still alive. The default is 600 seconds (10 minutes). **Number of Probes**—Number of probes the SLC device sends before closing a session. The default is 5. **Interval**—The number of seconds the SLC console manager waits between probes. The default is 60 seconds.

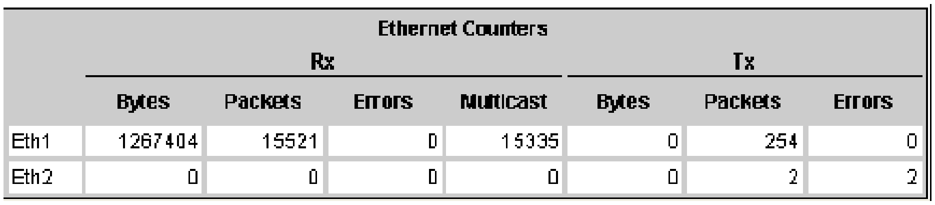
3. Click the **Apply** button. Changes take effect immediately and are saved for the next session after the SLC console manager reboots.

Ethernet Counters

In the middle of the Network Settings page, statistics display for each SLC ethernet port since boot-up as shown in *Figure 6-2*. The system automatically updates the statistics.

Note: *For Ethernet statistics for a smaller time period, use the* `diag perfstat` *command.*

Figure 6-2 Ethernet Counters Example



Ethernet Counters

	Rx				Tx		
	Bytes	Packets	Errors	Multicast	Bytes	Packets	Errors
Eth1	1267404	15521	0	15335	0	254	0
Eth2	0	0	0	0	0	2	2

Network Commands

The following CLI commands correspond to the **Network Settings** page. For more information, see 15: Command Reference.

- *set network (on page 240)*
- *set network bonding (on page 240)*
- *set network dns (on page 240)*
- *set network gateway (on page 240)*
- *set network host (on page 241)*
- *set network port (on page 241)*
- *set network ipv6 (on page 241)*
- *show network bonding (on page 241)*
- *show network dns (on page 242)*
- *show network gateway (on page 242)*
- *show network host (on page 242)*
- *show network port (on page 242)*
- *show network all (on page 241)*

IP Filters

IP filters (also called rulesets) act as a firewall to allow or deny individual or a range of IP addresses, ports, and protocols. When a network connection gets configured to use an IP filter, all network traffic through that connection gets compared to the rulesets of that filter by precedence. Network traffic may be allowed to pass, it may be dropped without notice, or it may be rejected (sends back an error packet) depending upon the rulesets of the filter.

The administrator uses the **IP Filter** page to view, add, edit, delete, and map IP filters.

Warning: ***IP filters configuration is a feature for advanced users. Adding and enabling IP filter sets incorrectly can disable your SLC console manager.***

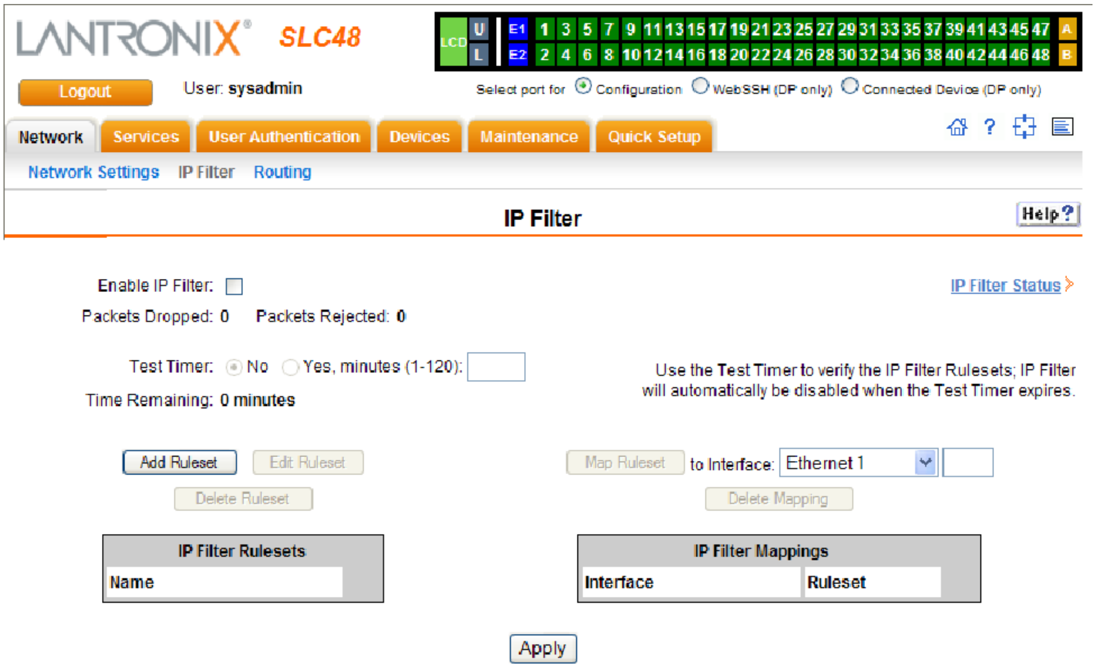
Enabling IP Filters

Enable or disable all filters by using the **IP Filter** page. There is no way to enable or disable individual filters.

To enable IP filters:

1. Click the **Network** tab and **IP Filter** option. *Figure 6-3* shows the page that displays.

Figure 6-3 IP Filter Page



Enable IP Filter: □

Packets Dropped: 0 Packets Rejected: 0

Test Timer: ● No ○ Yes, minutes (1-120):

Time Remaining: 0 minutes

Use the Test Timer to verify the IP Filter Rulesets; IP Filter will automatically be disabled when the Test Timer expires.

IP Filter Rulesets
Name

IP Filter Mappings	
Interface	Ruleset

1. Enter the following fields.

Enable IP Filter	Select the Enable IP Filter checkbox to enable all filters, or clear the checkbox to disable all filters. Disabled by default.
Packets Dropped (view only)	Displays the number of data packets that the filter ignored (did not respond to).
Packets Rejected (view only)	Displays the number of data packets that the filter sent a “rejected” response to.
Test Timer	Timer for testing IP Filter rulesets. Select No to disable the timer. Select Yes, minutes (1-120) to enable the timer and enter the number of minutes the timer should run. The timer automatically disables the IP Filters when the time expires.
Time Remaining (view only)	Indicates how many minutes are left on the timer before it expires and IP Filters are disabled.

2. Click the **Apply** button.

Note: *You cannot enable or disable individual filters.*

Configuring IP Filters Rulesets

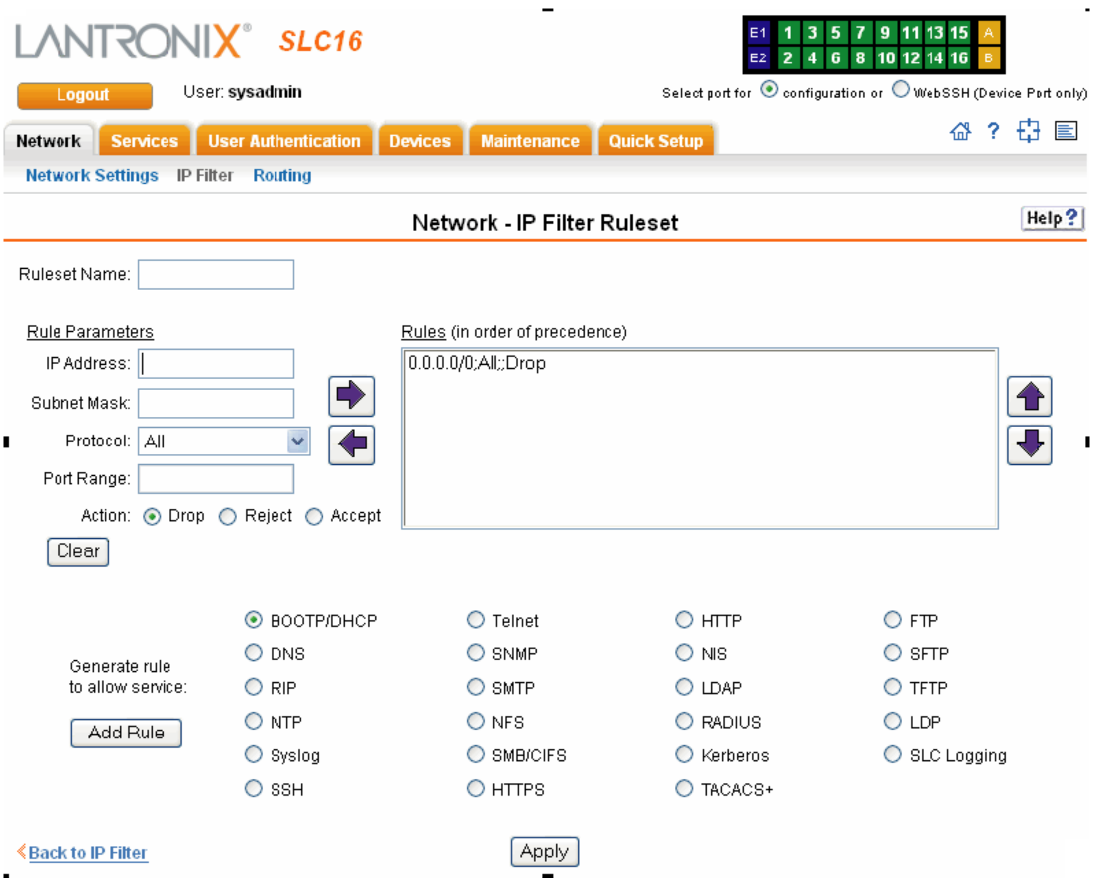
The administrator can add, edit, delete, and map IP filter rulesets.

Note: *A configured filter ruleset has no effect until it is mapped to a network interface. See To map a ruleset: on page 56*

To add an IP filter ruleset:

1. On the **IP Filter** page, click the **Add Ruleset** button. *Figure 6-4* shows the page that displays.

Figure 6-4 Adding Network IP Filter Rulesets



User: sysadmin

Select port for ● configuration or ○ WebSSH (Device Port only)

Network - IP Filter Ruleset

Ruleset Name:

Rule Parameters

IP Address:

Subnet Mask:

Protocol: All

Port Range:

Action: ● Drop ○ Reject ○ Accept

Rules (in order of precedence)

0.0.0.0/0;All;;Drop

Generate rule to allow service:

● BOOTP/DHCP	○ Telnet	○ HTTP	○ FTP
○ DNS	○ SNMP	○ NIS	○ SFTP
○ RIP	○ SMTP	○ LDAP	○ TFTP
○ NTP	○ NFS	○ RADIUS	○ LDP
○ Syslog	○ SMB/CIFS	○ Kerberos	○ SLC Logging
○ SSH	○ HTTPS	○ TACACS+	

2. Enter the **Ruleset Name**. The **Ruleset Name** identifies a filter. The name can be letters, numbers, and hyphens only but cannot start with a hyphen. For example, FILTER-2.
3. Enter following fields.

Rule Parameters

IP Address	Specify a single IP address to act as a filter. **Example:** 172.19.220.64 – this specific IP address only
Subnet Mask	Specify a subnet mask to act as a filter. **Example:** 255.255.0.0
Protocol	Select from the drop-down list the type of protocol through which the filter will operate. The default setting is **All**.
Port Range	Enter a range of destination TCP or UDP port numbers to be tested. An entry is required for TCP, TCP New, TCP Established, and UDP, and is not allowed for other protocols. Separate multiple ports with commas. Separate ranges of ports by colons. Examples: 22 – filter on port 22 only 23,64,80 – filter on ports 23, 64 and 80 23:64,80,143:150 – filter on ports 23 through 64, port 80 and ports 143 through 150

Action	Select whether to drop, reject, or allow communications for the specified IP address, subnet mask, protocol, and port range. **Drop** ignores the packet with no notification. **Reject** ignores the packet and sends back an error message. **Allow** permits the packet through the filter.
Generate rule to allow service	Allow a particular protocol or service in your filter set. For example, if you have configured your NIS server and want to allow traffic to pass, select the **NIS** option and click the **Add Rule** button. This entry adds a new rule to your filter set using the NIS -configured IP address. Other services and protocols that are added automatically generate the necessary rule to allow usage.

4. Click the **right arrow** button to add the new rule and its parameters to the bottom of the **Rules** list box on the right.
5. To modify a ruleset, highlight its name in the **Rules** list box and click the **left arrow**. The rule populates the rule definition fields, allowing you to make minor changes before reinserting the rule. To clear the definition fields, click the **Clear** button.
6. To change the order of priority of the rules in the list box, select the rule to move and use the **up** or **down arrow** buttons on the right side of the filter list box.
7. Click the **Apply** button. The new filter displays in the menu tree.

Note: *To add another new filter ruleset, click the **Back to IP Filter** link to return to the IP Filter page.*

To update an IP filter ruleset:

The administrator can update an IP filter ruleset.

1. On the **IP Filter** page, select the IP filter ruleset to be edited and click the **Edit Ruleset** button. The **IP Filter Ruleset** page displays.
2. Edit the information as desired and click the **Apply** button.

To delete an IP filter ruleset:

The administrator can delete an IP filter ruleset.

1. On the **IP Filter** page, select the IP filter ruleset to be deleted and click the **Delete** button.

To map a ruleset:

The administrator can assign an IP Filter ruleset to a network interface (Ethernet interface), a modem connected to a Device Port, a PC Card slot, or a USB port.

1. On the **IP Filter** page, select the IP filter ruleset to be mapped.
2. From the **Interface** drop-down list, select the interface and click the **Map Ruleset** button. The Interface and ruleset display in the IP Filter Mappings table.

To delete a map:

1. On the **IP Filter** page, select the mapping from the list and click the **Delete Mappings** button. The mapping no longer displays.
2. Click the **Apply** button.

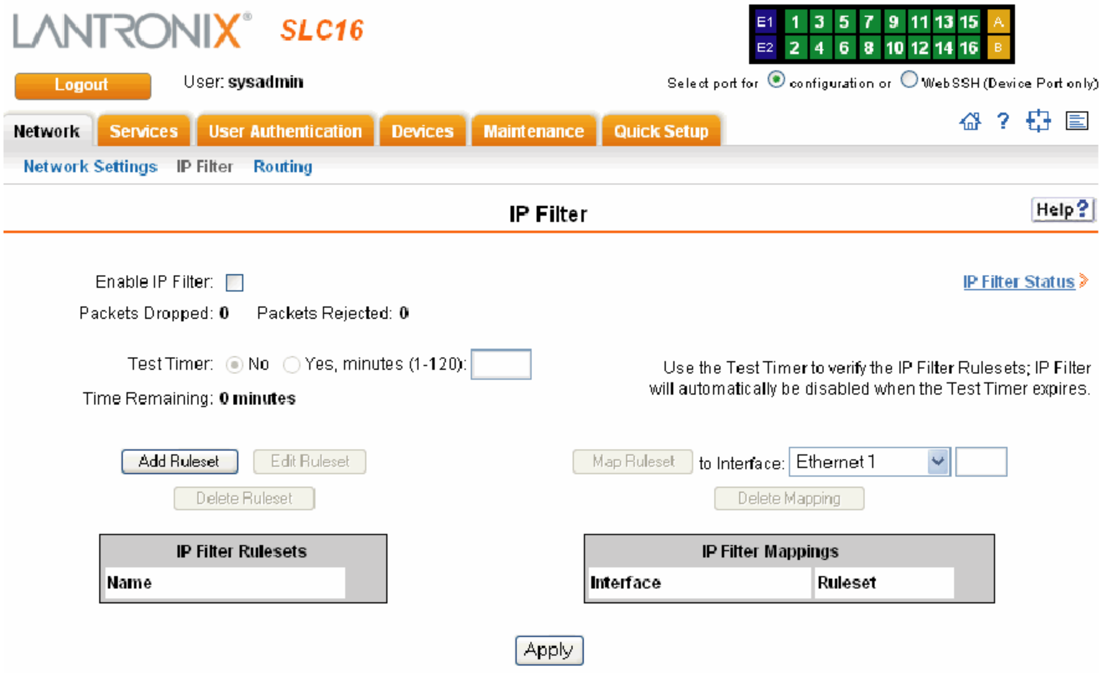
Viewing IP Filter Rulesets and Mapping

You can view a list of filter rulesets and a table showing how each filter is mapped to an interface. You can also view the status of the configured filter rulesets. The status page displays the number of incoming, outgoing, and forwarded packets.

To view a list of IP filter rulesets and mappings:

1. Click the **Network** tab and select the **IP Filter** option. *Figure 6-5* shows the page that displays.

Figure 6-5 IP Filter Page Displaying Rulesets and Mappings



User: sysadmin

Select port for ● configuration or ○ WebSSH (Device Port only)

Enable IP Filter: □

Packets Dropped: 0   Packets Rejected: 0

Test Timer: ● No ○ Yes, minutes (1-120):

Time Remaining: 0 minutes

Use the Test Timer to verify the IP Filter Rulesets; IP Filter will automatically be disabled when the Test Timer expires.

to Interface: Ethernet 1

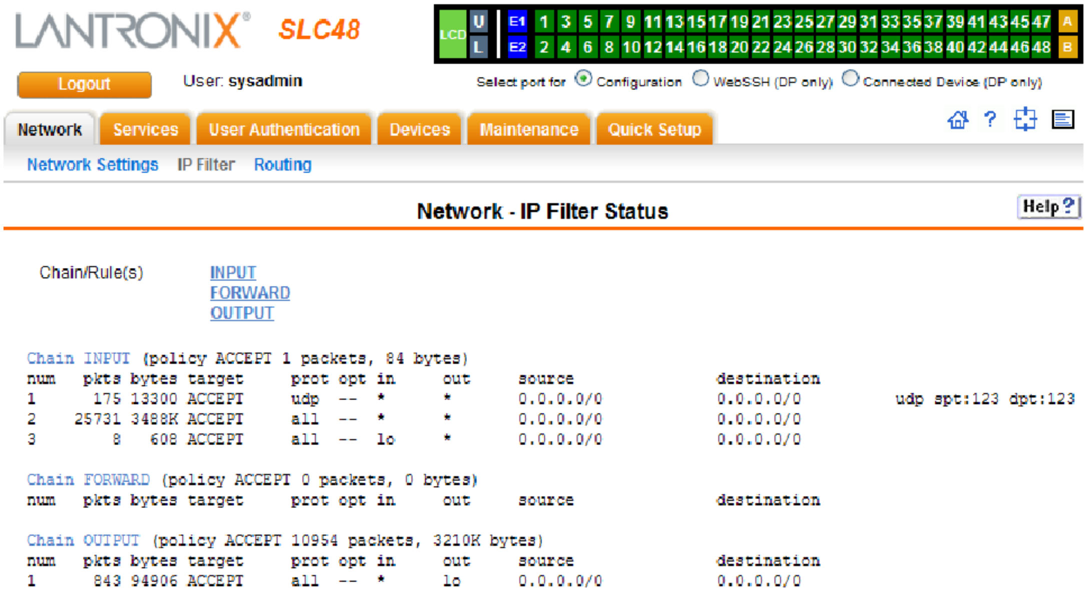
IP Filter Rulesets
Name

IP Filter Mappings	
Interface	Ruleset

To view IP Filter Status:

1. Click IP Filter Status link. *Figure 6-6* shows the page that displays.

Figure 6-6 IP Filter Status



User: sysadmin

Network - IP Filter Status

Chain/Rule(s) INPUT
FORWARD
OUTPUT

```
Chain INPUT (policy ACCEPT 1 packets, 84 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      175 13300 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:123 dpt:123
2    25731 3488K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
3        8   608 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 10954 packets, 3210K bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      843 94906 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
```

IP Filter Commands

The following CLI commands correspond to the **Network - IP Filter Status** page. For more information, see 15: Command Reference.

- *set ipfilter state (on page 233)*
- *set ipfilter mapping (on page 232)*
- *set ip filter rules (on page 232)*
- *show ipfilter (on page 233)*
- *show ipfilter ruleset (on page 233)*
- *show ipfilter status (on page 233)*

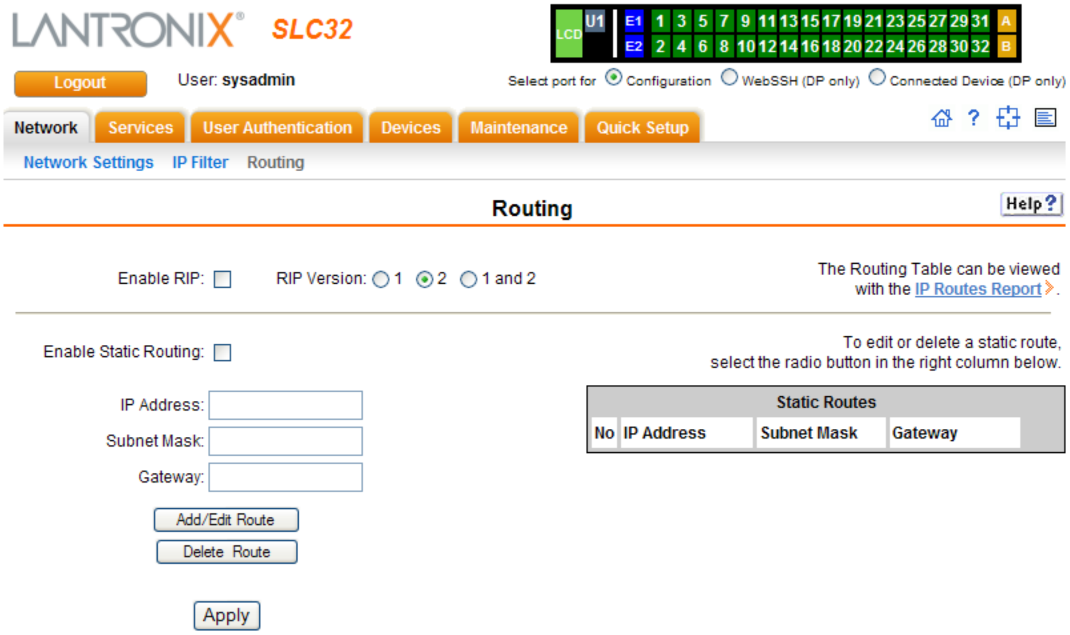
Routing

You can define static routes, and for networks using Routing Information Protocol (RIP), you can configure dynamic routes.

To configure routing settings:

1. Click the **Network** tab and select the **Routing** option. *Figure 6-7* shows the page that displays.

Figure 6-7 Routing Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Routing

Enable RIP: □ RIP Version: ○ 1 ● 2 ○ 1 and 2

The Routing Table can be viewed with the IP Routes Report.

Enable Static Routing: □

To edit or delete a static route, select the radio button in the right column below.

IP Address:

Subnet Mask:

Gateway:

Static Routes			
No	IP Address	Subnet Mask	Gateway

2. Enter the following fields.

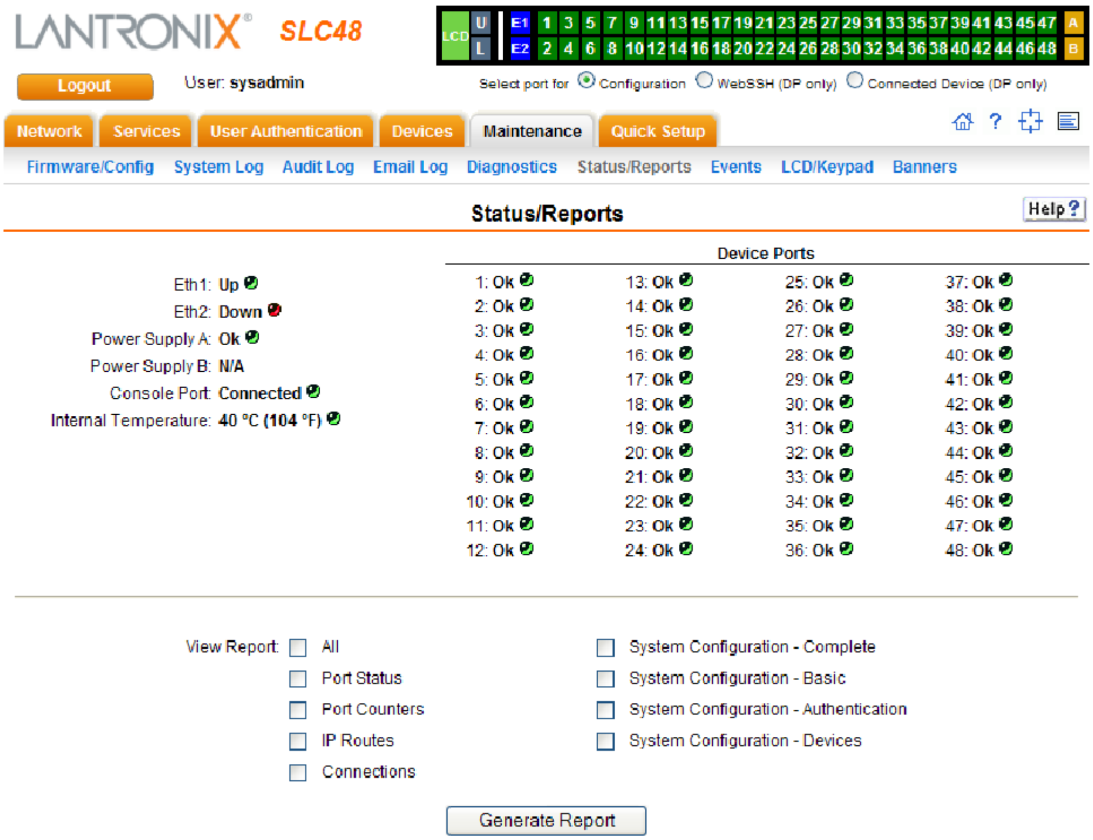
Enable RIP	Select to enable Dynamic Routing Information Protocol (RIP) to assign routes automatically. Disabled by default.
RIP Version	Select the RIP version. The default is **2**.
Enable Static Routing	Select to assign the routes manually. The system administrator usually provides the routes. Disabled by default. ◆ To add a static route, enter the **IP Address**, **Subnet Mask**, and **Gateway** for the route and click the **Add/Edit Route** button. The route displays in the Static Routes table. You can add up to 64 static routes. ◆ To edit a static route, select the radio button to the right of the route, change the **IP Address**, **Subnet Mask**, and **Gateway** fields as desired, and click the **Add/ Edit Route** button. ◆ To delete a static route, select the radio button to the right of the route and click the **Delete Route** button.

3. Click the **Apply** button.

To view the IP Routing Table:

1. Click the **IP Routes Report** link. *Figure 6-8* shows the page that displays.

Figure 6-8 Status/Reports Page


LANTRONIX SLC48
LCD U L E1 E2
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network Services User Authentication Devices Maintenance Quick Setup
Firmware/Config System Log Audit Log Email Log Diagnostics Status/Reports Events LCD/Keypad Banners
Help ?
Generate Report

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Status/Reports

Eth1: Up ●
Eth2: Down ●
Power Supply A: Ok ●
Power Supply B: N/A
Console Port: Connected ●
Internal Temperature: 40 °C (104 °F) ●

Device Ports

1: Ok ●	13: Ok ●	25: Ok ●	37: Ok ●
2: Ok ●	14: Ok ●	26: Ok ●	38: Ok ●
3: Ok ●	15: Ok ●	27: Ok ●	39: Ok ●
4: Ok ●	16: Ok ●	28: Ok ●	40: Ok ●
5: Ok ●	17: Ok ●	29: Ok ●	41: Ok ●
6: Ok ●	18: Ok ●	30: Ok ●	42: Ok ●
7: Ok ●	19: Ok ●	31: Ok ●	43: Ok ●
8: Ok ●	20: Ok ●	32: Ok ●	44: Ok ●
9: Ok ●	21: Ok ●	33: Ok ●	45: Ok ●
10: Ok ●	22: Ok ●	34: Ok ●	46: Ok ●
11: Ok ●	23: Ok ●	35: Ok ●	47: Ok ●
12: Ok ●	24: Ok ●	36: Ok ●	48: Ok ●

View Report: □ All
□ Port Status
□ Port Counters
□ IP Routes
□ Connections

□ System Configuration - Complete
□ System Configuration - Basic
□ System Configuration - Authentication
□ System Configuration - Devices

2. Click the **IP Routes** checkbox and **Generate Report**. You can also generate reports for port status and counters, connections, and system configurations in this page.

Routing Commands

The following CLI commands correspond to the **Status/Reports** page. For more information, see 15: Command Reference.

- *set routing (on page 250)*
- *show routing (on page 250)*

7: Services

This chapter describes how to use the **Services** web page to perform the following tasks:

- Configure the amount of data sent to the logs.
- Enable or disable SSH and Telnet logins.
- Enable a Simple Network Management Protocol (SNMP) agent.
- Identify a Simple Mail Transfer Protocol (SMTP) server.
- Enable or disable SSH and Telnet logins.
- Configure an audit log.
- View the status of and manage the SLC console manager on the secure Lantronix network.
- Set the date and time.
- Configure the web server.
- Import a site-specific SSL certificate.
- Enable an iGoogle gadget that displays the status of ports on multiple SLC console managers.
- View and terminate web sessions.

It contains the following sections:

Note: *The SLC console manager supports both MIB-II as defined by RFC 1213 and a private enterprise MIB. MIB definition files for the private enterprise MIB are available for download at http://www.lantronix.com/support/downloads/. The private enterprise MIB provides read-only access to all statistics and configurable items provided by the SLC device. It provides read-write access to a select set of functions for controlling the SLC console manager and device ports. See the MIB definition file for details.*

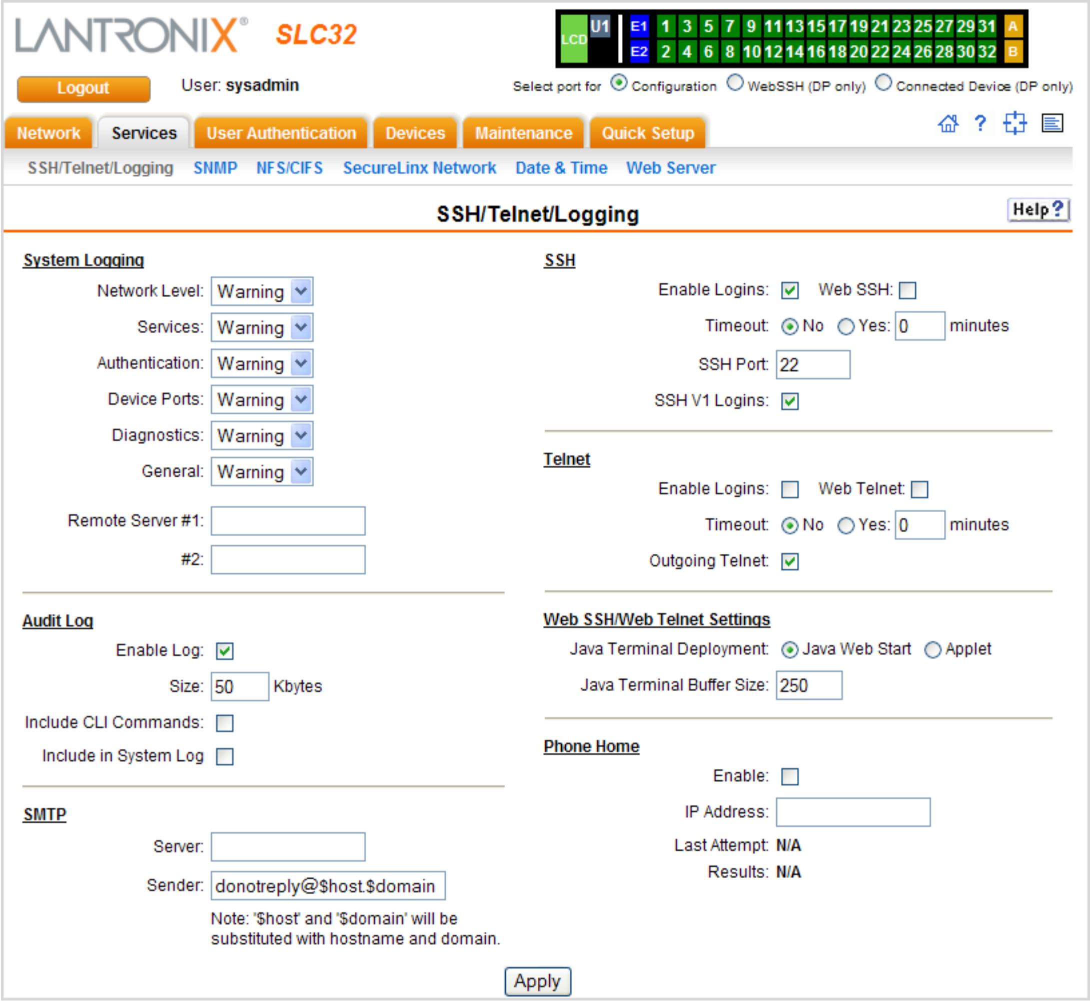
Note: *The features and functionality described in this chapter specific to PC Card use are supported on SLC-02 part numbers. The features and functionality specific to USB port use are supported on SLC-03 part numbers.*

SSH/Telnet/Logging

To configure SSH, Telnet, and Logging settings:

1. Click the **Services** tab and select the **SSH/Telnet /Logging** option. *Figure 7-1* shows the page that displays.

Figure 7-1 SSH/Telnet/Logging Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

SSH/Telnet/Logging

System Logging

Network Level: Warning

Services: Warning

Authentication: Warning

Device Ports: Warning

Diagnostics: Warning

General: Warning

Remote Server #1:

#2:

Audit Log

Enable Log: ☑

Size: 50 Kbytes

Include CLI Commands: □

Include in System Log □

SMTP

Server:

Sender: donotreply@$host.$domain

Note: '$host' and '$domain' will be substituted with hostname and domain.

SSH

Enable Logins: ☑ Web SSH: □

Timeout: ● No ○ Yes: 0 minutes

SSH Port: 22

SSH V1 Logins: ☑

Telnet

Enable Logins: □ Web Telnet: □

Timeout: ● No ○ Yes: 0 minutes

Outgoing Telnet: ☑

Web SSH/Web Telnet Settings

Java Terminal Deployment: ● Java Web Start ○ Applet

Java Terminal Buffer Size: 250

Phone Home

Enable: □

IP Address:

Last Attempt: N/A

Results: N/A

2. Enter the following fields.

System Logging

In **System Logging**, select one of the following alert levels from the drop-down list for each category:

- **Off:** Disables this type of logging.
- **Info:** Saves informative message, in addition to warning and error messages.
- **Warning:** Saves message output from a condition that may be cause for concern, in addition to error messages. This is the default for all message types.
- **Error:** Saves messages that are output because of an error.
- **Debug:** Saves extraneous detail that may be helpful in tracking down a problem, in addition to information, warning, and error messages.

Network Level	Specifies that messages concerning the network activity get logged. For example, messages regarding Ethernet and routing.

Services	Specifies that messages about SNMP and SMTP get logged.
Authentication	Specifies that messages concerning user authentication get logged.
Device Ports	Specifies that messages concerning device ports and connections get logged.
Diagnostics	Specifies that messages concerning system status and problems get logged.
General	Specifies that messages not in the categories above get logged.
Remote Servers (#1 and #2)	Specifies the IP address of remote server 1 and 2 for logged messages. The system log is always saved to local SLC storage. It is retained through SLC console manager reboots for files up to 200K. Saving the system log to a server that supports remote logging services (see RFC 3164) allows the administrator to save the complete system log history.

SSH

Enable Logins	Enables or disables SSH logins to the SLC console manager to allow users to access the CLI using SSH. Enabled by default. This setting does not control SSH access to individual device ports. (See Device Ports on page 81 for information on enabling SSH access to individual ports.) Most system administrators enable SSH logins, which is the preferred method of accessing the system.
Web SSH	Enables or disables the ability to access the SLC command line interface or device ports (connect direct) through the Web SSH window. Disabled by default.
Timeout	Enables a timeout if you enable SSH logins and an idle connection has disconnected. Select **Yes** and enter a value of from 1 to 30 minutes.
SSH Port	Allows you to change the SSH login port to a different value in the range of 1 - 65535. The default is **22**.
SSH V1 Logins	Enables or disables SSH version 1 connections to the SLC console manager. Enabled by default. *Note: Disabling SSH V1 blocks Web SSH CLI and Web SSH to device port connections on the SLC Network page. Also, you must reboot the SLC console manager before a change will take effect.*

Telnet

Enable Logins	Enables or disables Telnet logins to the SLC console manager to allow users to access the CLI using Telnet. Disabled by default. This setting does not control Telnet access to individual device ports. (See Device Ports on page 81 for information on enabling Telnet access to individual ports.) You may want to keep this option disabled for security reasons.
Web Telnet	Enables or disables the ability to access the SLC command line interface or device ports (connect direct) through the Web Telnet window. Disabled by default.
Timeout	Specifies a timeout for disconnect when telnet logins are enabled. Select **Yes** and enter a value of from 1 to 30 minutes. *Note: You must reboot the unit before a change will take effect.*
Outgoing Telnet	Enables or disables the ability to create Telnet out connections.

Audit Log

Enable Log	Select to save a history of all configuration changes in a circular log. Disabled by default. The audit log is saved through SLC reboots.
Size	Set the maximum size of a log from 1 to 500 Kbytes. The default maximum size of a log is **50** Kbytes (approximately 500 entries).
Include CLI Commands	Select to cause the audit log to include the CLI commands that have been executed. Disabled by default.
Include In System Log	Enable to include the audit log contents in the system log (under the General/Info category/level). Disabled by default.

Web SSH/Web Telnet

Java Terminal Deployment	Method used to launch Java applications, either Java Web Start or Applet.
Java Terminal Buffer Size	Number of lines in the Java terminal window that are available for scrolling back through output. The valid range is 24 to 5000 and the default is **250**.

SMTP

Server	IP address of your network's Simple Mail Transfer Protocol (SMTP) relay server.
Sender	The email address of the sender of outgoing emails. The strings "$host" and "$domain" can be part of the email address - they will be substituted with the actual hostname and domain. The default is donotreply@$host.$domain.

Phone Home

Enable	If enabled, the SLC console manager will attempt to phone home every hour until it has contacted a Lantronix SLM™ management appliance and provided it with its configuration.
IP Address	IP address of the SLM management appliance.
Last Attempt (view only)	Date and time of last connection attempt.
Results (view only)	Indicates whether the attempt was successful.

3. To save, click the **Apply** button.

SSH, Telnet, and Logging Commands

The following CLI commands correspond to the **SSH/Telnet/Logging** page. For more information, see *15: Command Reference*.

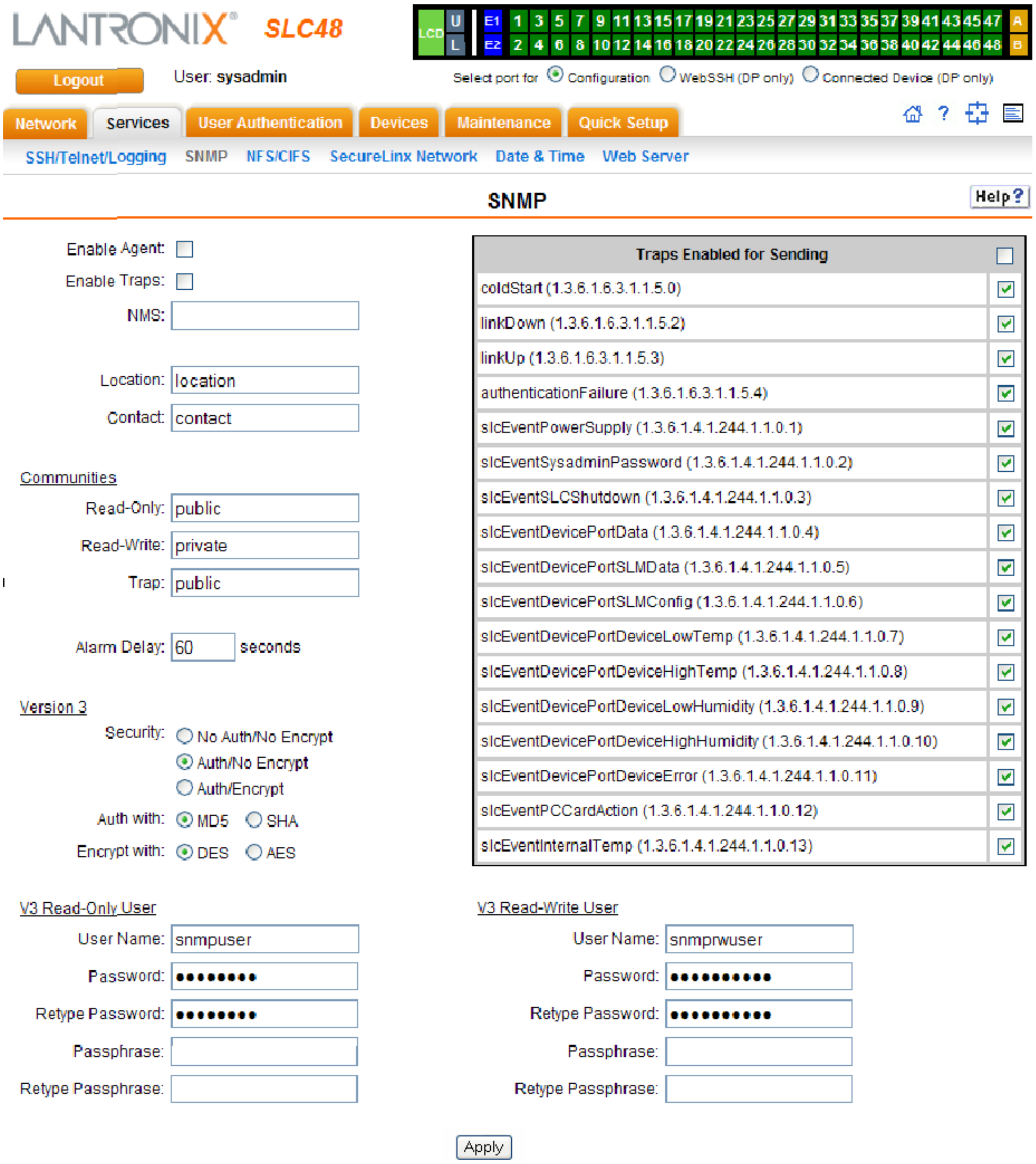
- *set services (on page 252)*
- *set services trapenable (on page 253)*
- *show services (on page 253)*

SNMP

Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks.

1. Click the **Services** tab and select the **SNMP** option. *Figure 7-2* shows the page that displays.

Figure 7-2 SNMP Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

SNMP

Enable Agent: □

Enable Traps: □

NMS:

Location: location

Contact: contact

Communities

Read-Only: public

Read-Write: private

Trap: public

Alarm Delay: 60 seconds

Version 3

Security: ○ No Auth/No Encrypt ● Auth/No Encrypt ○ Auth/Encrypt

Auth with: ● MD5 ○ SHA

Encrypt with: ● DES ○ AES

Traps Enabled for Sending	□
coldStart (1.3.6.1.6.3.1.1.5.0)	☑
linkDown (1.3.6.1.6.3.1.1.5.2)	☑
linkUp (1.3.6.1.6.3.1.1.5.3)	☑
authenticationFailure (1.3.6.1.6.3.1.1.5.4)	☑
slcEventPowerSupply (1.3.6.1.4.1.244.1.1.0.1)	☑
slcEventSysadminPassword (1.3.6.1.4.1.244.1.1.0.2)	☑
slcEventSLCShutdown (1.3.6.1.4.1.244.1.1.0.3)	☑
slcEventDevicePortData (1.3.6.1.4.1.244.1.1.0.4)	☑
slcEventDevicePortSLMData (1.3.6.1.4.1.244.1.1.0.5)	☑
slcEventDevicePortSLMConfig (1.3.6.1.4.1.244.1.1.0.6)	☑
slcEventDevicePortDeviceLowTemp (1.3.6.1.4.1.244.1.1.0.7)	☑
slcEventDevicePortDeviceHighTemp (1.3.6.1.4.1.244.1.1.0.8)	☑
slcEventDevicePortDeviceLowHumidity (1.3.6.1.4.1.244.1.1.0.9)	☑
slcEventDevicePortDeviceHighHumidity (1.3.6.1.4.1.244.1.1.0.10)	☑
slcEventDevicePortDeviceError (1.3.6.1.4.1.244.1.1.0.11)	☑
slcEventPCCardAction (1.3.6.1.4.1.244.1.1.0.12)	☑
slcEventInternalTemp (1.3.6.1.4.1.244.1.1.0.13)	☑

V3 Read-Only User

User Name: snmpuser

Password: ••••••••

Retype Password: ••••••••

Passphrase:

Retype Passphrase:

V3 Read-Write User

User Name: snmprwuser

Password: ••••••••••

Retype Password: ••••••••••

Passphrase:

Retype Passphrase:

2. Enter the following fields.

Enable Agent	Enables or disables SNMP agent, which allows read-only access to the system. Disabled by default.

Enable Traps	Traps are notifications of certain critical events. Disabled by default. This feature is applicable when SNMP is enabled. Examples of traps that the SLC console manager sends include: ◆ Ethernet Port Link Up ◆ Ethernet Port Link Down ◆ Authentication Failure ◆ SLC Booted ◆ SLC Shutdown ◆ Device Port Logging ◆ Power Supply Status ◆ Sysadmin user password changed The SLC device sends the traps to the host identified in the **NMS** field. **NMS**—When SNMP is enabled, an NMS (Network Management System) acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP. The NMS can request information from the SLC device and receive traps from the SLC console manager. Enter the IP address of the NMS server. Required if you selected **Enable Traps**. **Location**—Physical location of the SLC device (optional). Useful for managing the SLC console manager using SNMP. Up to 20 characters. **Contact**—Description of the person responsible for maintaining the SLC device, for example, a name (optional). Up to 20 characters.
Traps Enabled for Sending (Table listing types of traps)	Enables the sending of SNMP trap messages. Click the types of trap messages that you want to receive.

Communities

Read-Only	A string that acts like a password for an SNMP manager to access the read-only data the SLC SNMP agent provides. The default is **public**.
Read-Write	A string that acts like a password for an SNMP manager to access the read-only data the SLC SNMP agent provides and to modify data where permitted. The default is **private**.
Trap	The trap used for outgoing generic and enterprise traps. Traps sent with the Event trigger mechanism still use the trap community specified with the Event action. The default is **public**.
Alarm Delay	Number of seconds delay between outgoing SNMP traps.

Version 3

Security	Levels of security available with SNMP v. 3 are: ◆ **No Auth/No Encrypt:** No authentication or encryption. ◆ **Auth/No Encrypt:** Authentication but no encryption. (default) ◆ **Auth/Encrypt:** Authentication and encryption.
Auth with	For **Auth/No Encryp** or **Auth/Encrypt**, the authentication method: ◆ **MD5:** Message-Digest algorithm 5 (default) ◆ **SHA:** Secure Hash Algorithm

Encrypt with	Encryption standard to use: ◆ **DES:** Data Encryption Standard (default) ◆ **AES:** Advanced Encryption Standard

V3 Read-Only User

User Name	SNMP v3 is secure and requires user-based authorization to access SLC MIB objects. Enter a user ID. The default is **snmpuser**. Up to 20 characters.
Password/Retype Password	Password for a user with read-only authority to use to access SNMP v3. The default is **SNMPPASS**. Up to 20 characters.
Passphrase/ Retype Passphrase	Passphrase associated with the password for a user with read-only authority. Up to 20 characters.

V3 Read-Write User

User Name	SNMP v3 is secure and requires user-based authorization to access SLC MIB objects. Enter a user ID for users with read-write authority. The default is **snmprwuser**. Up to 20 characters.
Password/Retype Password	Password for the user with read-write authority to use to access SNMP v3. The default is **SNMPRWPASS**. Up to 20 characters.
Passphrase/ Retype Passphrase	Passphrase associated with the password for a user with read-write authority. Up to 20 characters.

3. Click the **Apply** button.

SNMP Commands

The following CLI commands correspond to the **SNMP** page. For more information, see *15: Command Reference*.

- *set services (on page 252)*
- *set services trapenable (on page 253)*

NFS and SMB/CIFS

If you want to save configuration and logging data to a remote NFS server, access the NFS & Server Message Block/Common Internet File System (**SMB/CIFS**) page. You can also export configuration and logging data by means of an exported CIFS share.

Mounting an NFS shared directory on a remote network server onto a local SLC directory enables the SLC console manager to store device port logging data on that network server. This configuration avoids possible limitations in the amount of disk space on the SLC device available for logging files. You may also save SLC configurations on the network server.

Similarly use SMB/CIFS, Microsoft file-sharing protocol, to export a directory on the SLC console manager as an SMB/CIFS share. The SLC device exports a single read-write CIFS share called “public,” with two subdirectories:

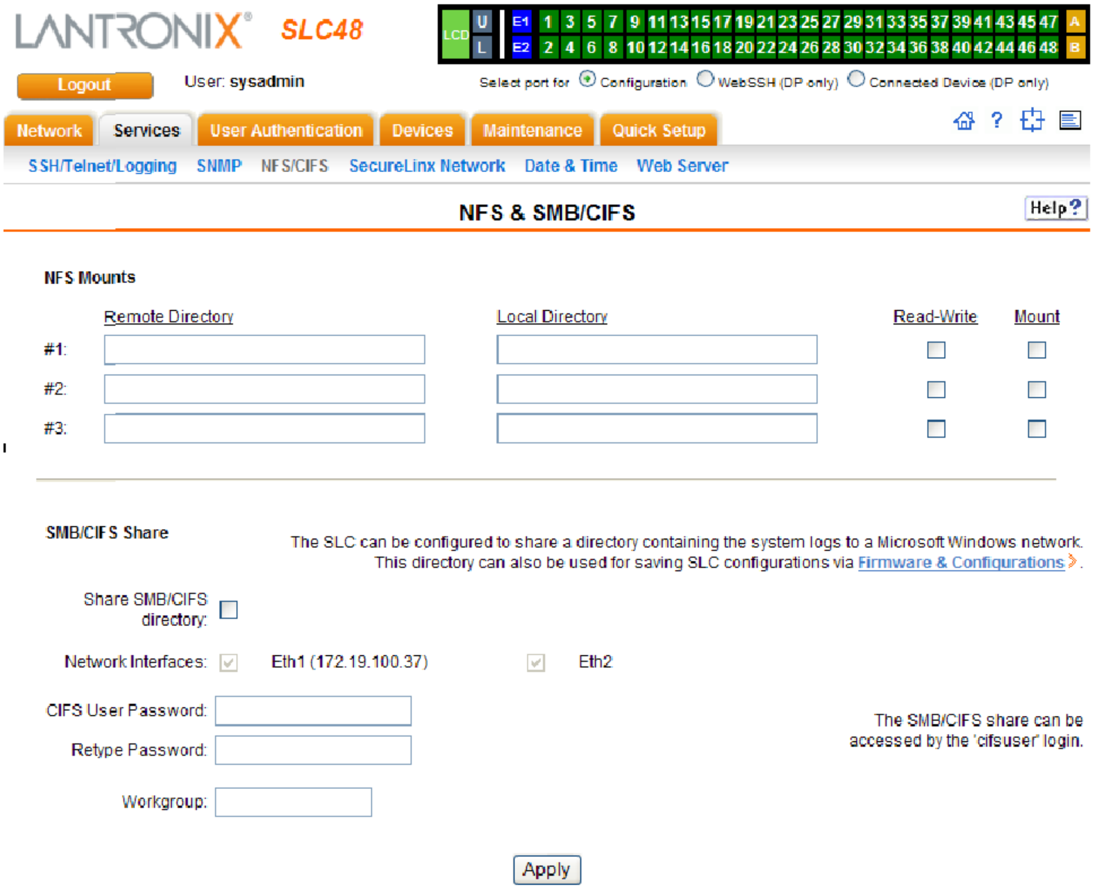
- Logs directory, which contains the system logs and the device port local buffers (see System Logs on page 183) and is read-only.
- Config directory, which contains saved configurations and is read-write.

The share allows users to access the contents of the directory or map the directory onto a Windows computer. Users can also access the device port local buffers from the CIFS share (see Device Ports – Logging on page 96).

To configure NFS and SMB/CIFS:

1. Click the **Services** tab and the **NFS/CIFS** option. *Figure 7-3* shows the page that displays.

Figure 7-3 NFS and SMB/CIFS Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

NFS & SMB/CIFS

NFS Mounts

	Remote Directory	Local Directory	Read-Write	Mount
#1:			□	□
#2:			□	□
#3:			□	□

SMB/CIFS Share

The SLC can be configured to share a directory containing the system logs to a Microsoft Windows network. This directory can also be used for saving SLC configurations via Firmware & Configurations.

Share SMB/CIFS directory: □

Network Interfaces: ☑ Eth1 (172.19.100.37) ☑ Eth2

CIFS User Password:

Retype Password:

Workgroup:

The SMB/CIFS share can be accessed by the 'cifsuser' login.

2. Enter the following fields.

NFS Mounts

Remote Directory	The remote NFS share directory in the format: **nfs_server_hostname** or **ipaddr:/exported/path**
Local Directory	The local directory on the SLC console manager on which to mount the remote directory. The SLC device creates the local directory automatically.

Read-Write	If enabled, indicates that the SLC console manager can write files to the remote directory. If you plan to log port data or save configurations to this directory, you must enable this option.
Mount	Select the checkbox to enable the SLC device to mount the file to the NFS server. Disabled by default.

SMB/CIFS Share

Share SMB/CIFS directory	Select the checkbox to enable the SLC console manager to export an SMB/CIFS share called “public.” Disabled by default.
Network Interfaces	Select the network ports from which the share can be seen. The default is for the share to be visible on Eth1 and Eth2.
CIFS User Password/Retype Password	Only one user special username (cifsuser) can access the CIFS share. Enter the CIFS user password in both password fields. The default user password is **CIFSPASS**. More than one user can access the share with the **cifsuser** user name and password at the same time.
Workgroup	The Windows workgroup to which the SLC console manager belongs. Every PC exporting a CIFS share must belong to a workgroup. Can have up to 15 characters.

3. Click the **Apply** button.

NFS and SMB/CIFS Commands

The following CLI commands correspond to the NFS & SMB/CIFS page. For more information, see *15: Command Reference*.

- *set nfs mount (on page 243)*
- *set nfs unmount (on page 243)*
- *set cifs (on page 242)*
- *set cifs password (on page 243)*
- *show cifs (on page 243)*
- *show nfs (on page 243)*

Secure Lantronix Network

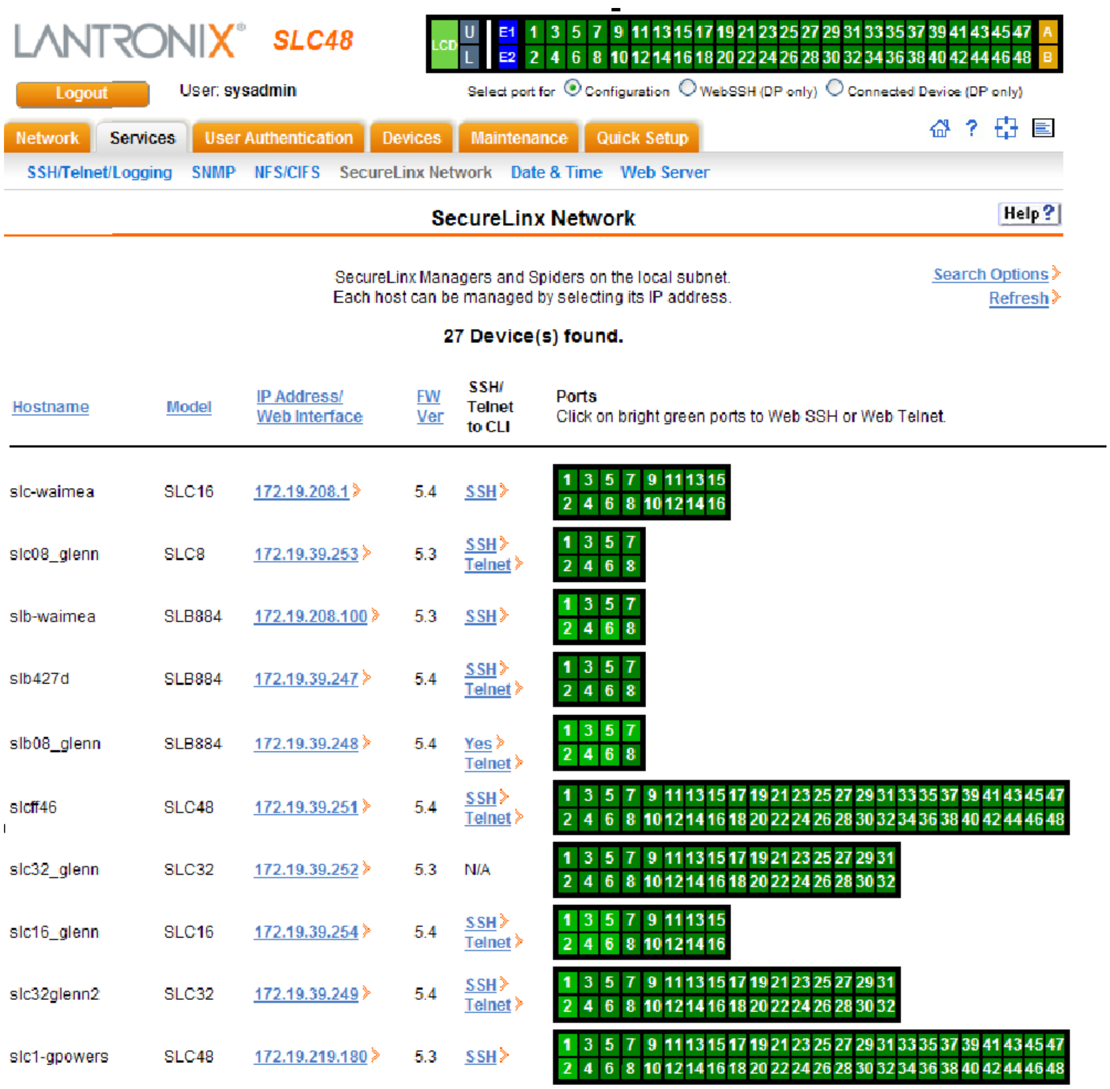
Use the Secure Lantronix Network option to view and manage SLC Console Managers and Lantronix® Spider™ devices on the local subnet.

Note: *Status and statistics shown on the web interface represent a snapshot in time. To see the most recent data, reload the web page.*

To view and manage SLC console managers and Spider devices on the local network:

1. Click the **Services** tab and click the **Secure Lantronix Network** option. *Figure 7-4* shows the page that displays.

Figure 7-4 Secure Lantronix Network Page with Local Subnet Addressing


LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
User: sysadmin
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network Services User Authentication Devices Maintenance Quick Setup
SSH/Telnet/Logging SNMP NFS/CIFS SecureLinx Network Date & Time Web Server
Help ?
Search Options
Refresh

SecureLinx Network

SecureLinx Managers and Spiders on the local subnet.
Each host can be managed by selecting its IP address.

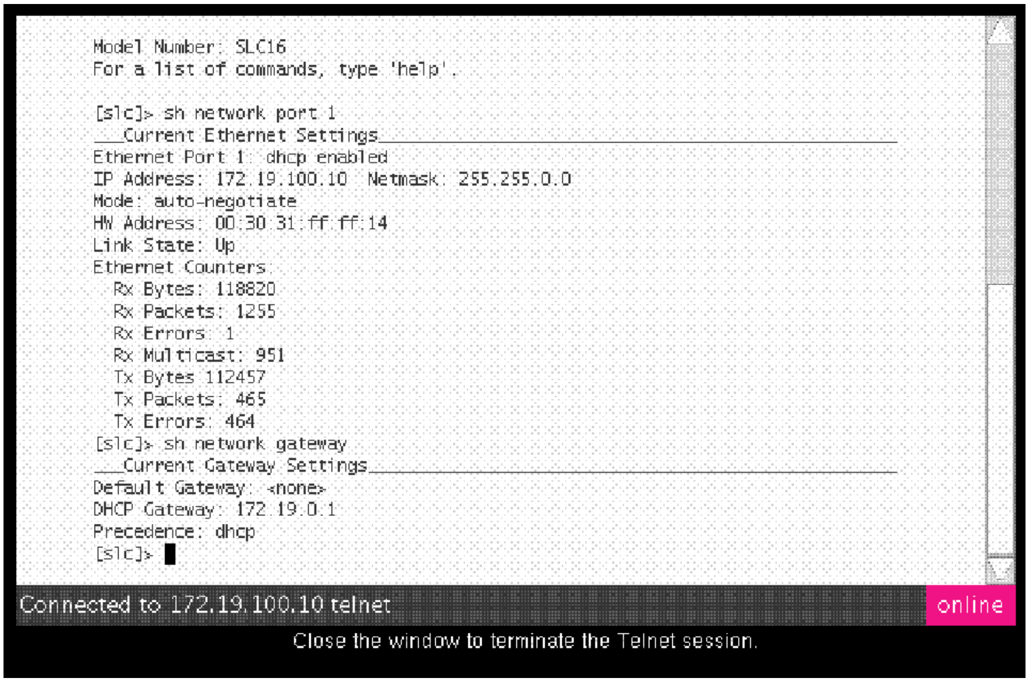
27 Device(s) found.

Hostname	Model	IP Address/ Web Interface	FW Ver	SSH/ Telnet to CLI	Ports Click on bright green ports to Web SSH or Web Telnet.
slc-waimea	SLC16	172.19.208.1	5.4	SSH	1 3 5 7 9 11 13 15 2 4 6 8 10 12 14 16
slc08_glenn	SLC8	172.19.39.253	5.3	SSH Telnet	1 3 5 7 2 4 6 8
slb-waimea	SLB884	172.19.208.100	5.3	SSH	1 3 5 7 2 4 6 8
slb427d	SLB884	172.19.39.247	5.4	SSH Telnet	1 3 5 7 2 4 6 8
slb08_glenn	SLB884	172.19.39.248	5.4	Yes Telnet	1 3 5 7 2 4 6 8
slcff46	SLC48	172.19.39.251	5.4	SSH Telnet	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
slc32_glenn	SLC32	172.19.39.252	5.3	N/A	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32
slc16_glenn	SLC16	172.19.39.254	5.4	SSH Telnet	1 3 5 7 9 11 13 15 2 4 6 8 10 12 14 16
slc32glenn2	SLC32	172.19.39.249	5.4	SSH Telnet	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32
slc1-gpowers	SLC48	172.19.219.180	5.3	SSH	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48

2. Click a device **IP Address** in the column labeled **IP Address/Web Interface**. A separate browser opens at the device **Home** page after you have logged in. In the separate browser page, you can manage the device.

3. To access a device port via SSH or Telnet, click on the bright green device ports in the Ports column. SSH/Telnet access to the CLI or a device port requires that Web SSH or Web Telnet is enabled. *Figure 7-5* shows the Telnet window that displays.

Figure 7-5 Telnet Session



```
Model Number: SLC16
For a list of commands, type 'help'.

[slc]> sh network port 1
___Current Ethernet Settings______________________________________________
Ethernet Port 1: dhcp enabled
IP Address: 172.19.100.10  Netmask: 255.255.0.0
Mode: auto-negotiate
HW Address: 00:30:31:ff:ff:14
Link State: Up
Ethernet Counters:
  Rx Bytes: 118820
  Rx Packets: 1255
  Rx Errors: 1
  Rx Multicast: 951
  Tx Bytes 112457
  Tx Packets: 465
  Tx Errors: 464
[slc]> sh network gateway
___Current Gateway Settings_______________________________________________
Default Gateway: <none>
DHCP Gateway: 172.19.0.1
Precedence: dhcp
[slc]> █
```

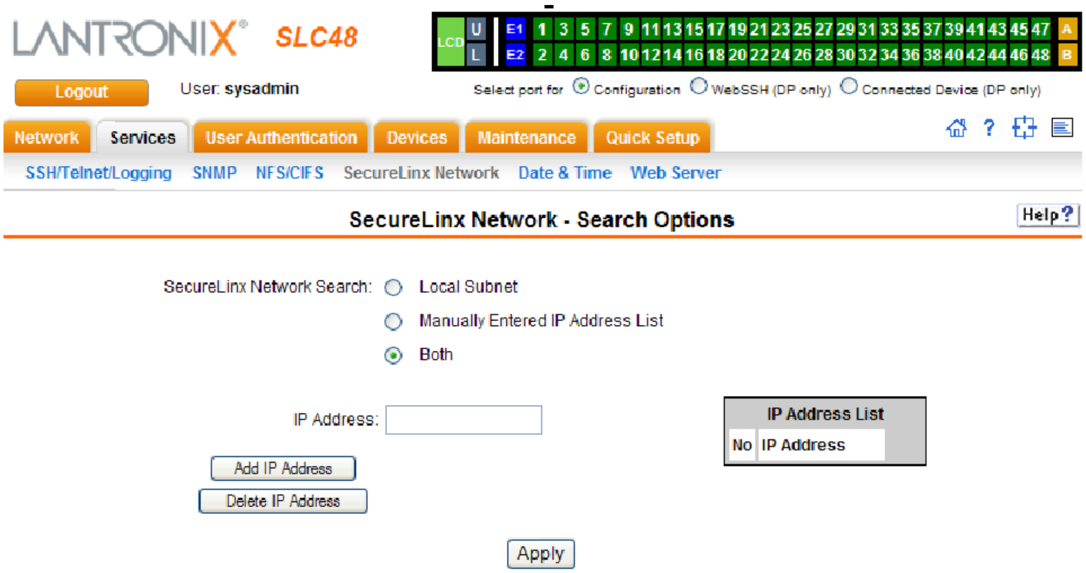
Connected to 172.19.100.10 telnet

Close the window to terminate the Telnet session.

To configure how SLC devices are searched for on the network:

1. Click the **Search Options** link on the top right of the **Secure Lantronix Network** page. *Figure 7-6* shows the page that displays.

Figure 7-6 Secure Lantronix Network - Search Options Page



LANTRONIX® SLC48
LCD U L E1 E2
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network Services User Authentication Devices Maintenance Quick Setup
SSH/Telnet/Logging SNMP NFS/CIFS SecureLinx Network Date & Time Web Server
Help?

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

SecureLinx Network - Search Options

SecureLinx Network Search: ○ Local Subnet

○ Manually Entered IP Address List

● Both

IP Address:

IP Address List	
No	IP Address

Add IP Address
Delete IP Address
Apply

2. Enter the following fields.

Secure Lantronix Network Search	Select the type of search you want to conduct. **Local Subnet:** Performs a broadcast to detect SLC devices on the local subnet. **Manually Entered IP Address List:** Provides a list of IP addresses that may not respond to a broadcast because of how the network is configured. The default is **Both**.
IP Address	If you selected **Manually Entered IP Address List** or **Both**, enter the IP address of the SLC device you want to find and manage.

3. If you entered an IP address, click the **Add IP Address** button. The IP address displays in the IP Address List.
4. Repeat steps 2 and 3 for each IP address you want to add.
5. To delete an IP address from the IP Address List, select the address and click the **Delete IP Address** button.
6. Click the **Apply** button. When the confirmation message displays, click **Secure Lantronix Network** on the main menu. The Secure Lantronix Network page displays the SLC devices resulting from the search. You can now manage these devices.

Secure Lantronix Network Commands

The following CLI commands correspond to the **Secure Lantronix Network** page. For more information, see *15: Command Reference*.

- *set slcnetwork (on page 254)*
- *show slcnetwork (on page 254)*

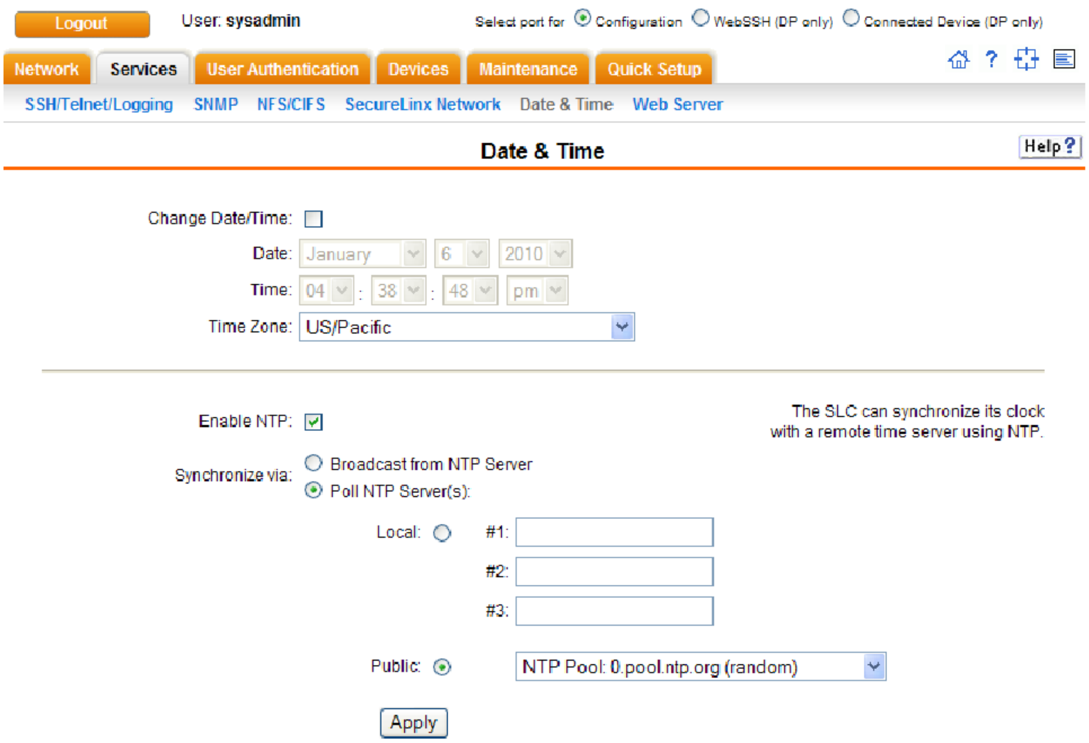
Date and Time

You can specify the current date, time, and time zone at the SLC location (default), or specify NTP to synchronize with other NTP devices on your network.

To set the local date, time, and time zone or enable NTP:

1. From the main menu, select **Date & Time**. *Figure 7-7* shows the page that displays.

Figure 7-7 Date & Time Page



Change Date/Time: □

Date: January 6 2010

Time: 04 : 38 : 48 pm

Time Zone: US/Pacific

Enable NTP: ☑

The SLC can synchronize its clock with a remote time server using NTP.

Synchronize via: ○ Broadcast from NTP Server ● Poll NTP Server(s):

Local: ○ #1: #2: #3:

Public: ● NTP Pool: 0.pool.ntp.org (random)

Apply

1. Enter the following fields.

Change Date/ Time	Select the checkbox to manually enter the date and time at the SLC location.
Date	Select the current month, day, and year from the drop-down lists.
Time	Select the current hour and minute from the drop-down lists.
Time Zone	Select the appropriate time zone.From the drop-down list.
Enable NTP	Click the checkbox to enable NTP synchronization. NTP is disabled by default.
Synchronize via	Select one of the following: ◆ **Broadcast from NTP Server:** Enables the SLC console manager to accept time information periodically transmitted by the NTP server. This is the default if you enable NTP. ◆ **Poll NTP Server:** Enables the SLC device to query the NTP Server for the correct time. If you select this option, complete one of the following: ◆ **Local:** Select this option if the NTP servers are on a local network, and enter the IP address of up to three NTP servers. This is the default, and it is highly recommended. ◆ **Public:** Select this option if you want to use a public NTP server, and select the address of the NTP server from the drop-down list. This is not recommended because of the high load on many public NTP servers. All servers in the drop-down list are stratum-2 servers. (See www.ntp.org for more information.) Each public NTP server has its own usage rules --please refer to the appropriate web site before using one. Our listing them here is to provide easy configuration but does not indicate any permission for use.

2. Click the **Apply** button.

Date and Time Commands

The following CLI commands correspond to the **Date & Time** page. For more information, see *15: Command Reference*.

- *set datetime (on page 221)*
- *set ntp (on page 221)*
- *show ntp (on page 222)*

Web Server

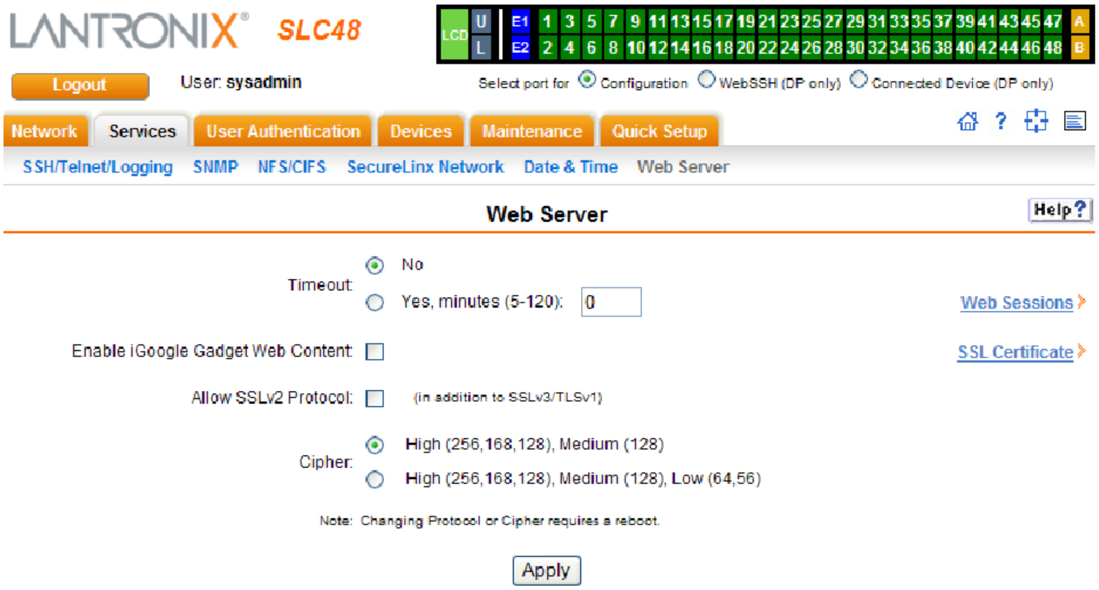
The Web Server page allows the system administrator to:

- Configure attributes of the web server.
- View and terminate current web sessions.
- Import a site-specific SSL certificate.
- Enable an iGoogle gadget that displays the status of ports on multiple SLC console managers.

To configure web server settings:

1. Click the Services tab and the Web Server option. *Figure 7-8* shows the page that displays.

Figure 7-8 Web Server Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Web Server

Timeout: ● No ○ Yes, minutes (5-120): 0

Enable iGoogle Gadget Web Content: □

Allow SSLv2 Protocol: □ (in addition to SSLv3/TLSv1)

Cipher: ● High (256,168,128), Medium (128) ○ High (256,168,128), Medium (128), Low (64,56)

Note: Changing Protocol or Cipher requires a reboot.

2. Enter the following fields.

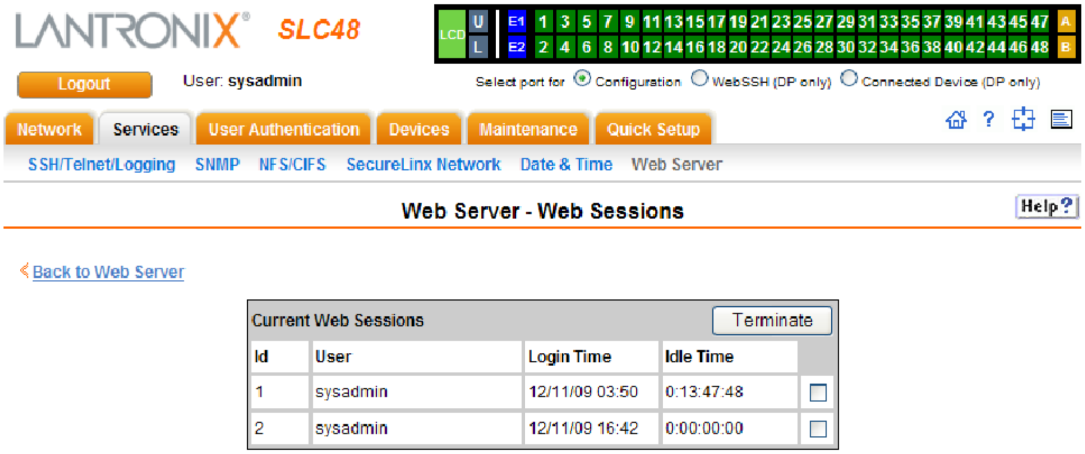
Timeout	Select the number of minutes (5-120) after which the SLC web session times out. The default is **5**. To avoid timeouts, select **No**. If the session times out, refresh the browser page and enter your user ID and password to open another web session. ***Note:*** *If you close the browser without logging off the SLC console manager first, you will have to wait for the timeout time to expire. You can also end a web session by using the admin web terminate command at the CLI or by asking your system administrator to terminate your active web session.*
Enable iGoogle Gadget Web Content	Click the check box to enable an SLC iGoogle gadget. The iGoogle gadget allows an iGoogle user to view the port status of many SLC console managers on one web page. See Google Gadgets on page 77 for more information regarding the XML code.
Allow SSLv2 Protocol	Click the checkbox to support SSLv2 protocol. By default, the web supports the SSLv3/ TLSv1 protocol. Changing this option requires a reboot for the change to take effect.
Cipher	Click one of the radio buttons to configure the web to support low security (less than 128 bits) or High/Medium security (128 bits or higher) for the cipher. By default, the web uses High/Medium. Changing this option requires a reboot for the change to take effect.

3. Click the **Apply** button.

To view or terminate web sessions:

1. Click the Web Sessions link. *Figure 7-9* shows the page that displays.

Figure 7-9 Web Server - Web Sessions Page


LANTRONIX
SLC48
LCD U L E1 E2
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
User: sysadmin
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network
Services
User Authentication
Devices
Maintenance
Quick Setup
SSH/Telnet/Logging
SNMP
NFS/CIFS
SecureLinx Network
Date & Time
Web Server
Help?
Back to Web Server
Terminate

Web Server - Web Sessions

Current Web Sessions

Id	User	Login Time	Idle Time	
1	sysadmin	12/11/09 03:50	0:13:47:48	□
2	sysadmin	12/11/09 16:42	0:00:00:00	□

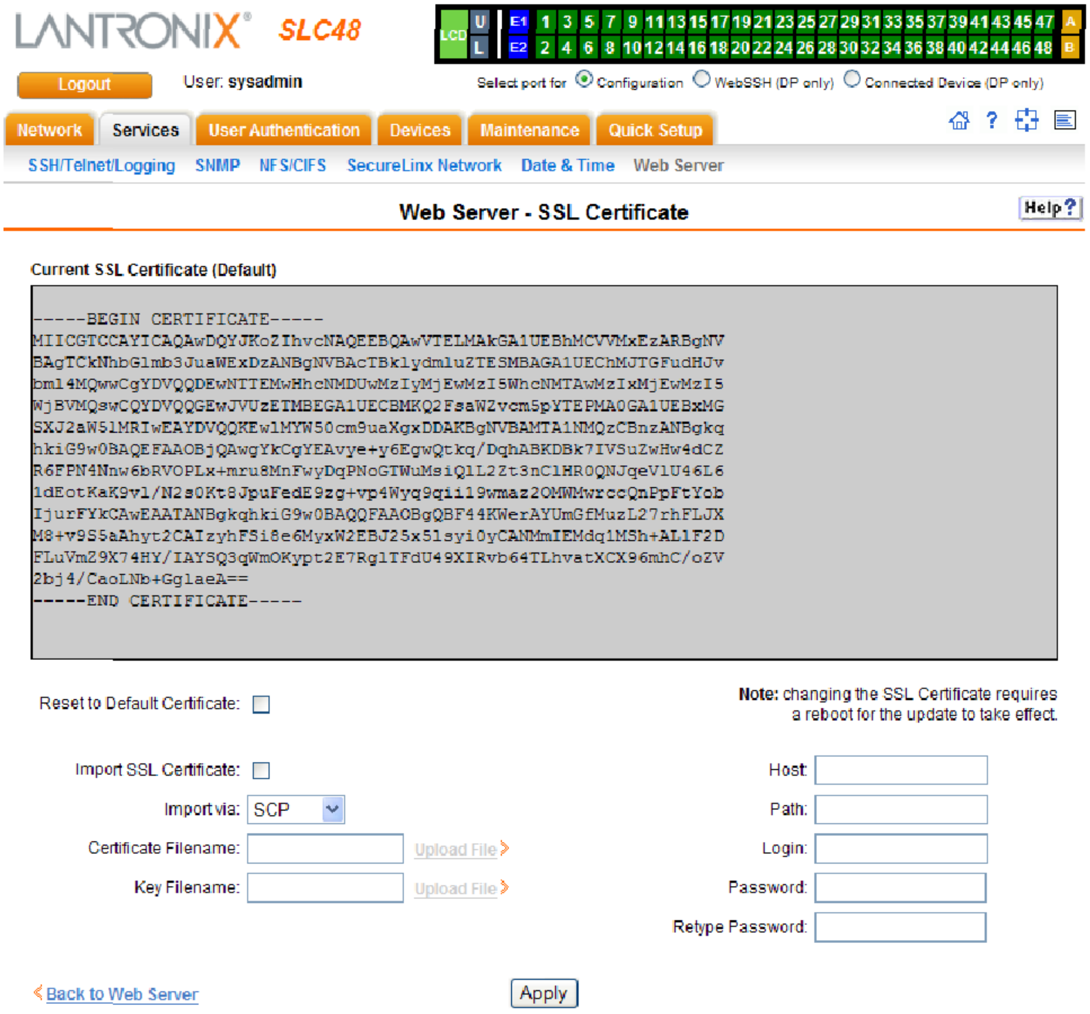
2. To terminate, click the check box in the row of the session you want to terminate.

3. To return to the Web Server page, click the link.

To view import, or reset the SSL Certificate:

1. Click the SSL Certificate link. *Figure 7-10* shows the page that displays.

Figure 7-10 Web Server - SSL Certificate Page


LANTRONIX
SLC48
LCD U L E1 E2
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
User: sysadmin
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network
Services
User Authentication
Devices
Maintenance
Quick Setup
SSH/Telnet/Logging
SNMP
NFS/CIFS
SecureLinx Network
Date & Time
Web Server
Help?

Web Server - SSL Certificate

Current SSL Certificate (Default)

```
-----BEGIN CERTIFICATE-----
MIICGTCCAYICAQAwDQYJKoZIhvcNAQEEBQAwVTELMAkGA1UEBhMCVVMxEzARBgNV
BAgTCkNhbGlmb3JuaWExDzANBgNVBAcTBklydmluZTESMBAGA1UEChMJTGFudHJv
bml4MQwwCgYDVQQDEwNTTEMwHhcNMDUwMzIyMjEwMzI5WhcNMTAwMzIxMjEwMzI5
WjBVMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEPMA0GA1UEBxMG
SXJ2aW5lMRIwEAYDVQQKEwlMYW50cm9uaXgxDDAKBgNVBAMTA1NMQzCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAvye+y6EgwQtkq/DqhABKDBk7IVSuZwHw4dCZ
R6FPN4Nnw6bRVOPLx+mru8MnFwyDqPNoGTWuMsiQ1L2Zt3nC1HR0QNJqeV1U46L6
1dEotKaK9vl/N2s0Kt8JpuFedE9zg+vp4Wyq9qii19wmaz2OMWMwrccQnPpFtYob
IjurFYkCAwEAATANBgkqhkiG9w0BAQQFAAOBgQBF44KWerAYUmGfMuzL27rhFLJX
M8+v9S5aAhyt2CAIzyhFSi8e6MyxW2EBJ25x51syi0yCANMmIEMdq1MSh+AL1F2D
FLuVmZ9X74HY/IAYSQ3qWmOKypt2E7Rg1TFdU49XIRvb64TLhvatXCX96mhC/oZV
2bj4/CaoLNb+GglaeA==
-----END CERTIFICATE-----
```

Reset to Default Certificate: □

Note: changing the SSL Certificate requires a reboot for the update to take effect.

Import SSL Certificate: □

Import via: SCP

Certificate Filename: Upload File

Key Filename: Upload File

Host:

Path:

Login:

Password:

Retype Password:

Back to Web Server

Apply

2. Enter the following fields.

Reset to Default Certificate	To reset to the default certificate, select the checkbox to reset to the default certificate. Unselected by default.
Import SSL Certificate	To import your own SSL Certificate, select the checkbox. Unselected by default.
Import via	Select the SCP, SFTP, or HTTPS method from the drop-down list. The default is **SCP.**
Certificate Filename	Assign a certificate filename. If HTTPS is selected as the import method, the **Upload File** link is selectable to upload a certificate file.
Key Filename	Assign a certificate filename that uses a private key. If HTTPS is selected as the import method, the **Upload File** link is selectable to upload a key file.
Host	Assign the host name or IP address of the host from which to import the file.
Path	Assign the directory path where the certificate will be stored.
Login	Assign the user ID to use to SCP or SFTP the file.

Password & Retype Password	Password to use to SCP or SFTP the file.

3. Click the **Apply** button.
4. Reboot the SLC console manager for the update to take effect.
5. Click the **Back to Web Server** link to return to the **Web Server** page.

Web Server Commands

The following CLI commands correspond to the **Web Server** page. For more information, see *15: Command Reference*.

- *admin web certificate (on page 212)*
- *admin web certificate reset (on page 212)*
- *admin web cipher (on page 212)*
- *admin web gadget (on page 212)*
- *admin web protocol (on page 213)*
- *admin web timeout (on page 213)*
- *admin web terminate (on page 213)*
- *admin web show (on page 213)*

Google Gadgets

You can create iGoogle gadgets that enable viewing port status of many SLC console managers on one web page. Anyone with a Google email account (gmail.com) can create an iGoogle gadget.

There are two types of iGoogle gadgets: public and private gadgets. Public gadgets are those that are submitted to Google, becoming a part of the iGoogle public gadgets, and listed for import on iGoogle web pages. Private gadgets are stored on a private server, stay private, and are usable only by users who have the server address.

To set up an SLC iGoogle gadget:

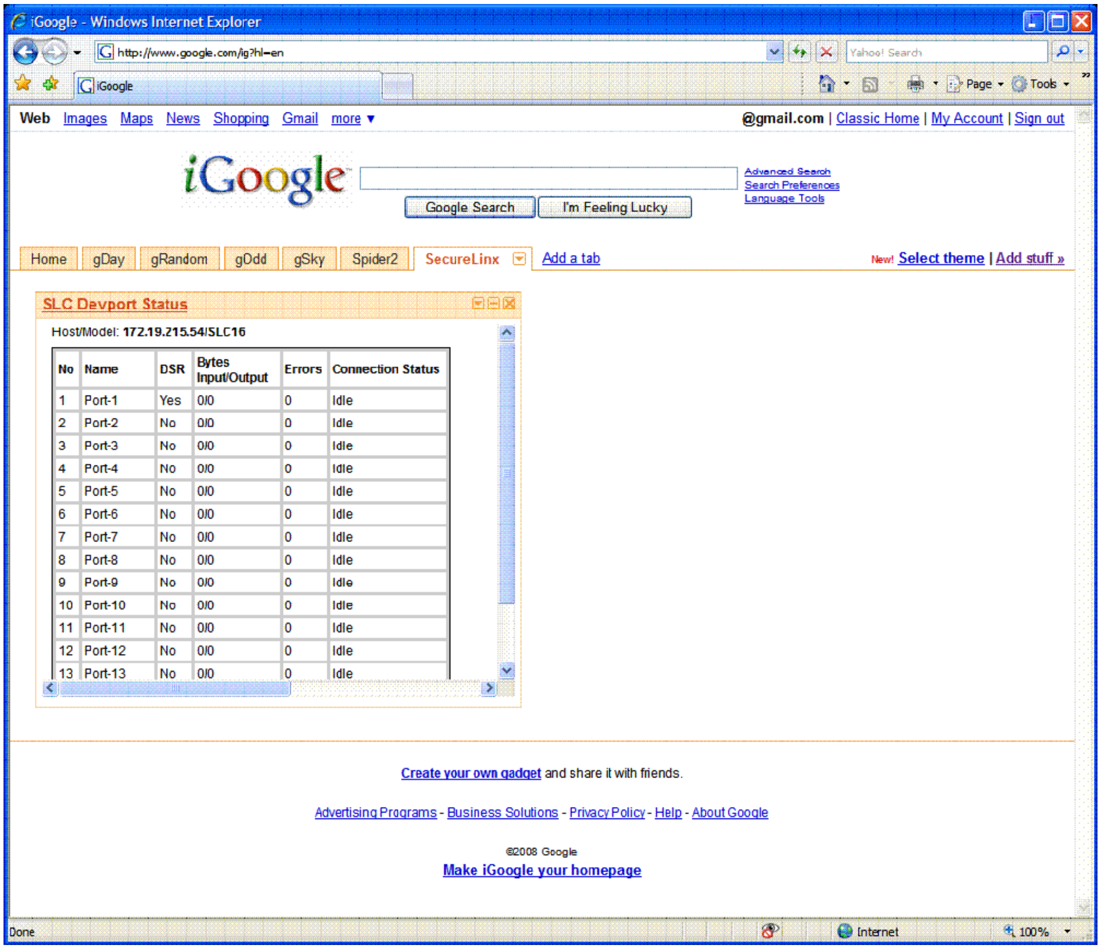
1. Load the following XML code on a web server that is accessible over the Internet. This code describes how to retrieve information and how to format the data for display.

```
<?xml version=”1.0” encoding=”UTF-8”?>
- <Module>
  <ModulePrefs title=”__UP_model__ Devport Status” title_url=”http://
www.lantronix.com” directory_title=”SLC/SLB Status”
description=”Devport status and counters” scrolling=”true”
width=”400” height=”360” />
- <UserPref name=”model” display_name=”Model” datatype=”enum”
default_value=”slc”>
  <EnumValue value=”SLC” display_value=”SLC” />
  <EnumValue value=”SLB” display_value=”SLB” />
  </UserPref>
  <UserPref name=”ip” display_name=”IP Address” required=”true” />
```

```
- <UserPref name=”rate” display_name=”Refresh Rate” datatype=”enum” 
default_value=”10”>
  <EnumValue value=”1” display_value=”1 second” />
  <EnumValue value=”5” display_value=”5 seconds” />
  <EnumValue value=”10” display_value=”10 seconds” />
  <EnumValue value=”30” display_value=”30 seconds” />
  <EnumValue value=”60” display_value=”1 minute” />
  <EnumValue value=”300” display_value=”5 minutes” />
  <EnumValue value=”600” display_value=”10 minutes” />
  </UserPref>
  <Content type=”url” href=”http://__UP_ip__/devstatus.htm” />
  </Module>
```

2. On the iGoogle web page, click the **Add stuff** link.
3. On the new page, click the **Add feed or gadget** link.
4. In the field that displays, type the URL of the gadget location.
5. Return to the gadget viewing page and complete the SLC gadget configuration fields. *Figure 7-11* shows the page that displays.

Figure 7-11 iGoogle Gadget Page



SLC Devport Status

Host/Model: 172.19.215.54/SLC16

No	Name	DSR	Bytes Input/Output	Errors	Connection Status
1	Port-1	Yes	0/0	0	Idle
2	Port-2	No	0/0	0	Idle
3	Port-3	No	0/0	0	Idle
4	Port-4	No	0/0	0	Idle
5	Port-5	No	0/0	0	Idle
6	Port-6	No	0/0	0	Idle
7	Port-7	No	0/0	0	Idle
8	Port-8	No	0/0	0	Idle
9	Port-9	No	0/0	0	Idle
10	Port-10	No	0/0	0	Idle
11	Port-11	No	0/0	0	Idle
12	Port-12	No	0/0	0	Idle
13	Port-13	No	0/0	0	Idle

Create your own gadget and share it with friends.

Advertising Programs - Business Solutions - Privacy Policy - Help - About Google

©2008 Google

Make iGoogle your homepage

8: Devices

This chapter describes how to view the device status, configure devices, and use an SLC device port connected to an external device, such as a server or a modem. *Chapter 11: Connections* describes how to use the **Connections** page to connect external devices and outbound network connections (such as Telnet or SSH) in various configurations. The **Console Port** page allows you to configure the console port, if required.

This chapter contains the following sections:

Note: *The features and functionality described in this chapter specific to PC Card use are supported on SLC -02 part numbers. The features and functionality specific to USB port use are supported on SLC -03 part numbers.*

Connection Methods

A user can connect to a device port in one of the following ways:

1. Telnet or SSH to the Eth1 or Eth2 IP address, or connect to the console port and log into the command line interface. At the command line interface, type the `connect direct` or `connect listen` command.
2. If Telnet is enabled for a device port, Telnet to <Eth1 IP address>:< telnet port number> or <Eth2 IP address>:<telnet port number>. The Telnet port number is uniquely assigned for each device port.
3. If SSH is enabled for a device port, SSH to <Eth1 IP address>:<ssh port number> or <Eth2 IP address>:<ssh port number>. The SSH port number is uniquely assigned for each device port.
4. If TCP is enabled for a device port, establish a raw TCP connection to <Eth1 IP address>:<tcp port number> or <Eth2 IP address>:<tcp port number>, where tcp port number is uniquely assigned for each device port.
5. If a device port has an IP address assigned to it, you can Telnet, SSH, or establish a raw TCP connection to the IP address. For Telnet and SSH, use the default TCP port number (23 and 22, respectively) to connect to the device port. For raw TCP, use the TCP port number defined for **TCP In** to the device port. See *Device Ports on page 81*.
6. Connect a terminal or a terminal emulation program directly to the device port. If logins are enabled, the user gets prompted for a username and password and logs into the command line interface.

For #2, #3, #4, #5, and #6, if logins or authentication are *not* enabled, the user is directly connected to the device port with no authentication.

For #1 and #6, if logins are enabled, the user is authenticated first, and then logged into the command line interface. The user login determines permissions for accessing device ports.

Permissions

There are three types of permissions:

- **Direct (or data) mode:** The user can interact with and monitor the device port (`connect direct` command).
- **Listen mode:** The user can only monitor the device port (`connect listen` command).
- **Clear mode:** The user can clear the contents of the device port buffer (`set log <port> clear buffer` command).

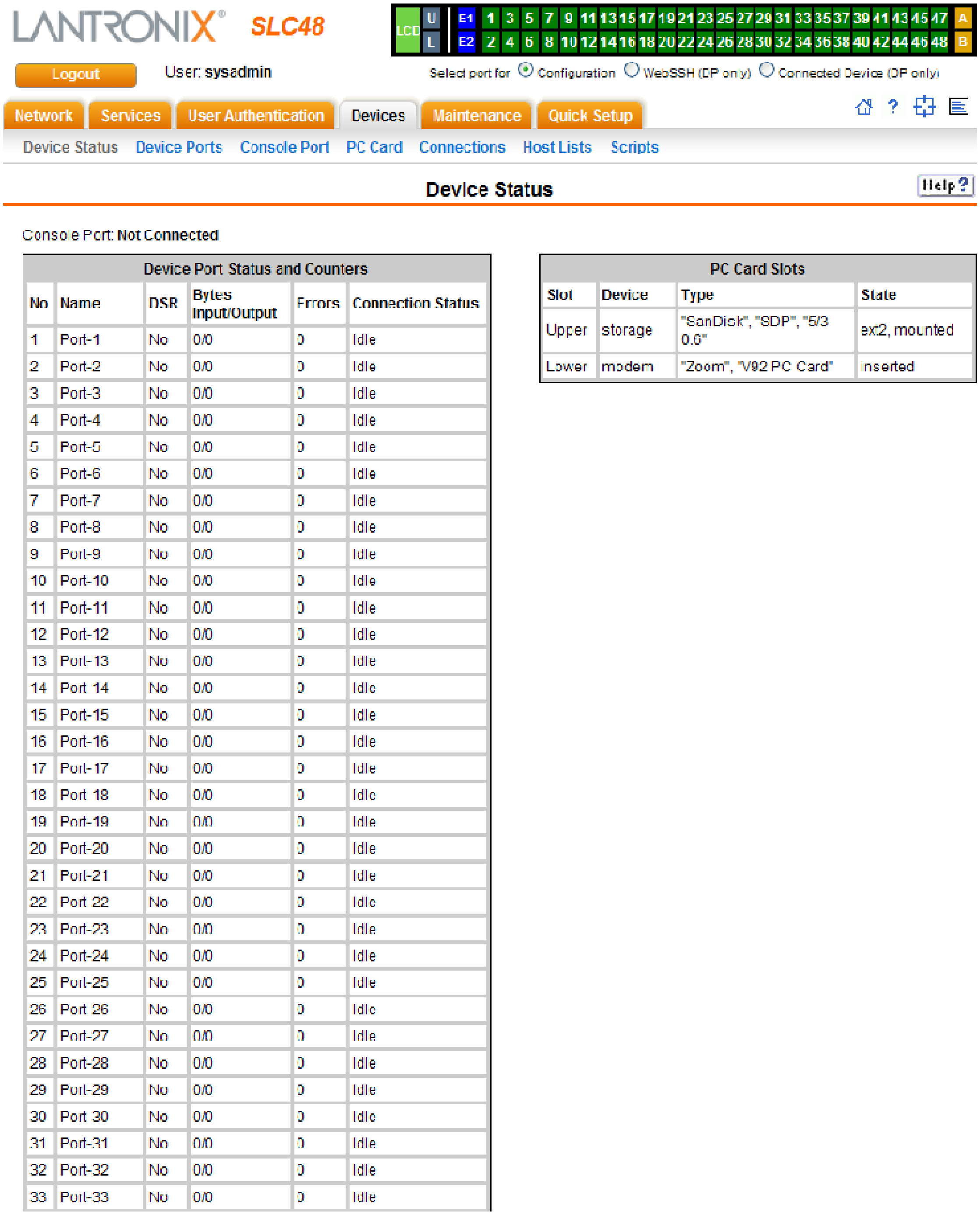
The administrator and users with local user rights may assign individual port permissions to local users. The administrator and users with remote authentication rights assign port access to users authenticated by NIS, RADIUS, LDAP, Kerberos and TACACS+.

Device Status

The **Device Status** page displays the status of SLC ports and PC card slots.

1. Click the **Devices** tab and select the **Device Status** option. *Figure 8-1* shows the page that displays.

Figure 8-1 Device Status Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Device Status

Console Port: Not Connected

Device Port Status and Counters

No	Name	DSR	Bytes Input/Output	Errors	Connection Status
1	Port-1	No	0/0	0	Idle
2	Port-2	No	0/0	0	Idle
3	Port-3	No	0/0	0	Idle
4	Port-4	No	0/0	0	Idle
5	Port-5	No	0/0	0	Idle
6	Port-6	No	0/0	0	Idle
7	Port-7	No	0/0	0	Idle
8	Port-8	No	0/0	0	Idle
9	Port-9	No	0/0	0	Idle
10	Port-10	No	0/0	0	Idle
11	Port-11	No	0/0	0	Idle
12	Port-12	No	0/0	0	Idle
13	Port-13	No	0/0	0	Idle
14	Port-14	No	0/0	0	Idle
15	Port-15	No	0/0	0	Idle
16	Port-16	No	0/0	0	Idle
17	Port-17	No	0/0	0	Idle
18	Port-18	No	0/0	0	Idle
19	Port-19	No	0/0	0	Idle
20	Port-20	No	0/0	0	Idle
21	Port-21	No	0/0	0	Idle
22	Port-22	No	0/0	0	Idle
23	Port-23	No	0/0	0	Idle
24	Port-24	No	0/0	0	Idle
25	Port-25	No	0/0	0	Idle
26	Port-26	No	0/0	0	Idle
27	Port-27	No	0/0	0	Idle
28	Port-28	No	0/0	0	Idle
29	Port-29	No	0/0	0	Idle
30	Port-30	No	0/0	0	Idle
31	Port-31	No	0/0	0	Idle
32	Port-32	No	0/0	0	Idle
33	Port-33	No	0/0	0	Idle

PC Card Slots

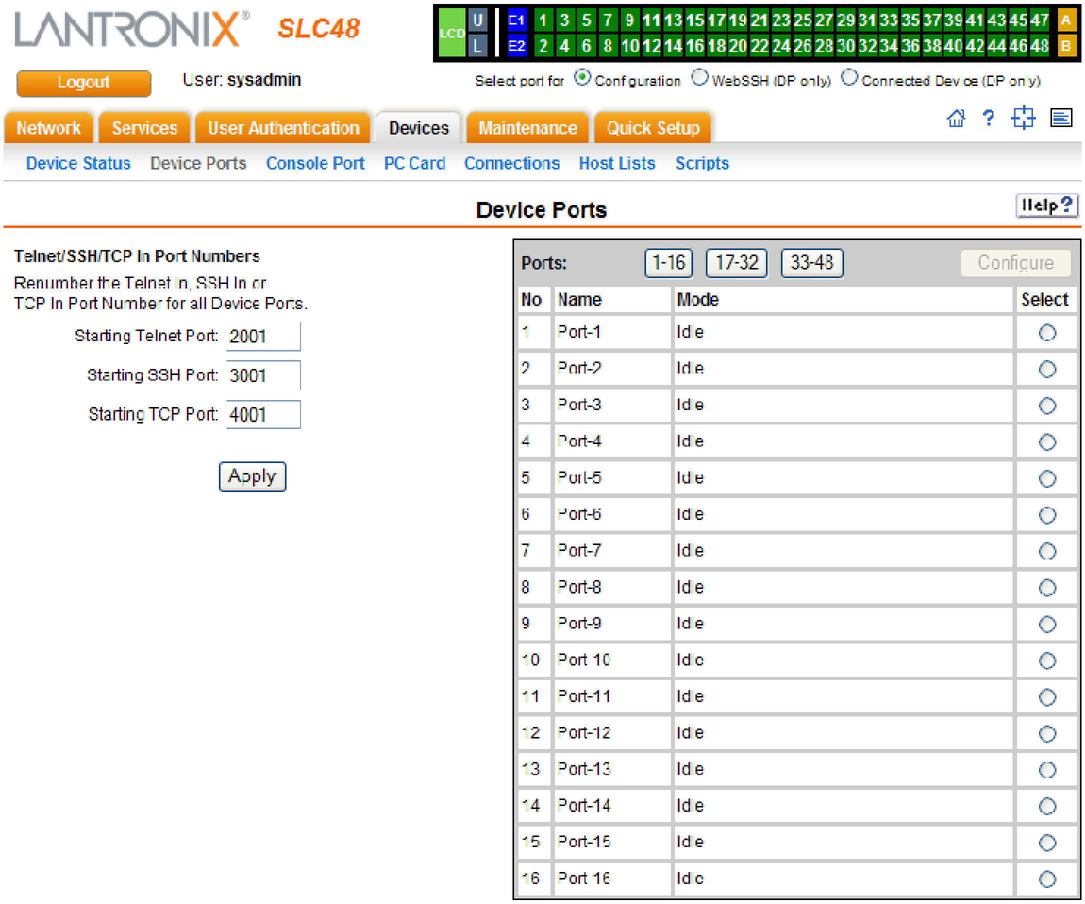
Slot	Device	Type	State
Upper	storage	"SanDisk", "SDP", "5/3 0.6"	ext2, mounted
Lower	modem	"Zoom", "V92 PC Card"	inserted

Device Ports

On the **Device Ports** page, you can set up the numbering of Telnet, SSH, and TCP ports, view current port modes, and select individual ports to configure.

1. Click the **Devices** tab and select the **Device Ports** option. *Figure 8-2* shows the page that displays.

Figure 8-2 Device Ports Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Device Ports

Telnet/SSH/TCP In Port Numbers

Renumber the Telnet In, SSH In or TCP In Port Number for all Device Ports.

Starting Telnet Port: 2001

Starting SSH Port: 3001

Starting TCP Port: 4001

Ports:

No	Name	Mode	Select
1	Port-1	Idle	○
2	Port-2	Idle	○
3	Port-3	Idle	○
4	Port-4	Idle	○
5	Port-5	Idle	○
6	Port-6	Idle	○
7	Port-7	Idle	○
8	Port-8	Idle	○
9	Port-9	Idle	○
10	Port-10	Idle	○
11	Port-11	Idle	○
12	Port-12	Idle	○
13	Port-13	Idle	○
14	Port-14	Idle	○
15	Port-15	Idle	○
16	Port-16	Idle	○

Starting port numbers for Telnet, SSH, and TCP display on the left. The list of ports on the right includes the individual ports and the current mode.

Note: *To view additional ports and depending on the SLC model, click the **17-32** button or the **33-48** button.*

Icons that represent some of the possible modes include the following.

Idle The port is not in use.

The port is in data/text mode.

You may set up ports to allow Telnet access using the IP Settings on the Device Ports – Settings page.

☎ An external modem is connected to the port. The user may dial into or out of the port.

Telnet in or SSH in is enabled for the device port. The device port is either waiting for a Telnet or SSH login or has received a Telnet or SSH login (a user has logged in).

To set up Telnet, SSH, and TCP port numbers:

1. Enter the following fields.

Starting Telnet Port	Assign a starting port number for connecting via Telnet. Enter a number between 1025 and 65535 that represents the first port. The default is 2000 plus the port number. For example, if you enter 2001, subsequent ports are automatically assigned numbers 2002, 2003, and so on.
Starting SSH Port	Assign a starting Each port connecting via SSH. Enter a number between 1025 and 65535 that represents the first port. The default is 3000 plus the port number. For example, if you enter 3001, subsequent ports are automatically assigned numbers 3002, 3003, and so on.
Starting TCP Port	Assign a starting port for connecting through a raw TCP connection. Enter a number between 1025 and 65535 that represents the first port. The default is 4000 plus the port number. For example, if you enter 4001, subsequent ports are automatically numbered 4002, 4003, and so on. You can use a raw TCP connection in which a TCP/IP connection communicates with a serial device. For example, you can connect a serial printer to a device port and use a raw TCP connection to spool print jobs to the printer over the network. ***Note:*** *When using raw TCP connections to transmit binary data, or when the break command (escape sequence) is not required, set the* ***Break Sequence*** *of the device port to null (clear it).*

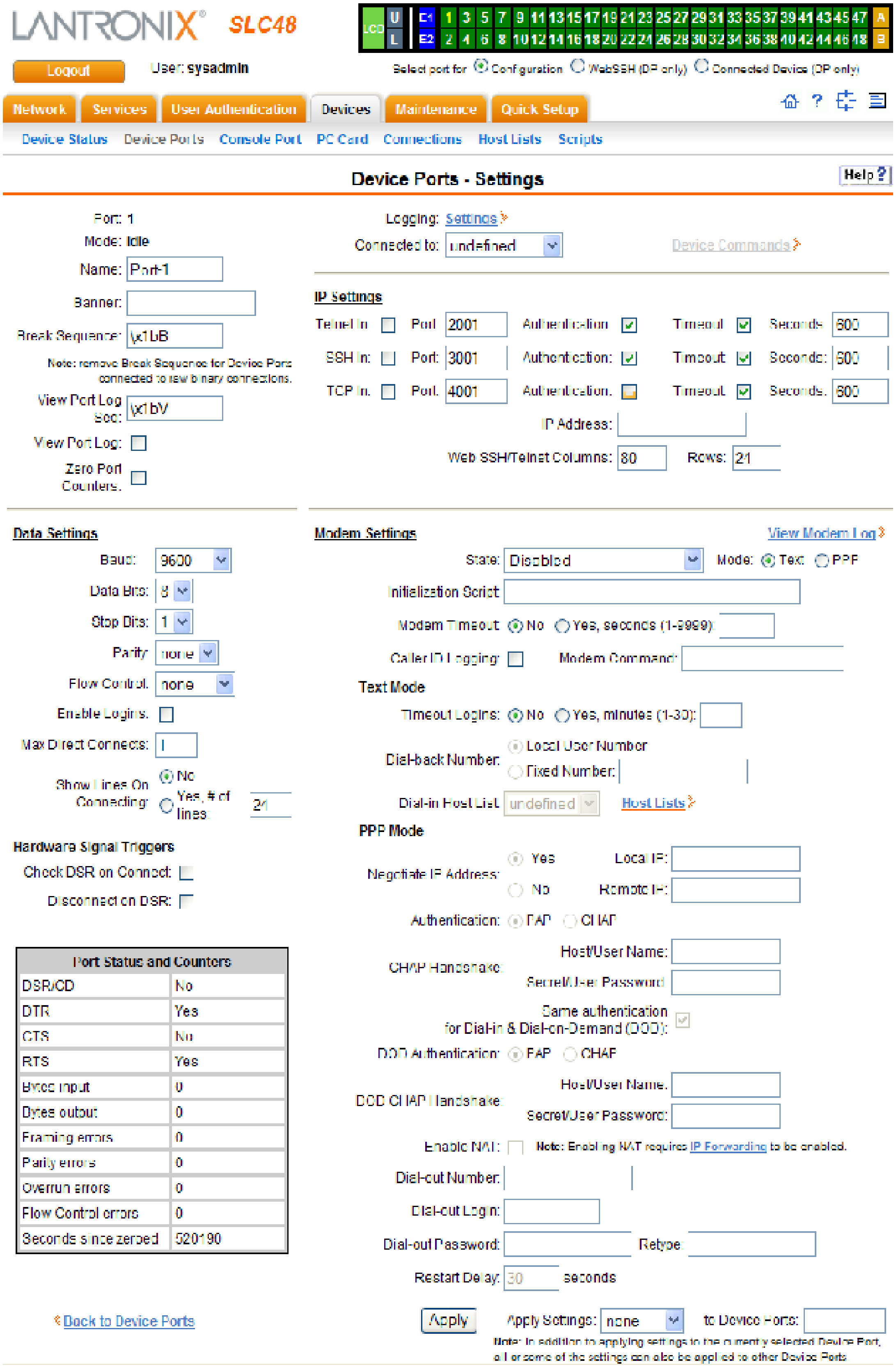
Caution: ***Ports 1-1024 are RFC-assigned and may conflict with services running on the SLC console manager. Avoid this range.***

2. Click the **Apply** button.

To configure a specific port:

1. Select the port from the ports list and click the **Configure** button. *Figure 8-3* shows the page that displays.

Figure 8-3 Device Ports - Settings Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Device Ports - Settings

Port: 1

Mode: Idle

Name: Port-1

Banner:

Break Sequence: \x1bB

Note: remove Break Sequence for Device Ports connected to raw binary connections.

View Port Log Seq: \x1bV

View Port Log: □

Zero Port Counters: □

Logging: Settings

Connected to: undefined

Device Commands

IP Settings

Telnet In: □ Port: 2001 Authentication: ☑ Timeout: ☑ Seconds: 600

SSH In: □ Port: 3001 Authentication: ☑ Timeout: ☑ Seconds: 600

TCP In: □ Port: 4001 Authentication: □ Timeout: ☑ Seconds: 600

IP Address:

Web SSH/Telnet Columns: 80 Rows: 24

Data Settings

Baud: 9600

Data Bits: 8

Stop Bits: 1

Parity: none

Flow Control: none

Enable Logins: □

Max Direct Connects: 1

Show Lines On Connecting: ● No ○ Yes, # of lines: 24

Hardware Signal Triggers

Check DSR on Connect: □

Disconnect on DSR: □

Port Status and Counters	
DSR/CD	No
DTR	Yes
CTS	No
RTS	Yes
Bytes input	0
Bytes output	0
Framing errors	0
Parity errors	0
Overrun errors	0
Flow Control errors	0
Seconds since zeroed	520190

Modem Settings

View Modem Log

State: Disabled Mode: ● Text ○ PPP

Initialization Script:

Modem Timeout: ● No ○ Yes, seconds (1-9999):

Caller ID Logging: □ Modem Command:

Text Mode

Timeout Logins: ● No ○ Yes, minutes (1-30):

Dial-back Number: ● Local User Number ○ Fixed Number:

Dial-in Host List: undefined Host Lists

PPP Mode

Negotiate IP Address: ● Yes ○ No Local IP: Remote IP:

Authentication: ● PAP ○ CHAP

CHAP Handshake Host/User Name: Secret/User Password:

Same authentication for Dial-in & Dial-on-Demand (DOD): ☑

DOD Authentication: ● PAP ○ CHAP

DOD CHAP Handshake Host/User Name: Secret/User Password:

Enable NAT: □ Note: Enabling NAT requires IP Forwarding to be enabled.

Dial-out Number:

Dial-out Login:

Dial-out Password: Retype:

Restart Delay: 30 seconds

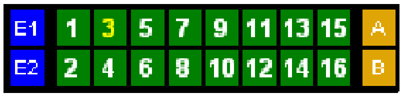
Back to Device Ports

Apply Apply Settings: none to Device Ports:

Note: In addition to applying settings to the currently selected Device Port, all or some of the settings can also be applied to other Device Ports.

OR

- Click the port number on the green bar at the top of each page (shown here). The same page displays as in *Figure 8-3*.



To enter device port settings:

1. Enter the following fields.

Port (view only)	Displays the port number.
Mode (view only)	Displays the port status automatically.
Name	Assign the port name. Valid characters are letters, numbers, dashes (-), periods, and underscores (_).
Banner	Input the text to display when a user connects to a device port by means of Telnet, SSH, or TCP. If authentication is enabled for the device port, the banner displays once the user successfully logs in. Blank is the default.
Break Sequence	Enter a series of one to ten characters that users can enter on the command line interface to send a break signal to the external device. A suggested value is **Esc+B** (escape key, then uppercase “B” performed quickly but not simultaneously). You would specify this value as **\x1bB**, which is hexadecimal **(\x)** character 27 (**1B**) followed by a **B**.
View Port Log Seq	Enter the key sequence used to view the Port Log while in Connect Direct mode. Non-printing characters can be specified by giving their hexadecimal code (see **Break Sequence** above). The default is **Esc+V**.
View Port Log	Select to allow the user to enter the View Port Log Sequence to view the Port Log during Connect Direct mode. The default is disabled.
Logging	Click the **Settings** link to configure file logging, email logging, local logging, USB logging, or PC Card logging. (See Device Ports – Logging on page 96.)
Zero Port Counters	Resets all of the numerical values in the Port Counters table at the bottom of the page to zero (0).
Connected to	Select the type of device connected to the device port. The SLC console manager supports the SLP power manager (SLP8 and SLP16) and Sensorsoft devices. If the type of device is not listed, select **undefined**. If you select anything other than **undefined**, click **Device Commands**. The web page displays for the device you selected.

IP Settings

Telnet In	Enables access to this port through Telnet. Disabled by default. ◆ **Port:** Automatically assigned Telnet, SSH, and TCP port numbers. You can override the value. ◆ **Timeout:** To cause an idle Telnet, SSH or TCP connection to disconnect after a specified number of seconds, select the checkbox and enter a value from 1 to 1800 seconds. The default is 600 seconds. ◆ **Authenticate:** If selected, the SLC requires user authentication before granting access to the port. **Authenticate** is selected by default for **Telnet in** and **SSH in,** but not for **TCP in**.
SSH In	Enables access to this port through SSH. Disabled by default. ◆ **Port:** Automatically assigned Telnet, SSH, and TCP port numbers. You can override the value. ◆ **Timeout:** To cause an idle Telnet, SSH or TCP connection to disconnect after a specified number of seconds, select the checkbox and enter a value from 1 to 1800 seconds. The default is 600 seconds. ◆ **Authenticate:** If selected, the SLC requires user authentication before granting access to the port. **Authenticate** is selected by default for **Telnet in** and **SSH in,** but not for **TCP in**.
TCP in	Enables access to this port through a raw TCP connection. Disabled by default. ◆ **Port:** Automatically assigned Telnet, SSH, and TCP port numbers. You can override the value. ◆ **Timeout:** To cause an idle Telnet, SSH or TCP connection to disconnect after a specified number of seconds, select the checkbox and enter a value from 1 to 1800 seconds. The default is 600 seconds ◆ **Authenticate:** If selected, the SLC requires user authentication before granting access to the port. **Authenticate** is selected by default for **Telnet in** and **SSH in,** but not for **TCP in**. ***Note:*** *When using raw TCP connections to transmit binary data, or where the break command (escape sequence) is not required, set the **Break Sequence** of the respective device port to null (clear it).*
IP Address	Enables an IP address used for this device port so a user can Telnet, SSH, or establish a raw TCP connection to this address and connect directly to the device port. For Telnet and SSH, the default TCP port numbers (22 and 23, respectively) are used to connect to the device port. For raw TCP, the TCP port number defined for **TCP In** to the device port is used.
Web SSH/Telnet Columns	Specifies the number of columns in the Web SSH/Telnet applet when this device port is accessed via the applet.
Web SSH/Telnet Rows	Specified the number of rows in the Web SSH/Telnet applet when this device port is accessed via the applet.

Data Settings

Note: *Check the serial device equipment settings and documentation for the proper settings. The device port and the attached serial device must have the same settings.*

Baud	Enables the speed (baud rate) with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate.
Data Bits	Enables the number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is **8** data bits.
Stop Bits	Enables the number of stop bits used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is **1**.
Parity	Select the parity for detecting simple, single-bit errors from the drop-down list. The default is **none**.
Enable Logins	Displays a login prompt and authenticates users for serial devices connected to the device port. Successfully authenticated users are logged into the command line interface. The default is **disabled** and is the correct setting if the device port is the endpoint for a connection.
Flow Control	Enables the method to prevent buffer overflow and loss of data. The available methods include none, xon/xoff (software), and RTS/CTS (hardware). The default is **none**.
Max Direct Connects	Enables the maximum number of simultaneous connections for a device port from 1 to 10. The default is **1**.
Show Lines on Connecting	Enables a number of lines of buffered data when the serial port connects to the SLC console manager. When enabled, the user can use the `connect direct` command using CLI or connect directly to the port using Telnet or SSH. The output is up to 24 lines. For example, an SLC device issues a `connect direct device 1` command to connect port 1 to a Linux server. Then the SLC console manager user gets a directory with the `ls` command exits the connection. When the SLC device user issues another `direct connect device 1`", the output of the `ls` command (or some portion of it) is output again, so the user can know what state the server was left in.

Hardware Signal Triggers

Check DSR on Connect	If this setting is enabled, the device port only establishes a connection if DSR (Data Set Ready) is in an asserted state. DSR should already be in an asserted state, not in transition, when a connection attempt is made. Disabled by default unless dial-in, dial-out, or dial-back is enabled for the device port.
Disconnect on DSR	If a connection to a device port is currently in session, and the DSR signal transitions to a de-asserted state, the connection disconnects immediately. Disabled is the default unless dial-in, dial-out, or dial-back is enabled for the device port.

Modem Settings

Note: *Depending on the **State** and **Mode** you select, different fields are available.*

State	Indicates whether an external modem is attached to the device port. If enabling, set the modem to dial-out, dial-in, dial-back, CBCP server, CBCP client, dial-on-demand, dial in & dial-on-demand, or dial-in/host list. Disabled by default. For more information, see Modem State Parameters on page 277.
Mode	The format in which the data flows back and forth: ◆ **Text:** In this mode, the SLC console manager assumes that the modem will be used for remotely logging into the command line. Text mode can only be used for dialing in or dialing back. Text is the default. ◆ **PPP:** This mode establishes an IP-based link over the modem. PPP connections can be used for dial-out (e.g., the SLC device connects to an external network), dial-in (e.g., the external computer connects to the network that the SLC console manager is part of), dial-back (dial-in followed by dial-out), dial-on-demand, CBCP server or CBCP client.
Initialization Script	Commands sent to configure the modem may have up to 100 characters. Consult your modem's documentation for recommended initialization options. If you do not specify an initialization script, the SLC uses a default initialization string of **AT S7=45 SO=0 L1 V1 X4 &D2 &c1 E1 Q0**. ***Note:*** *We recommend that the modem initialization script always be preceded with **AT** and include **E1 V1 x4 Q0** so that the SLC console manager may properly control the modem.*
Modem Timeout	Timeout for all modem connections. Select **Yes** (default) for the SLC device to terminate the connection if no traffic is received during the configured idle time. Enter a value of from 1 to 9999 seconds. The default is 30 seconds.
Caller ID Logging	Select to enable the SLC console manager to log caller IDs on incoming calls. Disabled by default. ***Note:*** *For the Caller ID **AT** command, refer to the modem user guide.*
Modem Command	Modem **AT** command used to initiate caller ID logging by the modem. ***Note:*** *For the **AT** command, refer to the modem user guide.*
Dial-back Number	Users with dial-back access can dial into the SLC device and enter their login and password (for text mode) or authenticate via PAP or CHAP (for PPP mode). Once the SLC console manager authenticates them, the modem hangs up and dials them back. Select the phone number the modem dials back on -a fixed number or a number associated with their login. If you select **Fixed Number,** enter the number (in the format 2123456789). The dial-back number is also used for CBCP client as the number for a user-defined number. For more information, see Modem State Parameters on page 277.
Dial-back Delay	For dial-back and CBCP Server, the number of seconds between the dial-in and dial-out portions of the dialing sequence.

Modem Settings: Text Mode

Timeout Logins	If you selected **Text** mode, you can enable logins to time out after the connection is inactive for a specified number of minutes. The default is **No**. This setting is only applicable for text mode connections. **PPP** mode connections stay connected until either side drops the connection. Disabled by default.
Dial-in Host List	From the drop-down list, select the desired host list. The host list is a prioritized list of SSH, Telnet, and TCP hosts that are available for establishing outgoing modem connections or for **connect direct** at the CLI. The hosts in the list are cycled through until the SLC device successfully connects to one. To establish and configure host lists, click the **Host Lists** link.

Modem Settings: PPP Mode

Negotiate IP Address	If the SLC console manager and/or the serial device have dynamic IP addresses (e.g., IP addresses assigned by a DHCP server), select Yes. Yes is the default. If the SLC device or the modem have fixed IP addresses, select **No,** and enter the **Local IP** (IP address of the port) and **Remote IP** (IP address of the modem).
Authentication	Enables **PAP** or **CHAP** authentication for modem logins. **PAP** is the default. With PAP, users are authenticated by means of the Local Users and any of the remote authentication methods that are enabled. With CHAP, the CHAP Handshake fields authenticate the user.
CHAP Handshake	The host/username (for UNIX systems) or secret/user password (for Windows systems) used for CHAP authentication. May have up to 128 characters.
Same authentication for Dial-in & Dial-on-Demand (DOD)	Select this option to let incoming connections (dial-in) use the same authentication settings as outgoing connections (dial-on-demand). If this option is not selected, then the dial-on-demand connections take their authentication settings from the DOD parameter settings. If DOD Authentication is PAP, then the DOD CHAP Handshake field is not used.
DOD Authentication	Enables **PAP** or **CHAP** authentication for dial-in & dial-on-demand. **PAP** is the default. With PAP, users are authenticated by means of the Local Users and any of the remote authentication methods that are enabled. With CHAP, the DOD CHAP Handshake fields authenticate the user.
DOD CHAP Handshake	For **DOD Authentication**, enter the host/username for UNIX systems) or secret/user password (for Windows systems) used for CHAP authentication. May have up to 128 characters.
Enable NAT	Select to enable Network Address Translation (NAT) for dial-in and dial-out PPP connections on a per modem (device port, USB port, or PC Card) basis. Users dialing into the SLC console manager access the network connected to Eth1 and/or Eth2. ***Note:*** *IP forwarding must be enabled on the Network - Settings page for NAT to work. See Chapter 6: Basic Parameters.*
Dial-out Number	Phone number for dialing out to a remote system or serial device. May have up to 20 characters. Any format is acceptable.
Dial-out Login	User ID for dialing out to a remote system. May have up to 32 characters.
Dial-out Password and Retype	Password for dialing out to a remote system. May have up to 64 characters.

Restart Delay	The number of seconds after the timeout and before the SLC device attempts another connection. The default is **30** seconds.

2. Click the **Apply** button.

To save selected settings to ports other than the one you are configuring:

1. From the **Apply Settings** drop-down box at the bottom of the **Device Ports - Settings** page, select **none**, **General**, **IP**, **Data**, **Modem**, or **All**.
2. In **to Device Ports,** type the device port numbers, separated by commas; indicate a range of port numbers with a hyphen (e.g., 2, 5, 7-10).

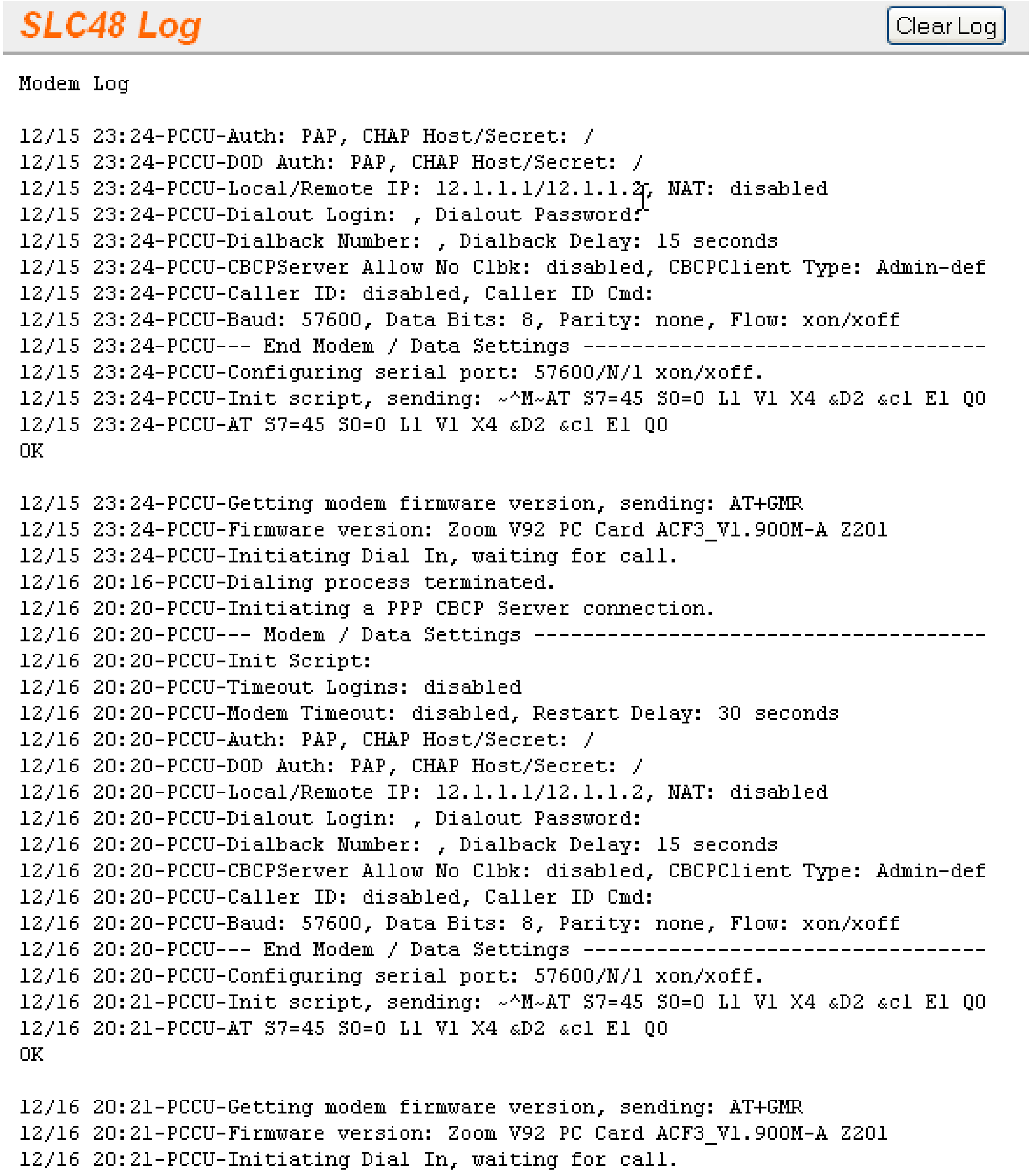
Note: *It may take a few minutes for the system to apply the settings to multiple ports.*

3. Click the **Apply** button.

To view logs of all modem activity:

1. Click the **View Modem Log** link on the **Device Ports - Settings** page.

Figure 8-4 Modem Log



```
Modem Log

12/15 23:24-PCCU-Auth: PAP, CHAP Host/Secret: /
12/15 23:24-PCCU-DOD Auth: PAP, CHAP Host/Secret: /
12/15 23:24-PCCU-Local/Remote IP: 12.1.1.1/12.1.1.2, NAT: disabled
12/15 23:24-PCCU-Dialout Login: , Dialout Password:
12/15 23:24-PCCU-Dialback Number: , Dialback Delay: 15 seconds
12/15 23:24-PCCU-CBCPServer Allow No Clbk: disabled, CBCPClient Type: Admin-def
12/15 23:24-PCCU-Caller ID: disabled, Caller ID Cmd:
12/15 23:24-PCCU-Baud: 57600, Data Bits: 8, Parity: none, Flow: xon/xoff
12/15 23:24-PCCU--- End Modem / Data Settings ---------------------------------
12/15 23:24-PCCU-Configuring serial port: 57600/N/1 xon/xoff.
12/15 23:24-PCCU-Init script, sending: ~^M~AT S7=45 S0=0 L1 V1 X4 &D2 &c1 E1 Q0
12/15 23:24-PCCU-AT S7=45 S0=0 L1 V1 X4 &D2 &c1 E1 Q0
OK

12/15 23:24-PCCU-Getting modem firmware version, sending: AT+GMR
12/15 23:24-PCCU-Firmware version: Zoom V92 PC Card ACF3_V1.900M-A Z201
12/15 23:24-PCCU-Initiating Dial In, waiting for call.
12/16 20:16-PCCU-Dialing process terminated.
12/16 20:20-PCCU-Initiating a PPP CBCP Server connection.
12/16 20:20-PCCU--- Modem / Data Settings -------------------------------------
12/16 20:20-PCCU-Init Script:
12/16 20:20-PCCU-Timeout Logins: disabled
12/16 20:20-PCCU-Modem Timeout: disabled, Restart Delay: 30 seconds
12/16 20:20-PCCU-Auth: PAP, CHAP Host/Secret: /
12/16 20:20-PCCU-DOD Auth: PAP, CHAP Host/Secret: /
12/16 20:20-PCCU-Local/Remote IP: 12.1.1.1/12.1.1.2, NAT: disabled
12/16 20:20-PCCU-Dialout Login: , Dialout Password:
12/16 20:20-PCCU-Dialback Number: , Dialback Delay: 15 seconds
12/16 20:20-PCCU-CBCPServer Allow No Clbk: disabled, CBCPClient Type: Admin-def
12/16 20:20-PCCU-Caller ID: disabled, Caller ID Cmd:
12/16 20:20-PCCU-Baud: 57600, Data Bits: 8, Parity: none, Flow: xon/xoff
12/16 20:20-PCCU--- End Modem / Data Settings ---------------------------------
12/16 20:20-PCCU-Configuring serial port: 57600/N/1 xon/xoff.
12/16 20:21-PCCU-Init script, sending: ~^M~AT S7=45 S0=0 L1 V1 X4 &D2 &c1 E1 Q0
12/16 20:21-PCCU-AT S7=45 S0=0 L1 V1 X4 &D2 &c1 E1 Q0
OK

12/16 20:21-PCCU-Getting modem firmware version, sending: AT+GMR
12/16 20:21-PCCU-Firmware version: Zoom V92 PC Card ACF3_V1.900M-A Z201
12/16 20:21-PCCU-Initiating Dial In, waiting for call.
```

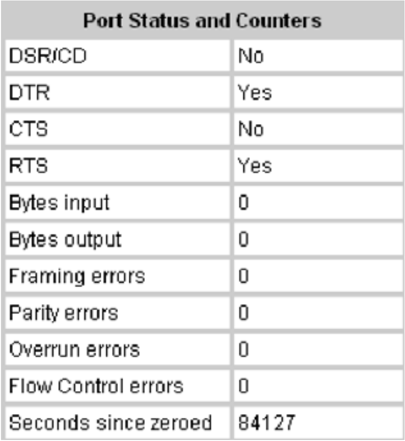
Port Status and Counters

Port Status and Counters list the status of signals and interfaces. SLC console manager updates and increments the port counters as signals change and data flows in and out of the system. These counters help troubleshoot connections or diagnose problems because they give the user an overview of the state of various parameters. By setting them to zero and then re-checking them later, the user can view changes in status. See *Figure 8-5* for an example.

The chart in the middle of the page displays the flow control lines and port statistics for the device port. The system automatically updates these values. To reset them to zeros, select the **Zero port counters** checkbox in the IP Settings section of the page.

Note: *Status and statistics shown on the web interface represent a snapshot in time. To see the most recent data, you must reload the web page.*

Figure 8-5 Port Status and Counters Section



Port Status and Counters	
DSR/CD	No
DTR	Yes
CTS	No
RTS	Yes
Bytes input	0
Bytes output	0
Framing errors	0
Parity errors	0
Overrun errors	0
Flow Control errors	0
Seconds since zeroed	84127

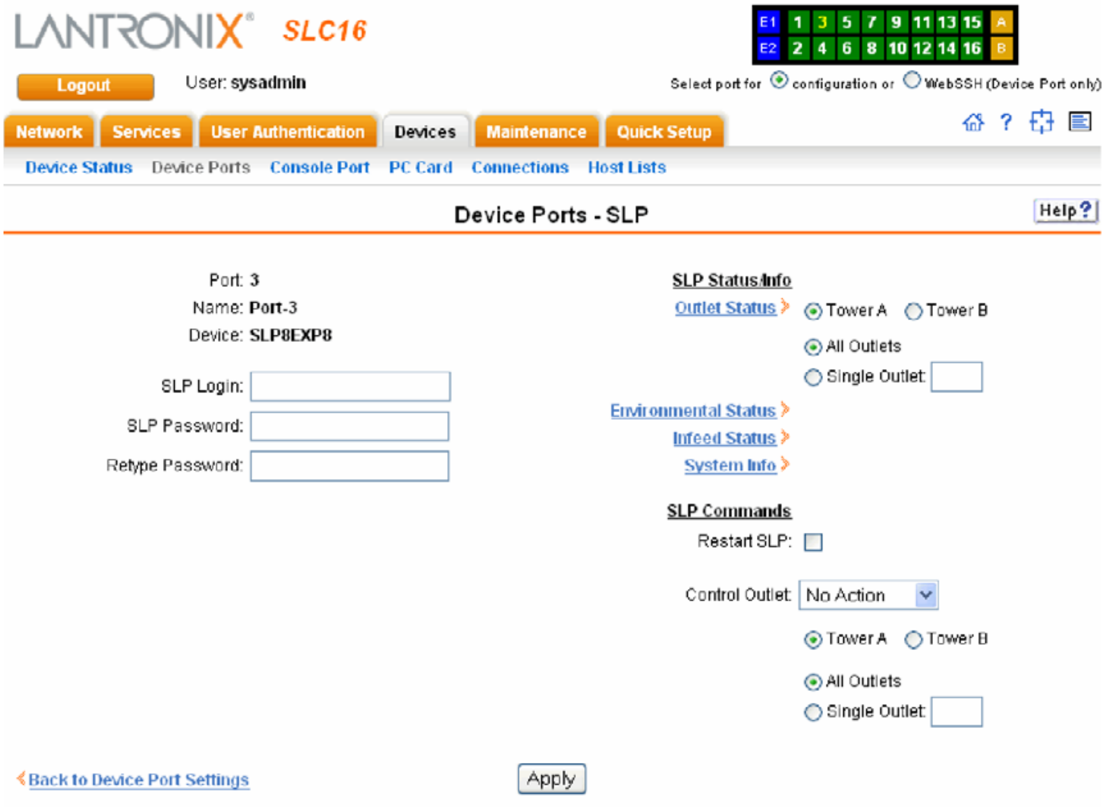
Device Port – SLP Power Manager

On the Device Ports – SLP page, configure commands to send to an SLP power manager or SLP power manager expansion chassis that expands the number of power ports.

To open the Device Ports – SLP page:

1. In the **Connected to** field above the IP Settings section of the **Device Ports – Settings** page, select an SLP or SLPEXP.
2. Click the **Device Commands** link. *Figure 8-6* shows the page that displays.

Figure 8-6 Device Ports - SLP Page



User: sysadmin

Select port for ● configuration or ○ WebSSH (Device Port only)

Device Ports - SLP

Port: 3
Name: Port-3
Device: SLP8EXP8

SLP Login:
SLP Password:
Retype Password:

SLP Status/Info

Outlet Status ● Tower A ○ Tower B
● All Outlets
○ Single Outlet:

Environmental Status
Infeed Status
System Info

SLP Commands

Restart SLP: □

Control Outlet: No Action

● Tower A ○ Tower B
● All Outlets
○ Single Outlet:

To configure the SLP power manager:

1. Enter the following fields.

Port (view only)	Displays the port number.
Name (view only)	Displays the port name.
Device (view only)	Displays the device type.
SLP Login	User ID for logging into the SLP power manager.
SLP Password/ Retype Password	Password for logging into the SLP power manager.

SLP Status/Info

Outlet Status	***Note:*** *If there is an SLP power manager and an SLP expansion chassis, the SLP power manager is Tower A and the Expansion chassis is Tower B.* For Tower A or Tower B, select **All Outlets** or **Single Outlet** to view the status of all outlets or a single outlet of the SLP power manager. If you select **Single Outlet**, enter a value of 1-8 for the SLP8 or 1-16 for the SLP16. Click the **Outlet Status** link to see the status of the selected outlet(s).

Environmental Status	Click the link to view the environmental status (e.g., temperature and humidity) of the SLP power manager.
Infeed Status	Click the link to view the status of the data the SLP power manager is receiving.
System Info	Click the link to see system information pertaining to the SLP power manager.

SLP Commands

Restart SLP	To restart the SLP power manager, select the checkbox.
Control Outlet	For Tower A or Tower B, select **All Outlets** or **Single Outlet** and the number of the outlet to be controlled (1-8 for the SLP8 or 1-16 for the SLP16) and select the command for the outlet (No Action, Power On, Power Off, Cycle Power). **No Action** is the default.

2. Click the **Apply** button.

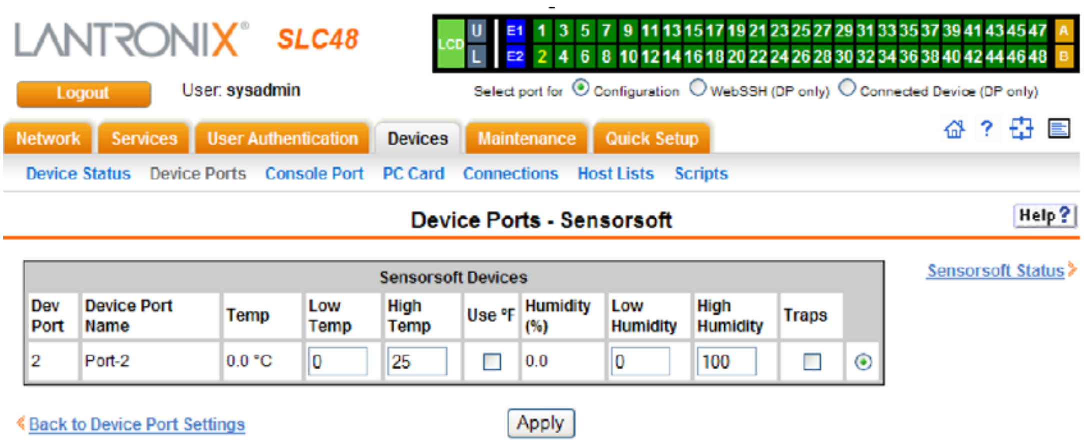
Device Port – Sensorsoft Device

Devices made by Sensorsoft are used to monitor environmental conditions.

To access the Sensorsoft device:

1. In the **Connected to** field above the IP Settings section of the **Device Ports – Settings** page, select **Sensorsoft.**
2. Click the **Device Commands** link. *Figure 8-7* shows the page that displays.

Figure 8-7 Device Ports - Sensorsoft


LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
User: sysadmin
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network
Services
User Authentication
Devices
Maintenance
Quick Setup
Device Status
Device Ports
Console Port
PC Card
Connections
Host Lists
Scripts
Help ?
Sensorsoft Status
Back to Device Port Settings
Apply

Device Ports - Sensorsoft

Sensorsoft Devices

Dev Port	Device Port Name	Temp	Low Temp	High Temp	Use °F	Humidity (%)	Low Humidity	High Humidity	Traps	
2	Port-2	0.0 °C	0	25	□	0.0	0	100	□	●

To configure Sensorsoft settings:

1. Select a port and enter the following fields.

Device Port (view only)	Displays the port number.
Device Port Name (view only)	Displays the port name.
Temp (°C)	Displays the current temperature (Celsius).
Low Temp	Enter the temperature (Celsius) permitted on the monitored device below which the SLC device sends a trap.
High Temp	Enter the temperature (degrees Celsius) permitted on the monitored device above which the SLC console manager sends a trap.
Use °F	Displays and sets the temperature for this device in degrees Fahrenheit, instead of Celsius, which is the default.
Humidity (%)	Displays the current relative humidity.
Low Humidity	Enter the relative humidity permitted on the device the sensor is monitoring below which the sensor sends a trap to the SLC device.
High Humidity	Enter the highest relative acceptable humidity permitted on the device above which the sensor sends a trap to the SLC console manager.
Traps	Select to indicate the SLC device should send a trap or configured Event Alert when the sensor detects an out-of-range configured threshold. See *SNMP on page 65*.

2. Click the **Apply** button.

To view the status detected by the Sensorsoft:

1. Click the **Sensorsoft Status** link to the right of the table.

Device Port Commands

The following CLI commands correspond to the **Device Ports** page. For more information, see 15: Command Reference.

- *set deviceport port (on page 223)*
- *set deviceport global (on page 225)*
- *set command (on page 222)*
- *connect listen (on page 217)*
- *connect direct (on page 216)*
- *show deviceport global (on page 226)*
- *show deviceport port (on page 226)*
- *show deviceport names (on page 226)*
- *show portstatus (on page 226)*
- *show portcounters (on page 226)*
- *show portcounters zerocounters (on page 226)*

Device Ports – Logging

The SLC products support port buffering of the data on the system's device ports as well as notification of receiving data on a device port. Port logging is disabled by default. You can enable more than one type of logging (local, NFS file, email/SNMP, USB port, or PC Card) at a time. The buffer containing device port data is cleared when any type of logging is enabled.

Local Logging

If local logging is enabled, each device port stores 256 Kbytes (approximately 400 screens) of I/O data in a true FIFO buffer. You may view this data (in ASCII format) at the CLI with the `show locallog` command or on the Device Ports – Logging web page. Buffered data is normally stored in RAM and is lost in the event of a power failure if it is not logged using an NFS mount solution. If the buffer data overflows the buffer capacity, only the oldest data is lost, and only in the amount of overrun (not in large blocks of memory).

NFS File Logging

Data can be logged to a file on a remote NFS server. Data logged locally to the SLC console manager is limited to 256 Kbytes and may be lost in the event of a power loss. Data logged to a file on an NFS server does not have these limitations. The system administrator can define the directory for saving logged data on a port-by-port basis and configure file size and number of files per port.

The directory path must be the local directory for one of the NFS mounts. For each logging file, once the file size reaches the maximum, a new file opens for logging. Once the number of files reaches the maximum, the oldest file is overwritten. The file naming convention is: <Device Port Number>_<Device Port Name>_<File number>.log.

Examples: 02_Port-2_1.log

02_Port-2_2.log

02_Port-2_3.log

02_Port-2_4.log

02_Port-2_5.log

PC Card Logging

Note: *The PC Card logging feature is only supported on SLC -02 part numbers.*

Data can be logged to a PC Card Compact Flash that is loaded into one of the PC Card slots on the front of the SLC device and properly mounted. Data logged locally to the SLC console manager is limited to 256 Kbytes and may be lost in the event of a power loss. Data logged to a PC Card Compact Flash does not have these limitations. The system administrator can define the file size and number of files per port. For each logging file, once the file size reaches the maximum, a new file opens for logging. Once the number of files reaches the maximum, the oldest file is overwritten. The file naming convention is: <Device Port Number>_<Device Port Name>_<File number>.log.

Examples: 02_Port-2_1.log

02_Port-2_2.log

02_Port-2_3.log

02_Port-2_4.log

02_Port-2_5.log

USB Port Logging

Note: *The USB port logging feature is only supported on SLC -03 part numbers.*

Data can also be logged to an thumb drive that is loaded in the USB port. Logged data to the USB port is limited to 2048 bytes and 10 files. The system administrator can define the file size and number of files per port. For each logging file, once the file size reaches the maximum, a new file opens for logging. Once the number of files reaches the maximum, the oldest file is overwritten. The file naming convention is: <Device Port Number>_<Device Port Name>_<File number>.log. See *Chapter 10: USB Port* for configuration tasks and *Chapter 15: Command Reference* for the commands, specifically the *USB Commands* section.

Email/SNMP Notification

The system administrator can configure the SLC console manager to send an email alert message indicating a particular condition detected in the device port log to the appropriate parties or an SNMP trap to the designated NMS (see *Chapter 7: Services*). The email or trap is triggered when a user-defined number of characters in the log from your server or device is exceeded, or a specific sequence of characters is received.

Use the **Device Ports – Logging** page to set logging parameters on individual ports.

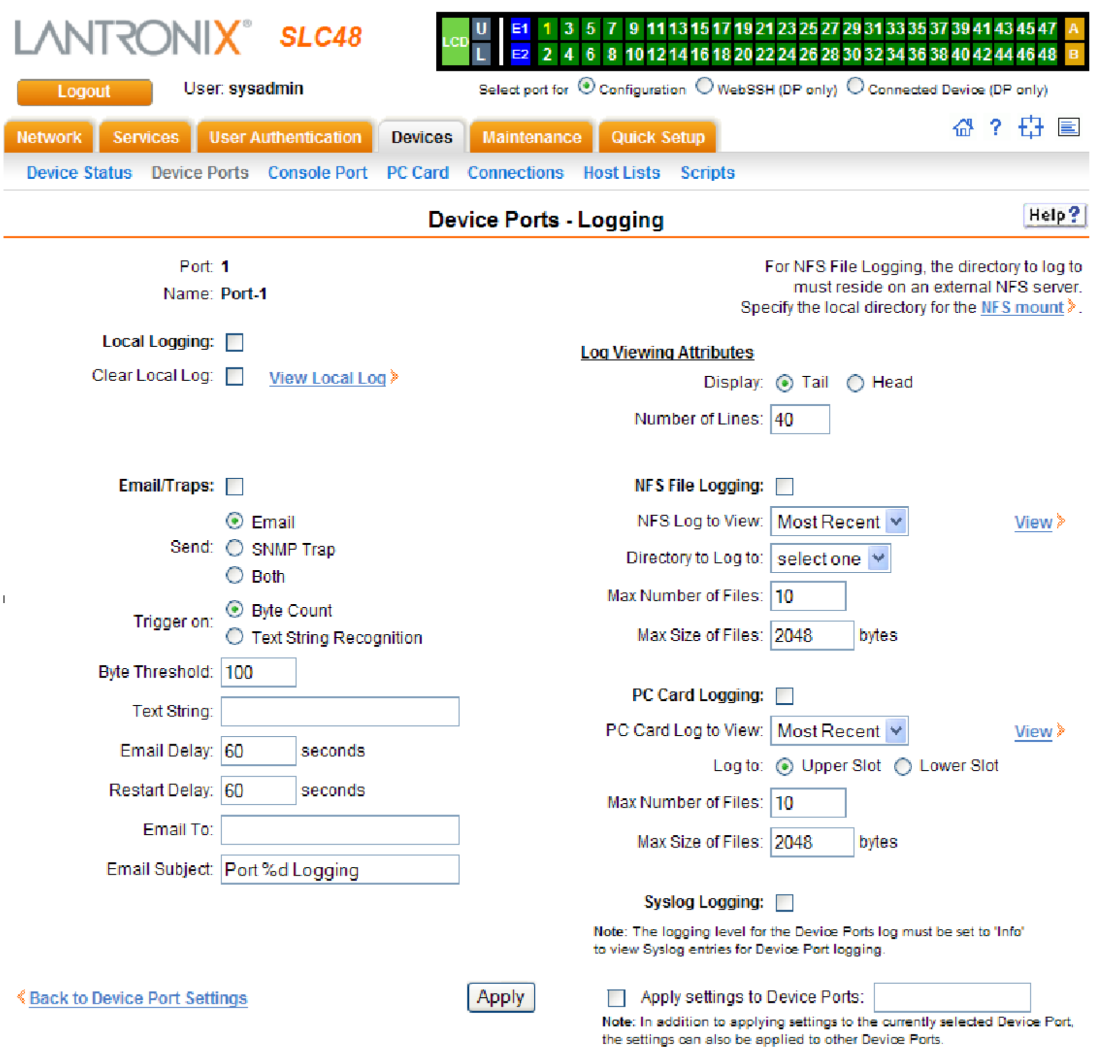
Syslog Logging

Data can be logged to the system log. If this feature is enabled, the data will appear in the Device Ports log, under the Info level. The log level for the Device Ports log must be set to Info for the data to be saved to the system log (see *Chapter 7: Services*).

To set logging parameters:

1. In the Device Ports – Settings page, click the **Logging: Settings** link. *Figure 8-8* shows the page that displays.

Figure 8-8 Device Ports - Logging


LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network Services User Authentication Devices Maintenance Quick Setup
Device Status Device Ports Console Port PC Card Connections Host Lists Scripts
Help?
View Local Log
View
Back to Device Port Settings
Apply

User: sysadmin

Select port for: ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Device Ports - Logging

Port: **1**
Name: **Port-1**

For NFS File Logging, the directory to log to must reside on an external NFS server. Specify the local directory for the NFS mount.

Local Logging: □
Clear Local Log: □

Log Viewing Attributes
Display: ● Tail ○ Head
Number of Lines: 40

Email/Traps: □
Send: ● Email ○ SNMP Trap ○ Both
Trigger on: ● Byte Count ○ Text String Recognition
Byte Threshold: 100
Text String:
Email Delay: 60 seconds
Restart Delay: 60 seconds
Email To:
Email Subject: Port %d Logging

NFS File Logging: □
NFS Log to View: Most Recent
Directory to Log to: select one
Max Number of Files: 10
Max Size of Files: 2048 bytes

PC Card Logging: □
PC Card Log to View: Most Recent
Log to: ● Upper Slot ○ Lower Slot
Max Number of Files: 10
Max Size of Files: 2048 bytes

Syslog Logging: □

Note: The logging level for the Device Ports log must be set to 'Info' to view Syslog entries for Device Port logging.

□ Apply settings to Device Ports:

Note: In addition to applying settings to the currently selected Device Port, the settings can also be applied to other Device Ports.

2. Enter the following fields.

Local Logging

Local Logging	Enable local logging and each device port stores 256 Kbytes (approximately 400 screens) of I/O data in a true FIFO buffer. **Disabled** by default.
Clear Local Log	Select the checkbox to clear the local log.
View Local Log	Click this link to see the local log in text format.

Email Traps

Email/Traps	Select the checkbox to enable email and SNMP logging. Email logging sends an email message to pre-defined email addresses or an SNMP trap to the designated NMS (see 7: Services) when alert criteria are met. Disabled by default.
Send	Select notification type to send: **Email**, **SNMP**, or **Both**. **Email** is the default. Email and SNMP logging must be enabled for this feature to work.
Trigger on	Select the method of triggering a notification: **Byte Count**: A specific number of bytes of data. This is the default. **Text String Recognition**: A specific pattern of characters, which you can define by a regular expression. ***Note:*** *Text string recognition may negatively impact SLC performance, particularly when regular expressions are used.*
Byte Threshold	Sets the threshold for the number of bytes of data the port receives before the SLC console manager captures log data and sends a notification. The default is **100** bytes. In most cases, the console port of your device does not send any data unless there is an alarm condition. After the SLC device receives a small number of bytes, it perceives that your device needs some attention. The SLC console manager notifies your technician when that point has been passed, and the notification includes the logged data. For example, a threshold preset at 30 characters means that as soon as the SLC device receives 30 bytes of data, it captures log data and sends an email regarding this port.
Text String	Sets the specific pattern of characters the SLC console manager must recognize before sending a notification to the technician about this port. The maximum is 100 characters. You may use a regular expression to define the pattern. For example, the regular expression “abc[def]g” recognizes the strings abcdg, abceg, abcfg. The SLC device supports GNU regular expressions; for more information, see: ◆ http://www.codeforge.com/help/GNURegularExpr.html ◆ http://www.delorie.com/gnu/docs/regex/regex.html
Email Delay	Sets a time limit of how long (in seconds), after the SLC console manager detects the trigger, that the device port captures data before closing the log file (with a fixed internal buffer maximum capacity of 1500 bytes) and sending a notification. The default is **60** seconds.
Restart Delay	Sets the number of seconds for the period *after* the notification has been sent during which the device port ignores additional characters received. The data is simply ignored and does not trigger additional alarms until this time elapses. The default is **60** seconds.
Email to	Sets the complete email address of the message recipients for each device port. Each device port has its own recipient list. To enter more than one email address, separate the addresses with a **single space**. You can enter up to 128 characters.

Email Subject	Input a subject text appropriate for your site. May have up to 128 characters. The email subject line is pre-defined for each port with its port number. You can use the email subject to inform the desired recipients of the problem on a certain server or location (e.g., server location or other classification of your equipment). This is helpful if the email message goes to the system administrator's or service technician's mobile or wireless device (e.g., text messaging by means of email). *Note: The character sequence**%d** anywhere in the email subject is replaced with the device port number automatically.*

Log Viewing Attributes

Display	Select to view either the beginning (head) or end (tail) of the log.
Number of Lines	Input the number of lines from the head or tail of the log to display.

NFS File Logging

NFS File Logging	Select the checkbox to log all data sent to the device port to one or more files on an external NFS server. Disabled by default.
NFS Log to View	A list of available log files saved to the selected directory to view.
Directory to Log to	The path of the directory where the log files will be stored. *Note: This directory must be a directory exported from an NFS server mounted on the SLC console manager. Specify the local directory path for the NFS mount.*
Max Number of Files	The maximum number of files to create to contain log data to the port. These files keep a history of the data received from the port. Once this limit is exceeded, the oldest file is overwritten. The default is **10**.
Max Size of Files	The maximum allowable file size in bytes. The default is **2048** bytes. Once the maximum size of a file is reached, the SLC console manager begins generating a new file.

PC Card Logging

Note: This PC Card logging feature is only supported on SLC -02 part numbers.

PC Card Logging	Select to enable PC Card logging. A PC Card Compact Flash must be loaded into one of the PC Card slots on the front of the SLC console manager and properly mounted (see *PC Card Logging on page 97*). Disabled by default.
PC Card Log to View	A list of saved log files for the selected PC Card slot to view.
Log To	Select the slot (**Upper** or **Lower**) in which the PC Card has been inserted. **Upper** is the default for a PC Card.
Max Number of Files	The maximum number of files to create to contain log data to the port. These files keep a history of the data received from the port. Once this limit is exceeded, the oldest file is overwritten. The default is **10**.
Max Size of Files	The maximum allowable file size in bytes. The default is 2048 bytes. Once the maximum size of a file is reached, the SLC console manager begins generating a new file. The default is **2048** bytes.

USB Logging

Note: This USB logging feature is only supported on SLC -03 part numbers.

USB Logging	Select to enable USB logging. See USB Port Logging on page 97. Disabled by default.
USB Log to View	A list of saved log files to view.
Log To	Port U1 is the default and is automatically selected.
Max Number of Files	The maximum number of files to create to contain log data to the port. These files keep a history of the data received from the port. Once this limit is exceeded, the oldest file is overwritten. The default is **10**.
Max Size of Files	The maximum allowable file size in bytes. The default is 2048 bytes. Once the maximum size of a file is reached, the SLC console manager begins generating a new file. The default is **2048** bytes.

Syslog Logging

Syslog Logging	Select to enable system logging. *Note: The logging level for the device ports log must be set to Info to view Syslog entries for Device Port logging on the Services page.*

Note: To apply the settings to additional device ports, in the Apply settings to Device Ports field, enter the additional ports, (e.g., 1-3, 5, 6)

3. To apply settings to other device ports in addition to the currently selected port, select the **Apply** settings to Device Ports and enter port numbers separated by commas. Indicate a range of port numbers with a hyphen (e.g., 2, 5, 7-10), and separate ranges with commas.
4. Click the **Apply** button.

Logging Commands

The following CLI commands correspond to the **Device - Ports Logging** page. For more information, see 15: Command Reference.

- *set deviceport port (on page 223)*
- *set log clear (on page 238)*
- *set log clear modem (on page 238)*
- *set log modem pppdebug (on page 239)*
- *show log modem (on page 239)*
- *show log local (on page 239)*
- *show log files (on page 239)*
- *show syslog (on page 257)*
- *show syslog clear (on page 257)*

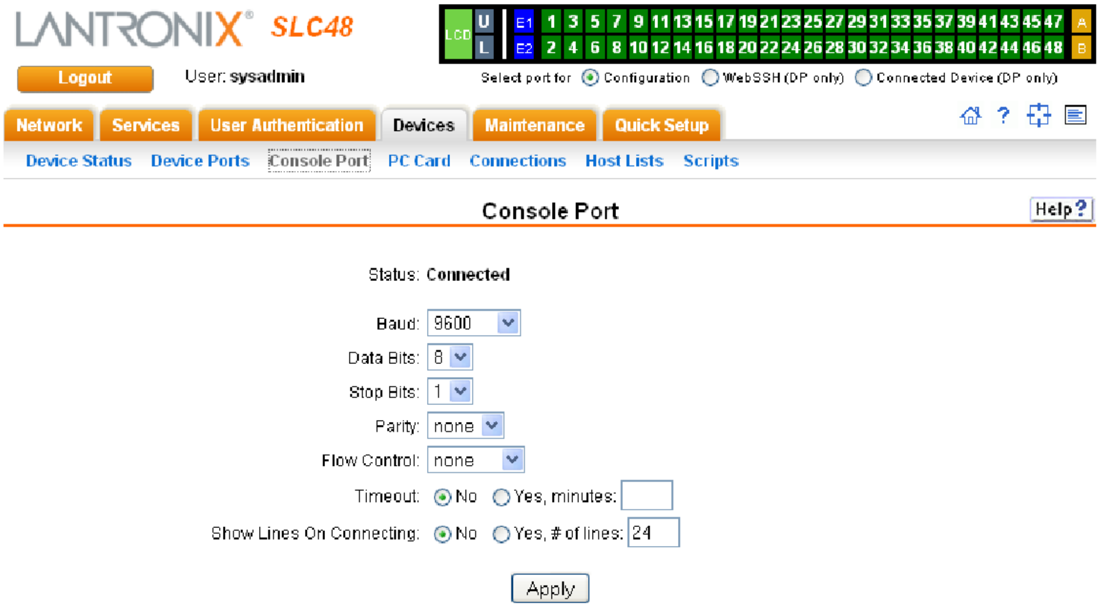
Console Port

The console port initially has the same defaults as the device ports. Use the Console Port page to change the settings, if desired.

To set console port parameters:

1. Click the **Devices** tab and select **Console Port**. *Figure 8-9* shows the page that displays.

Figure 8-9 Console Port Page


LANTRONIX SLC48
Logout
User: sysadmin
LCD U L E1 E2
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Select port for: ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network
Services
User Authentication
Devices
Maintenance
Quick Setup
Device Status
Device Ports
Console Port
PC Card
Connections
Host Lists
Scripts
Console Port
Help?
Apply

Status: Connected

Baud: 9600

Data Bits: 8

Stop Bits: 1

Parity: none

Flow Control: none

Timeout: ● No ○ Yes, minutes:

Show Lines On Connecting: ● No ○ Yes, # of lines: 24

2. Enter the following fields.

Status (view only)	Displays the status of the console port.
Baud	Select the baud rate (speed) with which the device port exchanges data with the attached serial device. Most devices use **9600** for the administration port, so the console port defaults to this value.
Data Bits	Select the number of data bits used to transmit a character. The default is **8** data bits.
Stop Bits	Select the number of stop bits that indicate that a byte of data has been transmitted. The default is **1**.
Parity	Select the parity checking which detects simple, single-bit errors. The default is **none**.
Flow Control	Select a method of preventing buffer overflow and loss of data. The available methods include none, xon/xoff (software), and RTS/CTS (hardware). The default is **none**.
Timeout	Click the **No** or **Yes** button. Input the number of minutes (1-30) if you clicked **Yes** after which an idle session on the console is automatically logged out. Disabled by default.

Show Lines on Connecting	Click the checkbox if you connect to the console port with a terminal emulator. You will see the last lines of output to the console. For example, the SLC boot messages or the last lines of output during a CLI session on the console.

3. Click the **Apply** button.

Console Port Commands

The following CLI commands correspond to the **Console Port** page. For more information, see *Chapter 15: Command Reference*.

- *set consoleport (on page 219)*
- *show consoleport (on page 219)*

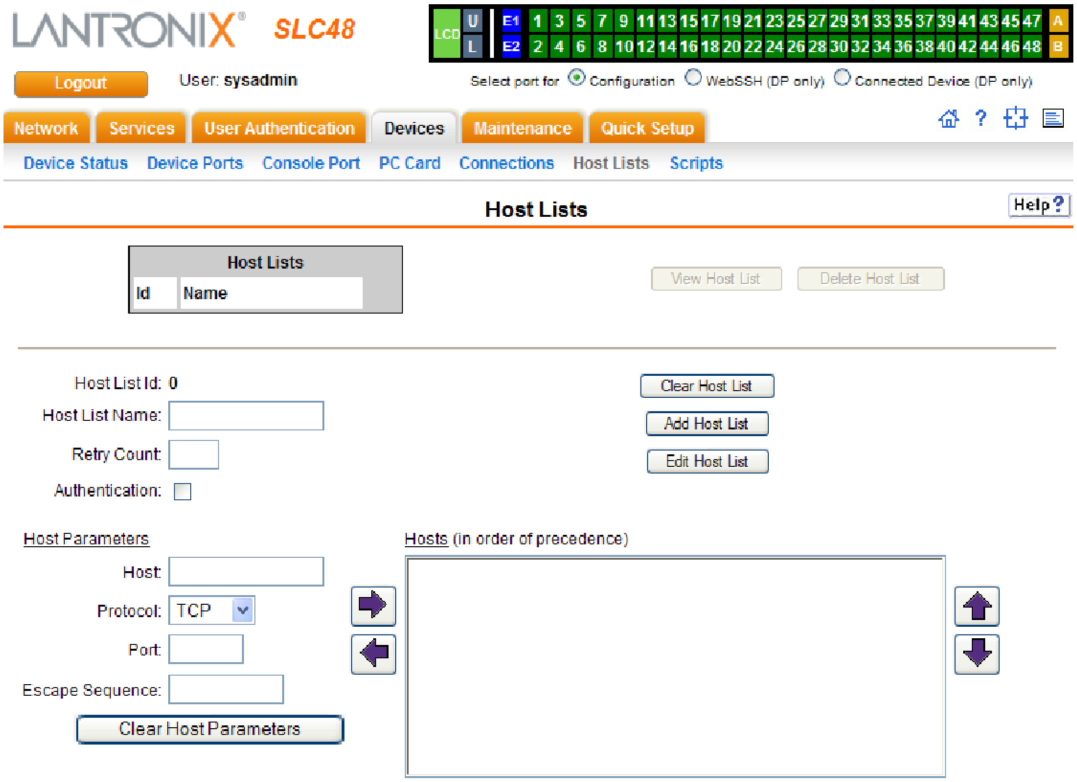
Host Lists

A host list is a prioritized list of SSH, Telnet, and TCP hosts available for establishing incoming modem connections or for the `connect direct` command on the CLI. The SLC console manager cycles through the list until it successfully connects to one.

To add a host list:

1. Click the **Devices** tab and the **Host Lists** option. *Figure 8-10* shows the page that displays.

Figure 8-10 Host Lists Page


LANTRONIX
SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network Services User Authentication Devices Maintenance Quick Setup
Device Status Device Ports Console Port PC Card Connections Host Lists Scripts
Help ?
Host Lists
Id Name
View Host List
Delete Host List
Clear Host List
Add Host List
Edit Host List
Host Parameters
Hosts (in order of precedence)
Clear Host Parameters

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Host Lists

Host List Id: 0
Host List Name:
Retry Count:
Authentication: □

Host:
Protocol: TCP
Port:
Escape Sequence:

2. Enter the following fields.

Note: *To clear fields in the lower part of the page, click the **Clear Host List** button.*

Host Lists (view only	Displays host lists by ID and Name.
Host List Id (view only)	Displays after a host list is saved.
Host List Name	Enter a name for the host list.
Retry Count	Enter the number of times the SLC console manager should attempt to retry connecting to the host list.
Authentication	Select to require authentication when the SLC device connects to a host.

Host Parameters

Host	Input the name or IP address of the host.
Protocol	Select the protocol for connecting to the host (TCP, SSH, or Telnet).
Port	Enter the port on the host to connect to.
Escape Sequence	Enter the escape character or sequence of characters used to get the attention of the SSH or Telnet client. It is optional, and if not specified, Telnet and SSH use the following default escape characters: ◆ Telnet—Single character or a two-character sequence consisting of '^' followed by one character. If the second character is '?', the DEL character is selected. Otherwise, the second character is converted to a control character and used as the escape character. ◆ SSH—Single character.

3. Click the **right arrow**. The host displays in the **Hosts** box.
4. Repeat steps 2-4 to add more hosts to the host list.

Note: *To clear fields before adding the next host, click the **Clear Host Parameters** button.*

5. Click the **Add Host List** button. After the process completes, a new window opens and when the addition completes, the message “Host List configuration is complete.” displays.
6. After the process completes, you can click the **Host Lists** tab.

To remove a host from the host list:

1. Select the host in the Hosts box and click the left arrow.

To give the host a higher precedence:

1. Select the host in the Hosts box and click the up arrow.

To give the host a lower precedence:

1. Select the host in the Hosts box and click the down arrow.

To edit a host list:

1. Click the host list name and the radio button in the list table.

2. Click **View Host Lists** button. The parameters display in the Host List Parameters section.
3. Click the **Edit Host List** button. A new window opens and when the changes are complete, the message "Host List configuration is complete." displays.
4. After the process completes, you can click the **Host Lists** tab.

To delete a host list:

1. Select the host list in the **Host Lists** table.
2. Click the **Delete Host List** button. A new window opens to confirm the deletion. When the deletion completes, the message "Host List configuration is complete." displays.
3. After the process completes, you can click the **Host Lists** tab.

To view or update a host list:

1. In the **Host Lists** table, select the host list and click the **View Host List** button.

Host List Commands

The following CLI commands correspond to the **Host Lists** page. For more information, see 15: Command Reference.

- *set hostlist (name) (on page 231)*
- *set hostlist (number) (on page 231)*
- *set hostlist edit (on page 232)*
- *set hostlist delete (on page 231)*
- *show hostlist (on page 232)*

Scripts

The SLC console manager supports the following two types of scripts:

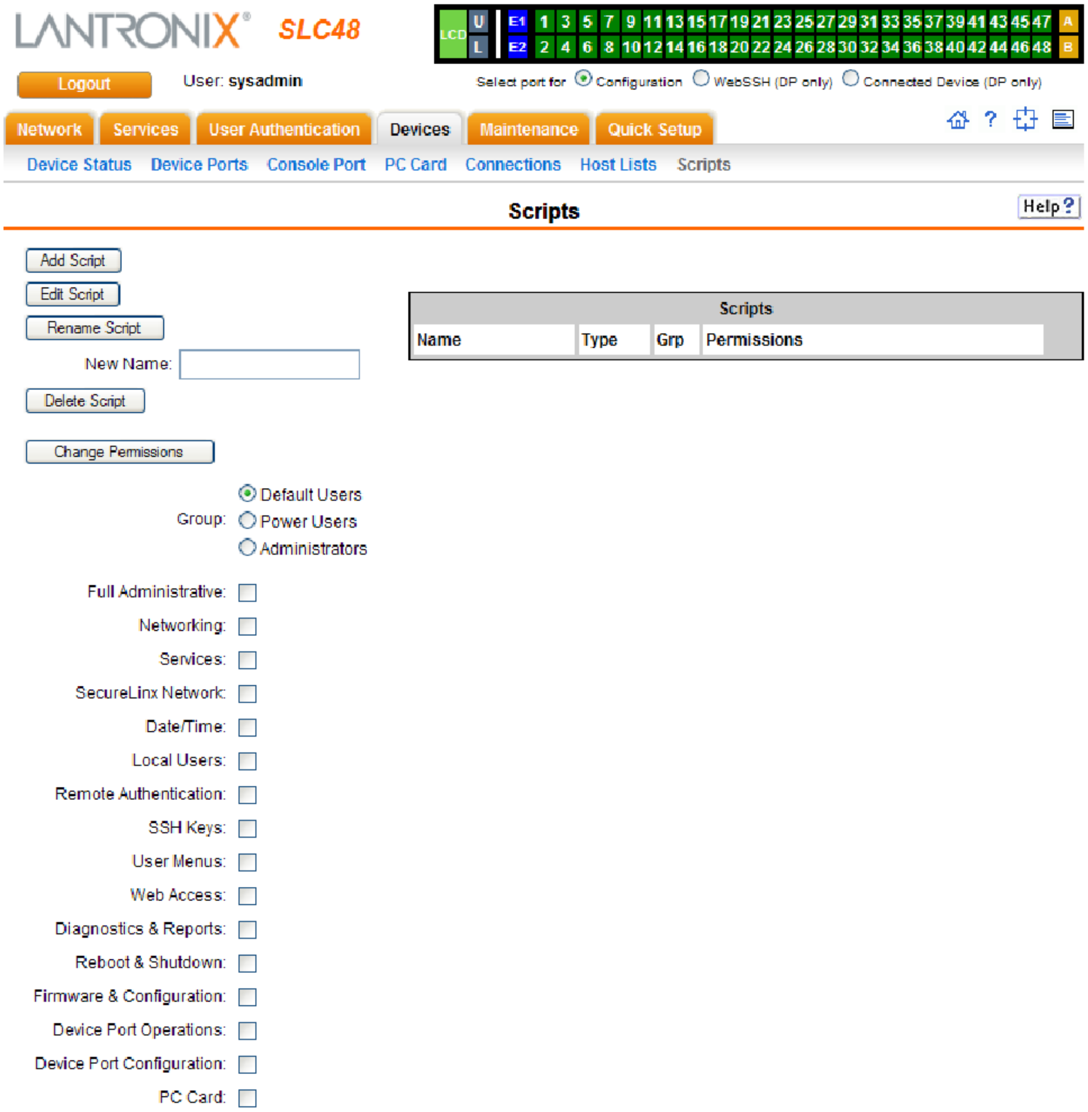
- Interface Scripts which use a subset of the Expect/Tcl scripting language to perform pattern detection and action generation on Device Port output. For a description of the syntax allowed in Interface Scripts, see *Interface Script Syntax on page 108*.
- Batch Scripts which are a series of CLI commands. A user can create scripts at the web, view scripts at the web and the CLI, and use scripts at the CLI. For a description of the syntax allowed in Batch Scripts, see *Batch Script Syntax on page 108*.

All scripts have associated permissions. A user who runs a script must have the permissions associated with the script in order to run it.

To add a script:

1. Click the Devices tab and select the Scripts option. *Figure 8-11* shows the page that displays.

Figure 8-11 Scripts Page


LANTRONIX
SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
User: sysadmin
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network
Services
User Authentication
Devices
Maintenance
Quick Setup
Device Status
Device Ports
Console Port
PC Card
Connections
Host Lists
Scripts
Help ?

Scripts

Add Script

Edit Script

Rename Script

New Name: ________

Delete Script

Change Permissions

Group: ● Default Users ○ Power Users ○ Administrators

Full Administrative: □

Networking: □

Services: □

SecureLinx Network: □

Date/Time: □

Local Users: □

Remote Authentication: □

SSH Keys: □

User Menus: □

Web Access: □

Diagnostics & Reports: □

Reboot & Shutdown: □

Firmware & Configuration: □

Device Port Operations: □

Device Port Configuration: □

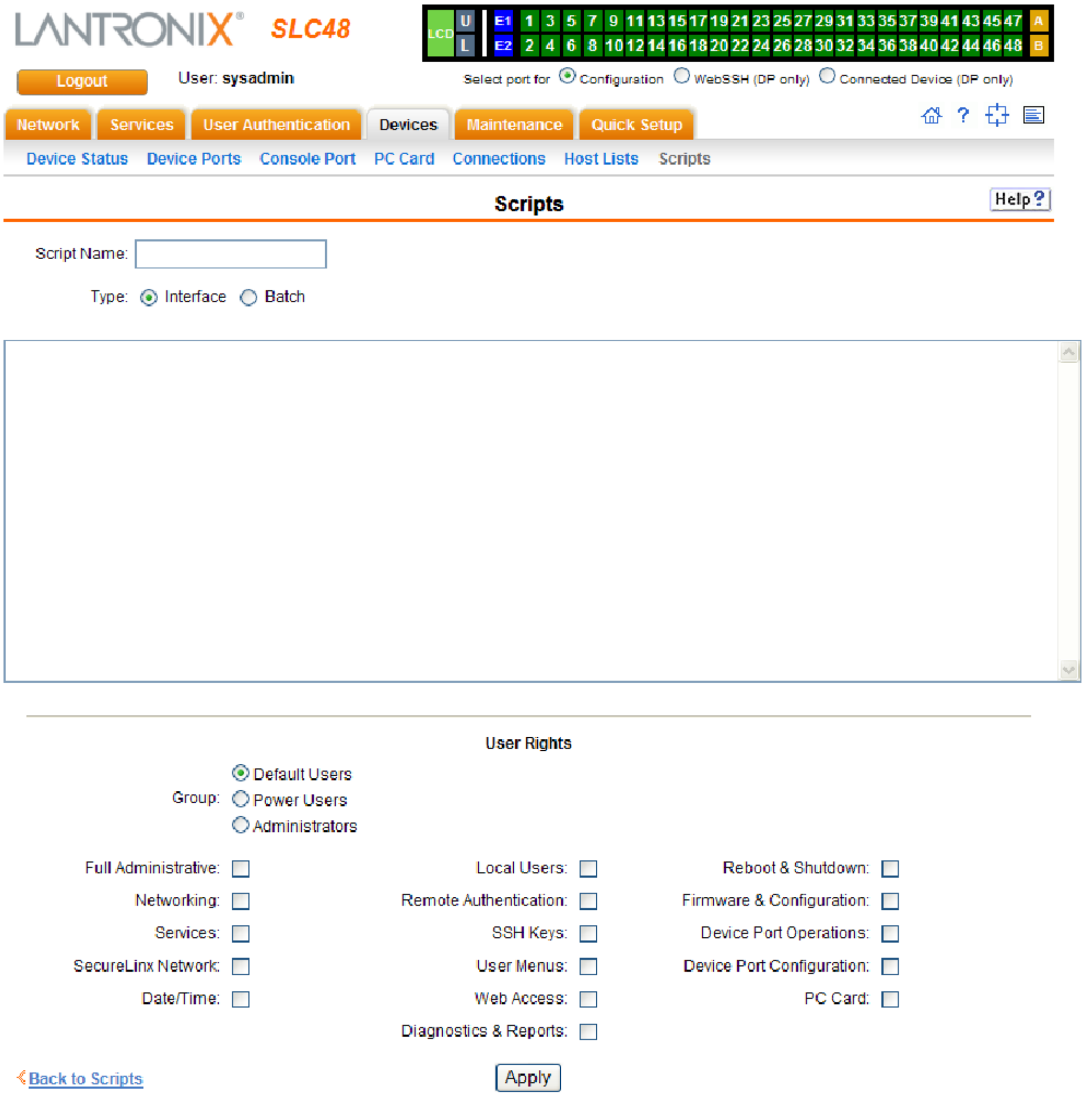
PC Card: □

Scripts

Name	Type	Grp	Permissions

2. Click the **Add** button. *Figure 8-11* shows the page that displays.

Figure 8-12 Adding New Scripts Page


LANTRONIX
SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
User: sysadmin
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network
Services
User Authentication
Devices
Maintenance
Quick Setup
Device Status
Device Ports
Console Port
PC Card
Connections
Host Lists
Scripts
Help ?
Back to Scripts
Apply

Scripts

Script Name:

Type: ● Interface ○ Batch

User Rights

Group: ● Default Users
○ Power Users
○ Administrators

Full Administrative: □	Local Users: □	Reboot & Shutdown: □
Networking: □	Remote Authentication: □	Firmware & Configuration: □
Services: □	SSH Keys: □	Device Port Operations: □
SecureLinx Network: □	User Menus: □	Device Port Configuration: □
Date/Time: □	Web Access: □	PC Card: □
	Diagnostics & Reports: □	

3. Enter the following fields.

Script Name	A unique identifier for the script.
Type	Select **Interface** for a script that utilizes Expect/Tcl to perform pattern detection and action generation on Device Port output. Select **Batch** for a script of CLI commands.
Script Text	In the free-form editing box, enter the contents of the script.
Group	Select the group to which the script will belong: ◆ Default Users—This group has only the most basic rights. You can specify additional rights for the individual user. ◆ Power Users—This group has the same rights as Default Users plus Networking, Date/Time, Reboot & Shutdown, and Diagnostics & Reports. You can specify additional rights for the individual user. ◆ Administrators—This group has all possible rights.

4. Click the **Apply** button. If your Interface script gets validated before it is saved. Once the script is saved, the main **Scripts** page displays.

To view or update a script:

1. In the Scripts table, select the script and click the **Edit Script** button. The page for editing script attributes displays.
2. Update the script attributes.
3. Click the **Apply** button.

To rename a script:

1. In the Scripts table, select the script and enter a new script name in the New Name field.
2. Click the **Rename Script** button. The script gets renamed and the **Scripts** page displays.

To delete a script:

1. In the Scripts table, select the script to delete.
2. Click the **Delete Script** button. After a confirmation, the script gets deleted and the **Scripts** page displays.

To change the permissions for a script:

1. In the Scripts table, select the script and select the new group and/or permissions.
2. Click the **Change Permissions** button. The script gets updated and the **Scripts** page displays.

To use a script at the CLI:

1. To run an Interface Script on a device port for pattern recognition and action generation, use the `connect script` <Script Name> `deviceport` <Device Port # or Name> command.
2. To run a Batch Script at the CLI with a series of CLI commands, use the `set script run cli` <Script Name> command.

Batch Script Syntax

The syntax for Batch Scripts is exactly the same as the commands that can be typed at the CLI, with the additions described in this section.

The sleep command suspends execution of the script (puts it to 'sleep') for the specified number of seconds. Syntax:

```
sleep <value>
```

Interface Script Syntax

This section describes the abbreviated scripting syntax for Interface Scripts. This limited syntax was created to prevent the creation of scripts containing potentially harmful commands. Script commands are divided into three groups: Primary, Secondary and Control Flow. Primary commands provide the basic functionality of a script and are generally the first element on a line of a script, as in:

```
send_user “Password:”
```

Secondary commands provide support for the primary commands and are generally not useful by themselves. For example, the `expr` command can be used to generate a value for a set command.

```
set <my_var> [expr 1 + 1]
```

Control Flow commands allow conditional execution of other commands based on the results of the evaluation of a Boolean expression.

Definitions

Word: A contiguous group of characters delimited on either side by spaces. Not enclosed by double quotes.

Primary Command: One of the primary commands listed in this section.

Secondary Command: One of the secondary commands defined in this section.

Quoted String: A group of characters enclosed by double quote (“) characters. A quoted string may include any characters, including space characters. If a double quote character is to be included in a quoted string it must be preceded (escaped) by a backslash character ('\').

Variable Reference: A word (as defined above) preceded by a dollar sign character ('$').

CLI Command: A quoted string containing a valid CLI 'show' command.

Arithmetic Operator: A single character representing a simple arithmetic operation. The character may be one of the following:

- A plus sign (+) representing addition
- A minus sign (-) representing subtraction
- An asterisk sign (-) representing multiplication
- A forward slash (/) representing division
- A percent sign (%) representing a modulus

Boolean Expression: An expression which evaluates to TRUE or FALSE. A Boolean expression has the following syntax:

```
<value> <Boolean operator> <value>
```

Each can be either a word or a variable reference.

Boolean Operator: A binary operator which expresses a comparison between two operands and evaluates to TRUE or FALSE. The following Boolean operators are valid:

- < less than
- > greater than
- <= less than or equal to
- >= greater than or equal to
- == equal to
- != not equal to

Primary Commands

These are stand-alone commands which provide the primary functionality in a script. These commands may rely on one or more of the Secondary Commands to provide values for some parameters. The preprocessor will require that these commands appear only as the first element of a command line. The start of a command line is delimited by any of the following:

- The start of a new line of text in the script
- A semicolon (;)
- A left brace ({)

set

The set command assigns a value to a variable. Syntax:

```
set <variable> <value>
```

where <variable> is a word, and <value> can be defined in one of the following ways:

- A quoted string
- A word
- A variable reference
- A value generated via one of the string secondary commands (compare, match, first, etc.)
- A value generated via the expr secondary command
- A value generated via the format secondary command
- A value generated via the expr timestamp command

unset

This command removes the definition of a variable within a script. Syntax:

```
unset <variable>
```

where <variable> is a word.

scan

The `scan` command is analogous to the C language scanf(). Syntax:

```
scan <variable> <format string> <value 1> <value 2>... <value n>
```

where <variable> a variable reference, and <format string> is a quoted string. Each of the <value x> elements will be a word.

sleep

The sleep command suspends execution of the script (puts it to 'sleep') for the specified number of seconds. Syntax:

```
sleep <value>
```

where <value> can be a word, a quoted string or a variable reference.

exec

The exec command executes a single CLI command. Currently only CLI 'show' commands may be executed via exec. Syntax:

```
exec <CLI command>
```

send, send_user

The send command sends output to a sub-process, The `send_user` command sends output to the standard output. Both commands have the same syntax:

```
send <string>
send_user <string>
```

where <string> can be either a quoted string or a variable reference.

expect, expect_user, expect_before, expect_after, expect_background

The `expect` command waits for input and attempts to match it against one or more patterns. If one of the patterns matches the input the corresponding (optional) command is executed. All expect commands have the same syntax:

```
expect {<string 1> {command 1} <string 2> {command 2}... <string n>
{command n}}
```

where <string x> will either be a quoted string, a variable reference or the reserved word 'timeout.' The command x is optional, but the curly braces ('{' and '}') are required. If present it must be a primary command.

return

The return command terminates execution of the script and returns an optional value to the calling environment. Syntax:

```
return <value>
```

where <value> can be a word or a variable reference.

Secondary Commands

These are commands which provide data or other support to the Primary commands. These commands are never used by themselves in a script. The preprocessor will require that these commands always follow a left square bracket ('[') character and be followed on a single line by a right bracket (']').

string

The string command provides a series of string manipulation operations. The string command will only be used with the set command to generate a value for a variable. There are nine operations provided by the string command. Syntax (varies by operation):

```
string compare <str 1> <str 2>

      Compare two strings
string match <str 1> <str 2>

      Determine if two strings are equal
string first <str needle> <str haystack>

      Find and return the index of the first occurrence of 'str_needle'
      in 'str_haystack'
string last <str needle> <str haystack>

      Find and return the index of the last occurrence of 'str_needle' in
      'str_haystack'
string length <str>

      Return the length of 'str'
string index <str> <int>

      Return the character located at position 'int' in 'str'
```

```
string range <str> <int start> <int end>

      Return a string consisting of the characters in 'str' between 'int
      start' and 'int end'
string tolower <str>

      Convert <str> to lowercase
string toupper <str>

      Convert <str> to uppercase
string trim <str 1> <str 2>

      Trim 'str 2' from 'str 1'
string trimleft <str 1> <str 2>

      Trim 'str 2' from the beginning of 'str 1'
string trimright <str 1> <str 2>

      Trim 'str 2' from the end of 'str 1'</
```

In each of the above operations, each <str *> element can either be a quoted string or a variable reference. The <int *> elements will be either words or variable references.

expr

This command evaluates an arithmetic expression and returns the result. The expr command will only be used in combination with the set command to generate a value for a variable. Syntax:

```
expr <value> <operation> <value>
```

Each <value> will be either a word or a variable reference, and <operation> an arithmetic operation.

timestamp

This command returns the current time of day as determined by the SLC console manager. The timestamp command will only be used in combination with the set command to produce the value for a variable. Syntax:

```
timestamp <format>
```

where <format> is a quoted string.

format

The `format` command is analogous to the C language sprintf(). The format command will only be used in combination with the set command to produce the value for a variable. Syntax:

```
format <format string> <value 1> <value 2>... <value n>
```

where <format string> will be a quoted string. Each of the <value x> elements will be a word, a quoted string or a variable reference.

Control Flow Commands

The control flow commands allow conditional execution of blocks of other commands. The preprocessor treats these as Primary commands, allowing them to appear anywhere in a script that a Primary command is appropriate.

while

The while command executes an associated block of commands as long as its Boolean expression evaluates to TRUE. After each iteration the Boolean expression is re-evaluated; when the Boolean expression evaluates to FALSE execution passes to the first command following the associated block. Each command within the block must be a Primary command. Syntax:

```
while (<Boolean expression>) {
      command 1
      command 2
      ...
      Command n
}
```

if, elseif and else

The if command executes an associated block of commands if its Boolean expression evaluates to TRUE. Each command within the block must be a Primary command. Syntax:

```
if (<Boolean expression>) {
      command 1
      command 2
      ...
      command n
}
```

The elseif command is used in association with an if command - it must immediately follow an if or elseif command. It executes an associated block of commands if its Boolean expression evaluates to TRUE. Each command within the block must be a Primary command. Syntax:

```
elseif (<Boolean expression>){
      command 1
      command 2
      ...
      command n
}
```

The else command is used in combination with an if or elseif command to provide a default path of execution. If the Boolean expressions for all preceding if and elseif commands evaluate to FALSE the associated block of commands is executed. Each command within the block must be a primary command. Syntax:

```
else {
      command 1
      command 2
      ...
      command n
}
```

Sample Scripts

Interface Script—Monitor Port

The Monitor Port (Monport) script connects directly to a device port by logging into the SLC port, gets the device hostname, loops a couple of times to get port interface statistics, and logs out. The following is the script:

```
set monPort 7
set monTime 5
set sleepTime 2
set prompt ">"
set login "sysadmin"
set pwd "PASS"
#Send CR to echo prompt
send "\r"
sleep $sleepTime
#Log in or check for Command Prompt
expect {
            #Did not capture "ogin" or Command Prompt
            timeout { send_user "Time out login......\r\n"; return }
            #Got login prompt
            "login" {
                send_user "Logging in....\r\n"
                send "$login\r"
                expect {
                      timeout { send_user "Time out waiting for pwd
prompt......\r\n"; return }
                      #Got password prompt
                      "password" {
   #Send Password
   send "$pwd\r"
                expect {
      timeout { send_user "Time out waiting for prompt......\r\n";
return }
      $prompt {}
                }
         }
                 }
              }
              #Already Logged in got Command Prompt
              $prompt {
               send_user "Already Logged....\r\n"
              }
}
#Get hostname info
send "show network port 1 host\r"
expect {
           timeout { send_user "Time out Getting Hostname 1\r\n"; return
}
            "Domain" {
                      #Get Hostname from slc
                      set hostname "[string range $expect_out(buffer)
         [string first Hostname: $expect_out(buffer)] [expr [string
         first Domain $expect_out(buffer)]-2]]"
            }
}
send_user "\r\n\r\n\r\n\r\n"
send_user "Device [string toupper $hostname]\r\n"
send_user
"_________________________________________________________________\r\n"
send_user "Monitored Port: Port $monPort \r\n"
send_user "Monitor Interval Time: $monTime Seconds \r\n"
set loopCtr 0
set loopMax 2
while { $loopCtr < $loopMax } {
    #Get current time
```

The following is the screen output:

```
slb247glenn]> conn script ex4 deviceport 7


login: Logging in....
sysadmin
sysadmin
Password: PASS



Welcome to the SLC Console Manager
Model Number: SLC48
For a list of commands, type 'help'.

[slc251glenn]> show network port 1 host
show network port 1 host
___Current Hostname Settings___________________________________________________
Hostname: slc251glenn
Domain: support.int.lantronix.com
[slc251glen



Device HOSTNAME: SLC251GLENN
__________________________________________________________________________
Monitored Port: Port 7
Monitor Interval Time: 5 Seconds

[Current Time:21:16:43]

show portcounter deviceport 7
n]> show portcounter deviceport 7
Device Port:                     7      Seconds since zeroed:      1453619
Bytes input:                     0      Bytes output:                    0
Framing errors:                  0      Flow control errors:             0
Overrun errors:                  0      Parity errors:                   0

[slc251glenn]>
[Current Time:21:16:58]

show portcounter deviceport 7
show portcounter deviceport 7
Device Port:                     7      Seconds since zeroed:      1453634
Bytes input:                     0      Bytes output:                    0
Framing errors:                  0      Flow control errors:             0
Overrun errors:                  0      Parity errors:                   0

[slc251glenn]>
Port Counter Monitor Script Ending......

__________________________________________________________________________
Login Out.......
logout


Returning to command line
[slb247glenn]>
```

Batch Script—SLC CLI

This script runs the following SLC CLI commands, then runs the Monport Interface script:

- show network port 1 host
- show deviceport names
- show script
- connect script monport deviceport 7

The following is the screen output of the script:

```
[slb247glenn]> se script runcli cli
[slb247glenn]> show network port 1 host
___Current Hostname Settings___________________________________________________
Hostname: slb247glenn
Domain: <none>
[slb247glenn]>
[slb247glenn]> show deviceport names
___Current Device Port Names___________________________________________________
 01 - SCS_ALIAS_Test                    05 - Port-5
 02 - Port-2                            06 - Port-6
 03 - Port-3                            07 - SLC-251
 04 - Port-4                            08 - Port-8
[slb247glenn]>
[slb247glenn]> show script
___Interface Scripts______Group/Permissions_____________________________________
getslc                    Adm/ad,nt,sv,dt,lu,ra,um,dp,pc,rs,fc,dr,sn,wb,sk,po,do
Test                      Adm/ad,nt,sv,dt,lu,ra,um,dp,pc,rs,fc,dr,sn,wb,sk,po,do
monport                   Adm/<none>
___Batch Scripts__________Group/Permissions_____________________________________
cli                       Adm/ad,nt,sv,dt,lu,ra,um,dp,pc,rs,fc,dr,sn,wb,sk,po,do
[slb247glenn]>
[slb247glenn]> connect script monport deviceport 7


login: Logging in....
sysadmin
sysadmin
Password: PASS



Welcome to the SLC Console Manager
Model Number: SLC48
For a list of commands, type 'help'.

[slc251glenn]> show network port 1 host
show network port 1 host
___Current Hostname Settings___________________________________________________
Hostname: slc251glenn
Domain: support.int.



Device HOSTNAME: SLC251GLENN
__________________________________________________________________________
Monitored Port: Port 7
Monitor Interval Time: 5 Seconds

[Current Time:21:25:04]

show portcounter deviceport 7
lantronix.com
[slc251glenn]> show portcounter deviceport 7
Device Port:                     7      Seconds since zeroed:      1454120
Bytes input:                     0      Bytes output:                    0
Framing errors:                  0      Flow control errors:             0
Overrun errors:                  0      Parity errors:                   0

[slc251glenn]>
[Current Time:21:25:20]

show portcounter deviceport 7
show portcounter deviceport 7
Device Port:                     7      Seconds since zeroed:      1454136
Bytes input:                     0      Bytes output:                    0
Framing errors:                  0      Flow control errors:             0
Overrun errors:                  0      Parity errors:                   0

[slc251glenn]>
Port Counter Monitor Script Ending......

__________________________________________________________________________
Login Out.......
logout

Returning to command line
```

9: PC Cards

This chapter describes how to configure storage by using the PC Card web page and CLI. The PC Card page can be used to configure Compact Flash storage and modem/ISDN PC cards. A Compact Flash is useful for saving and restoring configurations and for Device Port Logging (see *Device Ports – Logging on page 96*).

The SLC console manager supports a variety of Compact Flash-to-PC Card adapters, as well as modem and Basic Rate Interface (BRI) ISDN cards. See the Lantronix web site www.lantronix.com/products/pc-cards-slc.html for a complete list.

This chapter contains the following sections:

- *Set Up of PC Card Storage*
- *Modem Settings*
- *PC Card Commands*

Note: *This PC Cards chapter applies only to SLC -02 part numbers.*

Set Up of PC Card Storage

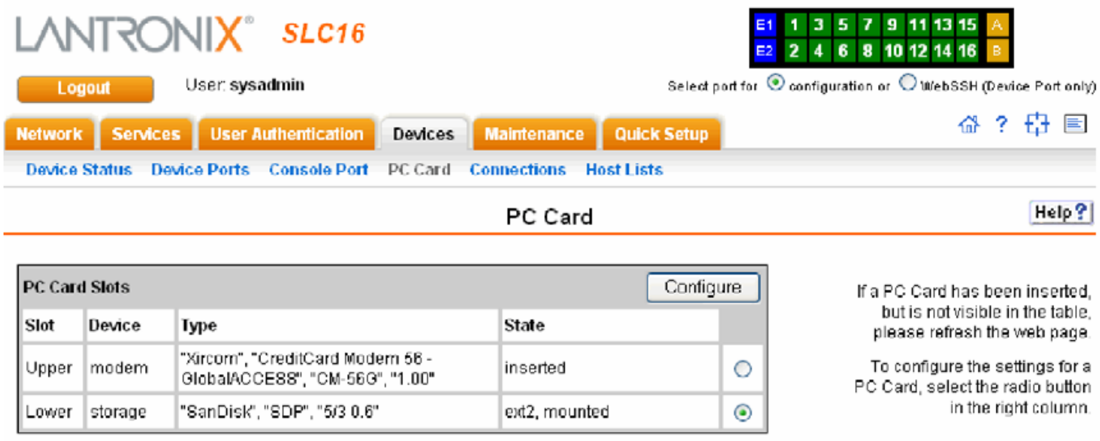
To set up PC Card storage in the SLC console manager, perform the following steps.

1. Insert any of the supported PC cards into either of the PC card bays on the front of the SLC device. You can do this before or after powering up the SLC console manager.

   If the card is a compact Flash-to-PC card adapter, and the first partition on the compact flash is formatted with a file system supported by the SLC device (ext2 and FAT), the card mounts automatically.

2. If the card does not mount automatically, or if you want to update its settings, click the **Devices** tab and select the **PC Card** option. *Figure 9-1* shows the page that displays.

Figure 9-1 PC Card Page



User: sysadmin

PC Card

PC Card Slots

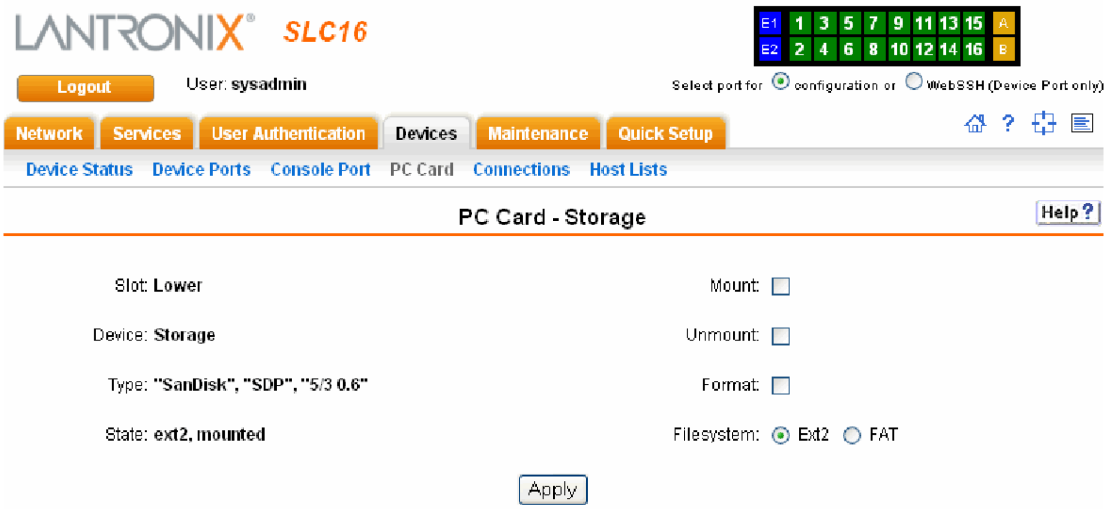
Slot	Device	Type	State	
Upper	modem	"Xircom", "CreditCard Modem 56 - GlobalACCE88", "CM-56G", "1.00"	inserted	○
Lower	storage	"SanDisk", "SDP", "5/3 0.6"	ext2, mounted	●

If a PC Card has been inserted, but is not visible in the table, please refresh the web page.

To configure the settings for a PC Card, select the radio button in the right column.

3. From the **PC Card Slots** table, click the button (on the right) for the PC card you want to configure for storage and click the **Configure** button. *Figure 9-2* shows the page that displays.

Figure 9-2 PC Card - Storage Page



Slot: Lower

Device: Storage

Type: "SanDisk", "SDP", "5/3 0.6"

State: ext2, mounted

Mount: ☐

Unmount: ☐

Format: ☐

Filesystem: ● Ext2 ○ FAT

4. Enter the following fields.

Slot (view only)	Slot on the SLC console manager where the PC Card is inserted.
Device (view only)	Type of PC Card (modem or storage).
Type (view only)	Information read from PC Card.
State (view only)	Applies to storage cards.
Mount	Click the checkbox to mount the first partition of the Compact Flash on the SLC device (if not currently mounted). Once mounted, a Compact Flash is used for device port logging and saving/restoring configurations.
Unmount	Click the checkbox to eject the compact flash from the SLC console manager after unmounting it. *Warning:* ***If you eject a Compact Flash from the SLC device without unmounting it, subsequent mounts of a PC Card Compact Flash in either slot may fail, and you will need to reboot the SLC console manager to restore PC Card functionality.***
Format	Select to unmount the Compact Flash (if it is mounted), remove all existing partitions, create one partition on the Compact Flash, format it with the selected file system (ext2 or FAT), and mount it.
Filesystem	Select ext2 or **FAT**, the file systems the SLC console manager supports.

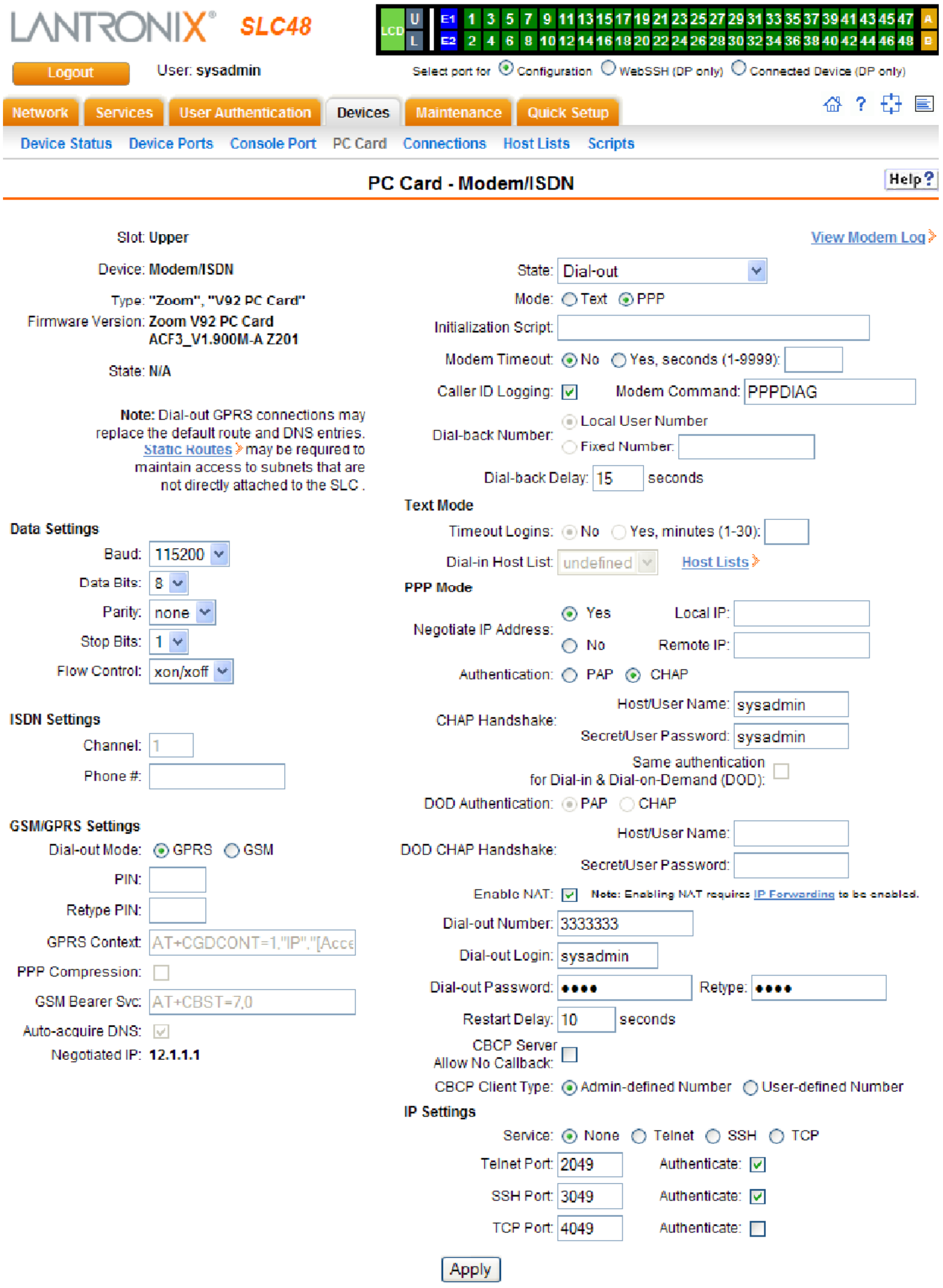
5. Click the **Apply** button.

Modem Settings

To enter modem settings for a PC card, perform the following steps.

1. Insert any of the supported modem or ISDN cards (see www.lantronix.com/slc) into one of the PC card bays on the front of the SLC device. You can do this before or after powering up the SLC console manager.
2. Click the **Devices** tab and select the **PC Card** option.
3. Click the radio button in the PC Card Slots table that shows a modem installed.
4. Click the **Configure** button. *Figure 9-3* shows the page that displays.

Figure 9-3 PC Card - Modem/ISDN Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

PC Card - Modem/ISDN

Slot: Upper

Device: Modem/ISDN

Type: "Zoom", "V92 PC Card"

Firmware Version: Zoom V92 PC Card ACF3_V1.900M-A Z201

State: N/A

Note: Dial-out GPRS connections may replace the default route and DNS entries. Static Routes may be required to maintain access to subnets that are not directly attached to the SLC .

Data Settings

Baud: 115200

Data Bits: 8

Parity: none

Stop Bits: 1

Flow Control: xon/xoff

ISDN Settings

Channel: 1

Phone #:

GSM/GPRS Settings

Dial-out Mode: ● GPRS ○ GSM

PIN:

Retype PIN:

GPRS Context: AT+CGDCONT=1,"IP","[Acce

PPP Compression: □

GSM Bearer Svc: AT+CBST=7,0

Auto-acquire DNS: ☑

Negotiated IP: **12.1.1.1**

State: Dial-out

Mode: ○ Text ● PPP

Initialization Script:

Modem Timeout: ● No ○ Yes, seconds (1-9999):

Caller ID Logging: ☑ Modem Command: PPPDIAG

Dial-back Number: ● Local User Number ○ Fixed Number:

Dial-back Delay: 15 seconds

Text Mode

Timeout Logins: ● No ○ Yes, minutes (1-30):

Dial-in Host List: undefined Host Lists

PPP Mode

Negotiate IP Address: ● Yes Local IP: ○ No Remote IP:

Authentication: ○ PAP ● CHAP

CHAP Handshake: Host/User Name: sysadmin Secret/User Password: sysadmin

Same authentication for Dial-in & Dial-on-Demand (DOD): □

DOD Authentication: ● PAP ○ CHAP

DOD CHAP Handshake: Host/User Name: Secret/User Password:

Enable NAT: ☑ **Note: Enabling NAT requires IP Forwarding to be enabled.**

Dial-out Number: 3333333

Dial-out Login: sysadmin

Dial-out Password: •••• Retype: ••••

Restart Delay: 10 seconds

CBCP Server Allow No Callback: □

CBCP Client Type: ● Admin-defined Number ○ User-defined Number

IP Settings

Service: ● None ○ Telnet ○ SSH ○ TCP

Telnet Port: 2049 Authenticate: ☑

SSH Port: 3049 Authenticate: ☑

TCP Port: 4049 Authenticate: □

5. Enter the following fields.

Slot (view only)	Displays the slot position.
Device (view only)	Displays the device type.
Type (view only)	Displays the card type.
Firmware Version (view only)	Displays the current firmware version.
State (view only)	Displays the state of the device.
State	Enables the modem to use dial-out, dial-in, dial-back, CBCP server, CBCP client, dial-on-demand, or dial in & dial-on-demand. Disabled by default. For more information on CBCP server and client, see *Modem State Parameters on page 277*.
Mode	Enables the format in which the data flows back and forth. With Text selected, the SLC console manager assumes that the modem will be used for remotely logging into the command line. Text mode is only for dialing in. This is the default. PPP establishes an IP-based link over the modem. PPP connections can be used in dial-out mode (e.g., the SLC device connects to an external network) or dial-in mode (e.g., the external computer connects to the network that the SLC console manager is part of), dial-back (dial-in followed by dial-out), CBCP server and CBCP client. For ISDN cards, only PPP connections are allowed.
Initialization Script	Sends commands to the modem. You can configure the modem to have up to 100 characters. Consult your modem documentation for recommended initialization options. If you do not specify an initialization script, the SLC device uses a uses a default initialization string of AT S7=45 SO=0 L1 V1 X4 &D2 &c1 E1 Q0. *Note: We recommend that the modem initialization script always be prepended with AT and include E1 V1 x4 Q0 so that the SLC console manager may properly control the modem.*
Modem Timeout	Timeout for modem connections. Select Yes (default) for the SLC device to terminate the connection if no traffic is received during the configured idle time. Enter a value of from 1 to 9999 seconds.
Caller ID Logging	Select to enable the SLC console manager to log caller IDs on incoming calls. Disabled by default. *Note: For the Caller ID AT command, refer to your Modem User Guide.*
Modem Command	Modem AT command used to initiate caller ID logging by the modem. *Note: For the AT command, refer to your Modem User Guide.*
Dial-back Number	Users with dial-back access can dial into the SLC device and enter their login and password. Once the SLC console manager authenticates them, the modem hangs up and dials them back. Select the phone number the modem dials back on--a fixed number or a number associated with their login. If you select Fixed **Number**, enter the number (in the format 2123456789).

Dial-back Delay	For dial-back and CBCP Server, the number of seconds between the dial-in and dial-out portions of the dialing sequence. For more information about CBCP, see *Modem State Parameters on page 277.*

Data Settings

Baud	The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use **9600** for the administration port, so this is the default. Check the equipment settings and documentation for the proper baud rate.
Data Bits	Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is **8** data bits.
Parity	Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is **none**.
Stop Bits	The number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is **1**.
Flow Control	A method of preventing buffer overflow and loss of data. The available methods include none, xon/xoff (software), and RTS/CTS (hardware). The default is **none**.

ISDN Settings

Note: *These fields are disabled if the PC Card inserted is not an ISDN card.*

Channel	Select to indicate which B channel on the ISDN card to use. Valid values are 1 and 2. (The B-channel is the channel that carries the main data.) Only one 64K channel can be used at a time.
Phone Number	Phone number associated with the B channel. May have up to 20 characters. Any format is acceptable.

GSM/GPRS Settings

These settings are only active when a GSM/GPRS PC card modem is in the appropriate slot.

Notes:

- *Please consult your wireless carrier configuration requirements for more detailed information.*
- *Dial-out GPRS connections may replace the default route and DNS entries. Static routes may be required to maintain access to subnets that are not directly attached to the SLC console manager. Click the **Static Routes** link (above **Data Settings**) to configure a static route. (See Routing on page 58.)*

Dial-out Mode	Select the type of dial-out connection: **GPRS:** (General Packet Radio Service) **GSM:** (Global System for Mobile communication)
PIN **Retype PIN**	PIN (personal identification number) for accessing the GSM/GPRS card.

GPRS Context	Command to specify the protocol data packet (PDP) context parameter values.
PPP Compression	Select to enable negotiation of data compression over PPP links. Disabled by default.
GSM Bearer Svc.	Command to select the bearer service, data rate, and connection element to use when data call originate.
Auto-acquire DNS	Select to enable the SLC console manager to acquire up to three DNS servers by means of GPRS. Enabled by default.
Negotiated IP	IP address associated with the GPRS connection.

Text Mode

Timeout Logins	If you selected **Text** mode, you can enable logins to time out after the connection is inactive for a specified number of minutes. The default is **No**. This setting only applies to text mode connections. **PPP** mode connections stay connected until either side drops the connection. Disabled by default.
Dial-in Host List	From the drop-down list, select the desired host list. The host list is a prioritized list of SSH, Telnet and TCP hosts that are available for establishing outgoing modem connections. The hosts in the list are cycled through until the modem successfully connects to one. To establish and configure host lists, click the **Host Lists** link. See *Hostname & Name Servers on page 52.*

PPP Mode

Negotiate IP Address	If the SLC device and/or the serial device have dynamic IP addresses (e.g., IP addresses assigned by a DHCP server), select **Yes**. This is the default. If the SLC console manager or the modem have fixed IP addresses, select **No,** and enter the **Local IP** (IP address of the port) and **Remote IP** (IP address of the modem).
Authentication	Enables **PAP** or **CHAP** authentication for modem logins. **PAP** is the default. With PAP, users are authenticated by means of the Local Users and any of the remote authentication methods that are enabled. With CHAP, the **CHAP Handshake** fields authenticate the user.
CHAP Handshake	The host/username (for UNIX systems) or secret/user password (for Windows systems) used for CHAP authentication. May have up to 128 characters.
Same authentication for Dial-in & Dial-on-Demand (DOD)	Select this option to let incoming connections (dial-in) use the same authentication settings as outgoing connections (dial-on-demand). If this option is not selected, then the dial-on-demand connections take their authentication settings from the DOD parameter settings. If **DOD Authentication** is PAP, then the **DOD CHAP Handshake** field is not used.
DOD Authentication	Enables **PAP** or **CHAP** authentication for dial-in & dial-on-demand. **PAP** is the default. With PAP, users are authenticated by means of the Local Users and any of the remote authentication methods that are enabled. With CHAP, the **DOD CHAP Handshake** fields authenticate the user.
DOD CHAP Handshake	For **DOD Authentication**, enter the host/username for UNIX systems) or secret/user password (for Windows systems) used for CHAP authentication. May have up to 128 characters.

Enable NAT	Select to enable Network Address Translation (NAT) for dial-in and dial-out PPP connections on a per modem (Device Port or PC Card) basis. Users dialing into the SLC console manager access the network connected to Eth1 and/or Eth2. ***Note:*** *IP forwarding must be enabled on the Network - Settings page for NAT to work. To enable, click the **IP Forwarding** link to display the Network Settings page.*
Dial-out Number	Phone number for dialing out to a remote system or serial device. May have up to 20 characters. Any format is acceptable.
Dial-out Login	User ID for dialing out to a remote system. May have up to 32 characters.
Dial-out Password and Retype	Password for dialing out to a remote system. May have up to 64 characters.
Restart Delay	The number of seconds after the timeout and before the SLC console manager attempts another connection. The default is **30** seconds.
CBCP Server Allow No Callback	For CBCP Server state, allows “No Callback” as an option in the CBCP handshake in addition to User-defined Number and Admin-defined Number. For more information about CBCP, see *Modem State Parameters on page 277.*
CBCP Client Type	For CBCP Client, this selects the number that the client would like to use for callback - either a user-defined number passed to the server (specified by the Fixed Dial-back Number) or an administrator-defined number determined by the server based on the login that is PAP or CHAP authenticated. For more information about CBCP, see *Modem State Parameters on page 277.*

IP Settings

Service	The available connection services for the modem port. Check Telnet, SSH, or TCP to enable. Only one can be active at a time. The default is **None**.
Telnet Port	Telnet session port number to use if you selected **Telnet**. Defaults: ◆ Upper PC Card Slot: **2049** ◆ Lower PC Card Slot: **2050** ◆ Range: **1025-65535** ◆ **Authenticate**: Checkbox and if selected, the SLC console manager requires user authentication before granting access to the port. **Authenticate** is selected by default for **Telnet Port** and **SSH Port,** but not for **TCP Port**.
SSH Port	The SSH session port number to use if you selected **SSH**. Defaults: ◆ Upper PC Card Slot: **3049** ◆ Lower PC Card Slot: **3050** ◆ Range: **1025-65535** ◆ **Authenticate**: Checkbox and if selected, the SLC device requires user authentication before granting access to the port. **Authenticate** is selected by default for **Telnet Port** and **SSH Port,** but not for **TCP Port**.
TCP Port	The TCP (raw) session port number to use if you selected **TCP**. Defaults: ◆ Upper PC Card Slot: **4049** ◆ Lower PC Card Slot: **4050** ◆ Range: **1025-65535** ◆ **Authenticate**: Checkbox and if selected, the SLC console manager requires user authentication before granting access to the port. **Authenticate** is selected by default for **Telnet Port** and **SSH Port,** but not for **TCP Port**.

6. Click the **Apply** button.

To view the log of all modem activity:

1. Click the **View Modem Log** link.

PC Card Commands

The following CLI commands correspond to the PC Card. For more information, see *Chapter 15: Command Reference* .

- *pccard storage copy (on page 246)*
- *pccard storage delete (on page 246)*
- *pccard storage dir (on page 246)*
- *pccard storage format (on page 247)*
- *pccard storage mount (on page 247)*
- *pccard storage rename (on page 247)*
- *pccard storage unmount (on page 247)*
- *show pccard storage (on page 247)*
- *pccard modem (on page 245)*
- *show pccard modem (on page 248)*
- *show pccard (on page 247)*
- *set log clear modem (on page 238)*
- *set log modem pppdebug (on page 239)*
- *show log modem (on page 239)*

10: USB Port

This chapter describes how to configure storage by using the USB web page and CLI. The USB web page can be used to configure the thumb drive and modems. The thumb drive is useful for saving and restoring configurations and for Device Port Logging (see *Device Ports – Logging on page 96*).

The SLC console manager supports a variety of thumb drives and modems. See the Lantronix web site for a complete list.

Note: *This USB port chapter applies only to SLC models with part numbers -03.*

This chapter describes the Web Manager pages and available CLI commands that configure the SLC USB. For information about quick setup, installation, services, device ports, connections, user authentication, and maintenance tasks, see those chapters.

This chapter contains the following sections:

- *Set Up of USB Storage*
- *Manage Firmware and Configuration Files*

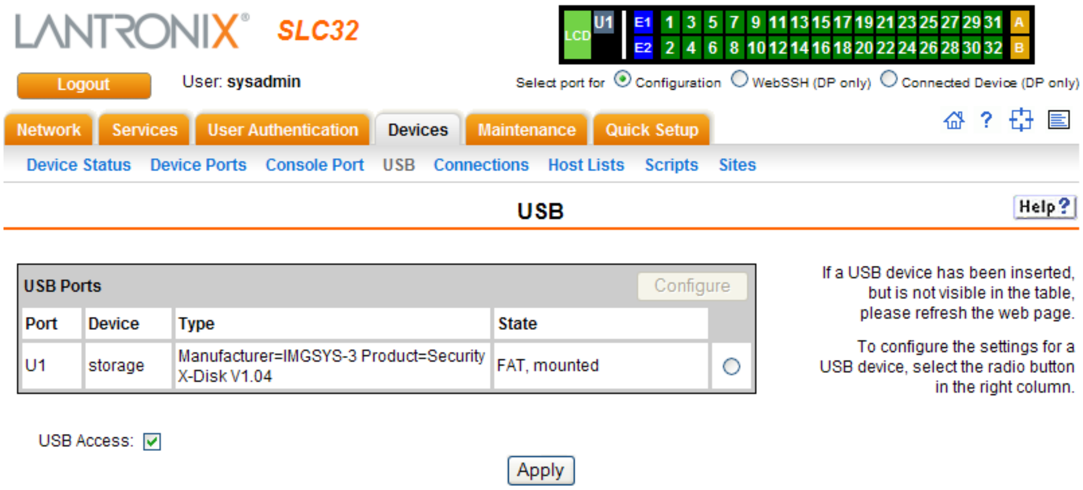
Set Up of USB Storage

The USB page has an USB Access checkbox. USB Access is a security feature ensures that access to any USB device is disabled if the box is unchecked. The SLC console manager ignores any USB device plugged into the port.

To set up USB storage in the SLC device, perform the following steps.

1. Insert any of the supported thumb drives into the USB port on the front of the SLC console manager. You can do this before or after powering up the SLC device.
2. Log into the SLC console manager and click **Devices**.
3. Click **USB**. *Figure 10-1* shows the page that displays. Your USB device should display if you have inserted it. If is does not display and you have inserted it, refresh the web page.

Figure 10-1 USB Main Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

USB

USB Ports

Port	Device	Type	State	
U1	storage	Manufacturer=IMGSYS-3 Product=Security X-Disk V1.04	FAT, mounted	○

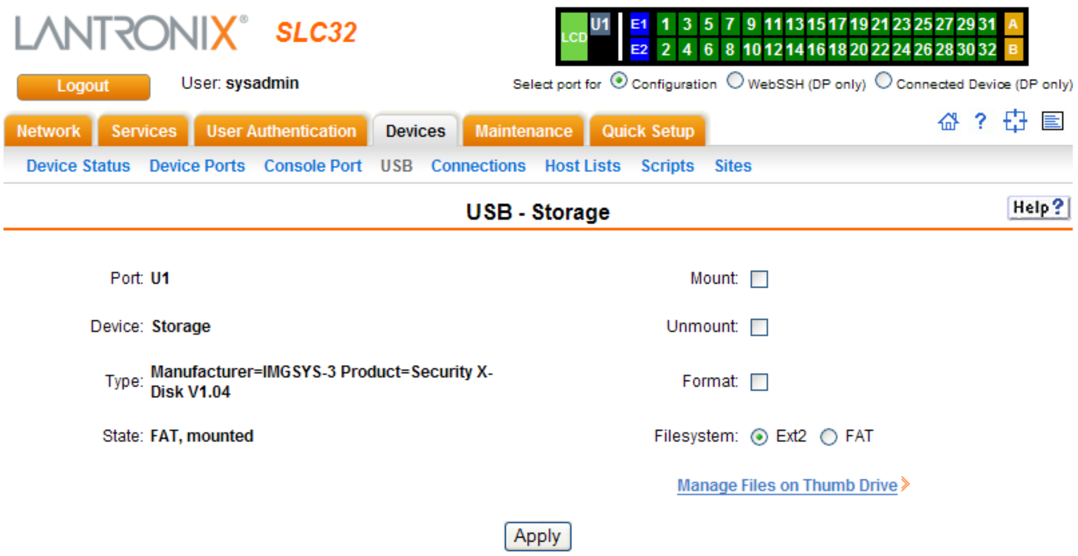
If a USB device has been inserted, but is not visible in the table, please refresh the web page.

To configure the settings for a USB device, select the radio button in the right column.

USB Access: ☑

4. To configure the USB port, from the **USB Ports** table, click the radio button (on the far right) for Port U1.
5. Click **Configure**. *Figure 10-2* shows the page that displays.

Figure 10-2 USB - Storage Page



USB - Storage

Port: U1

Device: Storage

Type: Manufacturer=IMGSYS-3 Product=Security X-Disk V1.04

State: FAT, mounted

Mount: □

Unmount: □

Format: □

Filesystem: ● Ext2 ○ FAT

Manage Files on Thumb Drive

Apply

6. Enter the following fields.

Port (view only)	Slot on the SLC console manager for the USB device.
Device (view only)	Type of device (modem or storage).
Type (view only)	Information read from USB device.
State (view only)	Applies to USB device.
Mount	Enables the first partition of the USB device (if not currently mounted). Once mounted, a device is used for device port logging and for saving/restoring configurations.
Unmount	Enables ejecting the USB device. ***Warning:* *If you eject a USB device from the SLC console manager without unmounting it, subsequent mounts may fail, and you will need to reboot the SLC device to restore the functionality.***
Format	Select to: ◆ Unmount the USB device (if it is mounted) ◆ Remove all existing partitions ◆ Create one partition ◆ Format it with the selected file system (ext2 or FAT) ◆ Mount the USB device
Filesystem	Select ext2 or **FAT**, the file systems the SLC console manager supports.

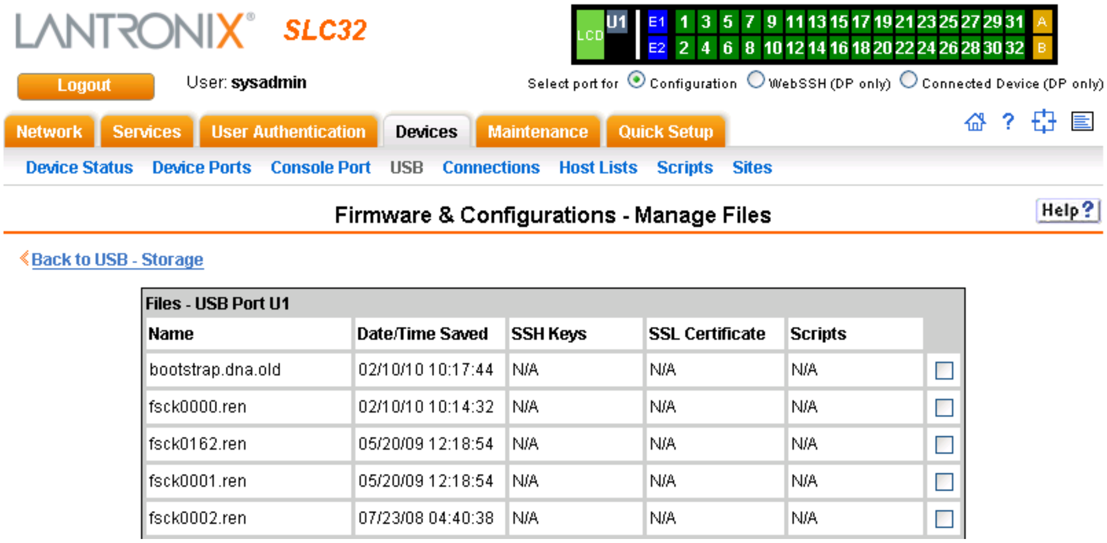
7. Click **Apply**.

Manage Firmware and Configuration Files

To manage the firmware and configuration files, perform the following steps.

1. Click the **Manage Files on the Thumb Drive** link on the **USB - Storage** page.

Figure 10-3 Firmware and Configurations - Manage Files (Top of Page)



LANTRONIX
SLC32
LCD U1 E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 B
Logout
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network Services User Authentication Devices Maintenance Quick Setup
Device Status Device Ports Console Port USB Connections Host Lists Scripts Sites
Help?

User: sysadmin

Firmware & Configurations - Manage Files

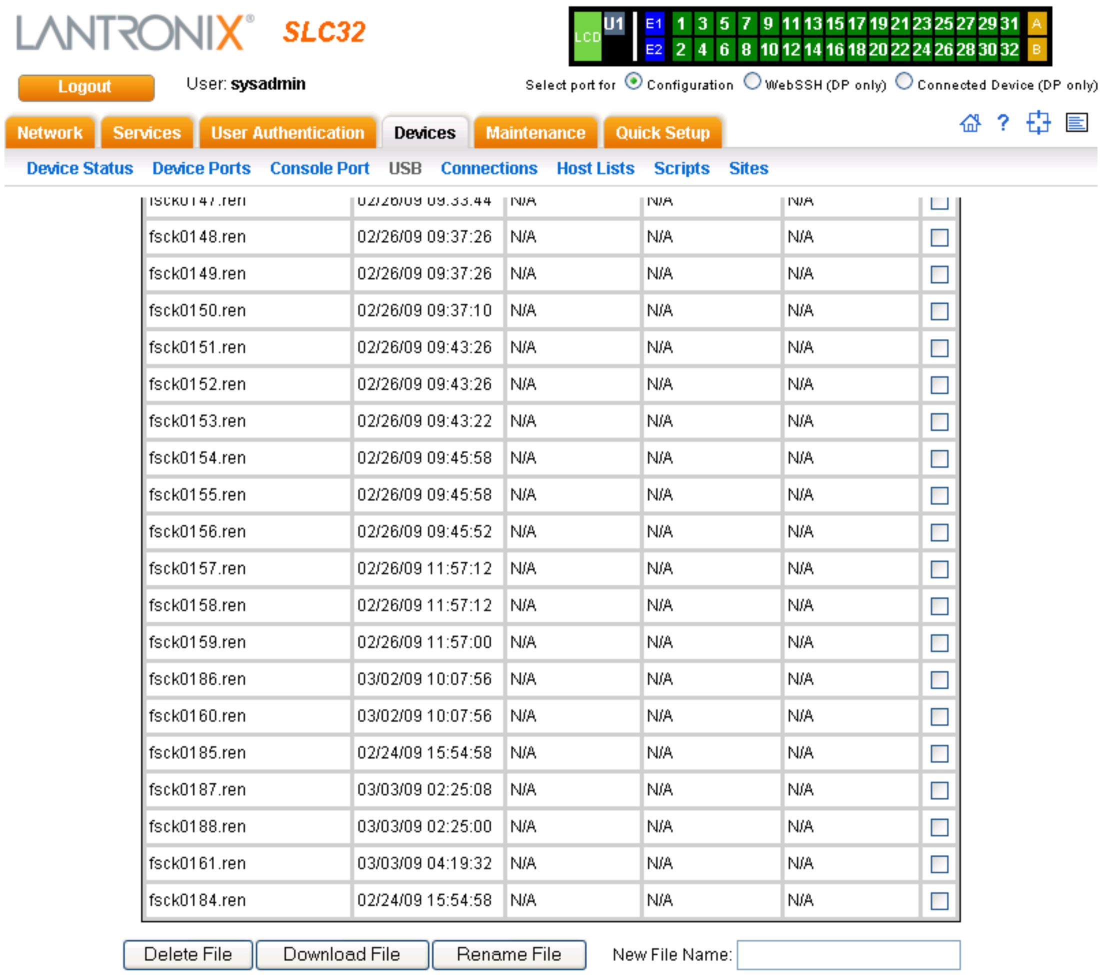
Back to USB - Storage

Files - USB Port U1

Name	Date/Time Saved	SSH Keys	SSL Certificate	Scripts	
bootstrap.dna.old	02/10/10 10:17:44	N/A	N/A	N/A	□
fsck0000.ren	02/10/10 10:14:32	N/A	N/A	N/A	□
fsck0162.ren	05/20/09 12:18:54	N/A	N/A	N/A	□
fsck0001.ren	05/20/09 12:18:54	N/A	N/A	N/A	□
fsck0002.ren	07/23/08 04:40:38	N/A	N/A	N/A	□

Note: *At the bottom of the page, shown in Figure 10-4, are the **Delete**, **Download**, and **Rename** options.*

Figure 10-4 Firmware and Configurations - Manage Files (Bottom of Page)


LANTRONIX
SLC32
LCD U1
E1 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 A
E2 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 B
Logout
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network Services User Authentication Devices Maintenance Quick Setup
Device Status Device Ports Console Port USB Connections Host Lists Scripts Sites
Delete File
Download File
Rename File
New File Name:

User: sysadmin

fsck0147.ren	02/26/09 09:33:44	N/A	N/A	N/A	□
fsck0148.ren	02/26/09 09:37:26	N/A	N/A	N/A	□
fsck0149.ren	02/26/09 09:37:26	N/A	N/A	N/A	□
fsck0150.ren	02/26/09 09:37:10	N/A	N/A	N/A	□
fsck0151.ren	02/26/09 09:43:26	N/A	N/A	N/A	□
fsck0152.ren	02/26/09 09:43:26	N/A	N/A	N/A	□
fsck0153.ren	02/26/09 09:43:22	N/A	N/A	N/A	□
fsck0154.ren	02/26/09 09:45:58	N/A	N/A	N/A	□
fsck0155.ren	02/26/09 09:45:58	N/A	N/A	N/A	□
fsck0156.ren	02/26/09 09:45:52	N/A	N/A	N/A	□
fsck0157.ren	02/26/09 11:57:12	N/A	N/A	N/A	□
fsck0158.ren	02/26/09 11:57:12	N/A	N/A	N/A	□
fsck0159.ren	02/26/09 11:57:00	N/A	N/A	N/A	□
fsck0186.ren	03/02/09 10:07:56	N/A	N/A	N/A	□
fsck0160.ren	03/02/09 10:07:56	N/A	N/A	N/A	□
fsck0185.ren	02/24/09 15:54:58	N/A	N/A	N/A	□
fsck0187.ren	03/03/09 02:25:08	N/A	N/A	N/A	□
fsck0188.ren	03/03/09 02:25:00	N/A	N/A	N/A	□
fsck0161.ren	03/03/09 04:19:32	N/A	N/A	N/A	□
fsck0184.ren	02/24/09 15:54:58	N/A	N/A	N/A	□

2. To delete a file, click the check box next to the filename and click **Delete File**. A confirmation message displays.
3. To download a file, click the **Download** button. Select the file from the list.
4. To rename a file, click the check box next to the filename and enter a new name in the **New File Name:** box. Click **Rename File**.

USB Commands

The following CLI commands correspond to the USB port. For more information, see *Chapter 15: Command Reference* .

- *set usb access (on page 259)*
- *set usb modem (on page 259)*
- *set usb storage mount (on page 261)*
- *set usb storage unmount (on page 261)*
- *set usb storage dir (on page 260)*
- *set usb storage rename (on page 260)*
- *set usb storage copy (on page 261)*

- *set usb storage delete (on page 261)*
- *set usb storage format (on page 261)*
- *show usb (on page 261)*
- *show usb storage (on page 262)*
- *show usb modem (on page 262)*

11: Connections

This chapter describes how to use the Connections web page to connect external devices and outbound network connections, such as Telnet or SSH, in various configurations. For information about how to configure devices to interact with an SLC device port connected to an external device, see *Chapter 8: Devices*.

This chapter contains the following sections:

- *Types of Endpoints and Connections*
- *Typical Configurations of SLC Connections*
- *Connection Configuration*

Types of Endpoints and Connections

An SLC device port attached to an external device can be connected to one of the following endpoint types:

- Another device port attached to an external device
- Another device port with a modem attached
- An outgoing Telnet or SSH session
- An outgoing TCP or UDP network connection

  You can set up connections such as those described below in *Typical Configurations of SLC Connections*.

You can establish the following types of connections:

- Immediately and always after reboot.
- At a specified date and time. These connections connect if the date and time have already passed.
- After a specified amount of data or a specified sequence of data passes through the connection. Following reboot, the connection is not reestablished until the specified data passes through the connection.

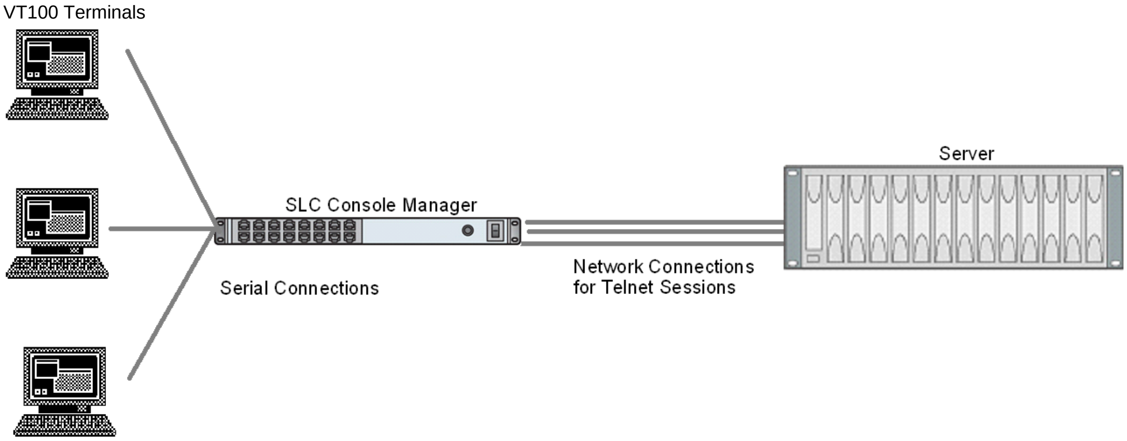
Typical Configurations of SLC Connections

The following configurations are typical.

Terminal Server

Figure 11-1 shows the SLC console manager as a multiplexer of serial data to a single server computer. Terminal devices are connected to the serial ports of the SLC device are configured as a **Device Port to Telnet out** type connection on the Connections page. The users of the terminals can access the server as if they were connected directly to it by local serial ports or a console.

Figure 11-1 Terminal Server

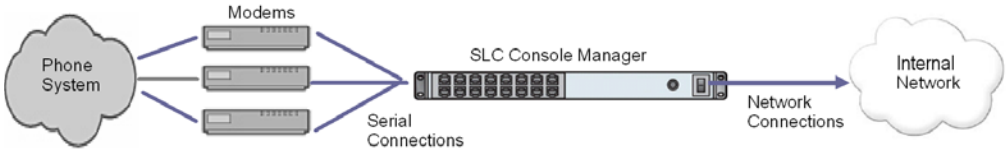


Remote Access Server

Figure 11-2 shows the SLC console manager connected to one or more modems by its device ports. Configure the device ports on the Device Ports - Settings web page by selecting the Dial-in option in the Modem Settings section.

Most customers use the modems in PPP mode to establish an IP connection to the SLC device and either Telnet or SSH into the SLC. They could also select text mode where, using a terminal emulation program, a user could dial into the SLC console manager and connect to the command line interface.

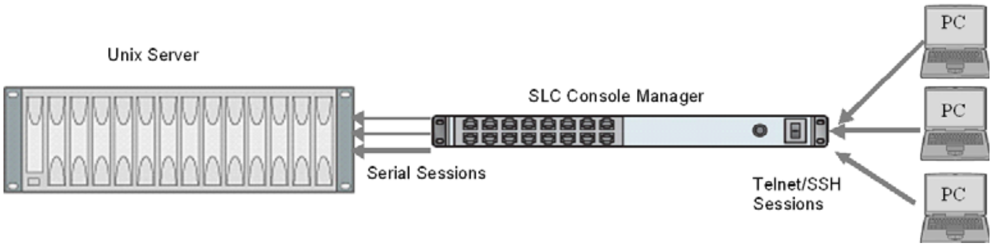
Figure 11-2 Remote Access Server



Reverse Terminal Server

Figure 11-3 shows the SLC device with one or more device ports connected to one or more serial ports of a mainframe server. Users can access a terminal session by establishing a Telnet or SSH session to the SLC console manager. To configure the SLC device, select the **Enable Telnet In** or **Enable SSH In** option on the **Device Ports – Settings** page.

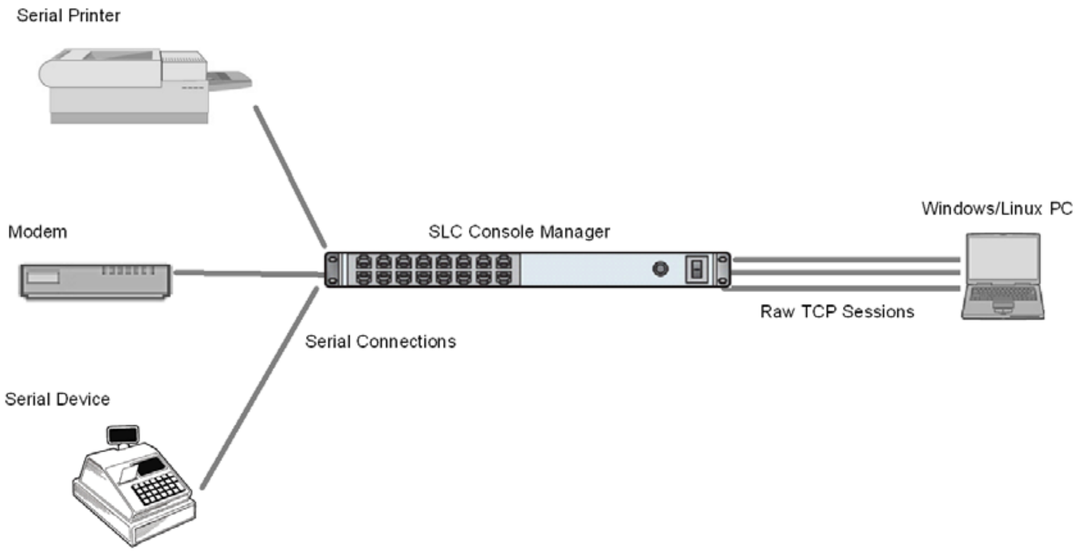
Figure 11-3 Reverse Terminal Server



Multiport Device Server

Figure 11-4 shows a PC connected to the device ports on the SLC console manager as virtual serial ports, enabling the ports to act as if they are local ports to the PC. Configure the SLC device for this setup by using special software, for example, Com Port Redirector (available on www.lantronix.com) or similar software.

Figure 11-4 Multiport Device Server



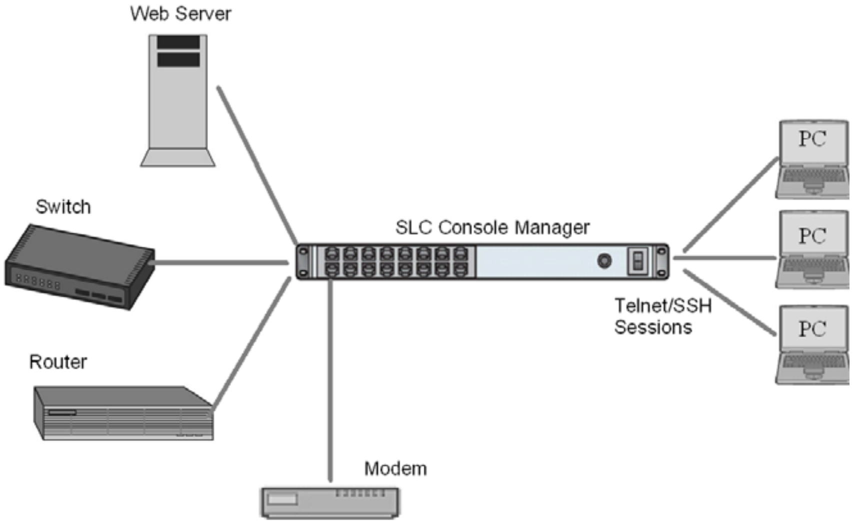
Console Server

Figure 11-5 shows the SLC console manager configured to manage a number of servers or network equipment using console ports. The SLC device device ports connect to the console ports of the server or equipment.

To manage a specific device, you can Telnet or SSH to a specific port or IP address on the SLC console manager and connect directly to the console port of the server or device.

Set the **Enable Telnet In** or **Enable SSH In** option on SLC device from the **Device Ports – Settings** page for the device port. You can implement an extra remote management capability by adding a modem to one of the device ports and setting the **Dial-in** option in the **Modem Settings** section of the **Device Ports – Settings** page. This enable you to dial into the SLC console manager using another modem and terminal emulation program at a remote location.

Figure 11-5 Console Server

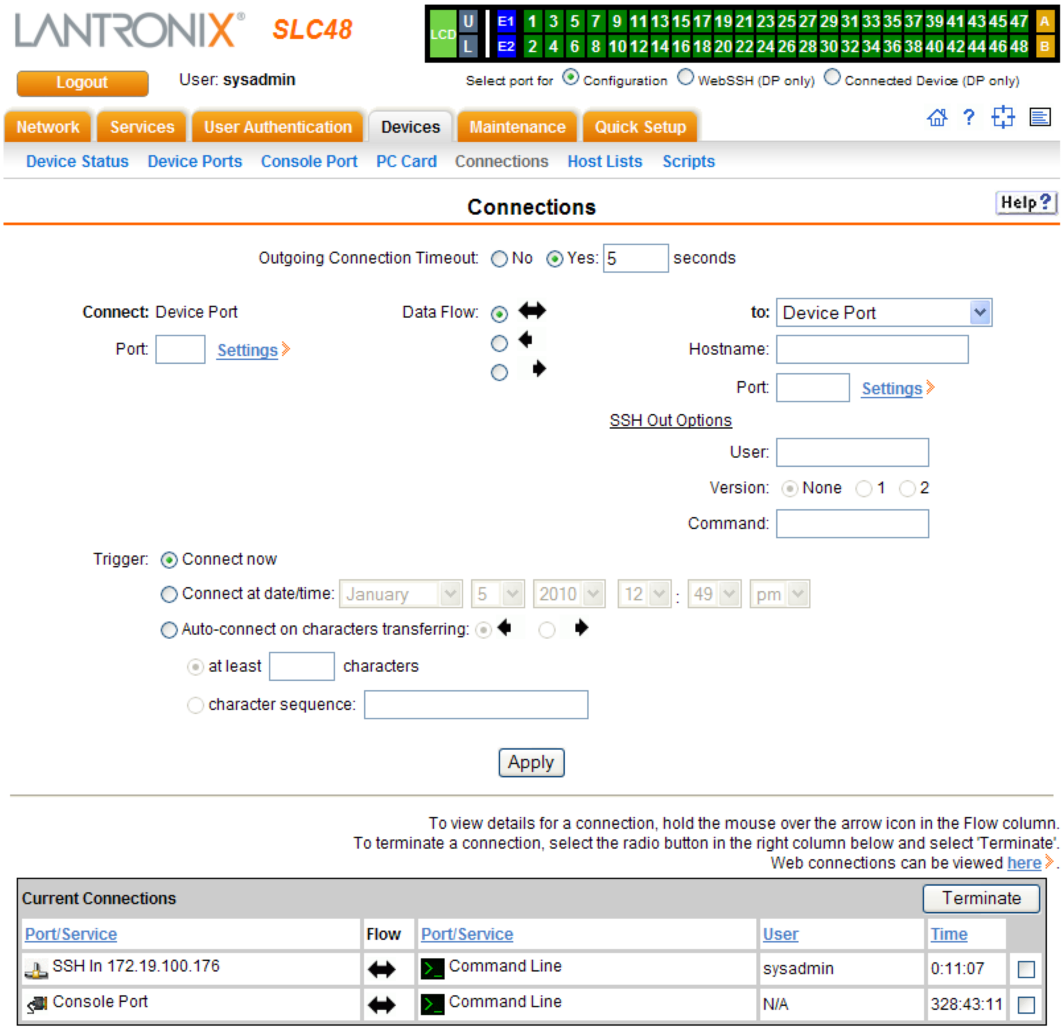


Connection Configuration

To create a connection:

1. Click the **Devices** tab and **Connections**. *Figure 11-6* shows the page that displays.

Figure 11-6 Connections Page


LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network Services User Authentication Devices Maintenance Quick Setup
Device Status Device Ports Console Port PC Card Connections Host Lists Scripts
Help ?
Settings
SSH Out Options
Apply
Terminate

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Connections

Outgoing Connection Timeout: ○ No ● Yes: 5 seconds

Connect: Device Port

Port: Settings

Data Flow: ● ⬌ ○ ◀ ○ ▶

to: Device Port

Hostname:

Port: Settings

SSH Out Options

User:

Version: ● None ○ 1 ○ 2

Command:

Trigger: ● Connect now

○ Connect at date/time: January 5 2010 12 : 49 pm

○ Auto-connect on characters transferring: ● ◀ ○ ▶

● at least characters

○ character sequence:

Apply

To view details for a connection, hold the mouse over the arrow icon in the Flow column.
To terminate a connection, select the radio button in the right column below and select 'Terminate'.
Web connections can be viewed here.

Current Connections

Port/Service	Flow	Port/Service	User	Time	
SSH In 172.19.100.176	⬌	Command Line	sysadmin	0:11:07	□
Console Port	⬌	Command Line	N/A	328:43:11	□

2. Enter the following fields.

Outgoing Connection Timeout	Enable an outgoing timeout by clicking the **Yes** radio button and specifying the seconds. The range is 1 to 9999 seconds. The default is 5 seconds.

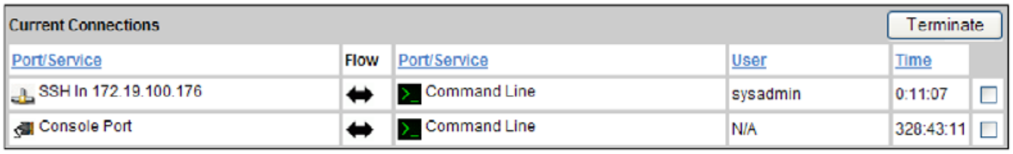
Connect: DevicePort	Input the port number that you are connecting. The device port must be connected to an external serial device and must *not* have command line interface logins enabled, be connected to a modem, or be running a loopback test. ***Note:*** *To see the current settings for this device port, click the **Settings** link.*
Data Flow	Select the arrow showing the direction (bidirectional or unidirectional) the data will flow in relationship to the device port you are connecting.
to	Select a destination for the connection from the drop-down list as follows: ◆ Device port connected to a serial device ◆ Device port connected to a modem ◆ Outbound network connection (Telnet, SSH, TCP Port, or UDP Port). ***Note:*** *To see the current settings for a selected device port, click the **Settings** link.*
Hostname	Input the host name or IP Address of the destination. This entry is required if the **to** field is set to Telnet out, SSH out, TCP port, or UDP port.
Port	Enter the device port number, if the **to** field is set to **Device Port** or **Modem on Device Port**. For all other options, this is the TCP/UDP port number, which is optional for Telnet out and SSH out, but required for TCP Port and UDP Port. **Notes:** ◆ *If you select **Device Port,** it must not have command line interface logins enabled or be running a loopback test.* ◆ *To view the device port's settings, click the **Settings** link to the right of the port number.*
SSH Out Options	Select one of the following optional flags to use for the SSH connection. ◆ **User:** Login ID to use for authenticating on the remote host. ◆ **Version:** Version of SSH. Select **1** or **2**. ◆ **Command:** Enter a specific command on the remote host (for example, `reboot`).
Trigger	Select the condition that will trigger a connection. Options include: ◆ **Connect now**: Connects immediately, or if you reboot the SLC console manager, immediately on reboot. ◆ **Connect at date/time**: Connects at a specified date and time. Use the drop-down lists to complete the date and time. Upon rebooting, the SLC device reestablishes the connection if the date/time has passed. ◆ **Auto-connect on characters transferring**: Select the arrow indicating the direction of the data transfer and either the minimum number of characters or a specific character sequence that will trigger the connection. You can select the direction of the data transfer only if **Data Flow** is bidirectional. Upon rebooting, the SLC console manager does not reestablish the connection until the specified data has passed through one of the endpoints of the connection.

3. Click the **Apply** button.

To view, update, or disconnect a current connection:

The bottom of the **Connections** page displays current connections as shown in *Figure 11-7*.

Figure 11-7 Current Connections Section of the Connections Page



Current Connections

Port/Service	Flow	Port/Service	User	Time	
SSH In 172.19.100.176	↔	Command Line	sysadmin	0:11:07	□
Console Port	↔	Command Line	N/A	328:43:11	□

To view details about a connection:

1. Hold the mouse over the arrow in the **Flow** column.

To disconnect/delete one or more connections:

1. Select one or more connections in the **Select** column and click the **Terminate** buttons.

To reestablish the connection:

1. Create the connection again in the top part of the page.

To view information about Web connections:

1. Click the **here** link in the text above the table. The **Firmware & Configurations - Web Sessions** page displays.

Connection Commands

The following CLI commands correspond to the **Connections** page. For more information, see 15: Command Reference.

- *connect direct (on page 216)*
- *connect global outgoingtimeout (on page 217)*
- *connect listen (on page 217)*
- *connect bidirection (on page 216)*
- *connect unidirection (on page 218)*
- *connect terminate (on page 217)*
- *show connections (on page 218)*
- *show connections connid (on page 218)*
- *connect global show (on page 217)*

12: User Authentication

This chapter describes authentication methods for users who attempt to log into the SLC console manager by Telnet, SSH, the console port, or one of the device ports. It includes descriptions of user rights, NIS, LDAP, RADIUS, Kerberos, and TACACS+ options.

The chapter contains the following sections:

- *Overview of Authentication*
- *User Rights*
- *Authentication Methods*
- *Local and Remote Users*
- *Local/Remote User Settings*
- *NIS*
- *LDAP*
- *RADIUS*
- *Kerberos*
- *TACACS+*
- *SSH Keys*
- *Custom User Menus*

Note: *The features and functionality described in this chapter specific to PC Card use are supported on SLC -02 part numbers. The features and functionality specific to USB port use are supported on SLC -03 part numbers.*

Overview of Authentication

The **User Authentication** tab enables you to assign the order in which the SLC console manager uses the authentication methods. The local/remote user authentication is the default and the first method the SLC device uses to authenticate users. You can disable local/remote user authentication or assign it a lower precedence.

Note: *Regardless of whether local/remote user authentication is enabled, the local/remote user sysadmin account is always available for login.*

Authentication occurs in the order of precedence until a successful authentication is obtained or by using the first authentication method that responds. If the server is down, the first responding authentication is used.

If you have the same username defined in multiple authentication methods, the result is unknown. For example, there is an LDAP user named “joe” and an NIS user named “joe” so the order of authentication is:

1. Local Users
2. LDAP
3. NIS

User “joe” tries to login. Because there is an LDAP user named “joe,” the SLC console manager tries to authenticate that user by using the LDAP password first. If that login fails, then the SLC device may or may not try to authenticate the user by using the NIS password.

User Rights

The SLC console manager has three default user groups: Administrators, Power Users, and Default Users. Each has a predefined set of rights; users inherit rights from the user group to which they belong. These rights are in addition to the current functions that a user can perform at the CLI.

```
connect direct/listen/script
set log/password/history/cli/script
show datetime/deviceport/log/portstatus/portcounters/history/cli/user/
script
```

Table 12-1 shows the mapping of groups and user rights.

Table 12-1 User Group Rights

User Right	Administrators	Power Users	Default Users
Full Administrative	◆		
Networking	◆	◆	
Services	◆		
Secure Lantronix Network	◆		
Date/Time	◆	◆	
Local Users	◆		
Remote Authentication	◆		
SSH Keys	◆		
User Menus	◆		
Web Access	◆	◆	
Reboot/Shutdown	◆	◆	
Firmware/Configuration	◆		
Diagnostics and Reports	◆	◆	
Device Ports Configuration	◆		
Device Port Operations	◆		
PC Card/USB	◆		

You cannot deny a user rights defined for the group, but you can add or remove all other rights at any time.

By default, the system assigns new users to the Default Users group, but you can change their group membership at any time. If you change a user's rights while the user is logged into the web or CLI, the results do not take effect until the next time the user logs in.

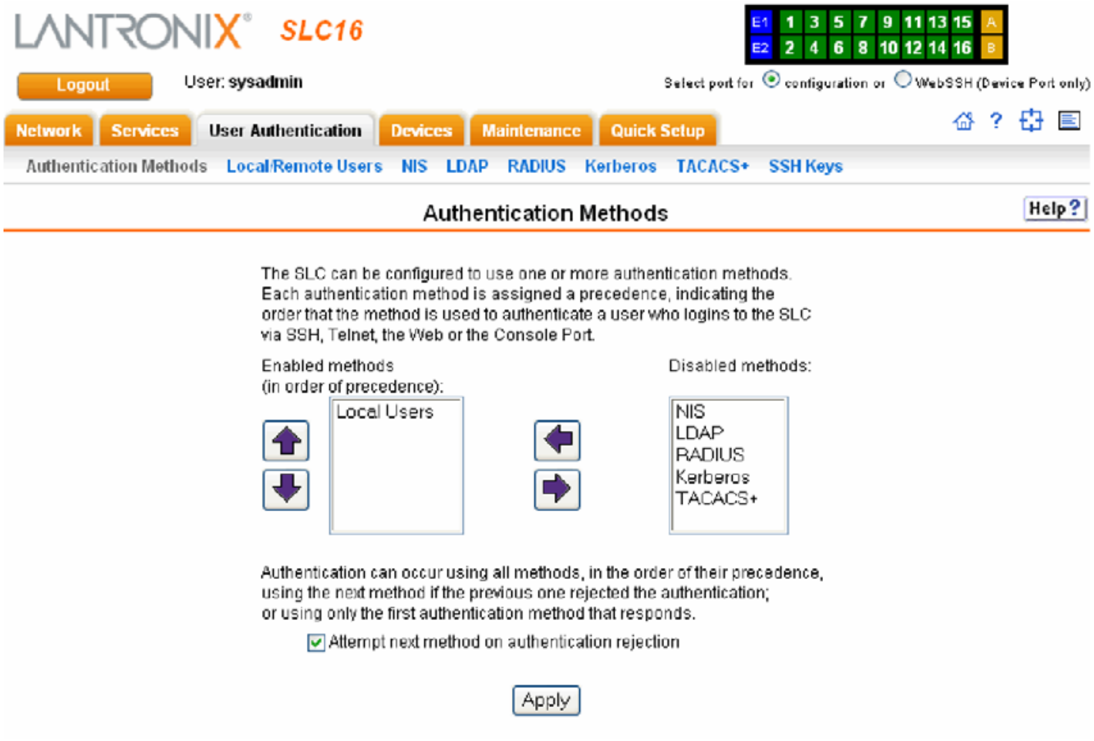
See *Local/Remote User Settings on page 145* for information about assigning rights to users.

Authentication Methods

To enable, disable, and set the precedence of authentication methods:

1. Click the **User Authentication** tab and the **Authentication Methods** option. *Figure 12-2* shows the page that displays.

Figure 12-2 Authentication Methods Page



Authentication Methods

The SLC can be configured to use one or more authentication methods. Each authentication method is assigned a precedence, indicating the order that the method is used to authenticate a user who logins to the SLC via SSH, Telnet, the Web or the Console Port.

Enabled methods (in order of precedence): Local Users

Disabled methods: NIS, LDAP, RADIUS, Kerberos, TACACS+

Authentication can occur using all methods, in the order of their precedence, using the next method if the previous one rejected the authentication; or using only the first authentication method that responds.

☑ Attempt next method on authentication rejection

2. To enable a method in the **Disabled methods:** list, select the method and click the **left arrow** to the left of the list. The methods include:

Local Users	Local accounts authenticate users who attempt to log in via SSH, Telnet, the Web, or the console port.

NIS (Network Information System)	A network naming and administration system developed by Sun Microsystems for smaller networks. Each host client or server in the network has knowledge about the entire network. A user at any host can access files or applications on any host in the network with a single user identification and password. NIS uses the client/server model and the Remote Procedure Call (RPC) interface for communication between hosts. NIS consists of a server, a library of client programs, and some administrative tools. NIS is often used with the Network File System (NFS).
LDAP (Lightweight Directory Access Protocol)	A set of protocols for accessing information directories, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection-oriented transfer services.
RADIUS (Remote Authentication Dial-In User Service)	An authentication and accounting system used by many Internet Service Providers (ISPs). A client/server protocol, it enables remote access servers to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It increases security, allowing a company to set up a policy that can be applied at a single administered network point.
Kerberos	Kerberos is a network authentication protocol that enables two parties to exchange private information across an unprotected network. It works by assigning a unique electronic credential, called a *ticket,* to each user who logs on to the network. The ticket is embedded in messages to identify the sender.
TACACS+ (Terminal Access Controller Access Control System)	TACACS+ allows a remote access server to communicate with an authentication server to determine whether the user has access to the network. TACACS+ is a completely new protocol and is not compatible with TACACS or XTACACS. The SLC console manager supports TACACS+ only.

3. Click the **Apply** button.

To disable a method in the Enabled methods list:

1. Select the method and click the **right arrow** between the lists.

To set the order in which the SLC console manager authenticates:

1. Use the **up** and **down arrows** to the left of the **Enabled methods** list.

To enable For Attempt next method on authentication rejection:

1. Choose one of the following options:

- To use all methods in order of precedence, until it obtains a successful authentication, select the check box. This is the default.
- To use only the first authentication method that responds (in case a server is down or unavailable), clear the check box.

After you have enabled the authentication method, you must configure it. Go to the following sections:

- *Local and Remote Users on page 143*
- *NIS on page 149*

- *LDAP on page 152*
- *RADIUS on page 157*
- *Kerberos on page 161*
- *TACACS+ on page 164*

Authentication Commands

The following CLI commands correspond to the **Authentication Methods** page. For more information, see *Chapter 15: Command Reference* .

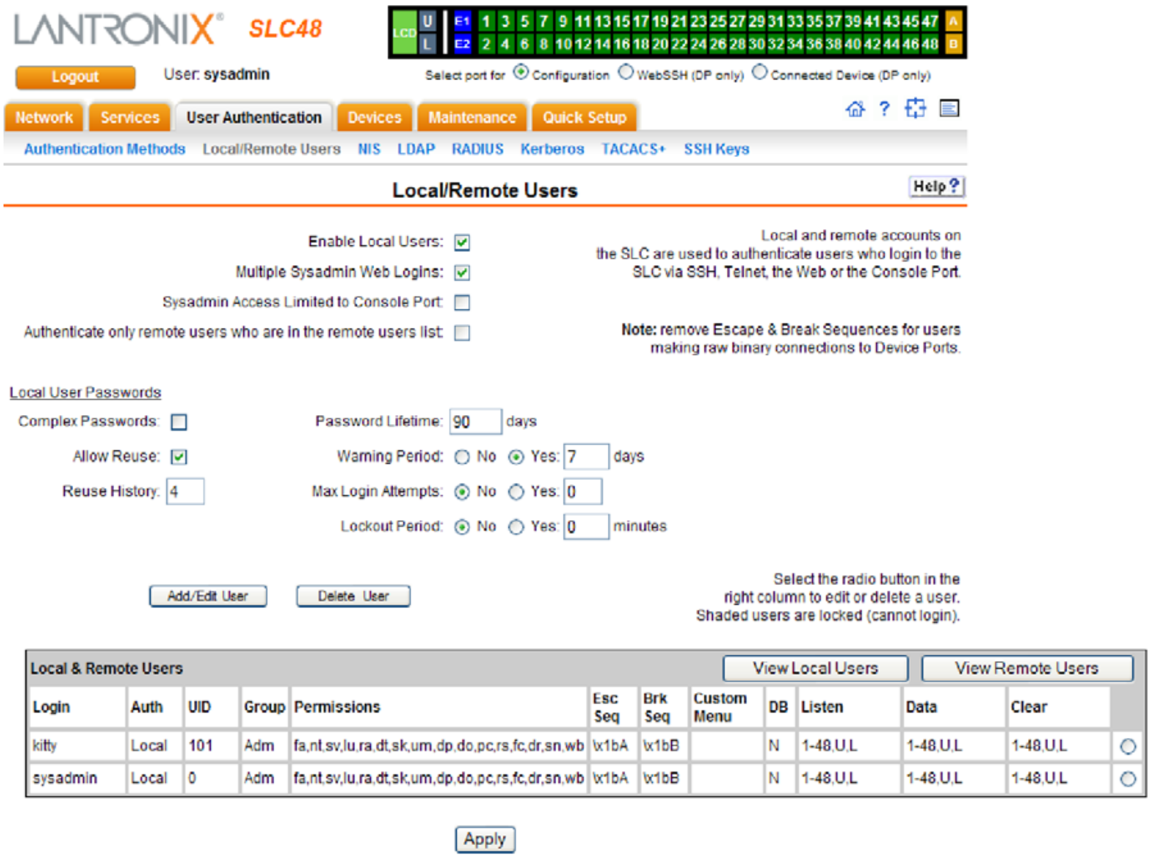
- *set auth (on page 214)*
- *show auth (on page 214)*

Local and Remote Users

The system administrator can configure the SLC console manager to use local/remote accounts to authenticate users.

1. Click the **User Authentication** tab and **Local/Remote Users** option. *Figure 12-3* shows the page that displays.

Figure 12-3 Local/Remote Users Page



Local/Remote Users

Enable Local Users: ☑

Multiple Sysadmin Web Logins: ☑

Sysadmin Access Limited to Console Port: □

Authenticate only remote users who are in the remote users list: □

Local and remote accounts on the SLC are used to authenticate users who login to the SLC via SSH, Telnet, the Web or the Console Port.

Note: remove Escape & Break Sequences for users making raw binary connections to Device Ports.

Local User Passwords

Complex Passwords: □

Allow Reuse: ☑

Reuse History: 4

Password Lifetime: 90 days

Warning Period: ○ No ● Yes: 7 days

Max Login Attempts: ● No ○ Yes: 0

Lockout Period: ● No ○ Yes: 0 minutes

Select the radio button in the right column to edit or delete a user. Shaded users are locked (cannot login).

Local & Remote Users

Login	Auth	UID	Group	Permissions	Esc Seq	Brk Seq	Custom Menu	DB	Listen	Data	Clear	
kitty	Local	101	Adm	fa,nt,sv,lu,ra,dt,sk,um,dp,do,pc,rs,fc,dr,sn,wb	\x1bA	\x1bB		N	1-48,U,L	1-48,U,L	1-48,U,L	○
sysadmin	Local	0	Adm	fa,nt,sv,lu,ra,dt,sk,um,dp,do,pc,rs,fc,dr,sn,wb	\x1bA	\x1bB		N	1-48,U,L	1-48,U,L	1-48,U,L	○

The top of the page has checkboxes for enabling local and remote users and for setting password requirements. The bottom of the page displays a table listing and describing all local and remote users.

To enable local and remote users capabilities:

1. Enter the following fields.

Enable Local Users	Select to enable all local users except sysadmin. The sysadmin is always available regardless of how you set the check box. Enabled by default.
Multiple Sysadmin Web Logins	Select to allow the sysadmin to have multiple simultaneous logins to the web interface. Disabled by default.
Sysadmin Access Limited to Console Port	Select to limit sysadmin logins to the Console Port only. Disabled by default.
Authenticate only users who are in the remote users list	Select the check box to authenticate users listed in the **Remote Users** list in the lower part of the page. Disabled by default.
Complex Passwords	Select to enable the SLC console manager to enforce rules concerning the password structure (e.g., alphanumeric requirements, number of characters, punctuation marks). Disabled by default. Complexity rules: ◆ Passwords must be at least eight characters long. ◆ They must contain one upper case letter (A-Z), one lower case letter (a-z), one digit (0-9), and one punctuation character (()`~!@#$%%^&*-+=\{}[]:;'"<>,.?/_).
Allow Reuse	Select to enable users to continue to reuse old passwords. If you disable the check box, they cannot use any of the **Reuse History** number of passwords. Enabled by default.
Reuse History	Set the number of passwords the user must use before reusing an old password. The default is 4. For example, if you set reuse history to 4, the user may reuse an old password after using 4 other passwords.
Lifetime (days)	Set the number of days until the password expires. The default setting is **90**.
Warning Period (days)	Set the number of days ahead that the system warns that the user password will expire. The default setting is **7**.
Max Login Attempts	Set the number of times (up to 8) the user can attempt to log in unsuccessfully before the system locks the user out. The default setting is **0** (disabled).
Lockout Time (minutes)	Set the number of minutes (up to 90) the locked-out user must wait before trying to log in to the web interface again. The default setting is **0** (disabled).

2. Click the **Apply** button.

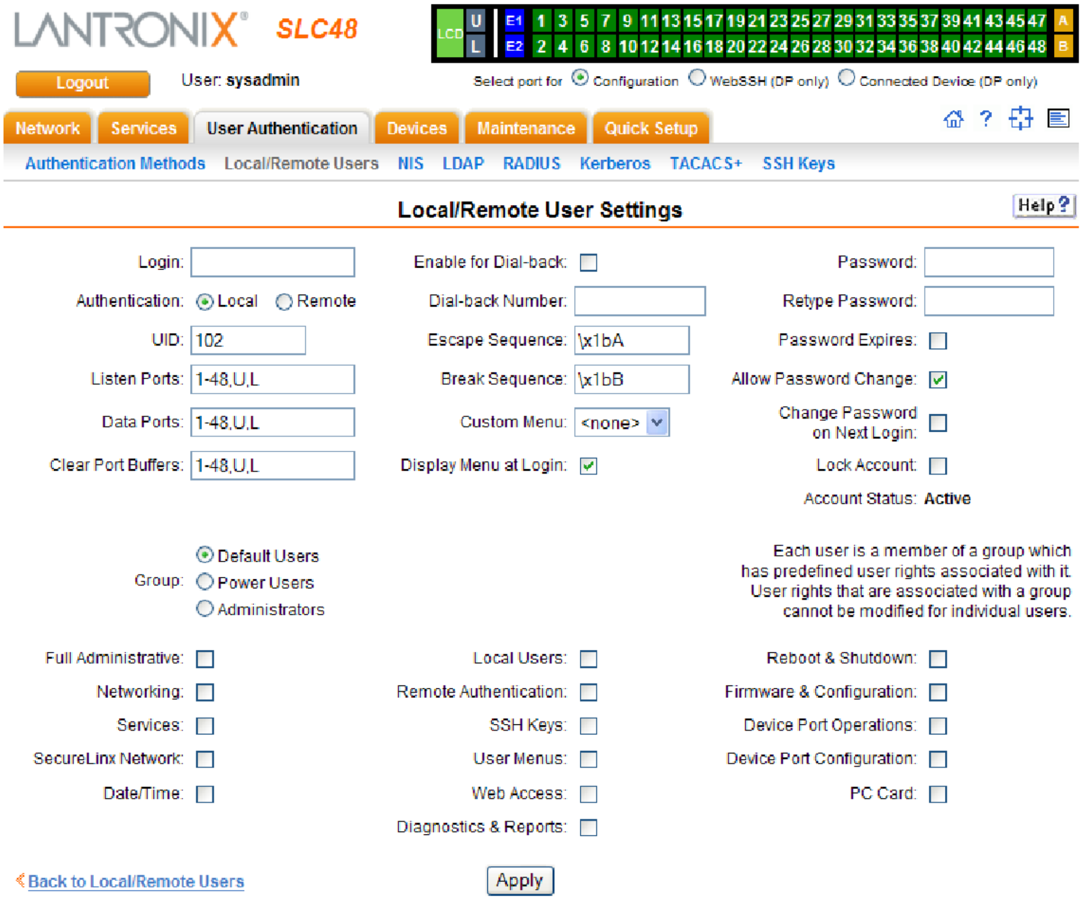
Local/Remote User Settings

You can add, edit, or delete a local or remote user.

To add a user:

1. On the **Local/Remote Users** page, click the **Add/Edit User** button. *Figure 12-4* shows the page that displays.

Figure 12-4 Local/Remote User Settings Page


LANTRONIX
SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network Services User Authentication Devices Maintenance Quick Setup
Authentication Methods Local/Remote Users NIS LDAP RADIUS Kerberos TACACS+ SSH Keys
Help ?
Back to Local/Remote Users
Apply

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Local/Remote User Settings

Login:
Authentication: ● Local ○ Remote
UID: 102
Listen Ports: 1-48,U,L
Data Ports: 1-48,U,L
Clear Port Buffers: 1-48,U,L

Enable for Dial-back: □
Dial-back Number:
Escape Sequence: \x1bA
Break Sequence: \x1bB
Custom Menu: <none>
Display Menu at Login: ☑

Password:
Retype Password:
Password Expires: □
Allow Password Change: ☑
Change Password on Next Login: □
Lock Account: □
Account Status: Active

Group: ● Default Users ○ Power Users ○ Administrators

Each user is a member of a group which has predefined user rights associated with it. User rights that are associated with a group cannot be modified for individual users.

Full Administrative: □
Networking: □
Services: □
SecureLinx Network: □
Date/Time: □

Local Users: □
Remote Authentication: □
SSH Keys: □
User Menus: □
Web Access: □
Diagnostics & Reports: □

Reboot & Shutdown: □
Firmware & Configuration: □
Device Port Operations: □
Device Port Configuration: □
PC Card: □

2. Enter the following fields.

Login	User ID of selected user.
Authentication	Select the type of authenticated user: **Local:** User listed in the SLC database. **Remote:** User not listed in the SLC database.
UID	A unique numeric identifier the system administrator assigns to each user. Valid UIDs are 101-4294967295. *Note: The UID must be unique. If it is not, SLC console manager automatically increments it. Starting at 101, the SLC device finds the next unused UID.*

Listen Ports	The device ports that the user may access to view data using the `connect listen` command. Enter the port numbers or the range of port numbers (for example, 1, 5, 8, 10-15). **U** and **L** denote the PC Card upper and lower slots. **U1** denotes the USB port.
Data Ports	The device ports with which the user may interact using the `connect direct` command. Enter the port numbers or the range of port numbers.
Clear Port Buffers	The device port buffers the users may clear using the `set log clear` command. Enter the port numbers or the range of port numbers.
Enable for Dial-back	Select to grant a local user dial-back access (see *Device Ports on page 81*). Users with dial-back access can dial into the SLC console manager and enter their login and password. Once the SLC device authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number (specified on the *Device Ports on page 81*), or on a number that is associated with the user's login (specified here).
Escape Sequence	A single character or a two-character sequence that causes the SLC console manager to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is **Esc+A** (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as **\x1bA**, which is hexadecimal **(\x)** character 27 (**1B**) followed by an **A**. This setting allows the user to terminate the `connect direct` command on the command line interface when the endpoint of the command is `deviceport`, `tcp`, or `udp`.
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is **Esc+B** (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as **\x1bB**, which is hexadecimal **(\x)** character 27 (**1B**) followed by a **B**.
Custom Menu	If custom menus have been created (see *Local/Remote Users Commands on page 148*), you can assign a default custom menu to the user. The custom menu will display at login. ***Note:*** *In the Local Users table, if the menu assigned to a local user no longer exists, it is marked with an asterisk (*).*
Display Menu at Login	If custom menus have been created, select to enable the menu to display when the user logs into the CLI.
Password/Retype Password	When a user logs into the SLC console manager, the SLC device prompts for a password (up to 64 characters). The sysadmin establishes that password here.
Password Expires	If not selected, allows the user to keep a password indefinitely. If selected the user keeps the password for a set period. (See *Local and Remote Users on page 143* for information on specifying the length of time before the password expires.)
Allow Password Change	Select to allow the user to change password.
Change Password on Next Login	Indicate whether the user must change the password at the next login.

Lock Account	Select to locks the account indefinitely.
Account Status	Current status of the account: Active, Locked, or Locked (invalid logins).

3. Assign rights to users.

   Each user is a member of a group that has a predefined user rights associated with it. You can assign or remove additional rights to the individual user.

Group	Select the group to which the user will belong: ◆ **Default Users:** This group has only the most basic rights. You can specify additional rights for the individual user. ◆ **Power Users:** This group has the same rights as Default Users plus **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. You can specify additional rights for the individual user. ◆ **Administrators:** This group has all possible rights.
Full Administrative	Right to perform any function on the SLC console manager.
Networking	Right to enter network and routing settings.
Services	Right to enable and disable system and audit logging, SSH and Telnet logins, SNMP, and SMTP. Includes NFS and CIFS.
Secure Lantronix Network	Right to view and manage secure IT management devices (e.g., SLP power managers, Spider devices, SLC console managers) on the local subnet.
Date/Time	Right to set the date and time.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user. Includes configuring remote authentication methods and ordering
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create or edit a custom user menu for the CLI.
Web Access	Right to access Web-Manager.
Reboot & Shutdown	Right to shutdown or reboot the SLC device.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings).
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
Device Port Configuration	Right to enter device port settings.
Device Port Operations	Right to control device ports.
PC Card or USB	Right to enter modem settings for PC Cards and USB devices. Includes managing storage PC Cards.

4. Click the **Apply** button.

5. Click the **Back to Local/Remote Users** link to return to the **Local/Remote User Settings** page. Add another user or click the **Back to Local/Remote Users** link. The **Local/Remote Users** page displays with the new user listed in the table.

Note: The logged-in username displays at the top of the web page. Only the tabs and options display for the user who has rights.

Shortcut to add a user based on an existing user:

1. Display the existing user on the **Local/Remote Users Settings** page. The fields in the top part of the page display the current values for the user.
2. Change the **Login** to that of the new user. It is best to change the **Password** too.
3. Click the **Apply** button.

To edit a local user:

1. On the **Local/Remote Users** page, select the user and click the **Add/Edit User** button. The **Local/Remote User Settings** page displays.
2. Update values as desired.
3. Click the **Apply** button.

To delete a local user:

1. On the **Local/Remote Users** page, select the user and click the **Add/Edit User** button. The **Local/Remote User Settings** page displays.
2. Click the **Delete User** button.
3. Click the **Apply** button.

To change the sysadmin password:

1. On the **Local/Remote Users** page, select **sysadmin** and click the **Add/Edit User** button. The **Local/Remote User Settings** page displays.
2. Enter the new password in the **Password** and **Retype Password** fields.

*Note: You can change **Escape Sequence** and **Break Sequence**, if desired. You cannot delete the UID or change the UID, port permissions, or custom menu.*

3. Click the **Apply** button.

Local/Remote Users Commands

The following CLI commands correspond to the **Local/Remote Users** page. For more information, see *Chapter 15: Command Reference* .

- *set localusers (on page 235)*
- *set localusers allowreuse (on page 236)*
- *set localusers complexpasswords (on page 236)*
- *set localusers consoleonlyadmin (on page 236)*
- *set localusers state (on page 238)*
- *set localusers password (on page 237)*
- *set localusers delete (on page 236)*
- *set localusers lifetime (on page 237)*
- *set localusers lock (on page 237)*

- *set localusers maxloginattempts (on page 237)*
- *set localusers multipleadminlogins (on page 237)*
- *set localusers periodlockout (on page 237)*
- *set localusers periodwarning (on page 238)*
- *set localusers reusehistory (on page 238)*
- *set remoteusers (on page 249)*
- *set remoteusers listonlyauth (on page 250)*
- *set remoteusers delete (on page 249)*
- *show localusers (on page 238)*
- *show remoteusers (on page 250)*
- *show user (on page 214)*

NIS

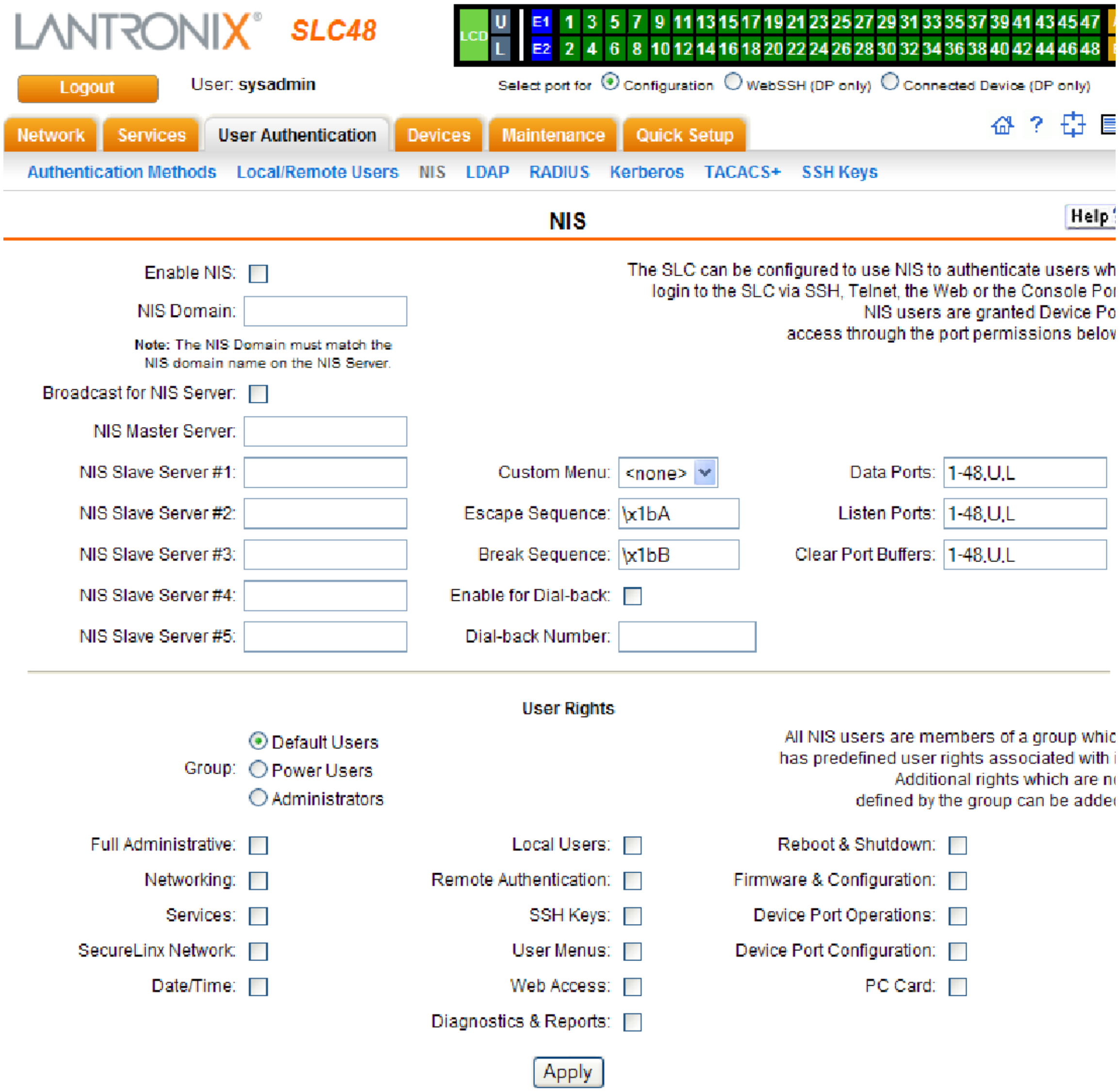
The system administrator can configure the SLC console manager to use NIS to authenticate users attempting to log in to the SLC device through the Web, SSH, Telnet, or the Console port. If NIS does not provide port permissions, you can use this page to grant device port access to users who are authenticated through NIS.

All NIS users are members of a group that has predefined user rights associated with it. You can assign additional user rights that are not defined by the group.

To configure the SLC console manager to use NIS to authenticate users:

1. Click the **User Authentication** tab and select the **NIS** option. *Figure 12-5* shows the page that displays.

Figure 12-5 NIS Page


LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
Logout
Network Services User Authentication Devices Maintenance Quick Setup
Authentication Methods Local/Remote Users NIS LDAP RADIUS Kerberos TACACS+ SSH Keys
Help

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

NIS

Enable NIS: □

NIS Domain:

Note: The NIS Domain must match the NIS domain name on the NIS Server.

Broadcast for NIS Server: □

NIS Master Server:

NIS Slave Server #1:

NIS Slave Server #2:

NIS Slave Server #3:

NIS Slave Server #4:

NIS Slave Server #5:

The SLC can be configured to use NIS to authenticate users wh login to the SLC via SSH, Telnet, the Web or the Console Po NIS users are granted Device Po access through the port permissions belov

Custom Menu: <none>

Escape Sequence: \x1bA

Break Sequence: \x1bB

Enable for Dial-back: □

Dial-back Number:

Data Ports: 1-48,U,L

Listen Ports: 1-48,U,L

Clear Port Buffers: 1-48,U,L

User Rights

Group: ● Default Users ○ Power Users ○ Administrators

All NIS users are members of a group whic has predefined user rights associated with i Additional rights which are n defined by the group can be addec

Full Administrative: □

Networking: □

Services: □

SecureLinx Network: □

Date/Time: □

Local Users: □

Remote Authentication: □

SSH Keys: □

User Menus: □

Web Access: □

Diagnostics & Reports: □

Reboot & Shutdown: □

Firmware & Configuration: □

Device Port Operations: □

Device Port Configuration: □

PC Card: □

Apply

2. Enter the following fields.

Enable NIS	Displays selected if you enabled this method on the Authentication Methods page. If you want to set up this authentication method but not enable it immediately, clear the checkbox. ***Note:*** *You can enable NIS here or on the first User Authentication page. If you enable NIS here, it automatically displays at the end of the order of precedence on the User Authentication page.*
NIS Domain	The NIS domain of the SLC console manager must be the same as the NIS domain of the NIS server.
Broadcast for NIS Server	If selected, the SLC device sends a broadcast datagram to find the NIS Server on the local network.
NIS Master Server (required)	The IP address or host name of the master server.

NIS Slave Servers #1 -5	The IP addresses or host names of up to five slave servers.
Custom Menu	If custom menus have been created (see *Local/Remote Users Commands on page 148*), you can assign a default custom menu to NIS users.
Escape Sequence	A single character or a two-character sequence that causes the SLC console manager to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is **Esc+A** (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as **\x1bA**, which is hexadecimal **(\x)** character 27 (**1B**) followed by an **A**. This setting allows the user to terminate the `connect direct` command on the command line interface when the endpoint of the command is `deviceport`, `tcp`, or `udp`.
Enable for Dial-back	Select to grant a user dial-back access. Users with dial-back access can dial into the SLC device and enter their login and password. Once the SLC console manager authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user's login (specified here).
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is **Esc+B** (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as **\x1bB**, which is hexadecimal **(\x)** character 27 (**1B**) followed by a **B**.
Data Ports	The ports users are able to monitor and interact with using the `connect direct` command. **U** and **L** denote the PC Card upper and lower slots. **U1** denotes the USB port.
Listen Ports	The ports users are able to monitor using the `connect listen` command.
Clear Port Buffers	The ports whose port buffer users may clear using the `set log clear` command.

3. In the **User Rights** section, select the user group to which NIS users will belong.

Group	Select the group to which the NIS users will belong: **Default Users:** This group has only the most basic rights (described above). **Power Users:** This group has the same rights as Default Users plus **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. **Administrators:** This group has all possible rights.

4. Select or clear the checkboxes for the following rights.

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Date/Time	Right to set the date and time.

Secure Lantronix Network	Right to view and manage secure IT management devices (e.g., SLP power managers, Spider devices, SLC console managers) on the local subnet.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI for NIS users.
Reboot & Shutdown	Right to use the CLI or shut down the SLC device and then reboot it.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects **Reboot & Shutdown**.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
SLC Network	Right to view and manage SLC console managers on the local subnet.
Web Access	Right to access Web-Manager.
Device Port Configuration	Right to enter device port settings.
Device Port Operations	Right to control device ports.
PC Card or USB	Right to enter modem settings for PC Cards or USB port.

5. Click the **Apply** button.

Note: *You must reboot the SLC console manager before your changes take effect.*

NIS Commands

The following CLI commands correspond to the **NIS** page. For more information, see *Chapter 15: Command Reference* .

- *set nis (on page 244)*
- *show nis (on page 244)*

LDAP

LDAP allows authentication of SLC users using a wide variety of LDAP servers, such as OpenLDAP and Microsoft Active Directory. The LDAP implementation supports LDAP servers that do not allow anonymous queries.

The system administrator can configure the SLC console manager to use LDAP to authenticate users attempting to login using the Web, Telnet, SSH, or the console port. Users who are authenticated through LDAP are granted device port access through the port permissions. All LDAP users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

Typically user authorization (operational rights and device port privileges parameters support only users who exist in the SLC local user database. If an SLC device user gets authenticated via a remote authentication server such as LDAP, configuration of the user is required in the remote authentication server (for authentication only, no authorization) and the SLC console manager (authorization only).

With extended support of LDAP active directory user attribute schemas in the SLC device, remote authenticated users get authenticated and authorized from the LDAP server. This provides a single point of user database management by no longer requiring remote authenticated user existence in the SLC local user database.

See *Appendix I: LDAP Schemas on page 288* for information about installing schema support in the Windows active directory and creating the Lantronix SLC schema attribute.

Schema Permissions versus Default User Rights

The User Rights shown on the SLC console manager under the LDAP settings are the ones that would be applied to a user logging in if the following are true:

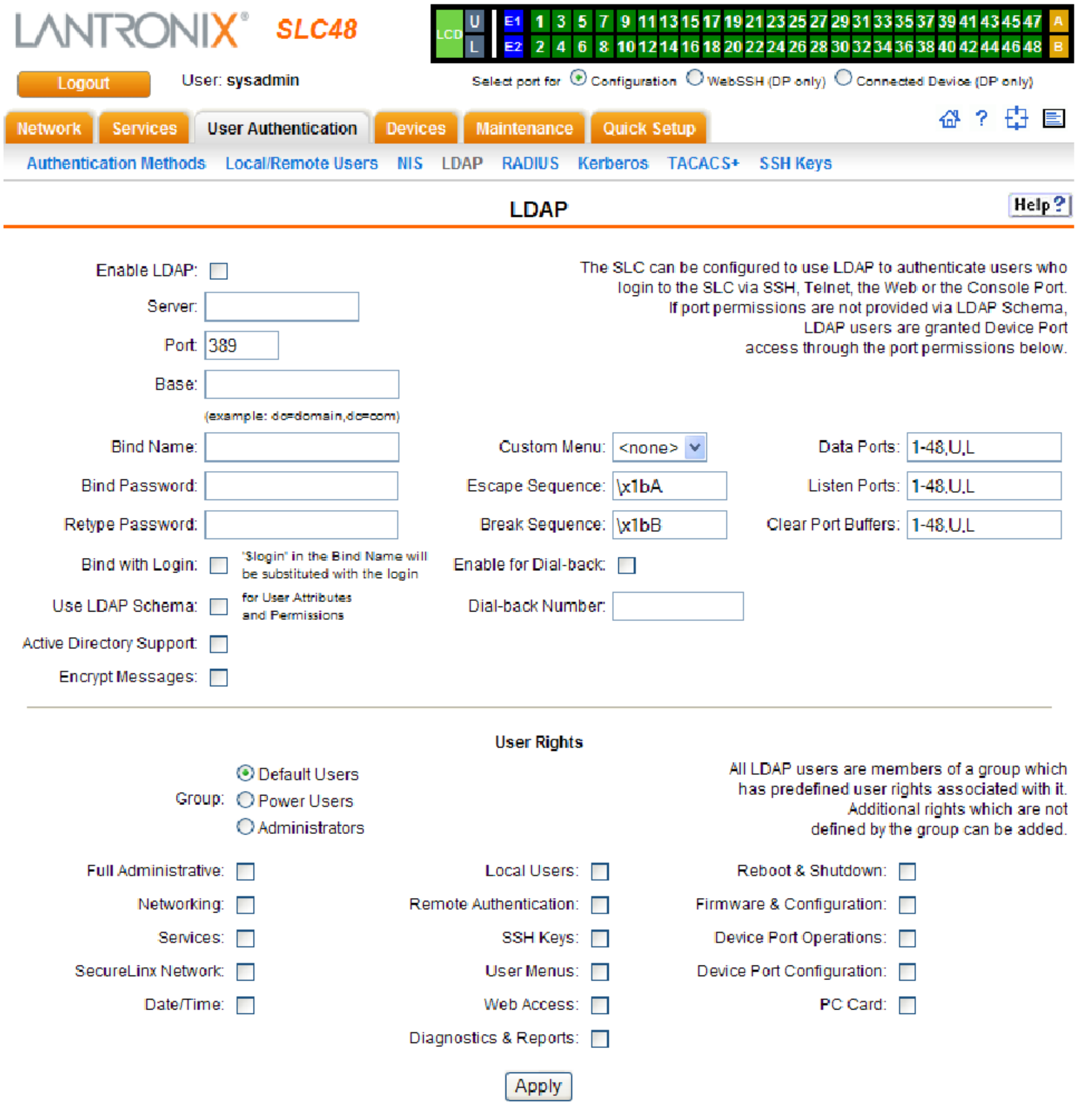
- A remote user for a particular username is not configured on the SLC device under the User Authentication-Local/Remote Users page.
- An AD user authenticated using LDAP does not have a Schema associated.
- Any AD user that has a Schema associated, but only certain rights are assigned.
- The checkbox next to Authenticate only remote users who are not in the remote users list: is unchecked under the User Authentication->Local/Remote Users page.

Dial-back and Dial-back Number are not supported via the Schema. These features were implemented after LDAP Schema support was added and will be added to the Schema after this release.

To configure the SLC console manager to use LDAP to authenticate users:

1. Click the **User Authentication** tab and select **LDAP**. *Figure 12-6* shows the page that displays.

Figure 12-6 LDAP Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

LDAP

Enable LDAP: □

Server:

Port: 389

Base:

(example: dc=domain,dc=com)

Bind Name:

Bind Password:

Retype Password:

Bind with Login: □ '$login' in the Bind Name will be substituted with the login

Use LDAP Schema: □ for User Attributes and Permissions

Active Directory Support: □

Encrypt Messages: □

The SLC can be configured to use LDAP to authenticate users who login to the SLC via SSH, Telnet, the Web or the Console Port. If port permissions are not provided via LDAP Schema, LDAP users are granted Device Port access through the port permissions below.

Custom Menu: <none>

Escape Sequence: \x1bA

Break Sequence: \x1bB

Enable for Dial-back: □

Dial-back Number:

Data Ports: 1-48,U,L

Listen Ports: 1-48,U,L

Clear Port Buffers: 1-48,U,L

User Rights

Group: ● Default Users ○ Power Users ○ Administrators

All LDAP users are members of a group which has predefined user rights associated with it. Additional rights which are not defined by the group can be added.

Full Administrative: □
Networking: □
Services: □
SecureLinx Network: □
Date/Time: □

Local Users: □
Remote Authentication: □
SSH Keys: □
User Menus: □
Web Access: □
Diagnostics & Reports: □

Reboot & Shutdown: □
Firmware & Configuration: □
Device Port Operations: □
Device Port Configuration: □
PC Card: □

2. Enter the following fields.

Enable LDAP	Displays as checked if you enabled this method in the User Authentication Methods page. If you want to set up this authentication method but not enable it immediately, clear the checkbox.
Server	Enter the IP address or host name of the AD server.
Port	Enter the TCP port number of the AD server. The default is **389**.
Base	Enter the LDAP search base for your AD Domain (e.g., dc=company, dc=com). Can have up to 80 characters.
Bind Name	Enter the Windows AD username that gets used for a non-anonymous bind to an LDAP server. This item has the same format as LDAP base. An example is: cn=administrator,cn=Users,dc=domain,dc=com

Bind Password and Retype Password	Enter the password for the user configured in Bind Name for a non-anonymous bind. This entry is optional. Acceptable characters are **a-z**, **A-Z,** and **0-9**. The maximum length is 127 characters.
Bind with Login	Select to bind with the login and password that a user is authenticating with. This requires that the Bind Name contain the **$login** token, which will be replaced with the current login. For example, if the Bind Name is **uid=$login,ou=People,dc=lantronix,dc=com**, and user **roberts** logs into the SLC console manager, LDAP will bind with **uid=roberts,ou=People,dc=lantronix,dc=com** and the password entered by roberts.
Use LDAP Schema	Click the check box to obtain remote user attributes (group/permissions and port access) from an Active Directory server scheme via the user attribute secure lantronixSLCPerms. Disabled by default. See *User Attributes and Permissions from LDAP Schema on page 157*.
Active Directory Support	Click to enable. Active Directory is a directory service from Microsoft that is a part of Windows 2000 and later versions of Windows. It is LDAP- and Kerberos-compliant. Disabled by default.
Encrypt Messages	Select to encrypt messages between the SLC device and the LDAP server. Disabled by default.
Custom Menu	Assign a default customer menu to LDAP users, if custom menus have been created (see *Local/Remote Users Commands on page 148*).
Escape Sequence	Enter a single character or a two-character sequence that causes the SLC console manager to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is **Esc+A** (escape key, then uppercase “A” performed quickly but not simultaneously). You would specify this value as **\x1bA**, which is hexadecimal **(\x)** character 27 (**1B**) followed by an **A**. This setting allows the user to terminate the `connect direct` command on the command line interface when the endpoint of the command is `deviceport`, `tcp`, or `udp`.
Break Sequence	Enter a series of 1-10 characters that users can enter on the command line interface to send a break signal to the external device. A suggested value is **Esc+B** (escape key, then uppercase “B” performed quickly but not simultaneously). You would specify this value as **\x1bB**, which is hexadecimal **(\x)** character 27 (**1B**) followed by a **B**.
Enable for Dial-back	Select to grant a user dial-back access. Users with dial-back access can dial into the SLC device and enter their login and password. Once the SLC console manager authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	Enter the device port that the modem dials to reach a user phone number. The user is dialed back on a fixed number or on a number that is associated with the user login (specified here).
Data Ports	Enter the ports that users can monitor and interact with using the `connect direct` command. **U** and **L** denote the PC Card upper and lower slots. **U1** denotes the USB port.
Listen Port	Enter the ports that users can monitor using the `connect listen` command.
Clear Port Buffers	Enter the ports that users can clear the port buffer by using the `set log clear` command.

3. In the User Rights section, select the user group to which LDAP users belong.

Group	Select the group to which the LDAP users will belong: ◆ **Default Users:** This group has only the most basic rights (described above). ◆ **Power Users:** This group has the same rights as Default Users plus **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. ◆ **Administrators:** This group has all possible rights.

4. Select or clear the checkboxes for the following rights.

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage SLC units (e.g., SLP power managers, Spider devices, SLC console managers) on the local subnet.
Date/Time	Right to set the date and time.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI for LDAP users.
Reboot & Shutdown	Right to use the CLI or shut down the SLC console manager and then reboot it.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects **Reboot & Shutdown**.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
SLC Network	Right to view and manage SLC console managers on the local subnet.
Web Access	Right to access Web-Manager.
Device Port Configuration	Right to enter device port settings.
Device Port Operations	Right to control device ports.
PC Card or USB	Right to enter modem settings for PC Cards or the USB port.

5. Click the **Apply** button.

Note: *You must reboot the SLC console manager before your changes take effect.*

User Attributes and Permissions from LDAP Schema

Remote user attributes (group/permissions and port access) can be obtained from an Active Directory server schema via the user attribute **secureLinxSLCPerms**. This attribute is a set of parameter-value pairs. Each parameter and value is separated by a space, and a space separates each parameter-value pair. White space is not supported in the value strings. See *Chapter 9: PC Cards* for the parameters and values.

LDAP Commands

The following CLI commands correspond to the **LDAP** page. For more information, see *Chapter 15: Command Reference* .

- *set ldap (on page 234)*
- *show ldap (on page 235)*

RADIUS

The system administrator can configure the SLC console manager to use RADIUS to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

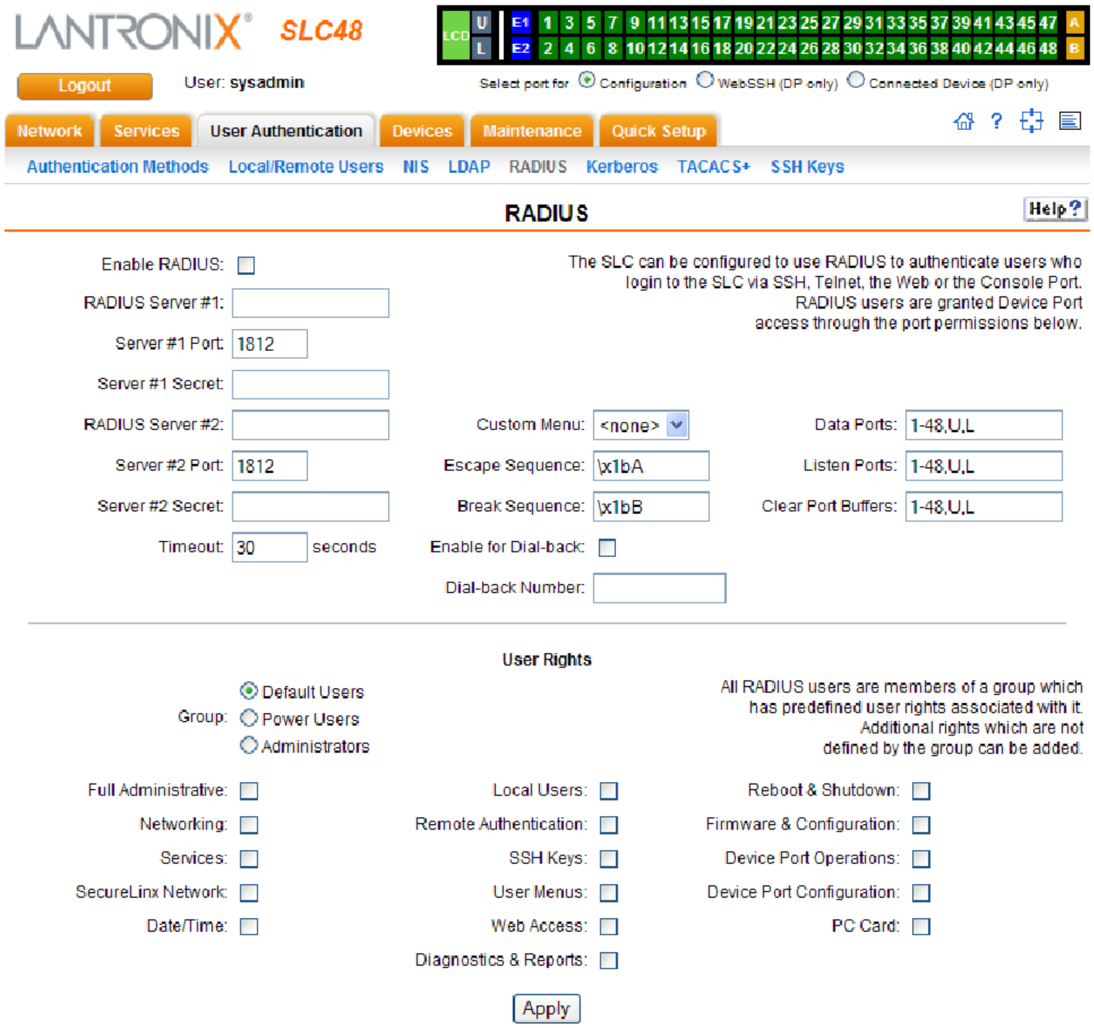
Users who are authenticated through RADIUS are granted device port access through the port permissions on this page.

All RADIUS users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

To configure the SLC console manager to use RADIUS to authenticate users:

1. Click the **User Authentication** tab and select **RADIUS**. *Figure 12-7* shows the page that displays.

Figure 12-7 RADIUS Page


LANTRONIX
SLC48
Logout
User: sysadmin
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network
Services
User Authentication
Devices
Maintenance
Quick Setup
Authentication Methods
Local/Remote Users
NIS
LDAP
RADIUS
Kerberos
TACACS+
SSH Keys
Help?
Apply

RADIUS

The SLC can be configured to use RADIUS to authenticate users who login to the SLC via SSH, Telnet, the Web or the Console Port. RADIUS users are granted Device Port access through the port permissions below.

Enable RADIUS: □
RADIUS Server #1:
Server #1 Port: 1812
Server #1 Secret:
RADIUS Server #2:
Server #2 Port: 1812
Server #2 Secret:
Timeout: 30 seconds

Custom Menu: <none>
Escape Sequence: \x1bA
Break Sequence: \x1bB
Enable for Dial-back: □
Dial-back Number:

Data Ports: 1-48,U,L
Listen Ports: 1-48,U,L
Clear Port Buffers: 1-48,U,L

User Rights

All RADIUS users are members of a group which has predefined user rights associated with it. Additional rights which are not defined by the group can be added.

Group: ● Default Users ○ Power Users ○ Administrators

Full Administrative: □
Networking: □
Services: □
SecureLinx Network: □
Date/Time: □
Local Users: □
Remote Authentication: □
SSH Keys: □
User Menus: □
Web Access: □
Diagnostics & Reports: □
Reboot & Shutdown: □
Firmware & Configuration: □
Device Port Operations: □
Device Port Configuration: □
PC Card: □

2. Enter the following fields.

Enable RADIUS	Displays selected if you enabled this method on the **User Authentication** page. If you want to set up this authentication method but not enable it immediately, clear the checkbox. ***Note:*** *You can enable RADIUS here or on the first **User Authentication** page. If you enable RADIUS here, it automatically displays at the end of the order of precedence on the **User Authentication** page.*
RADIUS Server #1	IP address or hostname of the primary RADIUS server. This RADIUS server may be a proxy for SecurID. SecurID is a two-factor authentication method based on the user's SecurID token and pin number. The SecurID token displays a string of digits called a token code that changes once a minute (some tokens are set to change codes every 30 seconds).
Server #1 Port	Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the SLC console manager uses the default RADIUS port (**1812**).

Server #1 Secret	Text that serves as a shared secret between a RADIUS client and the server (SLC device). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.
RADIUS Server #2	IP address or host name of the secondary RADIUS server. This server can be used as a SecurID proxy.
Server #2 Port	Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the SLC console manager uses the default RADIUS port (**1812**).
Server #2 Secret	Text that serves as a shared secret between a RADIUS client and the server (SLC device). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.
Timeout	The number of seconds (1-30) after which the connection attempt times out. The default is **30** seconds.
Custom Menu	If custom menus have been created (see *Local/Remote Users Commands on page 148*), you can assign a default custom menu to RADIUS users.
Escape Sequence	A single character or a two-character sequence that causes the SLC console manager to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is **Esc+A** (escape key, then uppercase “A” performed quickly but not simultaneously). You would specify this value as **\x1bA**, which is hexadecimal **(\x)** character 27 (**1B**) followed by an **A**. This setting allows the user to terminate the `connect direct` command on the command line interface when the endpoint of the command is `deviceport`, `tcp`, or `udp`.
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is **Esc+B** (escape key, then uppercase “B” performed quickly but not simultaneously). You would specify this value as **\x1bB**, which is hexadecimal **(\x)** character 27 (**1B**) followed by a **B**.
Enable for Dial-back	Select to grant a user dial-back access. Users with dial-back access can dial into the SLC device and enter their login and password. Once the SLC console manager authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user’s login (specified here).
Data Ports	The ports users are able to monitor and interact with using the `connect direct` command. **U** and **L** denote the PC Card upper and lower slots. **U1** denotes the USB port.
Listen Port	The ports users are able to monitor using the `connect listen` command.
Clear Port Buffers	The ports whose port buffer users may clear using the `set log clear` command.

Note: *Older RADIUS servers may use* ***1645*** *as the default port. Check your RADIUS server configuration.*

3. In the **User Rights** section, select the user group to which RADIUS users belong.

Group	Select the group to which the RADIUS users will belong: ◆ **Default Users:** This group has only the most basic rights (described above). ◆ **Power Users:** This group has the same rights as Default Users plus **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. ◆ **Administrators:** This group has all possible rights.

4. Select or clear the checkboxes for the following rights.

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure IT management devices (e.g., SLP power managers, Spider devices, SLC console managers) on the local subnet.
Date/Time	Right to set the date and time.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI for NIS users.
Reboot & Shutdown	Right to use the CLI or shut down the SLC device and then reboot it.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects **Reboot & Shutdown**.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
SLC Network	Right to view and manage SLC console managers on the local subnet.
Web Access	Right to access Web-Manager.
Device Port Configuration	Right to enter device port settings.
Device Port Operations	Right to control device ports.
PC Card or USB	Right to enter modem settings for PC Cards or the USB port.

5. Click the **Apply** button.

Note: *You must reboot the SLC console manager before your changes take effect.*

RADIUS Commands

The following CLI commands correspond to the **RADIUS** page. For more information, see *Chapter 15: Command Reference* .

- *set radius (on page 248)*
- *set radius server (on page 248)*
- *show radius (on page 249)*

Kerberos

Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

The system administrator can configure the SLC console manager to use Kerberos to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

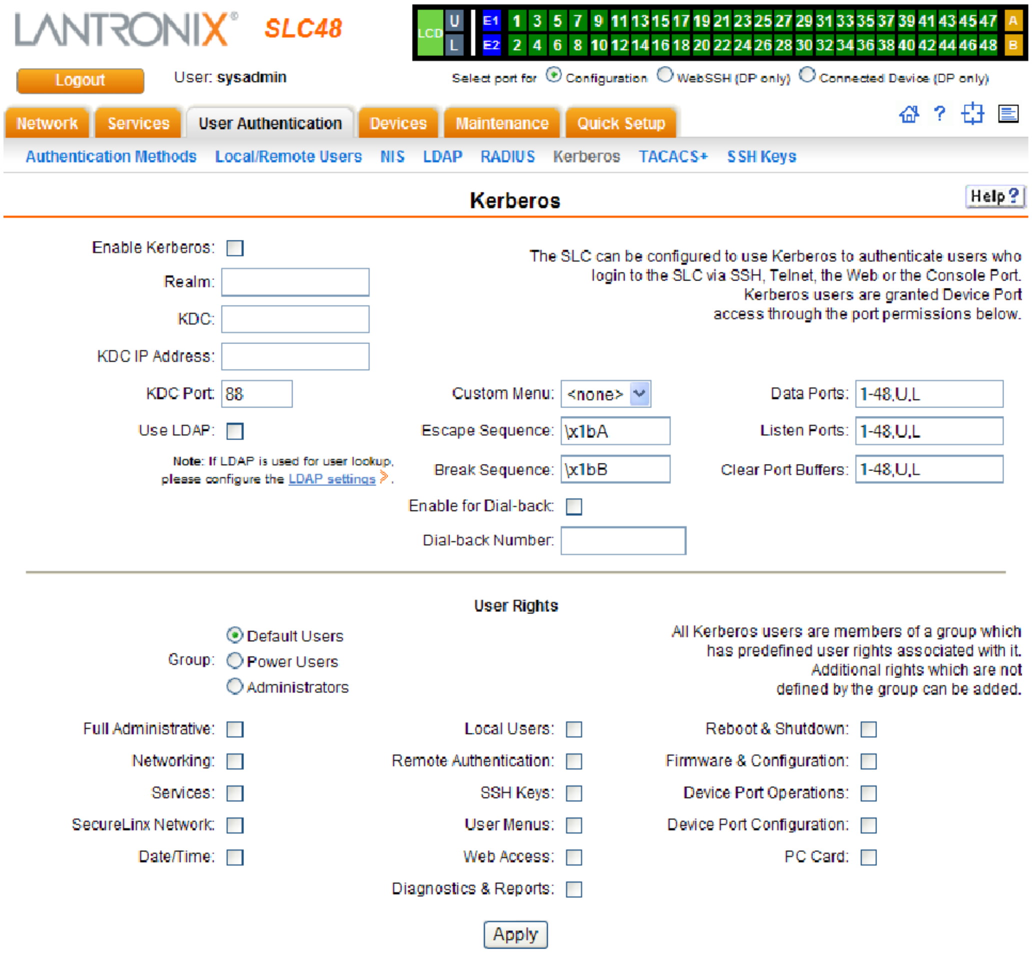
Users who are authenticated through Kerberos are granted device port access through the port permissions on this page.

All Kerberos users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

To configure the SLC console manager to use Kerberos to authenticate users:

1. Click the **User Authentication** tab and select the **Kerberos** option. *Figure 12-8* shows the page that displays.

Figure 12-8 Kerberos Page


LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network Services User Authentication Devices Maintenance Quick Setup
Authentication Methods Local/Remote Users NIS LDAP RADIUS Kerberos TACACS+ SSH Keys
Help ?
Apply

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Kerberos

The SLC can be configured to use Kerberos to authenticate users who login to the SLC via SSH, Telnet, the Web or the Console Port. Kerberos users are granted Device Port access through the port permissions below.

Enable Kerberos: □

Realm:

KDC:

KDC IP Address:

KDC Port: 88

Use LDAP: □

Note: If LDAP is used for user lookup, please configure the LDAP settings.

Custom Menu: <none>

Escape Sequence: \x1bA

Break Sequence: \x1bB

Enable for Dial-back: □

Dial-back Number:

Data Ports: 1-48,U,L

Listen Ports: 1-48,U,L

Clear Port Buffers: 1-48,U,L

User Rights

All Kerberos users are members of a group which has predefined user rights associated with it. Additional rights which are not defined by the group can be added.

Group: ● Default Users ○ Power Users ○ Administrators

Full Administrative: □
Networking: □
Services: □
SecureLinx Network: □
Date/Time: □

Local Users: □
Remote Authentication: □
SSH Keys: □
User Menus: □
Web Access: □
Diagnostics & Reports: □

Reboot & Shutdown: □
Firmware & Configuration: □
Device Port Operations: □
Device Port Configuration: □
PC Card: □

2. Enter the following fields.

Enable Kerberos	Displays selected if you enabled this method on the **User Authentication** page. If you want to set up this authentication method but not enable it immediately, clear the checkbox. ***Note:*** *You can enable Kerberos here or on the first **User Authentication** page. If you enable Kerberos here, it automatically displays at the end of the order of precedence on the **User Authentication** page.*
Realm	Enter the name of the logical network served by a single Kerberos database and a set of Key Distribution Centers. Usually, realm names are all uppercase letters to differentiate the realm from the Internet domain. Realm is similar in concept to an NT domain.
KDC	A key distribution center (KDC) is a server that issues Kerberos tickets. A ticket is a temporary set of electronic credentials that verify the identity of a client for a particular service. Enter the **KDC** in the fully qualified domain format (FQDN). An example is SLC.local.
KDC IP Address	Enter the IP address of the Key Distribution Center (KDC).

KDC Port	Port on the KDC listening for requests. Enter an integer with a maximum value of 65535. The default is **88**.
Custom Menu	If custom menus have been created (see *Local/Remote Users Commands on page 148*), you can assign a default custom menu to RADIUS users.
Escape Sequence	A single character or a two-character sequence that causes the SLC console manager to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is **Esc+A** (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as **\x1bA**, which is hexadecimal **(\x)** character 27 (**1B**) followed by an **A**. This setting allows the user to terminate the `connect direct` command on the command line interface when the endpoint of the command is `deviceport`, `tcp`, or `udp`.
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is **Esc+B** (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as **\x1bB**, which is hexadecimal **(\x)** character 27 (**1B**) followed by a **B**.
Enable for Dial-back	Select to grant a user dial-back access. Users with dial-back access can dial into the SLC device and enter their login and password. Once the SLC console manager authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user's login (specified here).
Use LDAP	Indicate whether Kerberos should rely on LDAP to look up user IDs and Group IDs. This setting is disabled by default. *Note: Make sure to configure LDAP if you select this option.*
Data Ports	The ports users are able to monitor and interact with using the `connect direct` command. **U** and **L** denote the PC Card upper and lower slots. **U1** denotes the USB port.
Listen Port	The ports users are able to monitor using the `connect listen` command.
Clear Port Buffers	The ports whose port buffer users may clear using the `set log clear` command.

3. In the **User Rights** section, select the user group to which Kerberos users will belong.

Group	Select the group to which the Kerberos users will belong: ◆ **Default Users:** This group has only the most basic rights (described above). ◆ **Power Users:** This group has the same rights as Default Users plus **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. ◆ **Administrators:** This group has all possible rights.

4. Select or clear the checkboxes for the following rights.

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.

Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure IT management devices (e.g., SLP power managers, Spider devices, SLC console managers) on the local subnet.
Date/Time	Right to set the date and time.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI for Kerberos users.
Reboot & Shutdown	Right to use the CLI or shut down the SLC device and then reboot it.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
SLC Network	Right to view and manage SLC console managers on the local subnet.
Web Access	Right to access Web-Manager.
Device Port Configuration	Right to enter device port settings.
Device Port Operations	Right to control device ports.
PC Card or USB	Right to enter modem settings for PC Cards or the USB port.

5. Click the **Apply** button.

Note: *You must reboot the SLC device before your changes take effect.*

Kerberos Commands

The following CLI commands correspond to the **Kerberos** page. For more information, see *Chapter 15: Command Reference* .

- *set kerberos (on page 234)*
- *show kerberos (on page 234)*

TACACS+

Similar to RADIUS, the main function of TACACS+ is to perform authentication for remote access. The SLC console manager supports the TACACS+ protocol (not the older TACACS or XTACACS protocols).

The system administrator can configure the SLC unit to use TACACS+ to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

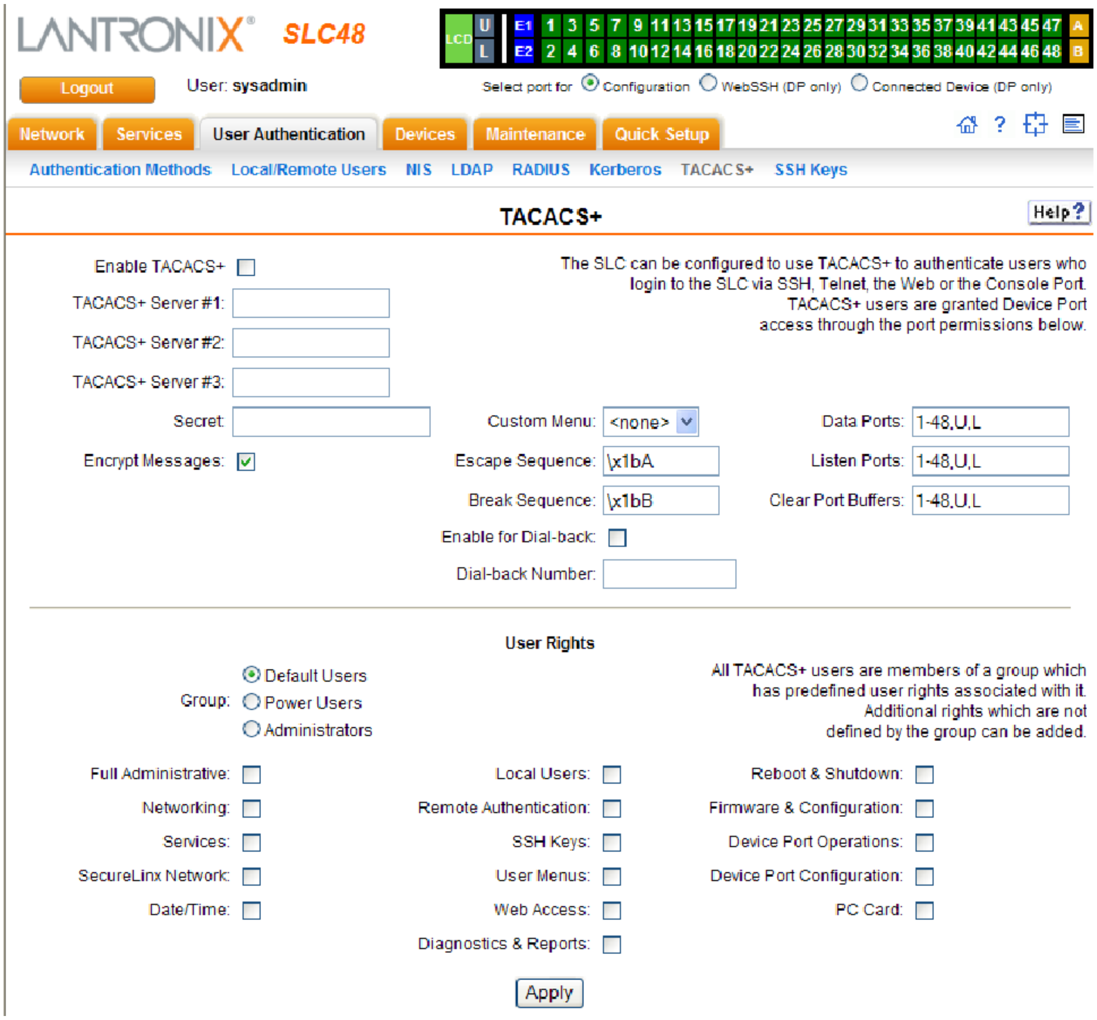
Users who are authenticated through Kerberos are granted device port access through the port permissions on this page.

All Kerberos users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

To configure the SLC console manager to use TACACS+ to authenticate users:

1. Click the **TACACS+** tab and select **TACACS+**. *Figure 12-9* shows the page that displays.

Figure 12-9 TACACS+ Page


LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network | Services | User Authentication | Devices | Maintenance | Quick Setup
Authentication Methods | Local/Remote Users | NIS | LDAP | RADIUS | Kerberos | TACACS+ | SSH Keys
Help?
Apply

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

TACACS+

Enable TACACS+ □

TACACS+ Server #1:

TACACS+ Server #2:

TACACS+ Server #3:

Secret:

Encrypt Messages: ☑

The SLC can be configured to use TACACS+ to authenticate users who login to the SLC via SSH, Telnet, the Web or the Console Port. TACACS+ users are granted Device Port access through the port permissions below.

Custom Menu: <none>

Escape Sequence: \x1bA

Break Sequence: \x1bB

Enable for Dial-back: □

Dial-back Number:

Data Ports: 1-48,U,L

Listen Ports: 1-48,U,L

Clear Port Buffers: 1-48,U,L

User Rights

Group: ● Default Users ○ Power Users ○ Administrators

All TACACS+ users are members of a group which has predefined user rights associated with it. Additional rights which are not defined by the group can be added.

Full Administrative: □ | Local Users: □ | Reboot & Shutdown: □
Networking: □ | Remote Authentication: □ | Firmware & Configuration: □
Services: □ | SSH Keys: □ | Device Port Operations: □
SecureLinx Network: □ | User Menus: □ | Device Port Configuration: □
Date/Time: □ | Web Access: □ | PC Card: □
Diagnostics & Reports: □

2. Enter the following fields.

Enable TACACS+	Displays selected if you enabled this method on the **User Authentication** page. If you want to set up this authentication method but not enable it immediately, clear the checkbox. You can enable TACACS+ here or on the first **User Authentication** page. If you enable TACACS+ here, it automatically displays at the end of the order of precedence on the **User Authentication** page.

TACACS+ Servers 1-3	IP address or host name of up to three TACACS+ servers.
Secret	Shared secret for message encryption between the SLC console manager and the TACACS+ server. Enter an alphanumeric secret of up to 127 characters.
Encrypt Messages	Select the checkbox to encrypt messages between the SLC device and the TACACS+ server. Selected by default.
Custom Menu	If custom menus have been created (see *the User Guide*), you can assign a default custom menu to TACACS+ users.
Escape Sequence	A single character or a two-character sequence that causes the SLC console manager to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is **Esc+A** (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as **\x1bA**, which is hexadecimal **(\x)** character 27 (**1B**) followed by an **A**. This setting allows the user to terminate the `connect direct` command on the command line interface when the endpoint of the command is `deviceport`, `tcp`, or `udp`.
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is **Esc+B** (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as **\x1bB**, which is hexadecimal **(\x)** character 27 (**1B**) followed by a **B**.
Enable for Dial-back	Select to grant a user dial-back access. Users with dial-back access can dial into the SLC unit and enter their login and password. Once the SLC console manager authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user's login (specified here).
Data Ports	The ports users are able to monitor and interact with using the `connect direct` command. **U** and **L** denote the upper and lower slots of the PC Card. U1 denotes the USB port.
Listen Port	The ports users are able to monitor using the `connect listen` command.
Clear Port Buffers	The ports whose port buffer users may clear using the `set log clear` command.

3. In the **User Rights** section, select the user group to which TACACS+ users belong.

Group	Select the group to which the TACACS+ users will belong: **Default Users:** This group has only the most basic rights (described above). **Power Users:** This group has the same rights as Default Users plus **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. **Administrators:** This group has all possible rights.

4. Select or clear the checkboxes for the following rights:

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.

Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure IT management devices (e.g., SLP power managers, Spider devices, SLC console managers) on the local subnet.
Date/Time	Right to set the date and time.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI for TACACS+ users.
Reboot & Shutdown	Right to use the CLI or shut down the SLC device and then reboot it.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
SLC Network	Right to view and manage SLC console managers on the local subnet.
Web Access	Right to access Web-Manager.
Device Port Configuration	Right to enter device port settings.
Device Port Operations	Right to control a device port.
PC Card or USB	Right to enter modem settings for PC Cards or USB port.

5. Click the **Apply** button.

Note: *You must reboot the unit before your changes will take effect.*

TACACS+ Commands

The following CLI commands correspond to the **TACACS+** page. For more information, see *Chapter 15: Command Reference* .

- *set tacacs+ (on page 258)*
- *show tacacs+ (on page 258)*

SSH Keys

The SLC console manager can import and export SSH keys to facilitate shared key authentication for all incoming and outgoing SSH connections. By using a public/private key pair, a user can access multiple hosts with a single passphrase, or, if a passphrase is not used, a user can access multiple hosts without entering a password. In either case, the authentication is protected against security attacks because both the public key and the private key are required to authenticate.

For both imported and exported SSH keys, the SLC device supports both RSA and DSA keys, and can import and export keys in OpenSSH and SECSH formats. Imported and exported keys are saved with the SLC configuration, and the administrator has the option of retaining the SSH keys during a reset to factory defaults.

The SLC console manager can also update the SSH RSA1, RSA and DSA host keys that the SSH server uses with site-specific host keys or reset them to the default values.

Imported Keys

Imported SSH keys must be associated with an SLC local user. The key can be generated on host “MyHost” for user “MyUser,” and when the key is imported into the SLC unit, it must be associated with either “MyUser” (if “MyUser” is an existing SLC local user) or an alternate SLC local user.

The public key file can be imported via SCP or FTP; once imported, you can view or delete the public key. Any SSH connection into the SLC console manager from the designated host/user combination uses the SSH key for authentication.

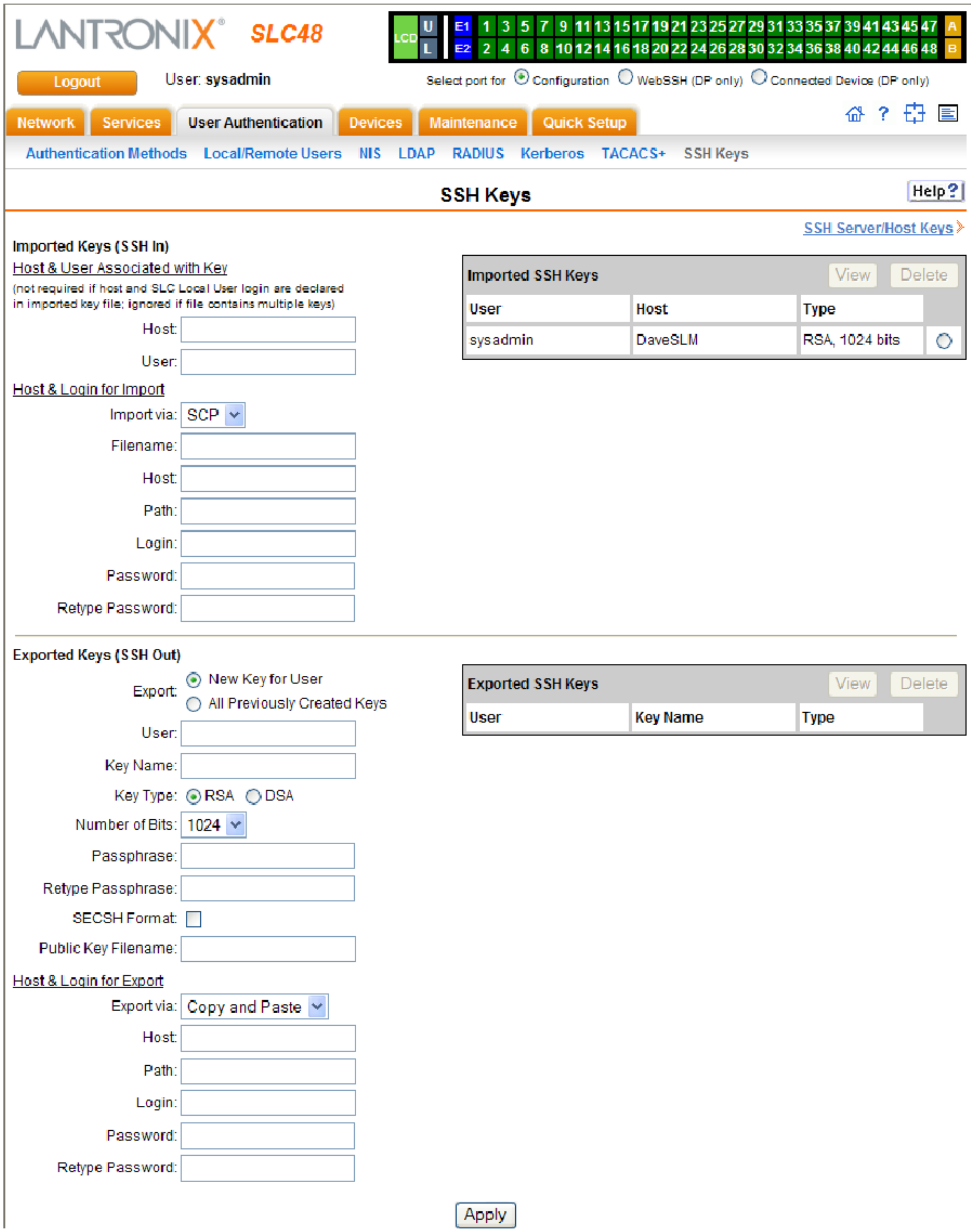
Exported Keys

The SLC device can generate SSH keys for SSH connections out of the SLC console manager for any SLC user. The SLC unit retains both the private and public key on the SLC console manager, and makes the public key available for export via SCP, FTP, or copy and paste. The name of the key is used to generate the name of the public key file that is exported (for example, <keyname>.pub), and the exported keys are organized by user and key name. Once a key is generated and exported, you can delete the key or view the public portion. Any SSH connection out of the SLC device for the designated host/user combination uses the SSH key for authentication.

To configure the SLC console manager to use SSH keys to authenticate users:

1. From the main menu, select **User Authentication – SSH Keys**. *Figure 12-10* shows the page that displays.

Figure 12-10 SSH Keys Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

SSH Keys

Imported Keys (SSH In)

Host & User Associated with Key

(not required if host and SLC Local User login are declared in imported key file; ignored if file contains multiple keys)

Host:

User:

Host & Login for Import

Import via: SCP

Filename:

Host:

Path:

Login:

Password:

Retype Password:

Imported SSH Keys

User	Host	Type	
sysadmin	DaveSLM	RSA, 1024 bits	○

Exported Keys (SSH Out)

Export: ● New Key for User ○ All Previously Created Keys

User:

Key Name:

Key Type: ● RSA ○ DSA

Number of Bits: 1024

Passphrase:

Retype Passphrase:

SECSH Format: □

Public Key Filename:

Host & Login for Export

Export via: Copy and Paste

Host:

Path:

Login:

Password:

Retype Password:

Exported SSH Keys

User	Key Name	Type

2. Enter the following fields.

Imported Keys (SSH In)

Host & User Associated with Key	These entries are required in the following cases:
	◆ The imported key file does not contain the host that the user will be making an SSH connection from, or
	◆ The SLC local user login for the connection is different from the user name the key was generated from or is not included in the imported key file.
	If either of these conditions is true, or the imported file is in SECSH format, you must specify the user and host. The following is an example of a public key file that includes the user and host:
	`ssh`
	`ssh-rsa`
	`AAAAB3NzaClyc2EAAAABIwAAAEEApUHCX9EWsHt+jmUGXa1YC3us`
	`ABYxIXUhSU1N+NU9HNaUADUFfd8LYz8/gUnUSH4Ksm8GRT7/`
	`8Sn9jCVfGPh`
	`UQ== asa11away@winserver`

Host	Host name or IP address from which the SSH connections to the SLC console manager will be made.
User	The User ID of the user being given secure access to the SLC device.

Host & Login for Import

Import via	Select **SCP** or **FTP** as the method for importing the SSH keys. **SCP** is the default.
Filename	Name of the public key file (for example, mykey.pub). May contain multiple keys.
Host	IP address of the remote server from which to SCP or FTP the public key file.
Path	Optional path name to the public key file.
Login	User ID to use to SCP or FTP the file.
Password/Retype Password	Password to use to SCP or FTP the file.

Exported Keys (SSH Out)

Export	Enables you to export created public keys. Select one of the following: **New Key for User:** Enables you to create a new key for a user and export the public key in a file. **All Previously Created Keys**: Does not create any keys, but exports all previously created public keys in one file.
User	User ID of the person given secure access to the remote server.
Key Name	Name of the key. This will generate the public key filename (e.g., <keyname>.pub).
Key Type	Select either the **RSA** or the **DSA** encryption standard. **RSA** is the default.
Number of Bits	Select the number of bits in the key (**512**, **1024**, or **2048**). The default is **1024**.

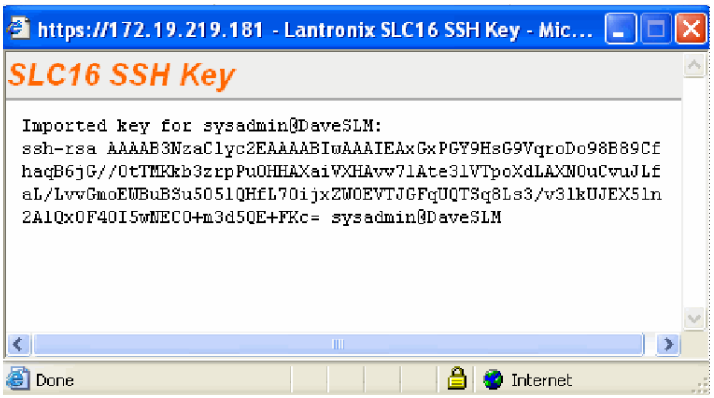
Passphrase/ Retype Passphrase	Optionally, enter a passphrase associated with the key. The passphrase may have up to 50 characters. The passphrase is an optional password that can be associated with an SSH key. It is unique to each user and to each key.
SECSH Format	Indicate whether the keys will be exported in **SECSH** format (by default the key is exported in **OpenSSH** format).
Public Key Filename	Filename of the public host key.

Host and Login for Export

Export via	Select the method (**SCP**, **FTP**, or **Cut and Paste)** of exporting the key to the remote server. **Cut and Paste**, the default, requires no other parameters for export.
Host	IP address of the remote server to which the SLC console manager will SCP or FTP the public key file.
Path	Optional path of the file on the host to SCP or FTP the public key too.
Login	User ID to use to SCP or FTP the public key file.
Password/Retype Password	Password to use to SCP or FTP the public key file.

To view or delete a key:

1. Select the key from the appropriate table. The **View** and **Delete** buttons become active.
2. To view the key, click the **View** button. A pop-up page displays the key.



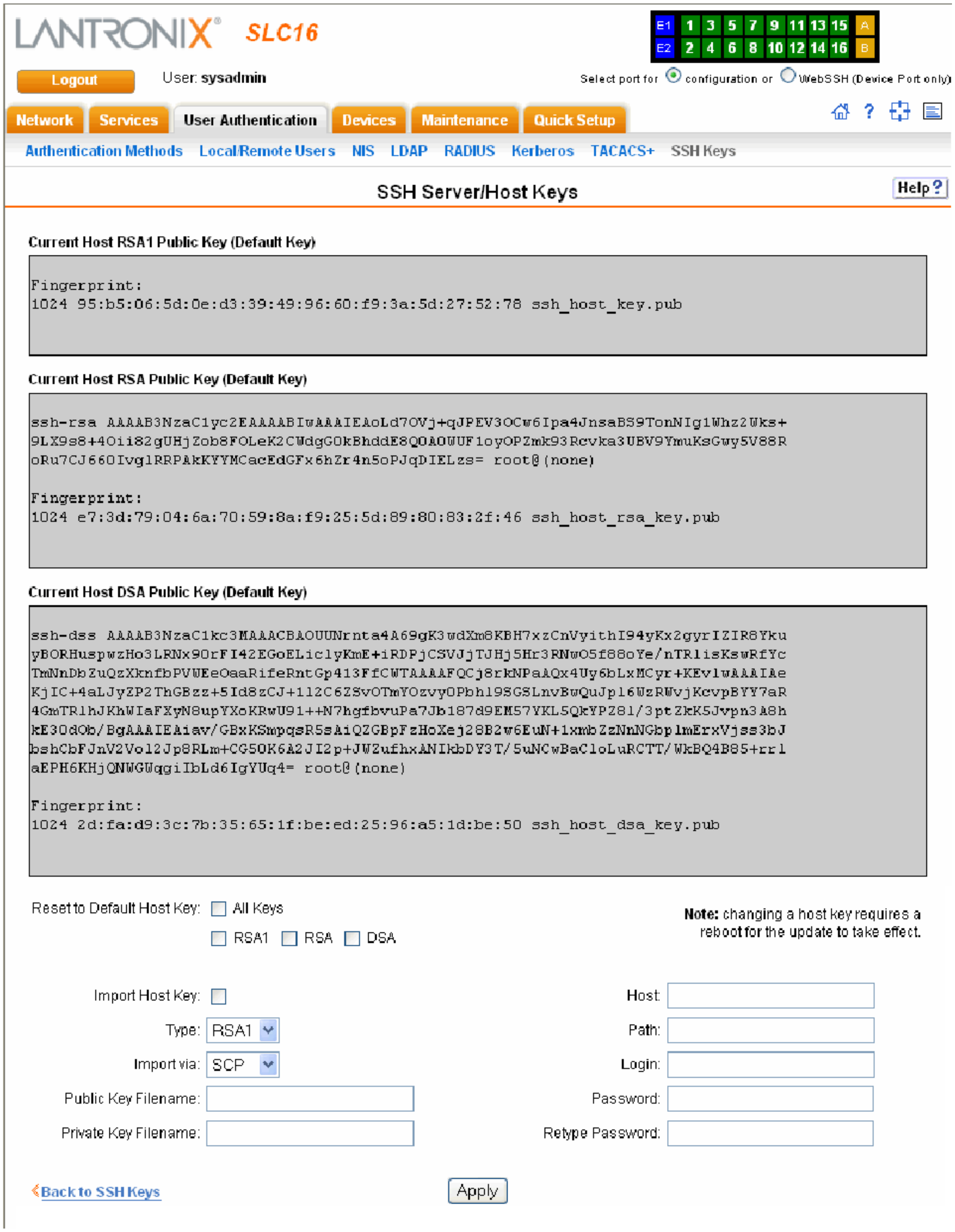
```
Imported key for sysadmin@DaveSLM:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxGxPGY9HsG9VqroDo98B89Cf
haqB6jG//0tTMKkb3zrpPuOHHAXaiVXHAvv7lAte3lVTpoXdLAXN0uCvuJLf
aL/LvvGmoEWBuBSu5051QHfL70ijxZW0EVTJGFqUQTSq8Ls3/v3lkUJEX5ln
2AlQx0F40I5wNEC0+m3d5QE+FKc= sysadmin@DaveSLM
```

3. To delete the key, click the **Delete** button.

To view, reset, or import SSH RSA1, RSA, And DSA host keys:

1. On the **User Authentication – SSH Keys** page, click the **SSH Server/Host Keys** link at the top right. *Figure 12-11* shows the page that displays. The current host keys that are also the defaults are listed.

Figure 12-11 SSH Server/Host Keys Page



SSH Server/Host Keys

Current Host RSA1 Public Key (Default Key)

```
Fingerprint:
1024 95:b5:06:5d:0e:d3:39:49:96:60:f9:3a:5d:27:52:78 ssh_host_key.pub
```

Current Host RSA Public Key (Default Key)

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAoLd7OVj+qJPEV3OCw6Ipa4JnsaBS9TonNIg1Whz2Wks+
9LX9s8+4Oii82gUHjZob8FOLeK2CWdgGOkBhddE8Q0AOWUF1oyOPZmk93Rcvka3UBV9YmuKsGwy5V88R
oRu7CJ66OIvglRRPAkKYYMCacEdGFx6hZr4n5oPJqDIELzs= root@(none)

Fingerprint:
1024 e7:3d:79:04:6a:70:59:8a:f9:25:5d:89:80:83:2f:46 ssh_host_rsa_key.pub
```

Current Host DSA Public Key (Default Key)

```
ssh-dss AAAAB3NzaC1kc3MAAACBAOUUNrnta4A69gK3wdXm8KBH7xzCnVyithI94yKx2gyrIZIR8Yku
yBORHuspwzHo3LRNx9OrFI42EGoELiclyKmE+iRDPjCSVJjTJHj5Hr3RNwO5f88oYe/nTRlisKswRfYc
TmNnDbZuQzXknfbPVWEeOaaRifeRntGp413FfCWTAAAAFQCj8rkNPaAQx4Uy6bLxMCyr+KEvlwAAAIAe
KjIC+4aLJyZP2ThGBzz+5Id8zCJ+112C6ZSvOTmYOzvy0Pbh19SGSLnvBwQuJp16WzRWvjKcvpBYY7aR
4GmTRlhJKhWIaFXyN8upYXoKRwU91++N7hgfbvuPa7Jb187d9EM57YKL5QkYPZ81/3ptZkK5Jvpn3A8h
kE3OdOb/BgAAAIEAiav/GBxKSmpqsR5sAiQZGBpFzHoXej28B2w6EuN+1xmbZzNnNGbplmErxVjss3bJ
bshCbFJnV2Vol2Jp8RLm+CG5OK6A2JI2p+JWZufhxANIkbDY3T/5uNCwBaCloLuRCTT/WkBQ4B85+rrl
aEPH6KHjQNWGWqgiIbLd6IgYUq4= root@(none)

Fingerprint:
1024 2d:fa:d9:3c:7b:35:65:1f:be:ed:25:96:a5:1d:be:50 ssh_host_dsa_key.pub
```

Reset to Default Host Key: □ All Keys

□ RSA1 □ RSA □ DSA

Note: changing a host key requires a reboot for the update to take effect.

Import Host Key: □

Type: RSA1

Import via: SCP

Public Key Filename:

Private Key Filename:

Host:

Path:

Login:

Password:

Retype Password:

2. Enter the following fields.

Reset to Default Host Key	Select the **All Keys** checkbox to reset all default key(s), or select one or more checkboxes to reset defaults for **RSA1**, **RSA**, or **DSA** keys. All checkboxes are unselected by default.
Import Host Key	To import a site-specific host key, select the checkbox. Unselected by default.

Type	From the drop-down list, select the type of host key to import.
Import via	From the drop-down list, select the method of importing the host key (SCP or SFTP). The default is **SCP.**
Public Key Filename	Filename of the public host key.
Private Key Filename	Filename of the private host key.
Host	Host name or IP address of the host from which to import the key.
Path	Path of the directory where the host key will be stored.
Login	User ID to use to SCP or SFTP the file.
Password & Retype Password	Password to use to SCP or SFTP the file.

3. Click the **Apply** button.

SSH Commands

The following CLI commands correspond to the **SSHKeys** page. For more information, see *Chapter 15: Command Reference* .

- *set sshkey allexport (on page 254)*
- *set sshkey delete (on page 254)*
- *set sshkey export (on page 255)*
- *set sshkey import (on page 255)*
- *set sshkey server import (on page 255)*
- *set sshkey server reset (on page 255)*
- *show sshkey export (on page 256)*
- *show sshkey import (on page 256)*
- *show sshkey server (on page 256)*

Custom User Menus

Local and remote users can have a custom user menu as their command line interface rather than the standard command set. Instead of typing each command, the user enters the number associated with the command. Each command can also have a nickname that can display in the menu instead of the command.

From one menu, a user can display another menu, so that menus are nested. The special command `show menu` displays a specified menu. The special command `return menu` displays the parent menu if the current menu was displayed from a `show menu` command.

The user with appropriate rights creates and manages custom user menus from the command line interface, but can assign a custom user menu to a user from either the command line or the web interface.

For example, the system administrator creates two custom user menus, with menu1 having a nested menu (menu2). Arrow keys can be used at the Command and Nickname prompts to cycle through previously entered commands and nicknames.

```
[slc]> set menu add menu1
Enter optional menu title (<return> for none): Menu1 Title
Specify nickname for each command? [no] y
Enter each command, up to 50 commands ('logout' is always the last command).
Press <return> when the menu command set is complete.

Command  #1: connect direct deviceport 1
Nickname #1: connect Port-1
Command  #2: connect direct deviceport 2
Nickname #2: connect Port-2
Command  #3: showmenu menu2
Warning: menu 'menu2' does not exist.
Nickname #3: menu2
Command  #4:
Command  #4: logout
Nickname #4: log off
Custom User Menu settings successfully updated.
[slc]> set menu add menu2
Enter optional menu title (<return> for none): Menu2 Title
Specify nickname for each command? [no]
Enter each command, up to 50 commands ('logout' is always the last command).
Press <return> when the menu command set is complete.

Command  #1: connect direct deviceport 3
Command  #2: connect direct deviceport 4
Command  #3: show datetime
Command  #4: returnmenu
Command  #5:
Command  #5: logout
Custom User Menu settings successfully updated.
[slc]> show menu all
___Custom User Menus___________________________________________________________
menu1             menu2
[slc]> show menu menu1
___Custom User Menus___________________________________________________________
Menu: menu1
Title: Menu1 Title
Show Nicknames: enabled
Redisplay Menu: disabled
Command   1: connect direct deviceport 1
Nickname  1: connect Port-1
Command   2: connect direct deviceport 2
Nickname  2: connect Port-2
Command   3: showmenu menu2
Nickname  3: menu2
Command   4: logout
Nickname  4: log off
[slc]> show menu menu2
```

```
__Custom User Menus___________________________________________________________
Menu: menu2
Title: Menu2 Title
Show Nicknames: disabled
Redisplay Menu: disabled
Command   1: connect direct deviceport 3
Nickname  1: <none>
Command   2: connect direct deviceport 4
Nickname  2: <none>
Command   3: show datetime
Nickname  3: <none>
Command   4: returnmenu
Nickname  4: <none>
Command   5: logout
Nickname  5: <none>
```

The system administrator configures local user “john” to use custom menu “menu1”:

```
[slc]> set localusers edit john custommenu menu1
Local users settings successfully updated.
[slc]> show localusers user john
___Current Local Users Settings________________________________________________
Login: john
    Password: <set>  UID: 101
    Listen Ports: 1-32
    Data Ports: 1-32
    Clear Ports: 1-32
    Escape Sequence: \x1bA  Break Sequence: \x1bB
    Custom Menu: menu1
    Allow Dialback: disabled
    Dialback Number: <none>
```

User “john” logs into the command line interface, initially sees menu1, executes the command to jump to nested menu menu2, and then returns to menu1:

```
Welcome to the SLC Console Manager
Model Number: SLC32
For a list of commands, type 'help'.

[Enter 1-4]> help
                                Menu1 Title
-------------------------------------------------------------------------
 1) connect Port-1                    3) menu2
 2) connect Port-2                    4) log off
[Enter 1-4]> 3
Executing: showmenu menu2

[Enter 1-5]> help
Menu2 Title
-----------
 1) connect direct deviceport 3
 2) connect direct deviceport 4
 3) show datetime
 4) returnmenu
 5) logout
[Enter 1-5]> 3
Executing: show datetime
Date/Time: Tue Sep  7 19:13:35 2004
Timezone: UTC
[Enter 1-5]> 4
Executing: returnmenu

[Enter 1-4]> help

                                Menu1 Title
-------------------------------------------------------------------------
1) connect Port-1                    3) menu2
2) connect Port-2                    4) log off
[Enter 1-4]> 4
Executing: logout
Logging out...
```

Creating custom menus has the following limitations:

- Maximum of 20 custom user menus.
- Maximum of 50 commands per custom user menu (`logout` is always the last command).
- Maximum of 15 characters for menu names.
- Maximum of five nested menus can be called.
- No syntax checking (Enter each command correctly).

Custom User Menus Commands

The following CLI commands configure and display custom menus. For more information, see *Chapter 15: Command Reference* .

- *set localusers menu (on page 220)*
- *set menu add (on page 220)*
- *set menu copy (on page 220)*

- *set menu edit (on page 220)*
- *set menu delete (on page 221)*
- *set cli menu (on page 220)*
- *show menu (on page 221)*

13: Maintenance

This chapter describes the tasks that the system administrator performs by using the pages of the **Maintenance** tab and additional commands on the command line interface. It contains the following sections:

- *Firmware and Configurations*
- *System Logs*
- *Audit Log*
- *Email Log*
- *Diagnostics*
- *Status/Reports*
- *Events*
- *Banners*
- *LCD and Keypad*

Note: *The features and functionality described in this chapter specific to PC Card use are supported on SLC-02 part numbers. The features and functionality specific to USB port use are supported on SLC-03 part numbers.*

Firmware and Configurations

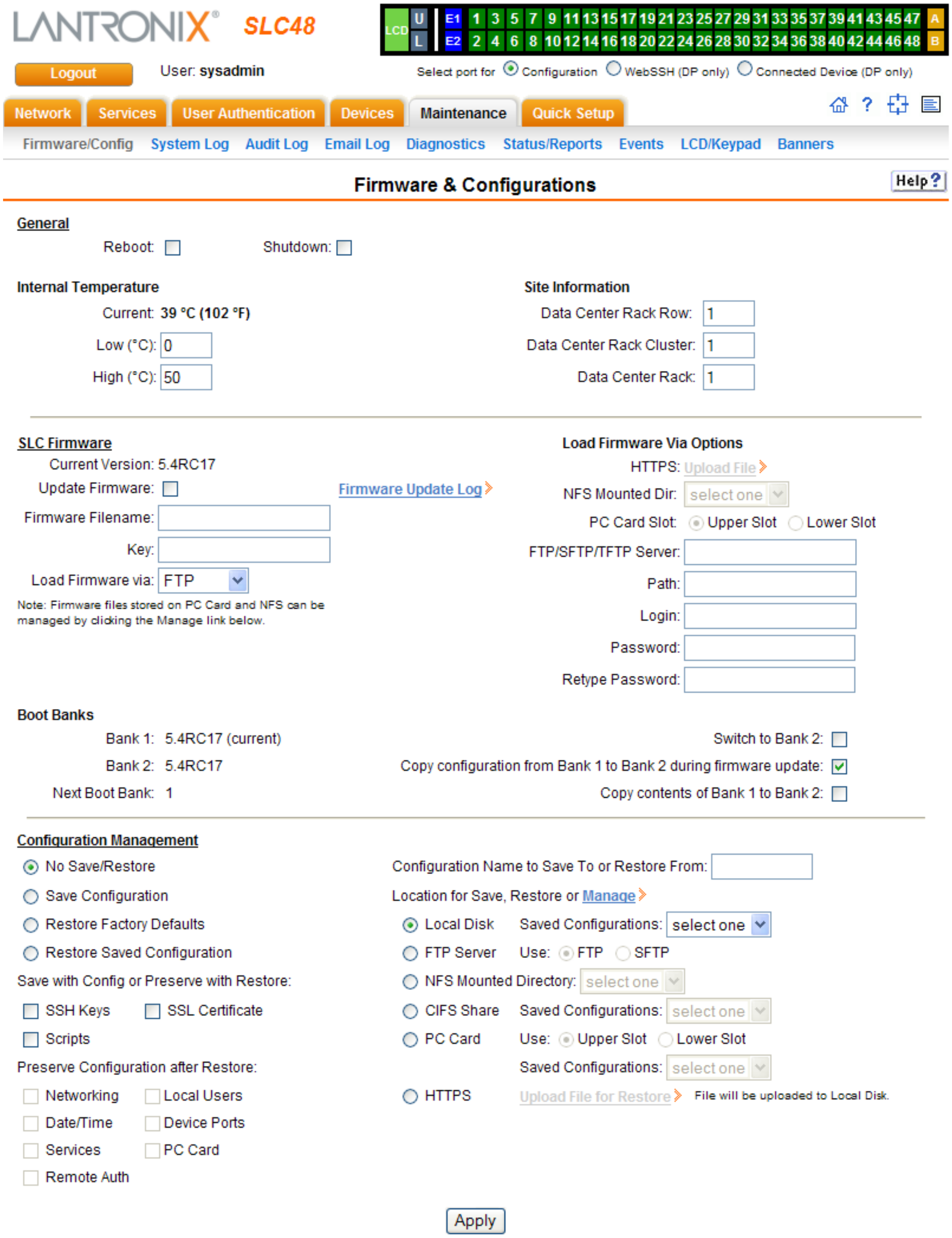
The SLC device **Firmware & Configurations** page allows the system administrator to:

- Configure the FTP, SFTP, or TFTP server that will be used to provide firmware updates and save/restore configurations. (TFTP is only used for firmware updates.)
- Set up the location or method that will be used to save or restore configurations (default, FTP, SFTP, NFS, CIFS, USB port, or PC Card). Update the version of the firmware running on the SLC console manager.
- Save a snapshot of all settings on the SLC device (save a configuration).
- Restore the configuration, either to a previously saved configuration, or to the factory defaults.
- For dual boot SLC console managers, view the firmware version on each boot bank, select the bank to boot from, and copy the contents of one boot bank to the other.

To configure settings:

1. Click the **Maintenance** tab. *Figure 13-1* shows the page that displays.

Figure 13-1 Firmware & Configurations Page



LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
Network Services User Authentication Devices Maintenance Quick Setup
Firmware/Config System Log Audit Log Email Log Diagnostics Status/Reports Events LCD/Keypad Banners
Help?

User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Firmware & Configurations

General

Reboot: □ Shutdown: □

Internal Temperature

Current: 39 °C (102 °F)

Low (°C): 0

High (°C): 50

Site Information

Data Center Rack Row: 1

Data Center Rack Cluster: 1

Data Center Rack: 1

SLC Firmware

Current Version: 5.4RC17

Update Firmware: □ Firmware Update Log

Firmware Filename:

Key:

Load Firmware via: FTP

Note: Firmware files stored on PC Card and NFS can be managed by clicking the Manage link below.

Load Firmware Via Options

HTTPS: Upload File

NFS Mounted Dir: select one

PC Card Slot: ● Upper Slot ○ Lower Slot

FTP/SFTP/TFTP Server:

Path:

Login:

Password:

Retype Password:

Boot Banks

Bank 1: 5.4RC17 (current)

Bank 2: 5.4RC17

Next Boot Bank: 1

Switch to Bank 2: □

Copy configuration from Bank 1 to Bank 2 during firmware update: ☑

Copy contents of Bank 1 to Bank 2: □

Configuration Management

● No Save/Restore

○ Save Configuration

○ Restore Factory Defaults

○ Restore Saved Configuration

Save with Config or Preserve with Restore:

□ SSH Keys □ SSL Certificate

□ Scripts

Preserve Configuration after Restore:

□ Networking □ Local Users

□ Date/Time □ Device Ports

□ Services □ PC Card

□ Remote Auth

Configuration Name to Save To or Restore From:

Location for Save, Restore or Manage

● Local Disk Saved Configurations: select one

○ FTP Server Use: ● FTP ○ SFTP

○ NFS Mounted Directory: select one

○ CIFS Share Saved Configurations: select one

○ PC Card Use: ● Upper Slot ○ Lower Slot

Saved Configurations: select one

○ HTTPS Upload File for Restore File will be uploaded to Local Disk.

Apply

2. Enter the following fields.

General

Reboot	Select this option to reboot the SLC console manager immediately. The default is **No**. **Note:** *The front panel LCD displays the "Rebooting the SLC message, and the normal boot sequence occurs.*
Shutdown	Select this option to shut down the SLC console manager. The default is **No**.
Internal Temperature-Current/Low/High	Sets the acceptable range for the internal temperature of the SLC device. If the temperature of the SLC console manager changes to be outside of this range, the SLC device will issue an SNMP trap.
Data Center Rack Row, Rack Cluster, Rack	Set these fields to define where the SLC console manager is located within a large data center. The default for these fields is 1.

SLC Firmware

Update Firmware	To update the SLC firmware, select the checkbox. If you select this option, the SLC console manager reboots after you apply the update. To view a log of all prior firmware updates, click the **Firmware Update Log** link. **Note:** *For dual boot SLC devices, the non-active boot bank is updated during the firmware update, without requiring a reboot. The configuration on the current boot bank may optionally be copied to the non-active boot bank during the firmware update.*
Load Firmware via	From the drop-down list, select the method of loading the firmware. Options are **FTP**, **TFTP**, **HTTPS**, **SFTP (Secure FTP)**, **PC Card**, **USB**, and **NFS**. **FTP** is the default. If you select **HTTPS**, the **Upload File** link becomes active. Select the link to open a popup window that allows you to browse to a firmware update file to upload. If you select **NFS**, the mount directory must be specified. If you select **PC Card**, the upper or lower slot must be selected. If you select **USB**, port U1 is automatically selected
Firmware Filename	The name of the firmware update file downloaded from the Lantronix web site.
Key	A 32-hex character key for validating the firmware file. The key is provided in the firmware Release Notes available with the SLC firmware at www.lantronix.com/support/downloads.

Load Firmware Via Options

HTTPS	Displays an **Upload File** link when HTTPS is selected from the **Load Firmware via:** pull-down menu (on the left of the page). When you click on the link, another window opens and enables you to browse for the file.

NFS Mounted Dir	Displays created NFS local directories. *Note: You must create NFS mounts by using the **Services** tab and accessing the **NFS/CIFS** page.*
PC Card Slot or USB	For the SLC device with the PC Card slots, select the upper slot or lower slot options. For the SLC console manager with the USB port, U1 is automatically selected.
FTP/SFTP/TFTP Server	The IP address or host name of the server used for obtaining updates and saving or restoring configurations. May have up to 64 alphanumeric characters; may include hyphens and underscores.
Path	The default path on the server for obtaining firmware update files and getting and putting configuration save files.
Login	The userid for accessing the FTP server. May be blank.
Password & Retype Password	The FTP user password.

Boot Banks

Bank 1	Version of SLC firmware in bank 1. *Note: The word “current” displays next to the bank the SLC console manager booted from.*
Bank 2	Version of SLC firmware in bank 2.
Next Boot Bank	Current setting for bank to boot from at next reboot.
Switch to Bank	If desired, select the alternate bank to boot from at next reboot.
Copy configuration from Bank 1 to Bank 2 during firmware update	If checked, will copy the configuration from the current bank to the bank being updated.
Copy contents of Bank 1 to Bank 2	If checked, enables you to copy the current boot bank to the alternate boot bank. This process takes a few minutes to complete.

Configuration Management

Configuration Management	From the option list, select one of the following: ◆ **No Save/Restore:** Does not save or restore a configuration. ◆ **Save Configuration:** Saves all settings to file, which can be backed up to a location that is not on the SLC console manager. ◆ **Restore Factory Defaults:** Restores factory defaults. If you select this option, the SLC device reboots after you apply the update. Select the **Save SSH Keys** checkbox to save any imported or exported SSH keys. Select the **Save SSL Certificate** checkbox to save any imported certificate. Select the Scripts checkbox to save any interface or batch scripts. Disabled by default. ◆ **Restore Saved Configuration:** Returns the SLC settings to a previously saved configuration. If you select this option, the SLC device reboots after you apply the update.
Configuration Name to Save To or Restore From	If you selected to save or restore a configuration, enter a name for the configuration file (up to 12 characters).

Location for Save, Restore, or Manage	If you selected to save or restore a configuration, select one of the following options: ◆ **Local Disk – Saved Configurations:** If restoring, select a saved configuration from the drop-down list. ◆ **FTP Server:** The FTP server specified in the FTP/SFTP/TFTP section. If you select this option, select FTP or SFTP to transfer the configuration file. ◆ **NFS Mounted Directory:** Local directory of the NFS server for mounting files. ◆ **CIFS Share – Saved Configurations:** If restoring, select a saved configuration from the drop-down list. ◆ **PC Card:** If a PC Card Compact Flash is loaded into one of the PC Card slots on the front of the SLC console manager, and properly mounted (see 9: PC Cards), the configuration can be saved to or restored from this location. If you select this option, select the slot (upper or lower) in which the PC Card Compact Flash is mounted, and then select a saved configuration from the drop-down list. ◆ **USB**: If a USB device is loaded into the USB port on the front of the SLC device and properly mounted, the configuration can be saved to or restored from this location (see 10: USB Port). ◆ **HTTPS**: This option allows a configuration to be uploaded to the local disk for restore or saved via HTTPS. ◆ **Manage:** The **Manage** option allows you to view and delete all configurations saved to the selected location. This feature is available for the local disk, NFS, CIFS Share, USB port, and PC Card locations. (See next procedure).
Preserve Configuration after Restore	Allows the user to keep a subset of the current configuration after restoring a configuration or resetting to factory defaults. Select the checkbox for each part of the current configuration you want to keep, for example, Networking, Services, or Device Ports.

3. Click the **Apply** button.

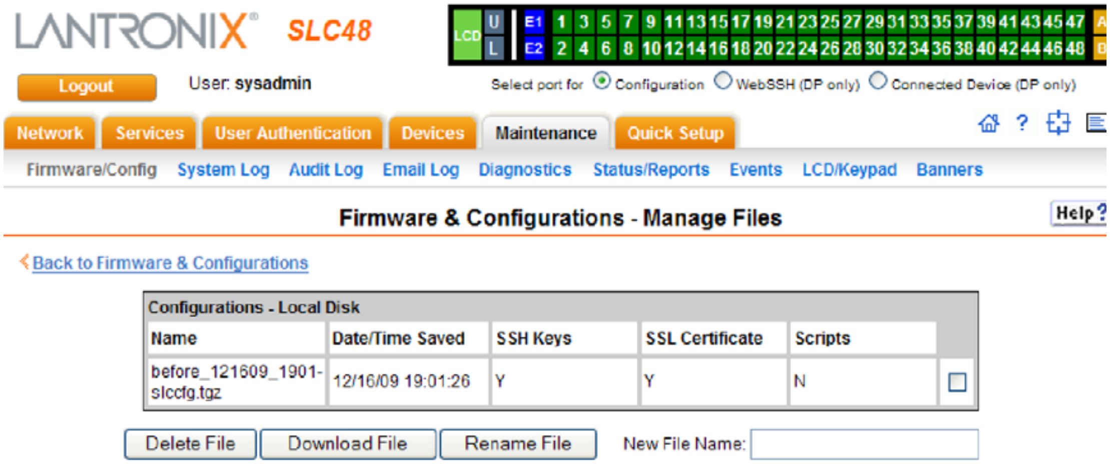
Note: If you selected an option that forces a reboot (restore configuration, update firmware, or reset factory defaults), the SLC console manager automatically reboots at the end of the process.

To manage configuration files:

The **Manage** option on the **Firmware & Configurations** page allows you to view all configurations saved to the selected location and delete any of the configurations. This feature is available for the local disk, NFS, CIFS Share, USB port, and PC Card locations.

1. On the **Firmware & Configurations** page, click the **Manage** link in the **Location for Save, Restore, or Manage** section of the page. *Figure 13-2* shows the page that displays.

Figure 13-2 Firmware & Configurations - Manage Configuration Files Page



Configurations - Local Disk

Name	Date/Time Saved	SSH Keys	SSL Certificate	Scripts	
before_121609_1901-slccfg.tgz	12/16/09 19:01:26	Y	Y	N	□

2. To download files, click the **Download File** button. A **File Download** window opens to confirm the download.
3. To rename files, check the box of the file that you want to rename and enter the new name in the text box. Click the **Rename File** button.
4. To delete files, select one or more files and click the **Delete File** button.

Firmware and Configurations Commands

The following CLI commands correspond to the **Firmware & Configurations** page. For more information, see *Chapter 15: Command Reference* .

- *admin reboot (on page 211)*
- *admin shutdown (on page 211)*
- *set temperature (on page 258)*
- *show temperature (on page 259)*
- *admin version (on page 212)*
- *admin firmware bootbank (on page 208)*
- *admin firmware copybank (on page 208)*
- *admin firmware show (on page 208)*
- *admin firmware update (on page 208)*
- *admin ftp password (on page 208)*
- *admin ftp server (on page 209)*
- *admin ftp show (on page 209)*
- *admin quicksetup (on page 211)*
- *admin config copy (on page 206)*
- *admin config rename|delete (on page 206)*
- *admin config factorydefaults (on page 206)*
- *admin config restore (on page 207)*

- *admin config save (on page 207)*
- *admin config show (on page 207)*

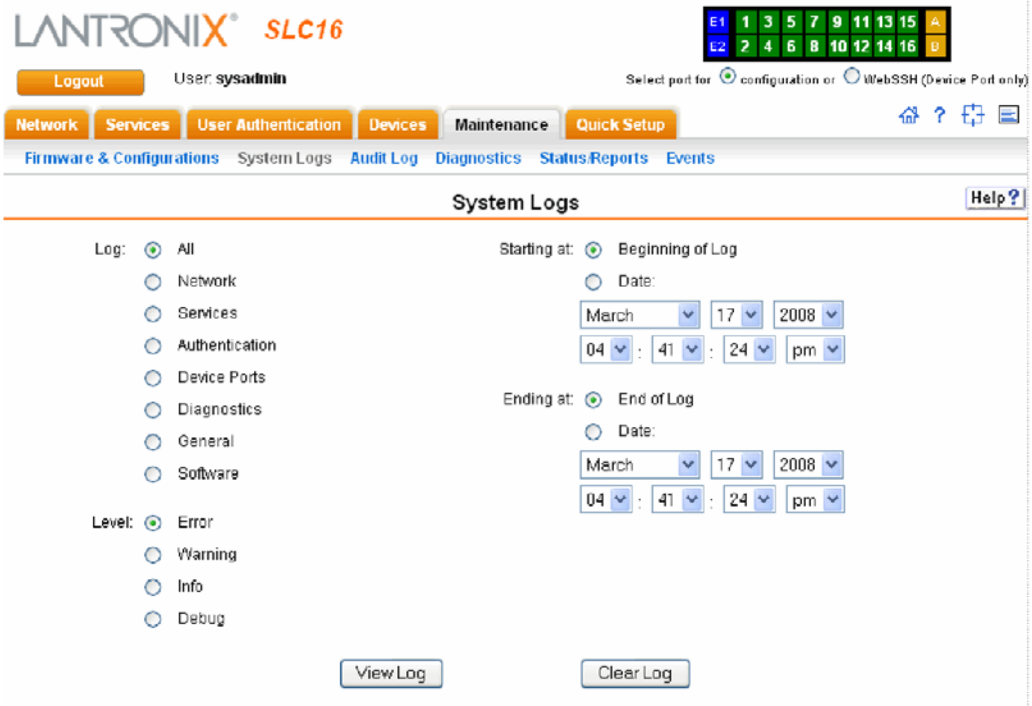
System Logs

The **System Logs** page allows you to view and clear system logs. See *Chapter 7: Services* for more information about system logs.

To view system logs:

1. Click the **Maintenance tab** and select the **System Logs** option. *Figure 13-3* shows the page that displays.

Figure 13-3 System Logs Page



User: sysadmin

Select port for ● configuration or ○ WebSSH (Device Port only)

System Logs

Log: ● All
○ Network
○ Services
○ Authentication
○ Device Ports
○ Diagnostics
○ General
○ Software

Level: ● Error
○ Warning
○ Info
○ Debug

Starting at: ● Beginning of Log
○ Date:
March 17 2008
04 : 41 : 24 pm

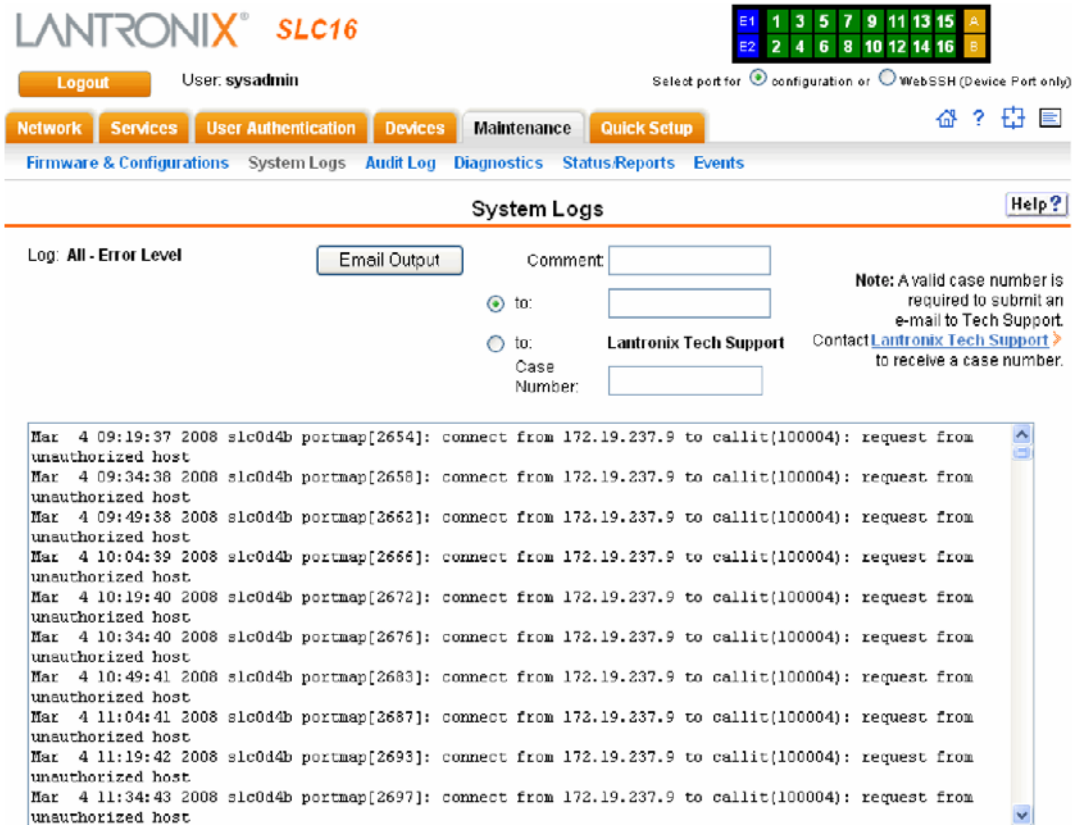
Ending at: ● End of Log
○ Date:
March 17 2008
04 : 41 : 24 pm

2. Enter the following fields.

Log	Select the type(s) of log you want to view.
Level	Select the alert level you want to view for the selected log.
Starting at	Select the starting point of the range you want to view: **Beginning of Log:** Beginning of the log. **Date:** Specific start date and time of the log.
Ending at	Select the endpoint of the range you want to view: **End of Log:** The end of the log. **Date:** Specific end date and time of the log.

3. Click the **View Log** button. The log displays. For example, if you select the type **All** and the level **Error**, the SLC device displays a log shown in *Figure 13-4*.

Figure 13-4 System Log Output Page



User: sysadmin

System Logs

Log: **All - Error Level**

Comment:

● to:

○ to: **Lantronix Tech Support**

Case Number:

Note: A valid case number is required to submit an e-mail to Tech Support. Contact Lantronix Tech Support to receive a case number.

```
Mar  4 09:19:37 2008 slc0d4b portmap[2654]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
Mar  4 09:34:38 2008 slc0d4b portmap[2658]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
Mar  4 09:49:38 2008 slc0d4b portmap[2662]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
Mar  4 10:04:39 2008 slc0d4b portmap[2666]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
Mar  4 10:19:40 2008 slc0d4b portmap[2672]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
Mar  4 10:34:40 2008 slc0d4b portmap[2676]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
Mar  4 10:49:41 2008 slc0d4b portmap[2683]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
Mar  4 11:04:41 2008 slc0d4b portmap[2687]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
Mar  4 11:19:42 2008 slc0d4b portmap[2693]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
Mar  4 11:34:43 2008 slc0d4b portmap[2697]: connect from 172.19.237.9 to callit(100004): request from
unauthorized host
```

4. To email the system log to an individual:
   a. In the **Comment** field, enter a comment (if desired).
   b. Select **to** and enter the person's email address.
   c. Press the **Email Output** button.
5. To email the system log to Lantronix Technical Support:
   a. In the **Comment** field, enter a comment (if desired).
   b. Select **to: Lantronix Tech Support.**
   c. Call Lantronix Tech Support and obtain a case number.

      For contact information, click the Lantronix Tech Support link.
   d. Enter the number in **Case Number**.
   e. Press the **Email Output** button.
6. A message asks for confirmation. Click **OK**.

To clear system logs:

1. Return to the System Logs page.
2. Select the logs you want to clear and click the **Clear Log** button.

System Logs Commands

The following CLI commands correspond to the **System Logs** page. For more information, see *Chapter 15: Command Reference* .

- *show syslog (on page 257)*
- *show syslog clear (on page 257)*

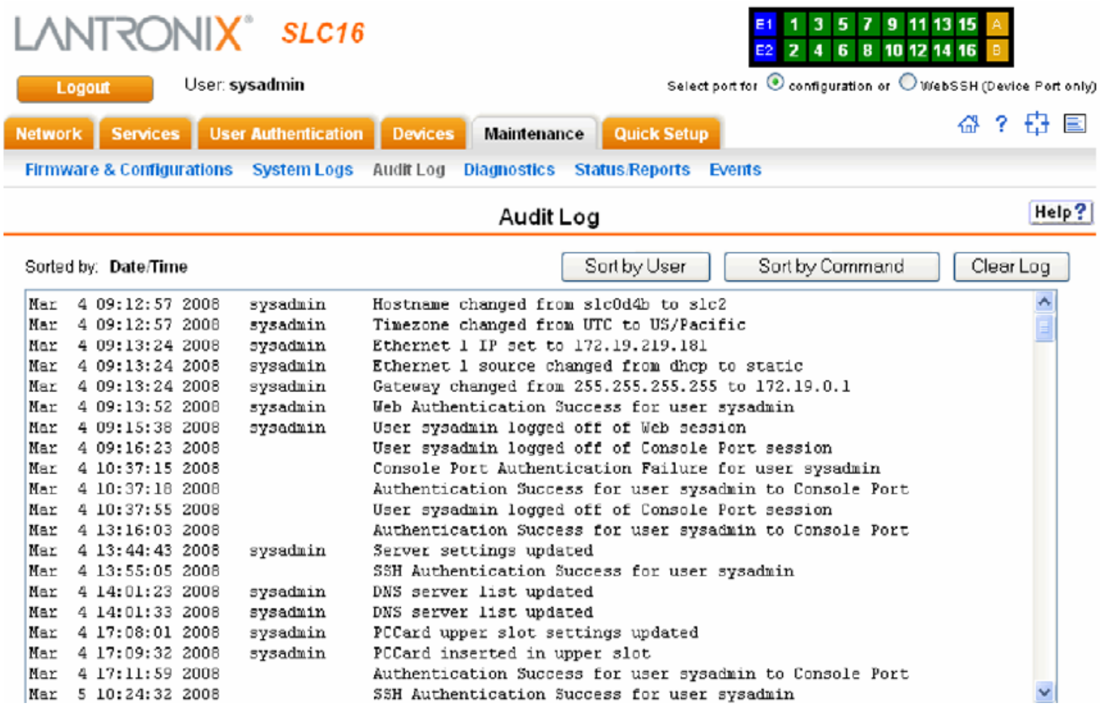
Audit Log

The Audit Log web page displays a log of all actions that have changed the configuration of the SLC console manager. The audit log is disabled by default. Use the **Services** web page (*Chapter 7: Services*) to enable the audit log and to configure its maximum size.

Each entry in the log file contains a date/time stamp, user login, and the action performed by the user. The user may clear the log file and sort the log by date/time, user, and command. The audit log is saved through SLC device reboots.

1. Click the **Maintenance** tab and select the **Audit Log** option. *Figure 13-5* shows the page that displays.

Figure 13-5 Audit Log Page



User: sysadmin

Select port for ● configuration or ○ WebSSH (Device Port only)

Audit Log

Sorted by: Date/Time

```
Mar  4 09:12:57 2008   sysadmin    Hostname changed from slc0d4b to slc2
Mar  4 09:12:57 2008   sysadmin    Timezone changed from UTC to US/Pacific
Mar  4 09:13:24 2008   sysadmin    Ethernet 1 IP set to 172.19.219.181
Mar  4 09:13:24 2008   sysadmin    Ethernet 1 source changed from dhcp to static
Mar  4 09:13:24 2008   sysadmin    Gateway changed from 255.255.255.255 to 172.19.0.1
Mar  4 09:13:52 2008   sysadmin    Web Authentication Success for user sysadmin
Mar  4 09:15:38 2008   sysadmin    User sysadmin logged off of Web session
Mar  4 09:16:23 2008               User sysadmin logged off of Console Port session
Mar  4 10:37:15 2008               Console Port Authentication Failure for user sysadmin
Mar  4 10:37:18 2008               Authentication Success for user sysadmin to Console Port
Mar  4 10:37:55 2008               User sysadmin logged off of Console Port session
Mar  4 13:16:03 2008               Authentication Success for user sysadmin to Console Port
Mar  4 13:44:43 2008   sysadmin    Server settings updated
Mar  4 13:55:05 2008               SSH Authentication Success for user sysadmin
Mar  4 14:01:23 2008   sysadmin    DNS server list updated
Mar  4 14:01:33 2008   sysadmin    DNS server list updated
Mar  4 17:08:01 2008   sysadmin    PCCard upper slot settings updated
Mar  4 17:09:32 2008   sysadmin    PCCard inserted in upper slot
Mar  4 17:11:59 2008               Authentication Success for user sysadmin to Console Port
Mar  5 10:24:32 2008               SSH Authentication Success for user sysadmin
```

2. To select a sort option (by User or Command) click the appropriate button:

- To sort by user, click the **Sort by User** button.
- To sort by command/action, click the **Sort by Command** button.

3. To clear the log, click the **Clear Log** button.

Audit Log Commands

The following CLI commands correspond to the **Audit Log** page. For more information, see *Chapter 15: Command Reference* .

- *show auditlog (on page 213)*

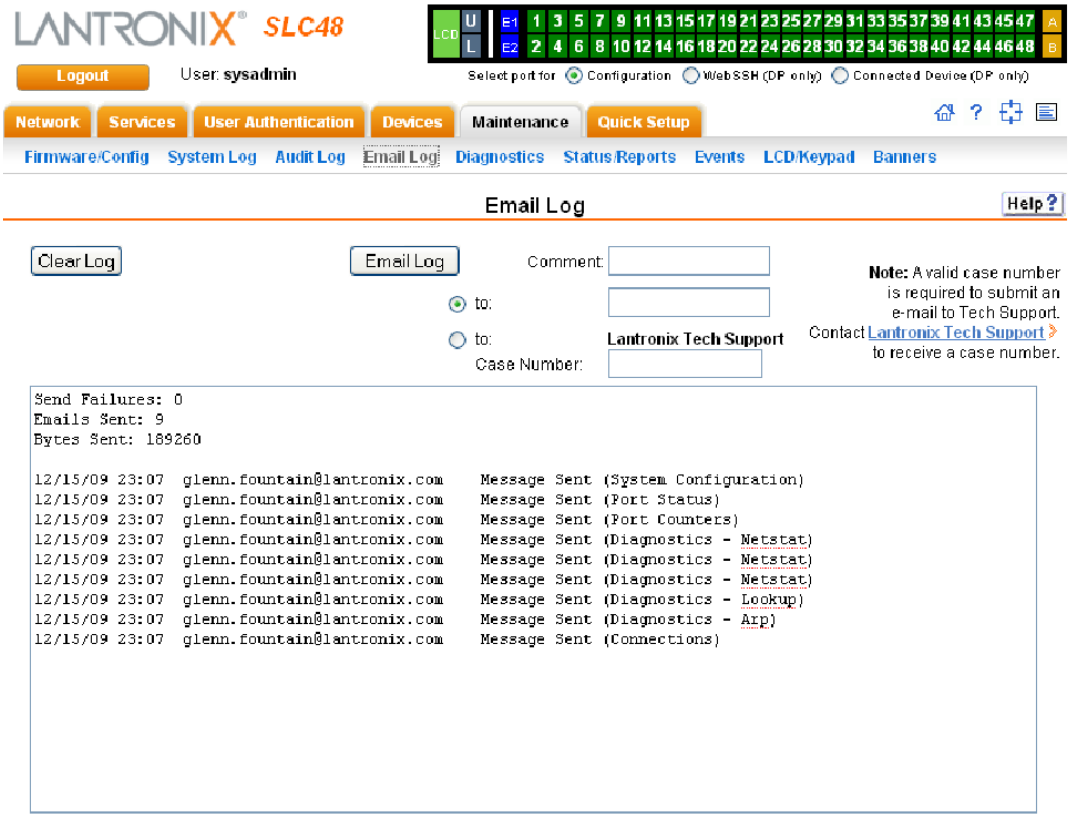
Email Log

The Email Log web page displays a log of all emails that have been sent by the SLC console manager, a count of the number of emails sent, the number of bytes sent, and the number of email errors. Use the **SSH/Telnet/Logging** page to configure the email (SMTP) server and sender.

Each entry in the log file contains a date/timestamp, email address the email was sent to, and either the type of email sent, or an error if there was an error sending the email. The user may clear the log file by clicking the **Clear Log** button.

From the **Maintenance** tab, click **Email Log**. *Figure 13-6* shows the page that displays.

Figure 13-6 Email Log Page


LANTRONIX SLC48
Logout
User: sysadmin
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network Services User Authentication Devices Maintenance Quick Setup
Firmware/Config System Log Audit Log Email Log Diagnostics Status/Reports Events LCD/Keypad Banners
Email Log
Help ?
Clear Log
Email Log
Comment:
● to:
○ to: Lantronix Tech Support
Case Number:

Note: A valid case number is required to submit an e-mail to Tech Support. Contact Lantronix Tech Support to receive a case number.

```
Send Failures: 0
Emails Sent: 9
Bytes Sent: 189260

12/15/09 23:07  glenn.fountain@lantronix.com   Message Sent (System Configuration)
12/15/09 23:07  glenn.fountain@lantronix.com   Message Sent (Port Status)
12/15/09 23:07  glenn.fountain@lantronix.com   Message Sent (Port Counters)
12/15/09 23:07  glenn.fountain@lantronix.com   Message Sent (Diagnostics - Netstat)
12/15/09 23:07  glenn.fountain@lantronix.com   Message Sent (Diagnostics - Netstat)
12/15/09 23:07  glenn.fountain@lantronix.com   Message Sent (Diagnostics - Netstat)
12/15/09 23:07  glenn.fountain@lantronix.com   Message Sent (Diagnostics - Lookup)
12/15/09 23:07  glenn.fountain@lantronix.com   Message Sent (Diagnostics - Arp)
12/15/09 23:07  glenn.fountain@lantronix.com   Message Sent (Connections)
```

Email Log Commands

The following CLI commands correspond to the **Email Log** page. For more information, see *Chapter 15: Command Reference* .

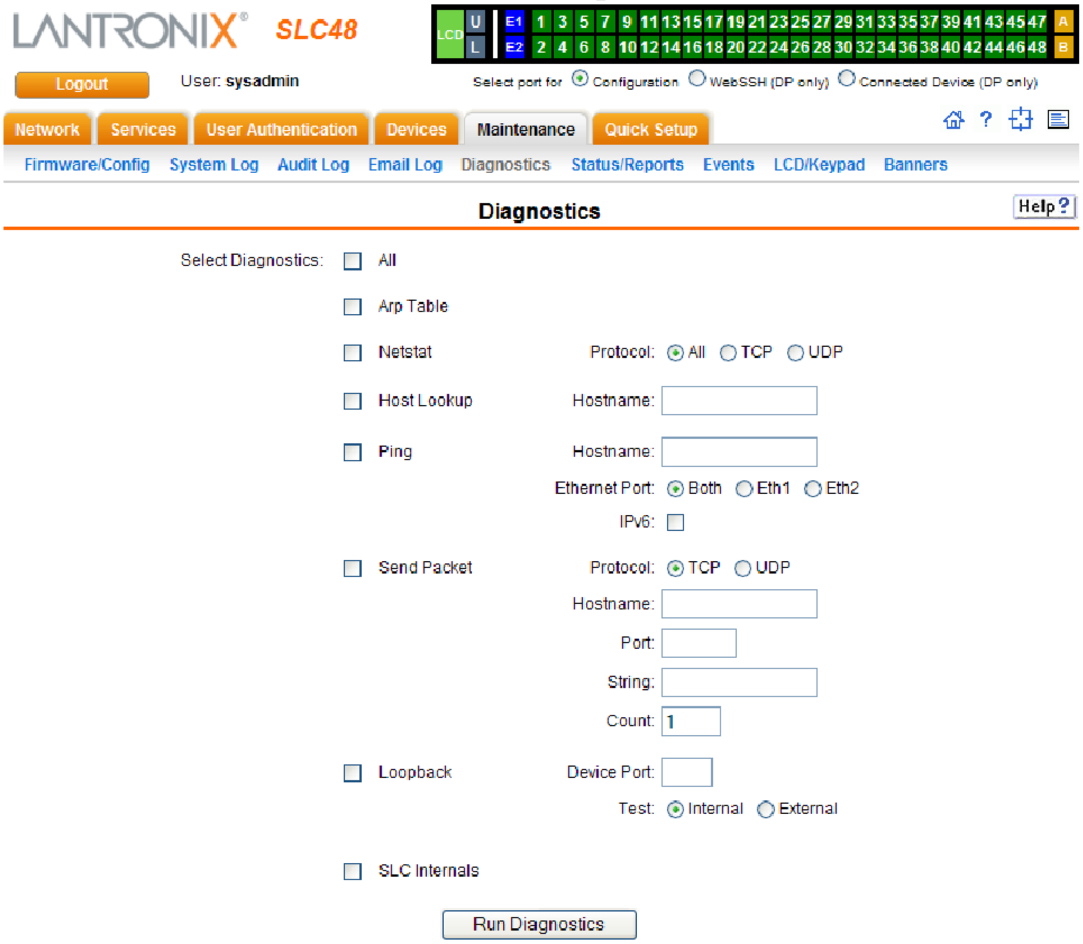
- *show emaillog (on page 229)*
- *show emaillog clear (on page 229)*

Diagnostics

The Diagnostics web page provides methods for diagnosing problems such as network connectivity and device port input/output problems. You can use equivalent commands on the command line interface. An additional diagnostic, loopback, is only available as a command.

1. Click the **Maintenance** tab and select the **Diagnostics** option. *Figure 13-7* shows the page that displays.

Figure 13-7 Diagnostics Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

Diagnostics

Select Diagnostics: □ All

□ Arp Table

□ Netstat — Protocol: ● All ○ TCP ○ UDP

□ Host Lookup — Hostname:

□ Ping — Hostname:

Ethernet Port: ● Both ○ Eth1 ○ Eth2

IPv6: □

□ Send Packet — Protocol: ● TCP ○ UDP

Hostname:

Port:

String:

Count: 1

□ Loopback — Device Port:

Test: ● Internal ○ External

□ SLC Internals

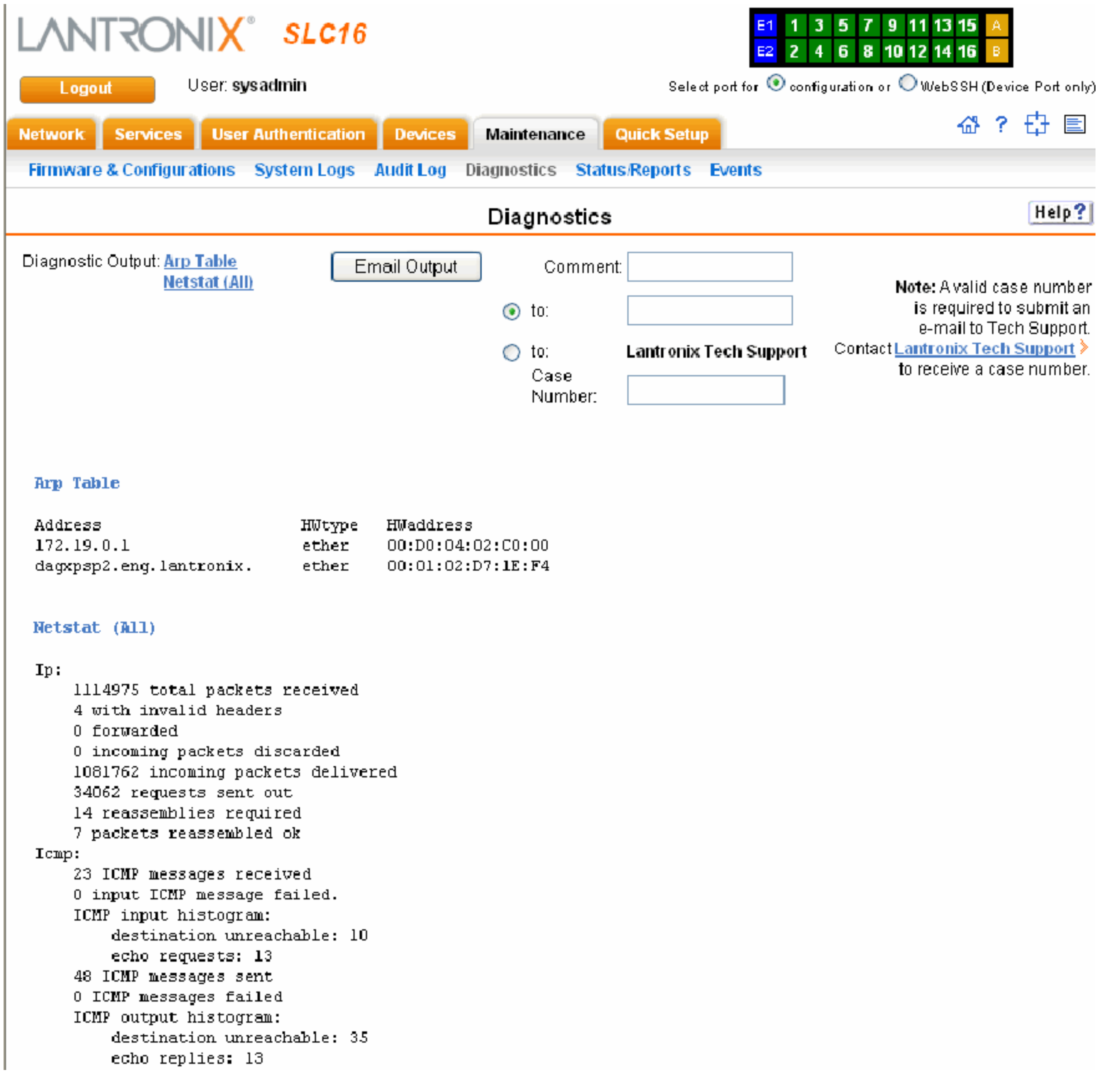
2. Enter the following fields.

Select Diagnostics	Select one or more diagnostic methods you want to run, or select **All** to run them all.
ARP Table	Address Resolution Protocol (ARP) table used to view the IP address-to-hardware address mapping.
Netstat	Displays network connections. If you select the checkbox, select a protocol or select **All** for both protocols to control the output of the Netstat report.
Host Lookup	If you enter a host name in the corresponding **Hostname** field, verifies that the SLC device can resolve the host name into an IP address (if DNS is enabled).

Ping	If you enter a host name in the corresponding **Hostname** field, the SLC console manager verifies that the host is up and running. Check the **Ethernet Port** button (Both, Eth1, or Eth2), and check the **IPv6** box. ***Note:*** *The Ethernet Port option restricts ping transmission to both Ethernet ports, Eth1, or Eth2. The IPv6 box should be checked if the host that is pinged requires IPv6 addressing or routing.*
Send Packet	This option sends an Ethernet packet out one of the Ethernet ports, mainly as a network connectivity test. Enter the following: **Protocol:** Select the type of packet to send. **Hostname:** Specify a host name or IP address of the host to send the packet to. **Port:** Specify a **TCP** or **UDP** port number of the host to send the packet to. **String:** Enter a set of up to 64 characters. The string is encapsulated in the packet (so you could use a network sniffer to track the packet and, by looking at its contents, verify that it was sent). **Count:** The count is the number of times the string is sent. For UDP, the number of times the string is sent is equal to the number of packets sent. For TCP, the number of times the string is sent may (or may not) be equal to the number of packets sent, because TCP controls how data is packetized and sent out.
Loopback	This option tests a Device Port by transmitting data out the port and verifying that it is received correctly (requires the loopback cable be plugged in the Device Port).
SLC Internals	This option displays information on the internal memory, storage and processes of the SLC console manager.

3. Click the **Run Diagnostics** button. *Figure 13-8* shows the page that displays.

Figure 13-8 Diagnostics Report Page



Diagnostic Output: Arp Table
Netstat (All)

Comment:

● to:

○ to: Lantronix Tech Support

Case Number:

Note: A valid case number is required to submit an e-mail to Tech Support. Contact Lantronix Tech Support to receive a case number.

```
Arp Table

Address                    HWtype   HWaddress
172.19.0.1                 ether    00:D0:04:02:C0:00
dagxpsp2.eng.lantronix.    ether    00:01:02:D7:1E:F4


Netstat (All)

Ip:
    1114975 total packets received
    4 with invalid headers
    0 forwarded
    0 incoming packets discarded
    1081762 incoming packets delivered
    34062 requests sent out
    14 reassemblies required
    7 packets reassembled ok
Icmp:
    23 ICMP messages received
    0 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 10
        echo requests: 13
    48 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 35
        echo replies: 13
```

4. To view a report, click the link for that report. The links display at the top left of the page.
5. To email the report to an individual:
   a. In the **Comment** field, enter a comment (if desired).
   b. Select **to** and enter the email address.
   c. Press the **Email Output** button.
6. To email the report to Lantronix Technical Support:
   a. In the **Comment** field, enter a comment (if desired).
   b. Select **to: Lantronix Tech Support**
   c. Call Lantronix Tech Support and obtain a case number.

      For contact information, click the **Lantronix Tech Support** link.
   d. Enter the number in **Case Number**.
   e. Press the **Email Output** button.

Diagnostics Commands

The following CLI commands correspond to the **Diagnostics** page. For more information, see *Chapter 15: Command Reference* .

- *diag arp (on page 227)*
- *diag internals (on page 227)*
- *diag netstat (on page 228)*
- *diag nettrace (on page 228)*
- *diag lookup (on page 227)*
- *diag loopback (on page 227)*
- *diag traceroute (on page 229)*
- *diag ping | ping6 (on page 228)*
- *diag perfstat (on page 228)*
- *diag sendpacket host (on page 229)*

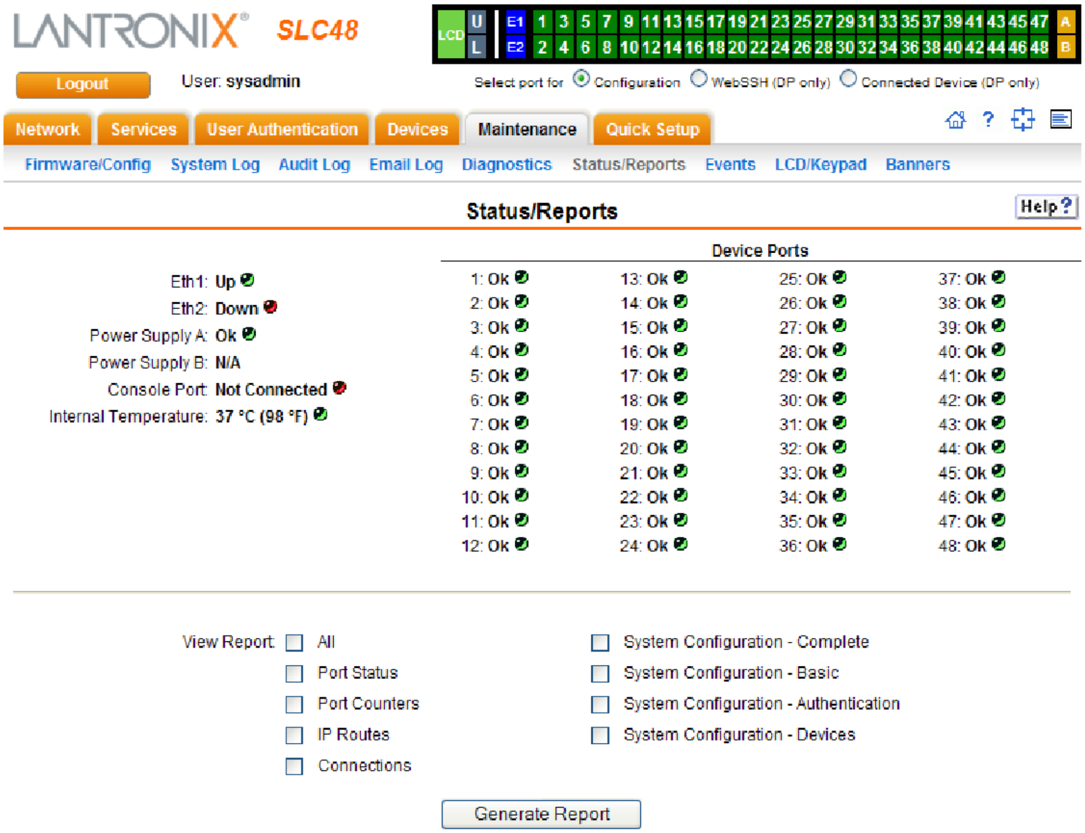
Status/Reports

On the **Status/Reports** page, you can view the status of the SLC ports and power supplies and generate a selection of reports.

Note: *Status and statistics shown on the web interface represent a snapshot in time. To see the most recent data, you must reload the web page.*

1. Click the **Maintenance** tab and select the **Status/Reports** option. The top half of the page displays the status of each port and the power supplies. Green indicates that the port connection or power supply is active and functioning correctly. Red indicates an error or failure. *Figure 13-9* shows the page that displays.

Figure 13-9 Status/Reports Page


LANTRONIX SLC48
LCD U L E1 E2 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 A
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 B
Logout
User: sysadmin
Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)
Network Services User Authentication Devices Maintenance Quick Setup
Firmware/Config System Log Audit Log Email Log Diagnostics Status/Reports Events LCD/Keypad Banners
Help ?

Status/Reports

Eth1: Up
Eth2: Down
Power Supply A: Ok
Power Supply B: N/A
Console Port: Not Connected
Internal Temperature: 37 °C (98 °F)

Device Ports			
1: Ok	13: Ok	25: Ok	37: Ok
2: Ok	14: Ok	26: Ok	38: Ok
3: Ok	15: Ok	27: Ok	39: Ok
4: Ok	16: Ok	28: Ok	40: Ok
5: Ok	17: Ok	29: Ok	41: Ok
6: Ok	18: Ok	30: Ok	42: Ok
7: Ok	19: Ok	31: Ok	43: Ok
8: Ok	20: Ok	32: Ok	44: Ok
9: Ok	21: Ok	33: Ok	45: Ok
10: Ok	22: Ok	34: Ok	46: Ok
11: Ok	23: Ok	35: Ok	47: Ok
12: Ok	24: Ok	36: Ok	48: Ok

View Report: □ All
□ Port Status
□ Port Counters
□ IP Routes
□ Connections
□ System Configuration - Complete
□ System Configuration - Basic
□ System Configuration - Authentication
□ System Configuration - Devices

Generate Report

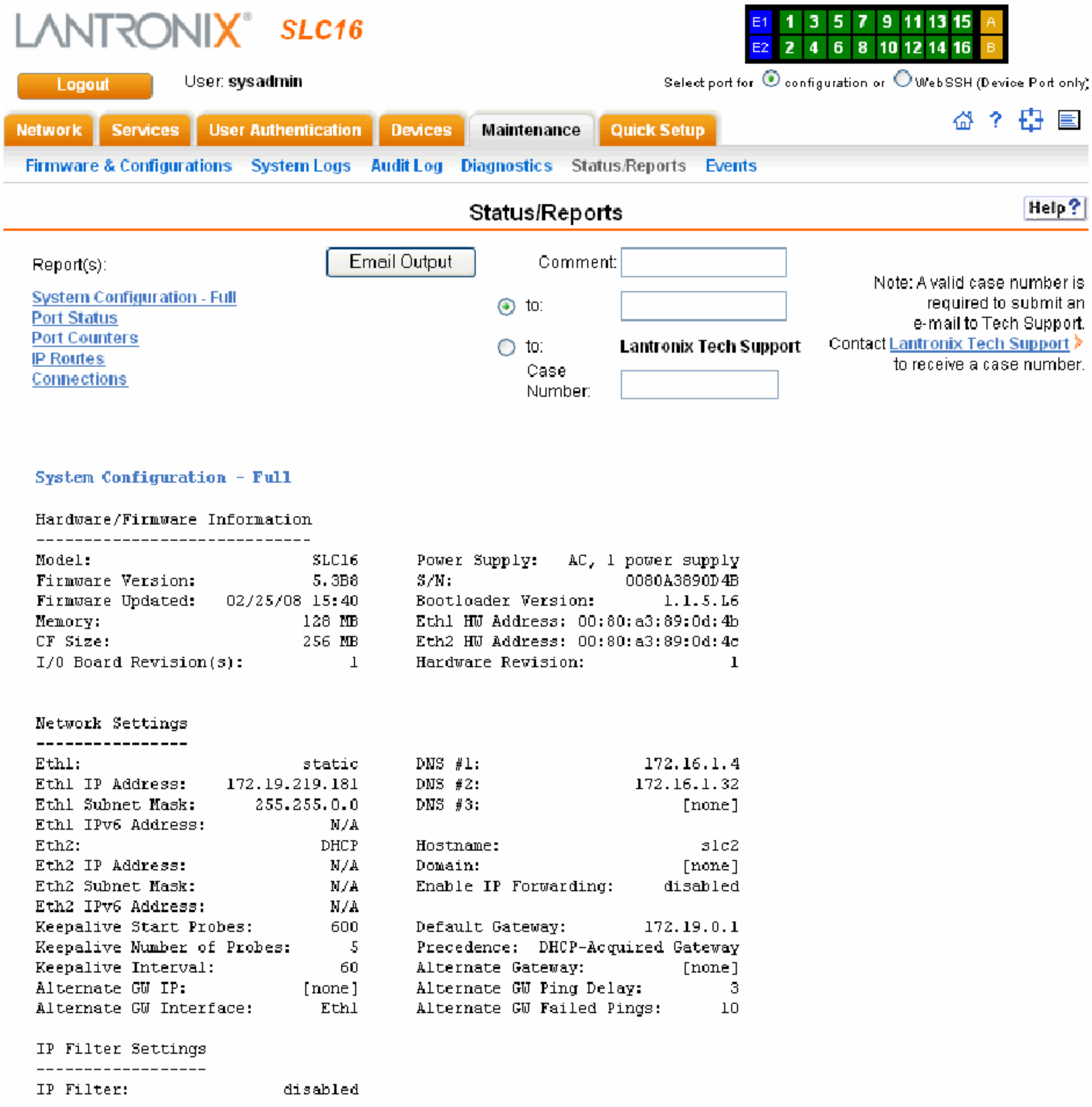
2. Enter the following fields.

View Report

View Report	Select as many of the reports as desired, or select **All**. ◆ **Port Status:** Displays the status of each device port: mode, user, any related connections, and serial port settings. ◆ **Port Counters:** Displays statistics related to the flow of data through each device port. ◆ **IP Routes:** Displays the routing table. ◆ **Connections:** Displays all active connections for the SLC console manager: Telnet, SSH, TCP, UDP, device port, and modem. ◆ **System Configuration – Complete:** Displays a complete snapshot of the SLC settings. ◆ **System Configuration – Basic:** Displays a snapshot of the SLC console manager's basic settings (for example, network, date/time, routing, services, console port). ◆ **System Configuration – Authentication:** Displays a snapshot of authentication settings only (including a list of all localusers). ◆ **System Configuration - Devices:** Displays a snapshot of settings for device ports, USB port, and each PC Card slot.

3. Click the **Generate Report** button. In the upper left, the report page displays a list of reports generated as shown in *Figure 13-10*.

Figure 13-10 Generated Reports Page



User: sysadmin

Status/Reports

Report(s):

System Configuration - Full
Port Status
Port Counters
IP Routes
Connections

Comment:

● to:

○ to: Lantronix Tech Support

Case Number:

Note: A valid case number is required to submit an e-mail to Tech Support. Contact Lantronix Tech Support to receive a case number.

```
System Configuration - Full

Hardware/Firmware Information
-----------------------------
Model:                        SLC16      Power Supply:   AC, 1 power supply
Firmware Version:              5.3B8     S/N:                  0080A3890D4B
Firmware Updated:   02/25/08 15:40       Bootloader Version:        1.1.5.L6
Memory:                       128 MB     Eth1 HW Address: 00:80:a3:89:0d:4b
CF Size:                      256 MB     Eth2 HW Address: 00:80:a3:89:0d:4c
I/O Board Revision(s):             1     Hardware Revision:                1


Network Settings
----------------
Eth1:                         static     DNS #1:                  172.16.1.4
Eth1 IP Address:    172.19.219.181       DNS #2:                 172.16.1.32
Eth1 Subnet Mask:      255.255.0.0       DNS #3:                      [none]
Eth1 IPv6 Address:               N/A
Eth2:                           DHCP     Hostname:                      slc2
Eth2 IP Address:                 N/A     Domain:                      [none]
Eth2 Subnet Mask:                N/A     Enable IP Forwarding:      disabled
Eth2 IPv6 Address:               N/A
Keepalive Start Probes:          600     Default Gateway:         172.19.0.1
Keepalive Number of Probes:        5     Precedence:  DHCP-Acquired Gateway
Keepalive Interval:               60     Alternate Gateway:           [none]
Alternate GW IP:              [none]     Alternate GW Ping Delay:          3
Alternate GW Interface:         Eth1     Alternate GW Failed Pings:       10

IP Filter Settings
------------------
IP Filter:                  disabled
```

4. To view a report, click the link for that report.
5. To email the report to Lantronix Technical Support:
   a. In the **Comment** field, enter a comment (if desired).
   b. Select **to: Lantronix Tech Support**
   c. Call Lantronix Tech Support and obtain a case number.

      For contact information, click the **Lantronix Tech Support** link.
   d. Enter the number in **Case Number**.
   e. Press the **Email Output** button.
6. To email the report to an individual:
   a. In the **Comment** field, enter a comment (if desired).
   b. Select **to:** and enter the email address.

c. Press the **Email Output** button.

Status/Reports Commands

The following CLI commands correspond to the **Status/Reports** page. For more information, see *Chapter 15: Command Reference* .

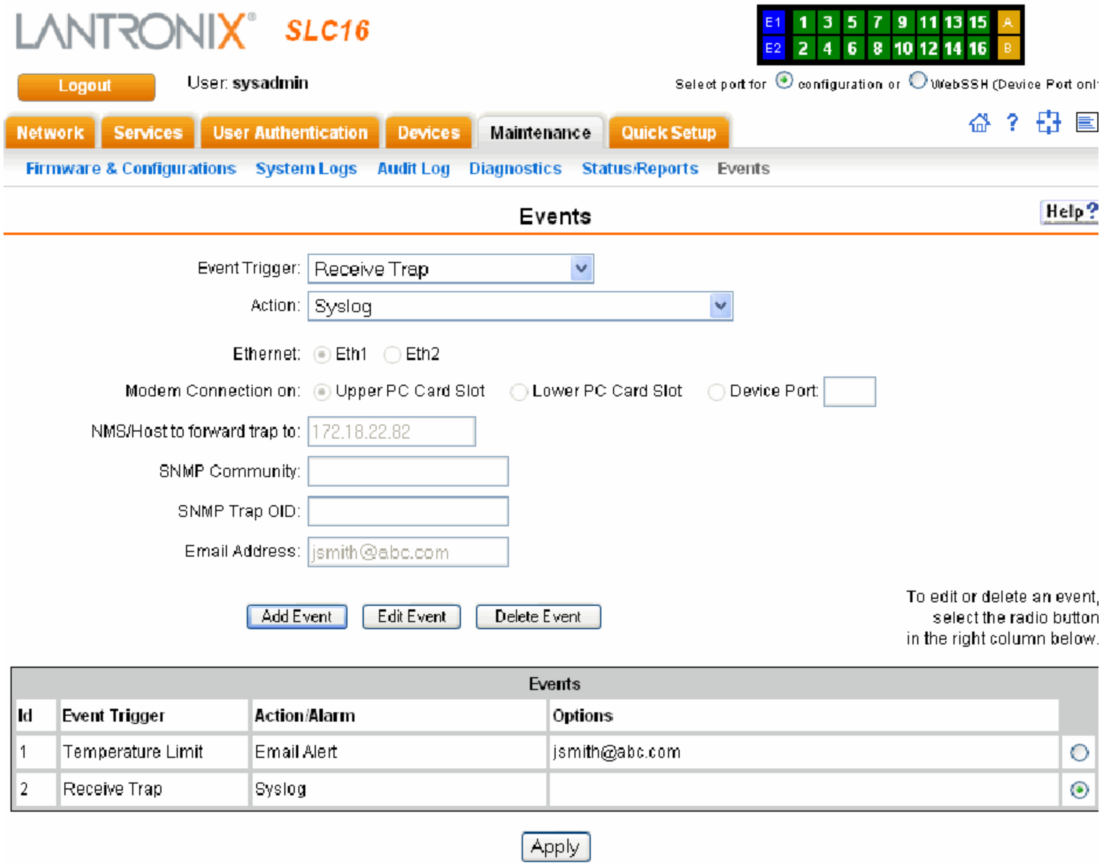
- *show sysconfig (on page 257)*
- *show sysstatus (on page 257)*
- *show connections (on page 218)*
- *show connections connid (on page 218)*
- *show portcounters (on page 226)*
- *show portstatus (on page 226)*

Events

On this page, you can define what action you want to take for events that may occur in the SLC device.

1. Click the **Maintenance** tab and select the **Events** option. *Figure 13-11* shows the page that displays.

Figure 13-11 Events Page



Events

Event Trigger:	Receive Trap
Action:	Syslog
Ethernet:	● Eth1 ○ Eth2
Modem Connection on:	● Upper PC Card Slot ○ Lower PC Card Slot ○ Device Port:
NMS/Host to forward trap to:	172.18.22.82
SNMP Community:	
SNMP Trap OID:	
Email Address:	jsmith@abc.com

To edit or delete an event, select the radio button in the right column below.

Events

Id	Event Trigger	Action/Alarm	Options	
1	Temperature Limit	Email Alert	jsmith@abc.com	○
2	Receive Trap	Syslog		●

2. Enter the following fields.

Event Trigger	From the drop-down list, select the type of incident that triggers an event. Currently, the options are: ◆ **Receive Trap** ◆ **Temperature Over/Under Limit:** For Sensorsoft devices. ◆ **Humidity Over/Under Limit:** For Sensorsoft devices.
Action	From the drop-down list, select the action taken because of the trigger. For example, the action can be writing an entry into the syslog with details of the event or sending the trap to the Ethernet or modem connection.
Ethernet	For actions that require an Ethernet connection (for example, **Forward All Traps to Ethernet**), select the Ethernet port to use.
Modem Connection on	For actions that require a modem connection (for example, **Forward All Traps to a Modem Connection**), select which device port, USB port, or PC Card slot with a modem connection to use.
NMS/Host to forward trap to	For actions that forward a trap, enter the IP address of the computer to forward the trap. The computer does not have to be an SNMP NMS; it just has to be capable of receiving SNMP traps.
SNMP Community	Forwarded traps are sent with this SNMP community value. There is no default.
SNMP Trap OID	Enter a unique identifier for an SNMP object. An SNMP object is anything that can hold a value and can be read using an SNMP “get” action. The OID consists of a string of numbers separated by periods (for example, 1.1.3.2.1). Each number is part of a group represented by the number on its left.
Email Address	Email address to receive email alerts.

3. Choose one of the following options:

- To add the defined event, click the **Add Event** button. The event displays in the Events table at the bottom of the page.
- To edit an event, select the event from the Events table and click the **Edit Event** button. The Events page displays the event.
- To delete an event, select the event from the Events table and click the **Delete Event** button. A message asks for confirmation. Click **OK**.

4. Click the **Apply** button.

Events Commands

The following CLI commands correspond to the **Events** page. For more information, see *Chapter 15: Command Reference* .

- *admin events add (on page 230)*
- *admin events delete (on page 230)*
- *admin events edit (on page 230)*
- *admin events show (on page 231)*

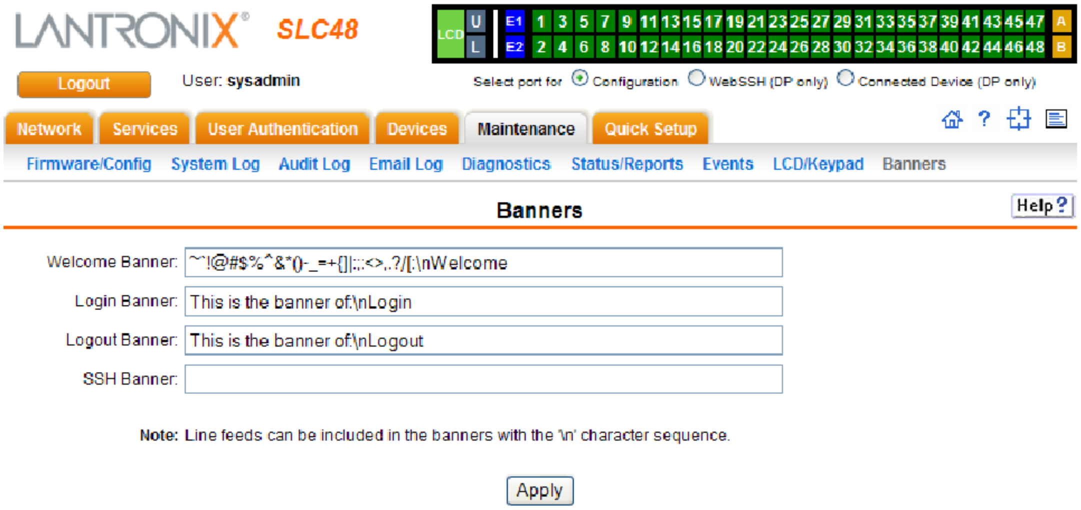
Banners

The **Banners** page allows the system administrator to customize text messages that display to users.

To configure banner settings:

1. Click Banners. *Figure 13-12* shows the page that displays.

Figure 13-12 Banners Page



Banners

Welcome Banner: ~`!@#$%^&*()-_=+{}[]|;;:<>,.?/[:\nWelcome

Login Banner: This is the banner of:\nLogin

Logout Banner: This is the banner of:\nLogout

SSH Banner:

Note: Line feeds can be included in the banners with the '\n' character sequence.

Apply

1. Enter the following fields.

Welcome Banner	The text to display on the command line interface before the user logs in. May contain up to 1024 characters. **Welcome to the** SLC console manager is the default. ***Note:*** *To create more lines use the* ***\n*** *character sequence.*
Login Banner	The text to display on the command line interface after the user logs in. May contain up to 1024 characters. Default is blank. ***Note:*** *To create more lines, use the* ***\n*** *character sequence.*
Logout Banner	The text to display on the command line interface after the user logs out. May contain up to 1024 characters. Default is blank. ***Note:*** *To create more lines use, the* ***\n*** *character sequence.*
SSH Banner	The text to display when a user logs into the SLC device via SSH, prior to authentication. May contain up to 1024 characters. Blank by default. ***Note:*** *To create more lines use the* ***\n*** *character sequence.*

2. Click the **Apply** button.

Banner Commands

The following CLI commands correspond to the **Banners** page. For more information, see *Chapter 15: Command Reference* .

- *admin banner login (on page 205)*
- *admin banner logout (on page 205)*
- *admin banner show (on page 205)*
- *admin banner ssh (on page 205)*
- *admin banner welcome (on page 206)*

LCD and Keypad

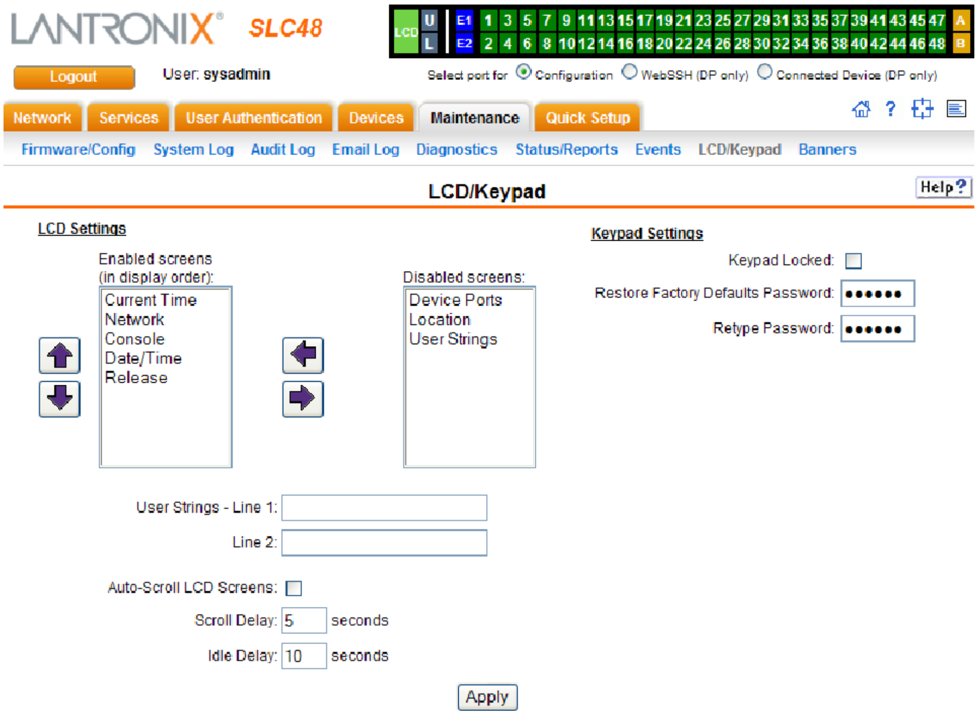
The LCD has a series of screens, consisting of 2 lines of 24 characters each. Specific screens and the display order can be configured. The keypad associated with the LCD can also be configured. The types of screens include: current time, network settings, console settings, date and time, release version, location, and custom user strings.

Enabling the **Auto-Scroll LCD Screens** option enables scrolling through the screens and pausing the number of seconds specified by the **Scroll Delay** between each screen. After any input to the keypad, the LCD waits until the keypad has been idle for the number of seconds specified by the **Idle Delay** before scrolling of the screens continues.

To configure the LCD and Keypad:

1. Click the **Maintenance** tab and select the **LCD/Keypad** option. *Figure 13-13* shows the page that displays.

Figure 13-13 LCD/Keypad Page



User: sysadmin

Select port for ● Configuration ○ WebSSH (DP only) ○ Connected Device (DP only)

LCD/Keypad

LCD Settings

Enabled screens (in display order):
Current Time
Network
Console
Date/Time
Release

Disabled screens:
Device Ports
Location
User Strings

User Strings - Line 1:

Line 2:

Auto-Scroll LCD Screens: □

Scroll Delay: 5 seconds

Idle Delay: 10 seconds

Keypad Settings

Keypad Locked: □

Restore Factory Defaults Password: ●●●●●●

Retype Password: ●●●●●●

To configure the Keypad:

1. Enter the following fields.

Keypad Locked	Select this to lock out any input to the keypad. The default is for the keypad to be unlocked.
Restore Factory Defaults Password	The 6 digit key sequence entered at the keypad to restore the SLC console manager to factory defaults. The default is **999999**.

To configure the LCD:

1. Select a screen and click the **up arrow** or the **down arrow** to change the order of the screens.
2. Select a screen to be removed and click the **right arrow**. The screen moves to the Disabled Screens list.
3. Select a screen from the Disabled Screens list and click the **left arrow**. The screen is added to the Enabled Screens list at the bottom.

Note: The ***User Strings*** *screen displays the 2 lines defined by the* ***User Strings - Line 1*** *and* ***Line 2*** *fields. By default, these user strings are blank.*

LCD/Keypad Commands

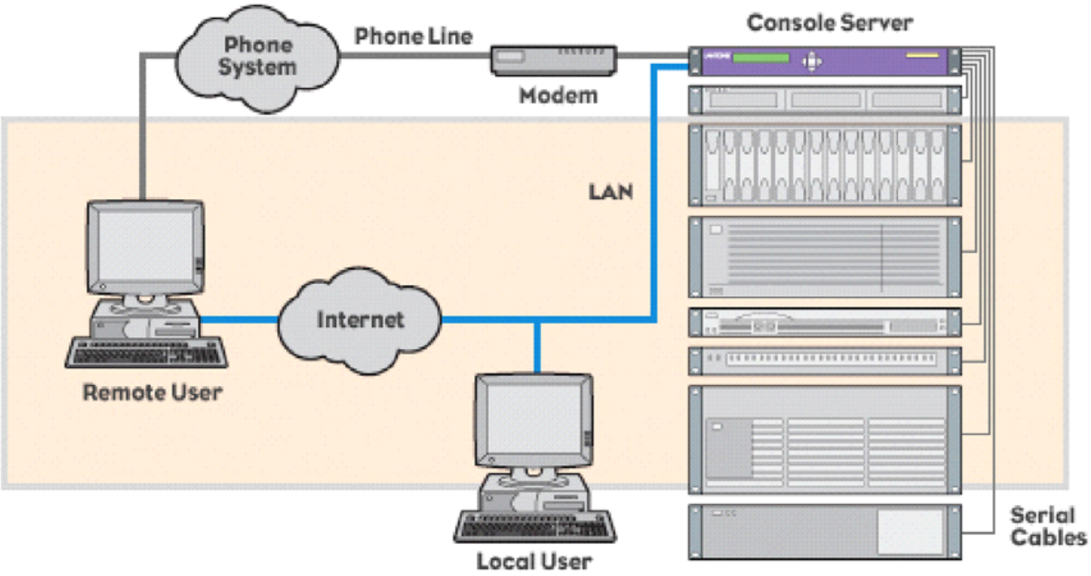
The following CLI commands correspond to the **LCD/Keypad** page. For more information, see *Chapter 15: Command Reference* .

- *admin keypad (on page 209)*
- *admin keypad password (on page 209)*
- *admin keypad show (on page 209)*
- *admin lcd reset (on page 210)*
- *admin lcd default (on page 209)*
- *admin lcd screens (on page 210)*
- *admin lcd line1 (on page 210)*
- *admin lcd scrolling (on page 210)*
- *admin lcd show (on page 210)*

14: Application Examples

Each SLC console manager has multiple serial ports and two network ports as shown in *Figure 14-1*. Each serial port can be connected to the console port of a device. Using a network in-band port or an out-of-band modem for a dial-up connection, an administrator can remotely access any of the connected devices using Telnet or SSH.

Figure 14-1 SLC Console Manager



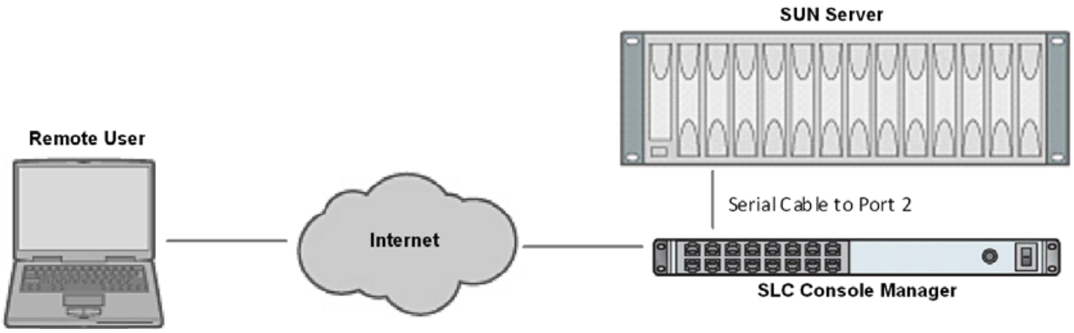
This chapter includes three examples that use the SLC device. The examples assume that the SLC console manager is connected to the network and has already been assigned an IP address.

In the examples, the command line interface is shown. You can perform the same configurations using the web page interface except for directly interacting with the SLC device (`direct` command).

Telnet/SSH to a Remote Device

Figure 14-2 shows a SUN server connected to port 2 of the SLC console manager .

Figure 14-2 Remote User Connected to a SUN Server via the SLC Device



In the example below, the system administrator performs the following steps:

1. Display the settings for device port 2 by using the `show deviceport` command.

```
[SLC]> show deviceport port 2
___Current Device Port Settings________________________________________________
Number: 2  Name: Port-2

Modem Settings-------------------Data Settings----------IP Settings---------
Modem State: disabled            Baud Rate: 9600        Telnet: disabled
Modem Mode: text                 Data Bits: 8           Telnet Port: 2002
Timeout Logins: disabled         Stop Bits: 1           SSH: disabled
Local IP: negotiate              Parity: none           SSH Port: 3002
Remote IP: negotiate             Flow Control: xon/xoff IP: <none>
Authentication: PAP              Logins: disabled
CHAP Host: <none>                Break Sequence: \x1bB
CHAP Secret: <none>              Check DSR: disabled
NAT: disabled                    Close DSR: disabled
Dial-out Login: <none>
Dial-out Password: <none>
Dial-out Number: <none>
Dial-back Number: usernumber
Initialization Script: <none>

Logging Settings---------------------------------------------------------------
Local Logging: disabled          PC Card Logging: disabled
Email Logging: disabled          Log to: upper slot
Byte Threshold: 100              Max number of files: 10
Email Delay: 60   seconds        Max size of files: 2048
Restart Delay: 60   seconds
Email To: <none>
Email Subject: Port%d Logging
Email String: <none>
NFS File Logging: disabled
Directory to log to: <none>
Max number of files: 10
Max size of files: 2048
```

2. Change the baud to 57600 and disable flow control by using the `baud` and `flowcontrol` parameters.

```
[SLC]> set deviceport port 2 baud 57600 flowcontrol none
Device Port settings successfully updated.
```

3. Connect to the device port y using the `connect direct` command.

```
[SLC]> connect direct deviceport 2
```

4. View messages from the SUN server console.

```
Mar 15 09:09:44 tssf280r sendmail[292]: [ID 702911 mail.info] starting daemon
(8.12.2+Sun): SMTP+queueing@00:15:00
Mar 15 09:09:44 tssf280r sendmail[293]: [ID 702911 mail.info] starting daemon
(8.12.2+Sun): queueing@00:15:00
Mar 15 14:44:40 tssf280r sendmail[275]: [ID 702911 mail.info] starting daemon
(8.12.2+Sun): SMTP+queueing@00:15:00
Mar 15 14:44:40 tssf280r sendmail[276]: [ID 702911 mail.info] starting daemon
(8.12.2+Sun): queueing@00:15:00
```

5. Reboot the SUN server by using the `reboot` command.

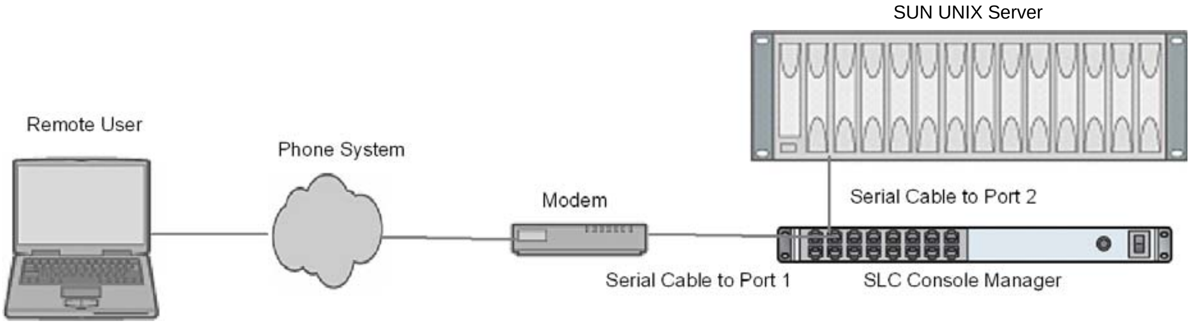
```
reboot
<shutdown messages from SUN>
```

6. Use the escape sequence to escape from direct mode back to the command line interface.

Dial-in (Text Mode) to a Remote Device

The example in *Figure 14-3* shows a modem connected to the SLC console manager device port 1, and a SUN server connected to the SLC device port 2. You can configure the modem for text mode dial-in, so a remote user can dial into the modem using a terminal emulation program and access the SUN server. HyperTerminal™ which comes with the Microsoft ® Windows™ operating system, is an example of a terminal emulation program.

Figure 14-3 Connection to SUN UNIX Server



In this example, the system administrator performs the following steps.

1. Configure the device port that the modem is connected to for dial-in by using the set deviceport command with the shown parameters.

```
[SLC]> set deviceport port 1 modemmode text
Device Port settings successfully updated.

[SLC]> set deviceport port 1 initscript "AT&F&K3&C1&D2%C0A"
Device Port settings successfully updated.

[SLC]> set deviceport port 1 auth pap
Device Port settings successfully updated.

[SLC]> set deviceport port 1 localsecret "password"
Device Port settings successfully updated.

[SLC]> set deviceport port 1 modemstate dialin
Device Port settings successfully updated.

[SLC]>
```

2. Configure the device port that is connected to the console port of the SUN UNIX server by using the `baud` and `flowcontrol` parameters.

```
[SLC]> set deviceport port 2 baud 57600 flowcontrol none
Device Port settings successfully updated.
```

3. Dial into the SLC console manager via the modem using a terminal emulation program on a remote PC. A command line prompt displays.

4. Log into the SLC console manager.

```
CONNECT 57600

Welcome to the SLC

login: sysadmin
Password:

Welcome to the SLC Console Manager
Model Number: SLC 48
For a list of commands, type 'help'.

[SLC]>
```

5. Connect to the SUN UNIX server using the `connect direct` command.

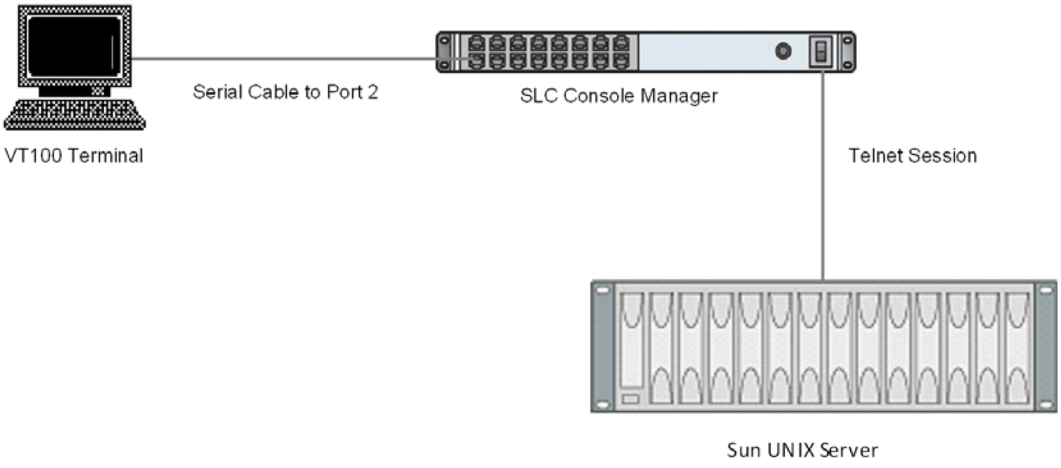
```
[SLC]> connect direct deviceport 2
SunOS 5.7

login: frank
Password:
Last login: Wed Jul 14 16:07:49 from computer
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
SunOS computer 5.7 Generic_123485-05 sun4m sparc SUNW,SPARCstation-20
$
```

6. Use the escape sequence to escape from direct mode back to the command line interface.

Local Serial Connection to Network Device via Telnet

Figure 14-4 shows a terminal device connected to the SLC console manager device port 2, and a SUN server connected over the internet to the SLC device. When a connection is established between the device port and an outbound Telnet session, users can access the SUN server as though directly connected to it. (See *Chapter 11: Connections* for more information).

Figure 14-4 Terminal Device Connection to the SLC Console Manager



The system administrator performs the following steps.

1. Display the settings for device port 2 by using the `show deviceport` command.

```
[SLC]> show deviceport port 2
___Current Device Port Settings________________________________________________
Number: 2  Name: Port-2

Modem Settings-------------------Data Settings----------IP Settings---------
Modem State: disabled            Baud Rate: 9600        Telnet: disabled
Modem Mode: text                 Data Bits: 8           Telnet Port: 2002
Timeout Logins: disabled         Stop Bits: 1           SSH: disabled
Local IP: negotiate              Parity: none           SSH Port: 3002
Remote IP: negotiate             Flow Control: xon/xoff IP: <none>
Authentication: PAP              Logins: disabled
CHAP Host: <none>                Break Sequence: \x1bB
CHAP Secret: <none>              Check DSR: disabled
NAT: disabled                    Close DSR: disabled
Dial-out Login: <none>
Dial-out Password: <none>
Dial-out Number: <none>
Dial-back Number: usernumber
Initialization Script: <none>

Logging Settings---------------------------------------------------------------
Local Logging: disabled          PC Card Logging: disabled
Email Logging: disabled          Log to: upper slot
Byte Threshold: 100              Max number of files: 10
Email Delay: 60   seconds        Max size of files: 2048
Restart Delay: 60   seconds
Email To: <none>
Email Subject: Port%d Logging
Email String: <none>
NFS File Logging: disabled
Directory to log to: <none>
Max number of files: 10
Max size of files: 2048
```

2. Change the serial settings to match the serial settings for the vt100 terminal by using the `baud` and `flowcontrol` parameters.

```
[SLC]> set deviceport port 2 baud 57600 flowcontrol none
Device Port settings successfully updated.
```

3. Create a connection between the vt100 terminal connected to device port 2 and an outbound telnet session to the server by using the `connect bidirection` command.

```
[SLC]> connect bidirection 2 telnet 192.168.1.1
Connection settings successfully updated.
```

4. At the VT100 terminal, press <return> a couple of times. The Telnet prompt from the server displays the following message.

```
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

Sun OS 8.0

login:
```

You can log in and interact with the SUN server at the VT100 terminal as if directly connected to the server.

15: Command Reference

This chapter lists and describes all of the commands available on the SLC command line interface (CLI) accessed by using Telnet, SSH, or a serial connection. In addition to the commands, this chapter contains the following sections:

- *Introduction to Commands*
- *Deprecated Commands*

The following is an alphabetical listing of categories and within each category there is a list of commands in alphabetical order:

- *Administrative Commands*
- *Audit Log Commands*
- *Authentication Commands*
- *CLI Commands*
- *Connection Commands*
- *Console Port Commands*
- *Custom User Menu Commands*
- *Date and Time Commands*
- *Device Commands*
- *Device Port Commands*
- *Diagnostic Commands*
- *Email Log Commands*
- *Events Commands*
- *Host List Commands*
- *IP Filter Commands*
- *Kerberos Commands*
- *LDAP Commands*
- *Local Users Commands*
- *Log Commands*
- *Network Commands*
- *NFS and SMB/CIFS Commands*
- *NIS Commands*
- *PC Card Commands*
- *RADIUS Commands*
- *Remote Users Commands*
- *Routing Commands*
- *Script Commands*
- *Services Commands*
- *SLC Network Commands*
- *SSH Key Commands*
- *Status Commands*
- *System Log Commands*
- *TACACS+ Commands*
- *Temperature Commands*
- *USB Commands*
- *User Permissions Commands*

Introduction to Commands

This section explains command syntax, command line help, and tips for using commands. For more detailed information about commands, see *Command Line Interface on page 42*.

Command Syntax

Commands have the following syntax: <action> <category> <parameters>. The <action> value can be one of the following: set, show, connect, diag, pccard, admin, or logout. The <category> value is a group of related parameters that you can configure or view. Examples are ntp, deviceport, and network.

The <parameters> value is one or more name-value pairs in one of the following formats:

- <aa | bb> User must specify one of the values (aa or bb) separated by a vertical line (|). The values are in all lowercase and must be entered exactly as shown. Bold indicates a default value.

- <value> User must specify an appropriate value, for example, an IP address. The parameter values are in mixed case. Square brackets [ ] indicate optional parameters.

Command Line Actions and Categories

Table 15-1 lists the actions and categories for each action.

Table 15-1 Actions and Category Options

Action	Category
set	auth | cifs | cli | command | consoleport | datetime | deviceport | history | hostlist | ipfilter | kerberos | ldap | localusers | log | menu | network | nfs | nis | ntp | password | radius | remoteusers | routing | script | services | slcnetwork | sshkey | tacacs+ | temperature | usb[1]
show	auth | auditlog | cifs | cli | connections | consoleport | datetime | deviceport | emaillog | history | hostlist | ipfilter | kerberos | ldap | localusers | log | menu | network | nfs | nis | ntp | pccard | portcounters | portstatus | radius | remoteusers | routing | script | services | slcnetwork | sshkey | sysconfig | syslog | sysstatus | tacacs+ | temperature | usb[1] | user
connect	bidirection | direct | global | listen | script | terminate | unidirection
diag	arp | internals | lookup | loopback | netstat | nettrace | perfstat | ping | ping6| sendpacket | traceroute
pccard	modem | storage
admin	banner | clear | config | events | firmware | ftp | keypad | lcd | quicksetup | reboot| shutdown | site | version | web
logout	terminates CLI session

[1] USB commands are only accessible on SLC USB part number -03.

For general help and to display the commands to which you have rights, type **help**. For general command line help, type **help** <command line>. For more information about a specific command, type **help** followed by the command. For example, **help set network** or **help admin firmware**.

Tips

- Type enough characters to identify the action, category, or parameter name uniquely. For parameter values, type the entire value. For example, you can shorten: **set network port 1 state static ipaddr 122.3.10.1 mask 255.255.0.**0 to **se net po 1 st static ip 122.3.10.1 ma 255.255.0.0**.
- Use the **Tab** key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** either to complete the name if only one is possible, or to display the possible names if more than one is possible. Following a space after the preceding name, **Tab** displays all possible names.
- Should you make a mistake while typing, backspace by pressing the **Backspace** key and/or the **Delete** key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the **left** and **right** arrow keys to move within a command.
- Use the **up** and **down arrows** to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.

- To clear an IP address, type **0.0.0.0**, or to clear a non-IP address value, type **CLEAR**.
- When the number of lines displayed by a command exceeds the size of the window (the default is 25), the command output is halted until you are ready to continue. To display the next line, press Enter, and to display the page, press the space bar. You can override the number of lines (or disable the feature altogether) with `set cli`.

Deprecated Commands

Deprecated commands in this release are as follows:

- set locallog (replaced by *set log clear (on page 238)*)
- show locallog (replaced by *show log local (on page 239)*)

Administrative Commands

admin banner login

Syntax

```
admin banner login <Banner Text>
```

Description

Configures the banner displayed after the user logs in.

Note: *To go to the next line, type \n and press Enter.*

admin banner logout

Syntax

```
admin banner logout <Banner Text>
```

Description

Configures the banner displayed after the user logs out.

Note: *To go to the next line, type \n and press Enter.*

admin banner show

Syntax

```
admin banner show
```

Description

Displays the welcome, login and logout banners.

admin banner ssh

Syntax

admin banner ssh <Banner Text>

Description

Configures the banner that displays prior to SSH authorization.

admin banner welcome

Syntax

```
admin banner welcome <Banner Text>
```

Description

Configures the banner displayed before the user logs in.

Note: *To go to the next line, type \n and press Enter.*

admin clear

Syntax

```
admin clear tmpdir
```

Description

Resets system resources and clears the temporary directory.

admin config copy

Syntax

```
admin config copy <current|Config Name> [location <local | nfs | cifs |
pccard> | usb] [nfsdir <NFS Mounted Directory>] [usbport
<U1>][pccardslot <upper|lower>]
```

Description

Copies the current configuration (or optionally, a configuration from another location) to the other bank (for dual-boot SLC console managers).

admin config rename|delete

Syntax

```
admin config rename|delete <Config Name> location <local | nfs | cifs |
<upper|lower>]
```

Description

Deletes or renames a configuration (the user is prompted for the new name when renaming.

admin config factorydefaults

Syntax

```
admin config factorydefaults [savesshkeys <enable|disable>][savesslcert
<enable|disable>] [savescripts <enable|disable>] [preserveconfig <Config
Params to Preserve>]
```

<Config Params to Preserve>

```
      nt - Networking    ra - Remote Authentication
      sv - Services      dp - Device Ports
```

dt - Date/Time	pc - PC Card
lu - Local Users	ub - USB

Note: *The Config Params to Preserve get contained as a comma-separated list of current configuration parameters that are kept after the config restore or factorydefaults.*

Description

Restores the factory default settings.

admin config restore

Syntax

```
admin config restore <Config Name> location <local | ftp | sftp | nfs |
cifs | pccard | usb> [nfsdir <NFS Mounted Directory>] [usbport
<U1>][pccardslot <upper|lower>] [savesshkeys <enable|disable>]
[savesslcert <enable|disable>] [savescripts <enable|disable>]
[preserveconfig <Config Params to Preserve>]
```

<Config Params to Preserve>

nt - Networking	ra - Remote Authentication
sv - Services	dp - Device Ports
dt - Date/Time	pc - PC Card
lu - Local Users	ub - USB

Note: *The Config Params to Preserve get contained as a comma-separated list of current configuration parameters that are kept after the config restore or factorydefaults.*

Description

Restores a saved configuration to the SLC console manager.

admin config save

Syntax

```
admin config save <Config Name> location <local | ftp | sftp | nfs | cifs
| pccard | usb> [nfsdir <NFS Mounted Directory>] [usbport <U1>]
[pccardslot <upper|lower>] [savesshkeys <enable|disable>] [savesslcert
<enable|disable>] [savescripts <enable|disable>]
```

Description

Saves the current SLC configuration to a selected location.

admin config show

Syntax

```
admin config show <default|ftp|sftp|nfs|cifs|pccard |usb> [nfsdir <NFS
Mounted Dir>] [usbport <U1>][pccardslot <upper|lower>]
```

Description

Lists the configurations saved to a location.

admin firmware bootbank

Syntax

```
admin firmware bootbank <1|2>
```

Description

Sets the boot bank to be used at the next SLC console manager reboot. Applies to dual-boot SLC devices only.

admin firmware copybank

Syntax

```
admin firmware copybank
```

Description

Copies the boot bank from the currently booted bank to the alternate bank (for dual-boot SLC console managers).

admin firmware show

Syntax

```
admin firmware show [viewlog <enable|disable>]
```

Description

Lists the current firmware revision, the boot bank status (for dual-boot SLC console managers), and optionally displays the log containing details about firmware updates.

admin firmware update

Syntax

```
admin firmware update <ftp | tftp | sftp | nfs | pccard |usb> file
<Firmware File> key <Checksum Key> [nfsdir <NFS Mounted
Directory>][usbport <U1>] [pccardslot <upper|lower>]
```

Description

Updates SLC firmware to a new revision. You should be able to access the firmware file using the settings admin ftp show displays. The SLC console manager automatically reboots after successful update.

admin ftp password

Syntax

```
admin ftp password
```

Description

Sets the FTP server password and prevent it from being echoed.

admin ftp server

Syntax

```
admin ftp server <IP Address or Name> [login <User Login>] [path
<Directory>]
```

Description

Sets the FTP/TFTP/SFTP server used for firmware updates and configuration save/restore.

admin ftp show

Syntax

```
admin ftp show
```

Description

Displays FTP settings.

admin keypad

Syntax

```
admin keypad <lock|unlock>
```

Description

Locks or unlocks the LCD keypad. If the keypad is locked, you can scroll through settings but not change them.

admin keypad password

Syntax

```
admin keypad password (Must be 6 digits.)
```

Description

Changes the Restore Factory Defaults password used at the LCD to return the SLC console manager to the factory settings.

admin keypad show

Syntax

```
admin keypad show
```

Description

Displays keypad settings.

admin lcd default

Syntax

```
admin lcd default
```

Description

Restores the LCD screens to their factory default settings.

admin lcd reset

Syntax

```
admin lcd reset
```

Description

Restarts the program that controls the LCD.

admin lcd line1

Syntax

```
admin lcd line1 <1-24 Chars> line2 <1-24 Chars>
```

Description

Sets the strings displayed on the LCD user string screen.

admin lcd screens

Syntax

```
admin lcd screens <zero or more parameters>
```

Parameters

```
currtime <1-8>
network <1-8>
console <1-8>
datetime <1-8>
release <1-8>
devports <1-8>
location <1-8>
userstrings <1-8>
```

Description

Sets which screens that display on the LCD, and the display order. Any screens omitted from the `admin lcd screens` command are disabled. Omitting all screens results in a blank LCD.

admin lcd scrolling

Syntax

```
admin lcd scrolling <enable|disable> [scrolldelay <Delay in Seconds>]
[idledelay <Delay in Seconds>]
```

Description

Configures auto-scroll of the LCD screens, including the number of seconds after keypad input before auto-scrolling restarts.

admin lcd show

Syntax

```
admin lcd show
```

Description

Displays the LCD screens.

admin quicksetup

Syntax

```
admin quicksetup
```

Description

Runs the quick setup script.

admin reboot

Syntax

```
admin reboot
```

Description

Terminates all connections and reboots the SLC console manager. The front panel LCD displays the “Rebooting the SLC” message, and the normal boot sequence occurs.

admin site

Syntax

```
admin site row <Data Center Rack Row Number>
admin site cluster <Data Center Rack Group Number>
admin site rack <Data Center Rack Number>
```

Description

Configures information about the SLC location.

admin site show

Syntax

```
admin site show
```

Description

Displays the row, cluster, and rack on which the SLC console manager is installed.

admin shutdown

Syntax

```
admin shutdown
```

Description

Prepares the SLC console manager to be powered off.

When you use this command to shut down the SLC console manager, the LCD front panel displays the “Shutting down the SLC” message, followed by a pause, and then “Shutdown complete.” When “Shutdown complete” displays, it is safe to power off the SLC console manager. This command is not available on the Web page.

admin version

Syntax

```
admin version
```

Description

Displays current hardware and firmware information.

admin web certificate

Syntax

```
admin web certificate import via <sftp|scp> certfile <Certificate File>
privfile <Private Key File> host <IP Address or Name> login <User Login>
[path <Path to Files>]
```

Description

Imports an SSL certificate.

admin web certificate reset

Syntax

```
admin web certificate reset
```

Description

Resets a web certificate.

admin web certificate show

Syntax

```
admin web certificate show
```

Description

Displays a web certificate.

admin web cipher

Syntax

```
admin web cipher <himed|himedlow>
```

Description

Configures the strength of the cipher used by the web server (high is 256 or 128 bit, medium is 128 bit, low is 64, 56 or 40 bit).

admin web gadget

Syntax

```
admin web gadget <enable|disable>
```

Description

Enables or disables iGoogle Gadget web content.

admin web protocol

Syntax

```
admin web protocol <sslv2|nosslv2>
```

Description

Configures the web server to use SSLv2 in addition to SSLv3 and TLSv1.

admin web timeout

Syntax

```
admin web timeout <disable|5-120>
```

Description

Configures the timeout for web sessions.

admin web terminate

Syntax

```
admin web terminate <Session ID>
```

Description

Terminates a web session.

admin web show

Syntax

```
admin web show [viewslmsessions <enable|disable>]
```

Description

Displays the current sessions and their ID.

Audit Log Commands

show auditlog

Syntax

```
show auditlog [command|user|clear] [email <Email Address>]
```

Description

Displays audit log. By default, shows the audit log sorted by date/time. You can sort it by user or command, or clear the audit log.

Authentication Commands

set auth

Syntax

```
set auth <one or more parameters>
```

Parameters

```
authusenextmethod <enable|disable>
kerberos <1-6>
ldap <1-6>
localusers <1-6>
nis <1-6>
radius <1-6>
tacacs+ <1-6>
```

Description

Sets ordering of authentication methods. Local Users authentication is always the first method used. Any methods omitted from the command are disabled.

show auth

Syntax

```
show auth
```

Description

Displays authentication methods and their order of precedence.

show user

Syntax

```
show user
```

Description

Displays attributes of the currently logged in user.

CLI Commands

set cli scscommands

Syntax

```
set cli scscommands <enable|disable>
```

Commands:

```
info        direct <Device Port # or Name>
version     listen <Device Port # or Name>
reboot      clear <Device Port # or Name>
poweroff    telnet <IP Address or Name>
```

```
      listdev     ssh <IP Address or Name>
```

Description

Allows you to use SCS-compatible commands as shortcuts for executing commands. Enabling this feature enables it only for the current cli session. It is disabled by default.

Note: *Settings are retained between CLI sessions for local users and users listed in the remote users list.*

Description

Starts the menu if the menu associated with the current user does not display.

set cli menu

Syntax

```
set cli menu <start|menu name>
```

Description

Starts a menu if the menu associated with the user does not display.

set cli terminallines

Syntax

```
set cli terminallines <disable|Number of lines>
```

Description

Sets the number of lines in the terminal emulation screen for paging through text one screen at a time, if the SLC console manager cannot detect the size of the terminal automatically.

Note: *Settings are retained between CLI sessions for local users and users listed in the remote users list.*

set history

Syntax

```
set history clear
```

Description

Clears the CLI commands history.

show history

Syntax

```
show history
```

Description

Displays the last 100 commands entered during a session.

Connection Commands

connect bidirection

Syntax

```
connect bidirection <Device Port # or Name> <endpoint> <one or more
parameters>
```

<endpoint> is one of:

```
      deviceport <Device Port # or Name>
      telnet <IP Address or Name> [port <TCP Port>]
      ssh <IP Address or Name> [port <TCP Port>] [<SSH flags>]
      tcp <IP Address> port <TCP Port>
      udp <IP Address> [port <UDP Port>]
```

Parameters

```
      exclusive <enable|disable>
      trigger <now|datetime|chars>
      date <MMDDYYhhmm[ss]>
      charcount <# of Chars>
      charseq <Char Sequence>
      charxfer <toendpoint|fromendpoint>
```

<SSH flags> is one or more of:

```
      user <Login Name>
      version <1|2>
      command <Command to Execute>
```

Note: *If the trigger is datetime (establish connection at a specified date/time), enter the date parameter. If the trigger is chars (establish connection on receipt of a specified number or characters or a character sequence), enter the charxfer parameter and either the charcount or the charseq parameter.*

connect direct

Syntax

```
connect direct <endpoint>
```

Parameters

```
      deviceport <Device Port # or Name>
      hostlist <Host List>
      ssh <IP Address or Name> [port <TCP Port>][<SSH flags>]
      tcp <IP Address> [port <TCP Port>]
      telnet <IP Address or Name> [port <TCP Port>]
      udp <IP Address> [port <UDP Port>
```

<SSH flags> is one or more of:

```
      user <Login Name>
      version <1|2>
      command <Command to Execute>
```

Description

Connects to a device port to monitor and/or interact with it, or establishes an outbound network connection.

connect listen

Syntax

```
connect listen <Device Port # or Name>
```

Description

Monitors a device port.

connect global outgoingtimeout

Syntax

```
connect global outgoingtimeout <disable|1-9999 seconds>
```

Description

Sets the amount of time the SLC console manager will wait for a response (sign of life) from an SSH/Telnet server that it is trying to connect to.

connect global show

Syntax

```
connect global show
```

Description

To display global connections.

connect script

Syntax

```
connect script <Script Name> deviceport <Device Port # or Name>
```

Description

Connect an interface script to a Device Port and run it.

connect terminate

Syntax

```
connect terminate <Connection ID List>
```

Description

Terminates a bidirectional or unidirectional connection.

connect unidirection

Syntax

```
connect unidirection <Device Port # or Name> dataflow
<toendpoint|fromendpoint> <endpoint> <one or more parameters>
```

<endpoint> is one of:

```
      deviceport <Device Port # or Name>
      telnet <IP Address or Name> [port <TCP Port>]
      ssh <IP Address or Name> [port <TCP Port>] [<SSH flags>]
      tcp <IP Address> port <TCP Port>
      udp <IP Address> port <UDP Port>
```

<SSH flags> is one or more of:

```
      user <Login Name>
      version <1|2>
      command <Command to Execute>
```

Parameters

```
      exclusive <enable|disable>
      trigger <now|datetime|chars>
      date <MMDDYYhhmm[ss]>
      charcount <# of Chars>
      charseq <Char Sequence>
```

Note: *If the trigger is datetime (establish connection at a specified date/time), enter the date parameter. If the trigger is chars (establish connection on receipt of a specified number or characters or a character sequence), enter either the charcount or the charseq parameter.*

Description

Connects a device port to another device port or an outbound network connection (data flows in one direction).

show connections

Syntax

```
show connections [email <Email Address>]
```

Description

Displays connections and their IDs. You can optionally email the displayed information. The connection IDs are in the left column of the resulting table. The connection ID associated with a particular connection may change if the connection times out and is restarted.

show connections connid

Syntax

```
show connections connid <Connection ID> [email <Email Address>]
```

Description

Displays details for a single connection. You can optionally email the displayed information.

Console Port Commands

set consoleport

Syntax

```
set consoleport <one or more parameters>
```

Parameters

```
      baud <300-230400>
      databits <7|8>
      flowcontrol <none|xon/xoff|rts/cts>
      parity <none|odd|even>
      showlines <disable|1-50 lines>
      stopbits <1|2>
      timeout <disable|1-30 minutes>
```

Description

Configures console port settings.

show consoleport

Syntax

```
show consoleport
```

Description

Displays console port settings.

Custom User Menu Commands

Users can have custom user menus as their command line interface, rather than the standard CLI command set. Each custom user menu can contain up to 50 commands ('logout' is always the last command). Instead of typing each command, the user enters the number associated with the command. Each command can also have a nickname associated with it, which can be displayed in the menu instead of the command. The commands “showmenu <Menu Name>” and “returnmenu” can be entered to display another menu from a menu, or to return to the prior menu.

When creating a custom user menu, note the following limitations:

- Maximum of 20 custom user menus.
- Maximum of 50 commands per custom user menu (`logout` is always the last command).
- Maximum of 15 characters for menu names.
- Maximum of five nested menus can be called.

- No syntax checking. (Enter each command correctly.)

set cli menu

Syntax

```
set cli menu <start | Menu Name>
```

Description

Tests a CLI menu.

set localusers menu

Syntax

```
set localusers add|edit <User Login> menu <Menu Name>
```

Description

Assigns a custom user menu to a local user.

set menu add

Syntax

```
set menu add <Menu Name> [command <Command Number>]
```

Description

Creates a new custom user menu or adds a command to an existing custom user menu.

set menu copy

Syntax

```
set menu copy <Menu Name> newmenu <New Menu Name>
```

Description

Make a copy of an existing menu.

set menu edit

Syntax

```
set menu edit <Menu Name> <parameter>
```

Parameters

```
      command <Command Number>
      nickname <Command Number>
      redisplaymenu <enable|disable>
      shownicknames <enable|disable>
      title <Menu Title>
```

Description

Changes a command within an existing custom user menu, changes a nickname within an existing custom user menu, enables or disables the redisplay of the menu before each prompt, enables or disables the display of command nicknames instead of commands, and sets the optional title for a menu.

set menu delete

Syntax

```
set menu delete <Menu Name> [command <Command Number>]
```

Description

Deletes a custom user menu or one command within a custom user menu.

show menu

Syntax

```
show menu <all|Menu Name>
```

Description

Displays a list of all menu names or all commands for a specific menu.

Date and Time Commands

set datetime

Syntax

```
set datetime <one date/time parameter>
```

Parameters

```
date <MMDDYYhhmm[ss]>
timezone <Time Zone>
```

Note: *If you do not have a valid <Time Zone>, enter "timezone <invalid time zone>" and the system guides you through the process of selecting a time zone.*

Description

Sets the local date, time, and local time zone (one parameter at a time).

show datetime

Syntax

```
show datetime
```

Description

Displays the local date, time, and time zone.

set ntp

Syntax

```
set ntp <one or more parameters>
```

Parameters

```
localserver1 <IP Address or Name>
localserver2 <IP Address or Name>
```

```
localserver3 <IP Address or Name>
poll <local|public>
publicserver <IP Address or Name>
state <enable|disable>
sync <broadcast|poll>
```

Description

Synchronizes the SLC console manager with a remote time server using NTP.

show ntp

Syntax

```
show ntp
```

Description

Displays NTP settings.

Device Commands

set command

Syntax

```
set command <Device Port # or Name or List> <one or more parameters>
```

Parameters

```
slp auth login <User Login>
slp restart
slp outletcontrol state <on|off|cyclepower> [outlet <Outlet
#>][tower <A|B>] (Outlet # is 1-8 for SLP8 and 1-16 for SLP16. The
outletcontrol parameters control individual outlets.)
slp outletstate [outlet <Outlet #>] [tower <A | B>]
slp envmon
slp infeedstatus
slp system
sensorsoft degrees <celsius | fahrenheit>
sensorsoft lowtemp <Low Temperature in C.>
sensorsoft hightemp <High Temperature in C.>
sensorsoft lowhumidity <Low Humidity%>
sensorsoft highhumidity <High Humidity%>
sensorsoft traps <enable|disable>
sensorsoft status
```

Description

Sends commands to (or control) a device connected to an SLC device port over the serial port.

Note: *Currently the only devices supported for this type of interaction are the SLP power manager and Sensorsoft devices.*

Device Port Commands

set deviceport port

Syntax

```
set deviceport port <Device Port # or List or Name> <one or more
parameters>
```

Note: *An example would be* `set deviceport port 2-5,6,12,15-16 baud 2400`*.*

Parameters

```
auth <pap|chap>
banner <Banner Text>
baud <300-230400>
breakseq <1-10 Chars>
calleridcmd <Modem Command String>
calleridlogging <enable|disable>
cbcptype <admin|user>
cbcpnocallback <enable|disable>
chaphost <CHAP Host or User Name>
chapsecret <CHAP Secret or User Password>
checkdsr <enable|disable>
closedsr <enable|disable>
databits <7|8>
device <none | slp8 | slp16 | slp8exp8 | slp8exp16 | slp16exp8 |
                              slp16exp16 | sensorsoft>
dialbackdelay <PPP Dial-back Delay>
dialbacknumber <usernumber|Phone Number>
dialinlist <Host List for Dial-in>
dialoutlogin <User Login>
dialoutnumber <Phone Number>
dialoutpassword <Password>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
```

```
dodchapsecret <CHAP Secret or User Password>
emaildelay <Email Delay>
emaillogging <disable|bytecnt|charstr>
emailrestart <Restart Delay>
emailsend <email|trap|both>
emailstring <Regex String>
emailsubj <Email Subject>
emailthreshold <Threshold>
emailto <Email Address>
flowcontrol <none|xon/xoff|rts/cts>
initscript <Modem Initialization Script>
ipaddr <IP Address>
localipaddr <negotiate|IP Address>
locallogging <enable|disable>
logins <enable|disable>
maxdirect <1-10>
modemmode <text|ppp>
modemstate <disable | dialin | dialout | dialback | dialondemand |
                              dialin+ondemand | dialinhostlist |
                              cbcpserver | cbcpclient>
modemtimeout <disable|1-9999 seconds>
name <Device Port Name>
nat <enable|disable>
nfsdir <Logging Directory>
nfslogging <enable|disable>
nfsmaxfiles <Max # of Files>
nfsmaxsize <Size in Bytes>
parity <none|odd|even>
pccardlogging <enable|disable>
pccardmaxfiles <Max # of Files>
pccardmaxsize <Size in Bytes>
pcccardslot <upper|lower>
portlogseq <1-10 Chars>
remoteipaddr <negotiate|IP Address>
restartdelay <PPP Restart Delay>
showlines <disable|1-50 lines>
slmlogging <enable|disable>
slmnms <NMS IP Address>
slmthreshold <Threshold>
```

```
        slmtime <Time Frame>
        sshauth <enable|disable>
        sshin <enable|disable>
        sshport <TCP Port>
        sshtimeout <disable|1-1800 seconds>
        stopbits <1|2>
        sysloglogging <enable|disable>
        tcpauth <enable|disable>
        tcpin <enable|disable>
        tcpport <TCP Port>
        tcptimeout <disable|1-1800 seconds>
        telnetauth <enable|disable>
        telnetin <enable|disable>
        telnetport <TCP Port>
        telnettimeout <disable|1-1800 sec>
        timeoutlogins <disable|1-30 minutes>
        usblogging <enable|disable>
        usbmaxfiles <Max # of Files>
        usbmaxsize <Size in Bytes>
        usbport <U1>
        viewportlog <enable|disable>
        webcolumns <Web SSH/Telnet Cols>
        webrows <Web SSH/Telnet Rows>
```

Note: *A group of device ports can be configured by specifying a comma-separated list of ports (i.e., '1-4,8,10-12') or 'ALL'. Remove breakseq for Device Ports connected to raw binary connections. The logging level for the Device Ports log must be set to 'Info' to view Syslog entries for Device Port logging. To send commands to devices such as SLP power manager and Sensorsoft, see the help for 'set command'.*

Description

Configures a single port or a group of ports.

set deviceport global

Syntax

```
set deviceport global <one or more parameters>
```

Parameters

```
        sshport <TCP Port>
        telnetport <TCP Port>
        tcpport <TCP Port>
```

Description

Configures settings for all or a group of device ports.

show deviceport global

Syntax

```
show deviceport global
```

Description

Displays global settings for device ports.

show deviceport names

Syntax

```
show deviceport names
```

Description

Displays a list of all device port names.

show deviceport port

Syntax

```
show deviceport port <Device Port List or Name> [display
<ip|data|modem|logging|device>]
```

Description

Displays the settings for one or more device ports.

show portcounters

Syntax

```
show portcounters [deviceport <Device Port List or Name>] [email <Email
Address>]
```

Description

Displays device port statistics and errors for one or more ports. You can optionally email the displayed information.

show portcounters zerocounters

Syntax

```
show portcounters zerocounters <Device Port List or Name>
```

Description

Zeros the port counters for one or more device ports.

show portstatus

Syntax

```
show portstatus [deviceport <Device Port List or Name>] [email <Email
Address>]
```

Description

Displays the modes and states of one or more device port(s). You can optionally email the displayed information.

Diagnostic Commands

diag arp

Syntax

```
diag arp [email <Email Address>]
```

Description

Displays the ARP table of IP address-to-hardware address mapping. You can optionally email the displayed information.

diag internals

Syntax

```
diag internals
```

Description

Displays information on the internal memory, storage and processes of the SLC console manager.

diag lookup

Syntax

```
diag lookup <Name> [email <Email Address>]
```

Description

Resolves a host name into an IP address. You can optionally email the displayed information.

diag loopback

Syntax

```
diag loopback <Device Port Number or Name>[<parameters>]
```

Parameters

```
test <internal|external>
xferdatasize <Size In Kbytes to Transfer> (Default is 1 Kbyte.)
```

Description

Tests a device port by transmitting data out the port and verifying that it is received correctly. A special loopback cable comes with the SLC console manager. To test a device port, plug the cable into the device port and run this command. The command sends the specified Kbytes to the device port and reports success or failure. The test is performed at 9600 baud. Only an external test requires a loopback cable.

diag netstat

Syntax

```
diag netstat [protocol <all|tcp|udp>] [email <Email Address>]
```

Description

To display a report of network connections. You can optionally email the displayed information.

diag nettrace

Syntax

```
diag nettrace <one or more parameters>
```

Parameters

```
      ethport <1|2>
      host <IP Address or Name>
      numpackets <Number of Packets>
      protocol <tcp|udp|icmp>
      verbose <low | medium | high | disable>
```

Description

Displays all network traffic, applying optional filters. This command is not available on the web page.

diag ping | ping6

Syntax

```
diag ping | ping6 <IP Address or Name> [<parameters>]
```

Parameters

```
      count <Number Of Times To Ping>
      packetsize <Size In Bytes>
      ethport <1|2>
```

Defaults

```
      count:5
      packetsize:64
```

Description

Verifies if the SLC console manager can reach a host over the network.

diag perfstat

Syntax

```
diag perfstat [ethport <1|2>] [deviceport <Device Port # or Name>]
```

Note: *You must specify an Ethernet Port or Device Port.*

Description

Displays performance statistics for an Ethernet Port or Device Port, averaged over the last 5 seconds.

diag sendpacket host

Syntax

```
diag sendpacket host <IP Address or Name> port <TCP or UDP Port Number>
[string <Packet String>] [protocol <tcp | udp>] [count <Number of
Packets>]
```

Defaults

```
protocol:tcp
count:1
```

Description

Generate and send Ethernet packets.

diag traceroute

Syntax

```
diag traceroute <IP Address or Name>
```

Description

Displays the route that packets take to get to a network host.

Email Log Commands

show emaillog

Syntax

```
show emaillog [email <Email Address>]
```

Description

Display the email log.

show emaillog clear

Syntax

```
show emaillog clear
```

Description

Clear the email log.

Events Commands

admin events add

Syntax

```
admin events add <trigger> <response>
```

<trigger> is one of:

```
      receivetrap, templimit, humidlimit or overcurrent
```

<response> is one of:

```
      action <syslog>

      action <fwdalltrapseth|fwdseltrapeth> ethport <1|2> nms <SNMP NMS>
            community <SNMP Community> [oid <SNMP OID>]

      action <fwdalltrapsmodem|fwdseltrapmodem> deviceport <Device Port
            # or Name> nms <SNMP NMS> community <SNMP Community> [oid
            <SNMP Trap OID>]

      action <fwdalltrapsmodem|fwdseltrapmodem> pccardslot <upper|lower>
            usbport <U1> nms <SNMP NMS> community <SNMP Community> [oid
            <SNMP Trap OID>]

      action <emailalert> emailaddress <destination email address>
```

Description

Adds SNMP event triggers and responses.

admin events delete

Syntax

```
admin events delete <Event ID>
```

Description

Deletes an event definition.

admin events edit

Syntax

```
admin events edit <Event ID> <parameters>
```

Parameters

```
      community <SNMP Community>

      deviceport <Device Port # or Name>

      ethport <1|2>

      nms <SNMP NMS>

      oid <SNMP Trap OID>

      pccardslot <upper|lower>

      emailaddress <destination email address>
```

Description

Edits event definitions.

admin events show

Syntax

```
admin events show
```

Description

Displays event definitions.

Host List Commands

set hostlist (name)

Syntax

```
set hostlist add|edit <Host List Name> [<parameters>]
```

Parameters

```
      name <Host List Name> (edit only)
      retrycount <1-10> (Default is 3.)
      auth <enable|disable>
```

Description

Configures a prioritized list of hosts to be used for modem dial-in connections.

set hostlist (number)

Syntax

```
set hostlist add|edit <Host List Name> entry <Host Number>
[<parameters>]
```

Parameters

```
      host <IP Address or Name>
      protocol <ssh|telnet|tcp>
      port <TCP Port>
      escapeseq <1-10 Chars>
```

Description

Adds a new host entry to a list or edit an existing entry.

set hostlist delete

Syntax

```
set hostlist delete <Host List> [entry <Host Number>]
```

Description

Deletes a host list, or a single host entry from a host list.

set hostlist edit

Syntax

```
set hostlist edit <Host List Name> move <Host Number> position <Host
Number>
```

Description

Moves a host entry to a new position in the host list.

show hostlist

Syntax

```
show hostlist <all|names|Host List Name>
```

Description

Displays the members of a host list.

IP Filter Commands

set ipfilter mapping

Syntax

```
set ipfilter mapping <parameters>
```

Parameters

```
ethernet <1|2> state <disable>
ethernet <1|2> state <enable> ruleset <Ruleset Name>
deviceport <1..48> state <disable>
deviceport <1..48> state <enable> ruleset <Ruleset Name>
pccardslot <upper|lower> state <disable>
pccardslot <upper|lower> state <enable> ruleset <Ruleset Name>
usbport <U1> state <disable>
usbport <U1> state <enable> ruleset <Ruleset Name>
```

Description

Maps an IP filter to an interface.

set ip filter rules

Syntax

```
set ipfilter rules <parameters>
```

Parameters:

```
add <Ruleset Name>
delete <Ruleset Name>
edit <Ruleset Name> <Edit Parameters>
```

```
      append
      insert <Rule Number>
      replace <Rule Number>
      delete <Rule Number>
```

Description

Sets IP filter rules.

set ipfilter state

Syntax

```
set ipfilter state <enable|disable> [testtimer <disable|1-120 minutes>]
```

Description

Enables or disables IP filtering for incoming network traffic.

show ipfilter

Syntax

```
show ipfilter
```

Description

Displays IP filters.

show ipfilter mapping

Syntax

```
show ipfilter mapping
```

Description

Displays the IP filter mapping.

show ipfilter ruleset

Syntax

```
show ipfilter ruleset <all|Ruleset Name>
```

Description

Displays the rulesets for the IP filters.

show ipfilter status

Syntax

```
show ipfilter status <all|Ruleset Name>
```

Description

Displays the IP filter status.

Kerberos Commands

set kerberos

Syntax

```
set kerberos <one or more parameters>
```

Parameters

```
breakseq <1-10 Chars>
clearports <Port List>
custommenu <Menu Name>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
dataports <Port List>
escapeseq <1-10 Chars>
group <default|power|admin>
ipaddr <Key Distribution Center IP Address>
kdc <Key Distribution Center>
listenports <Port List>
port <Key Distribution Center TCP Port>
realm <Kerberos Realm>
state <enable|disable>
useldapforlookup <enable|disable>
permissions <Permission List>
```

Description

Configures the SLC console manager to use Kerberos to authenticate users who log in via the Web, SSH, Telnet, or the console port.

show kerberos

Syntax

```
show kerberos
```

Description

Displays Kerberos settings.

LDAP Commands

set ldap

Syntax

```
set ldap <one or more parameters>
```

Parameters

```
      adsupport <enable|disable>
      base <LDAP Base>
      bindname <Bind Name>
      bindpassword <Bind Password>
      bindwithlogin <enable|disable>
      useldapschema <enable|disable>
      breakseq <1-10 Chars>
      clearports <Port List>
      custommenu <Menu Name>
      allowdialback <enable|disable>
      dialbacknumber <Phone Number>
      dataports <Ports List>
      encrypt <enable|disable>
      escapeseq <1-10 Chars>
      group <default|power|admin>
      listenports <Port List>
      permissions <Permission List>
      port <TCP Port> (Default is 389.)
      server <IP Address or Hostname>
      state <enable|disable>
```

Description

Configures the SLC console manager to use LDAP to authenticate users who log in via the Web, SSH, Telnet, or the console port.

show ldap

Syntax

```
show ldap
```

Description

Displays LDAP settings.

Local Users Commands

set localusers

Syntax

```
set localusers add|edit <User Login> <one or more parameters>
```

Parameters

```
      uid <User Identifier>
      allowdialback <enable|disable>
```

```
        breakseq <1-10 Chars>
        changenextlogin <enable|disable>
        changepassword <enable|disable>
        clearports <Port List>
        custommenu <Menu Name>
        dataports <Port List>
        dialbacknumber <Phone Number>
        displaymenu <enable|disable>
        escapeseq <1-10 Chars>
        group <default|power|admin>
        listenports <Port List>
        passwordexpires <enable|disable>
        permissions <Permission List>
```

Description

Configures local accounts including sysadmin who log in to the SLC console manager by means of the Web, SSH, Telnet, or the console port.

set localusers allowreuse

Syntax

```
set localusers allowreuse <enable|disable>
```

Description

Sets whether a login password can be reused.

set localusers complexpasswords

Syntax

```
set localusers complexpasswords <enable|disable>
```

Description

Sets whether a complex login password is required.

set localusers consoleonlyadmin

Syntax

```
set localusers consoleonlyadmin <enable|disable>
```

Description

```
Sets console-only admin usage.
```

set localusers delete

Syntax

```
set localusers delete <User Login>
```

Description

Deletes a local user.

set localusers lifetime

Syntax

```
set localusers lifetime <Number of Days>
```

Description

Sets the number of days the login password may be used. The default is 90 days.

set localusers lock

Syntax

```
set localusers lock|unlock <User Login>
```

Description

Allows or blocks a user login.

set localusers maxloginattempts

Syntax

```
set localusers maxloginattempts <Number of Logins>
```

Description

Sets the maximum number of login attempts before the account is locked. Disabled by default.

set localusers multipleadminlogins

Syntax

```
set localusers multipleadminlogins <enable|disable>
```

Description

Sets multiple admin logins.

set localusers password

Syntax

```
set localusers password <User Login>
```

Description

Sets a login password for the local user.

set localusers periodlockout

Syntax

```
set localusers periodlockout <Number of Minutes>
```

Description

Sets the number of minutes after a lockout before the user can try to log in again. Disabled by default.

set localusers periodwarning

Syntax

```
set localusers periodwarning <Number of Days>
```

Description

Sets the number of days the system warns the user that the password will be expiring. The default is 7 days.

set localusers reusehistory

Syntax

```
set localusers reusehistory <Number of Passwords>
```

Description

Sets the number of passwords the user must use before reusing an old password. The default is 4.

set localusers state

Syntax

```
set localusers state <enable|disable>
```

Description

Enables or disables authentication of local users.

show localusers

Syntax

```
show localusers [user <User Login>]
```

Description

Displays local users.

Log Commands

set log clear

Syntax

```
set log clear <Device Port # or Name>
```

Description

Clears the Device Port local buffer. Local logging must be enabled for a Device Port in order to use this command.

set log clear modem

Syntax

```
set log clear modem
```

Description

Clears the modem log the modem log is automatically pruned when it reaches 50K.

set log modem pppdebug

Syntax

```
set log modem pppdebug <enable|disable>
```

Description

Enables PPP debugging in the modem log. When enabled, performance could be impacted.

show log files

Syntax

```
show log files nfs | pccard | usb [locdir <NFS Mount Local
Directory>][pccardslot <upper|lower>] [usbport <U1>] [deviceport <Device
Port # or Name>]
```

Description

Lists the NFS, USB, or PC Card log files, either for a specific Device Port, or all log files in a PC Card or NFS location.

show log local

Syntax

```
show log local |nfs | pccard <Device Port # or Name> [<parameters>]
```

Parameters

```
      display <head|tail>
      numlines <Number of Lines>
      bytes <Bytes to Display>
      startbyte <Byte Index>
      logfile <NFS or PC Card Log File>
```

Defaults

```
      bytes:1000
      startbyte:1
      numlines:40
```

Description

Views the log for local, NFS, or PC card logging. NFS and PC card use the current logging settings for the device port. The default is to show the tail of the log.

show log modem

Syntax

```
show log modem [display <head|tail>] [numlines <Number of Lines>]
```

Description

View the modem activity log for external modems and PC Card modems.

Network Commands

set network

Syntax

```
set network <parameters>
```

Parameters

```
        interval <1-99999 Seconds>
        ipforwarding <enable|disable>
        probes <Number of Probes>
        startprobes <1-99999 Seconds>
```

Description

Sets TCP Keepalive and IP Forwarding network parameters.

set network bonding

Syntax

```
set network bonding <disabled|active-backup|802.3ad|load-balancing>
```

Description

Configures ethernet bonding.

set network dns

Syntax

```
set network dns <1|2|3> ipaddr <IP Address>
```

Description

```
Configures up to three DNS servers.
```

set network gateway

Syntax

```
set network gateway <parameters>
```

Parameters

```
        default <IP Address>
        precedence <dhcp|gprs|default>
        alternate <IP Address>
        pingip <IP Address>
        ethport <1 | 2>
        pingdelay <1-250 seconds>
        failedpings <1-250>
```

Description

Sets default and alternate gateways. The alternate gateway is used if an IP address usually accessible through the default gateway fails to return one or more pings.

set network host

Syntax

```
set network host <Hostname> [domain <Domain Name>]
```

Description

Sets the SLC host name and domain name.

set network ipv6

Syntax

```
set network ipv6 <enable|disable>
```

Description

Enables or disables IPv6 networking.

set network port

Syntax

```
set network port <1|2> <parameters>
```

Parameters

```
      mode <auto|10mbit-half|100mbit-half|10mbit-full|100mbit-full>
      state <dhcp|bootp|static|disable>
      [ipaddr <IP Address> mask <Mask>]
      [ipv6addr <IP v6 Address/Prefix>]
      mtu <Maximum Transmission Unit>
```

Description

Configures Ethernet port 1 or 2.

show network all

Syntax

```
show network all
```

Description

Displays all network settings.

show network bonding

Syntax

```
show network bonding
```

Description

Displays network connections that are bonded.

`show network dns`

Syntax

```
show network dns
```

Description

Displays DNS settings.

`show network gateway`

Syntax

```
show network gateway
```

Description

Displays gateway settings.

`show network host`

Syntax

```
show network host
```

Description

Displays the network host name of the SLC console manager.

`show network port`

Syntax

```
show network port <1|2>
```

Description

Displays Ethernet port settings and counters.

NFS and SMB/CIFS Commands

`set cifs`

Syntax

```
set cifs <one or more parameters>
```

Parameters

```
      eth1 <enable|disable>
      eth2 <enable|disable>
      state <enable|disable>
      workgroup <Windows workgroup>
```

Description

Configures the SMB/CIFS share, which contains the system and device port logs.

Note: *The* `admin config` *command saves SLC configurations on the SMB/CIFS share.*

set cifs password

Syntax

```
set cifs password
```

Description

Changes the password for the SMB/CIFS share login (default is cifsuser).

set nfs mount

Syntax

```
set nfs mount <1|2|3> <one or more parameters>
```

Parameters

```
      remdir <NFS Share>
      locdir <Directory>
      rw <enable|disable>
      mount <enable|disable>
```

Note: *Specification of rmdir and locdir parameters are required. Once specified, the parameters do not need to be re-specified.*

Description

Mounts a remote NFS share. The `remdir` and `locdir` parameters are required, but if they have been specified previously, you do not need to provide them again.

set nfs unmount

Syntax

```
set nfs unmount <1|2|3>
```

Description

Unmounts a remote NFS share.

show cifs

Syntax

```
show cifs
```

Description

Displays SMB/CIFS settings.

show nfs

Syntax

```
show nfs
```

Description

Displays NFS share settings.

NIS Commands

set nis

Syntax

```
set nis <one or more parameters>
```

Parameters

```
      breakseq <1-10 Chars>
      broadcast <enable|disable>
      clearports <Port List>
      custommenu <Menu Name>
      allowdialback <enable|disable>
      dialbacknumber <Phone Number>
      dataports <Port List>
      domain <NIS Domain Name>
      escapeseq <1-10 Chars>
      group <default|power|admin>
      listenports <Port List>
      master <IP Address or Hostname>
      permissions <Permission List>
      slave1 <IP Address or Hostname>
      slave2 <IP Address or Hostname>
      slave3 <IP Address or Hostname>
      slave4 <IP Address or Hostname>
      slave5 <IP Address or Hostname>
      state <enable|disable>
```

Description

Configures the SLC console manager to use NIS to authenticate users who log in via the Web, SSH, Telnet, or the console port.

show nis

Syntax

```
show nis
```

Description

Displays NIS settings.

PC Card Commands

pccard modem

Syntax

```
pccard modem <upper|lower> <parameters>
```

Parameters

```
auth <pap|chap>
baud <300-115200> (Default is 9600)
cbcpnocallback <enable|disable>
cbcptype <admin|user>
calleridcmd <Modem Command String>
calleridlogging <enable|disable>
chaphost <CHAP Host or User Name>
chapsecret <CHAP Secret or User Password>
databits <7|8>
dialbackdelay <PPP Dialback Delay>
dialbacknumber <usernumber|Phone Number>
dialinlist <Host List for Dial-in>
dialoutlogin <User Login>
dialoutnumber <Phone Number>
dialoutpassword <Password>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
dodchapsecret <CHAP Secret or User Password>
flowcontrol <none|xon/xoff|rts/cts>
gsmautodns <enable|disable>
gsmbearerservice <GSM Bearer Service>
gsmcompression <enable|disable>
gsmcontext <GPRS Context Id>
gsmdialoutmode <gprs|gsm>
gsmpin <GSM/GPRS PIN Number>
initscript <Modem Initialization Script>
isdnchannel <1|2>
isdnnumber <Phone Number>
localipaddr <negotiate|IP Address>
modemmode <text|ppp>
modemstate <disable | dialin | dialout | dialback | cbcpserver |
                              cbcpclient | dialondemand |
                              dialin+ondemand | dialinhostlist>
```

```
        modemtimeout <disable|1-9999 sec>
        nat <enable|disable>
        parity <none|odd|even>
        remoteipaddr <negotiate|IP Address>
        restartdelay <PPP Restart Delay>
        service <none|telnet|ssh|tcp>
        sshauth <enable|disable>
        sshport <TCP Port>
        stopbits <1|2>
        tcpauth <enable|disable>
        tcpport <TCP Port>
        telnetauth <enable|disable>
        telnetport <TCP Port>
        timeoutlogins <disable|1-30 minutes>
```

Note: *Dial-out GPRS connections may replace the default route and DNS entries. Static routes (see* `set routing`*) may be required to maintain access to subnets that are not directly attached to the SLC console manager. It is recommended that the initscript be prepended with AT and include E1 V1 x4 Q0 so that the SLC device may properly control the modem.*

Description

Configures a currently loaded PC Card.

pccard storage copy

Syntax

```
pccard storage copy <upper|lower> file <Filename> newfile <New Filename>
```

Description

Copies a file on a Compact Flash card.

pccard storage delete

Syntax

```
pccard storage delete <upper|lower> file <Current Filename>
```

Description

Removes a file on a Compact Flash card.

pccard storage dir

Syntax

```
pccard storage dir <upper|lower>
```

Description

Views a directory listing of a Compact Flash card.

pccard storage format

Syntax

```
pccard storage format <upper|lower> [filesystem <ext2|fat>]
```

Description

Formats a Compact Flash card.

pccard storage mount

Syntax

```
pccard storage mount <upper|lower>
```

Description

Mounts a Compact Flash card in the SLC console manager for use as a storage device. The Compact Flash card must be formatted with an ext2 or FAT file system before you mount it.

pccard storage rename

Syntax

```
pccard storage rename <upper|lower> file <Filename> newfile <New
Filename>
```

Description

To rename a file on a Compact Flash card.

pccard storage unmount

Syntax

```
pccard storage unmount <upper|lower>
```

Description

Unmounts a Compact Flash card. Enter this command before ejecting the card.

show pccard

Syntax

```
show pccard
```

Description

Displays currently loaded PC cards with product information and settings.

show pccard storage

Syntax

```
show pccard storage
```

Description

Displays product information and settings for any PC card compact flash.

show pccard modem

Syntax

```
show pccard modem
```

Description

Displays product information and settings for any PC card modem.

RADIUS Commands

set radius

Syntax

```
set radius <one or more parameters>
```

Parameters

```
      breakseq <1-10 Chars>
      clearports <Port List>
      custommenu <Menu Name>
      allowdialback <enable|disable>
      dialbacknumber <Phone Number>
      dataports <Port List>
      escapeseq <1-10 Chars>
      group <default|power|admin>
      listenports <Port List>
      state <enable|disable>
      permissions <Permission List>
      timeout <enable|1-30 seconds>
```

Description

Configures the SLC console manager to use RADIUS to authenticate users who log in via the Web, SSH, Telnet, or the console port.

set radius server

Syntax

```
set radius server <1|2> host <IP Address or Hostname> secret <Secret>
[port <TCP Port>]
```

Description

Identifies the RADIUS server, the text secret, and the TCP port number.

Note: *The default port is 1812.*

show radius

Syntax

```
show radius
```

Description

Displays RADIUS settings.

Remote Users Commands

set remoteusers

Syntax

```
set remoteusers add|edit <User Login> [<parameters>]
```

Parameters

```
      allowdialback <enable|disable>
      breakseq <1-10 Chars> listenports <Port List>
      clearports <Port List>
      custommenu <Menu Name>
      dataports <Port List>
      dialbacknumber <Phone Number>
      displaymenu <enable|disable>
      escapeseq <1-10 Chars>
      group <default|power|admin>
      permissions <Permissions List>
```

where <Permission List> is one or more of:

```
      nt, sv, dt, lu, ra, sk, um, dp, pc, rs, rc, dr, wb, sn, ad, do, ub
```

Note: *To remove a permission, type a minus sign before the two-letter abbreviation for a user right.*

Description

Sets attributes for users who log in by a remote authentication method.

set remoteusers delete

Syntax

```
set remoteusers delete <User Login>
```

Description

Removes a remote user.

set remoteusers listonlyauth

Syntax

```
set remoteusers listonlyauth <enable|disable>
```

Description

Sets whether remote users who are not part of the remote user list will be authenticated.

show remoteusers

Syntax

```
show remoteusers
```

Description

Displays settings for all remote users.

Routing Commands

set routing

Syntax

```
set routing [parameters]
```

Parameters

```
rip <enable|disable>
route <1-64> ipaddr <IP Address> mask <Netmask> gateway <IP Address>
static <enable|disable>
version <1|2|both>
```

Note: *To delete a static route, set the ipaddr, mask, and gateway to 0.0.0.0.*

Description

Configures static or dynamic routing. To delete a static route, set the IP address, mask, and gateway parameters to 0.0.0.0.

show routing

Syntax

```
show routing [sort <destination|iface>] [display <IP Address>]
[resolveip <enable|disable>] [email <Email Address>]
```

Description

Sets the routing table to display IP addresses (disable) or the corresponding host names (enable). You can email the displayed information.

Script Commands

set script delete

Syntax

```
set script delete <interface|batch> name <Script Name>
```

Description

Delete a script.

set script import

Syntax

```
set script import <interface|batch> via <ftp|scp|copypaste> [file
<Script File>] [name <Script Name>] [host <IP Address or Name>] [login
<User Login>] [path <Path to Script File>]
```

Note: *Interface scripts have default/do user rights. Batch scripts have admin/ad user rights. The script name is the same as the file name (if it is a valid script name), otherwise a script name must be specified for import.*

Description

Import a script.

set script rename

Syntax

```
set script rename <interface|batch> name <Script Name> newname <New
Script Name>
```

Description

Rename a script.

set script runcli

Syntax

```
set script runcli <Script Name>
```

Description

Run a CLI batch script.

set script update

Syntax

```
set script update <interface|batch> name <Script Name> [group
<default|power|admin>] [permissions <Permission List>]
```

Description

Updates a script.

show script

Syntax

```
show script [type <interface|batch> [name <Script Name>]]
```

Description

Display list of Device Port (interface) scripts or CLI (batch) scripts, or view the contents of a script.

Services Commands

set services

Syntax

```
set services <one or more services parameters>
```

Parameters

```
      alarmdelay <1-6000 Seconds>
      auditlog <enable|disable>
      auditsize <1-500 Kbytes>
      authlog <off|error|warning|info|debug>
      clicommands <enable|disable>
      contact <Admin Contact Info>
      devlog <off|error|warning|info|debug>
      diaglog <off|error|warning|info|debug>
      genlog <off|error|warning|info|debug>
      includesyslog <enable|disable>
      javabufsize <Number of Lines>
      javaterminal <jws|applet>
      location <Physical Location>
      netlog <off|error|warning|info|debug>
      nms <IP Address or Name>
      outgoingtelnet <enable|disable>
      phoneip <IP Address>
      phonehome <enable|disable>
      portssh <TCP Port>
      rocommunity <Read-Only Community>
      rwcommunity <Read-Write Community>
      servlog <off|error|warning|info|debug>
      smtpsender <Email Address>
      smtpserver <IP Address or Name>
      snmp <enable|disable>
```

```
        ssh <enable|disable>
        syslogserver1 <IP Address or Name>
        syslogserver2 <IP Address or Name>
        telnet <enable|disable>
        timeoutssh <disable|1-30 minutes>
        timeouttelnet <disable|1-30 minutes>
        traps <enable|disable>
        trapcommunity <Trap Community>
        v1ssh <enable|disable>
        webssh <enable|disable>
        webtelnet <enable|disable>
        v3auth <md5|sha>
        v3encrypt <des|aes>
        v3password <V3 RO User Password>
        v3phrase <V3 RO User Passphrase>
        v3rwpassword <V3 RW User Password>
        v3rwphrase <V3 RW User Passphrase>
        v3rwuser <V3 RW User>
        v3security <noauth|auth|authencrypt>
        v3user <V3 RO User>
```

Description

Configures services (system logging, SSH and Telnet access, SSH and Telnet timeout, SNMP agent, email (SMTP) server, and audit log). Sets a password for an SNMP manager to access the read-only data the SLC SNMP agent provides and to modify data when permitted.

set services trapenable

Syntax

```
set services trapenable
```

Description

Defines the set of SNMP traps that are sent by the SLC console manager.

show services

Syntax

```
show services
```

Description

Displays current services.

SLC Network Commands

set slcnetwork

Syntax

```
set slcnetwork <parameters>
```

Parameters

```
add <IP Address>
delete <IP Address>
search <localsubnet|ipaddrlist|both>
```

Description

Detects and displays all SLC console manager or user-defined IP addresses on the local network.

show slcnetwork

Syntax

```
show slcnetwork[ipaddrlist <all|Address Mask>]
```

Description

Detects and displays all SLC console managers on the local network. Without the `ipaddrlist` parameter, the command searches the SLC network. With the `ipaddrlist` parameter, the command displays a sorted list of all IP addresses or displays the IP addresses that match the mask (for example, 172.19.255.255 would display all IP addresses that start with 172.19).

SSH Key Commands

set sshkey allexport

Syntax

```
set sshkey allexport <ftp|scp|copypaste> [pubfile <Public Key File>]
[host <IP Address or Name>] [login <User Login>] [path <Path to Copy
Keys>]
```

Description

Exports the public keys of all previously created SSH keys.

set sshkey delete

Syntax

```
set sshkey delete <one or more parameters>
```

Parameters

```
keyhost <SSH Key Host>
keyname <SSH Key Name>
keyuser <SSH Key User>
```

Description

Deletes an ssh key. Specify the `keyuser` and `keyhost` to delete an imported key; specify the `keyuser` and `keyname` to delete exported key.

set sshkey export

Syntax

```
set sshkey export <ftp|scp|copypaste> <one or more parameters>
```

Parameters

```
      [format <openssh|secsh>]
      [host <IP Address or Name>]
      [login <User Login>]
      [path <Path to Copy Key>]
      [bits <512 | 1024 | 2048>]
      keyname <SSH Key Name>
      keyuser <SSH Key User>
      type <rsa|dsa>
```

Description

Exports an sshkey. RSA keys must be 1024 or 2048 bits.

set sshkey import

Syntax

```
set sshkey import <ftp|scp|copypaste> [file <Public Key File>] [host <IP
Address or Name>] [login <User Login>] [path <Path to Public Key File>]
[keyuser <SSH Key User>] [keyhost <SSH Key IP Address or Name>]
```

Note: *The key file may contain multiple keys; in this case the keyuser and keyhost will be ignored.*

Description

Imports an SSH key.

set sshkey server import

Syntax

```
set sshkey server import type <rsa1|rsa|dsa> via <sftp|scp> pubfile
<Public Key File> privfile <Private Key File> host <IP Address or Name>
login <User Login> [path <Path to Key File>]
```

Description

Imports an SLC host key.

set sshkey server reset

Syntax

```
set sshkey server reset [type <all|rsa1|rsa|dsa>]
```

Description

Resets defaults for all or selected host keys.

show sshkey export

Syntax

```
show sshkey export <one or more parameters>
```

Parameters

```
      [keyhost <SSH Key IP Address or Name>]
      [keyuser <SSH Key User>]
      [viewkey <enable|disable>]
```

Description

Displays all exported keys or keys for a specific user, IP address, or name.

show sshkey import

Syntax

```
show sshkey import <one or more parameters>]
```

Parameters

```
      [keyhost <SSH Key IP Address or Name>]
      [keyuser <SSH Key User>]
      [viewkey <enable|disable>]
```

Description

Displays all keys that have been imported or keys for a specific user, IP address, or name.

show sshkey server

Syntax

```
show sshkey server [type <all|rsa1|rsa|dsa>]
```

Description

Displays host keys (public key only).

Status Commands

`show sysconfig`

Syntax

```
show sysconfig [display <basic|auth|devices>] [email <Email Address]
```

Description

Displays a snapshot of all configurable parameters. Optionally emails the displayed information.

`show sysstatus`

Syntax

```
show sysstatus [email <Email Address>]
```

Description

To display the overall status of all SLC devices. Optionally emails the displayed information.

System Log Commands

`show syslog`

Syntax

```
show syslog [<parameters>]
```

Parameters

```
      email <Email Address>]
      level <error|warning|info|debug>
      log <all|netlog|servlog|authlog|devlog|diaglog|genlog>
      display <head|tail> [numlines <Number of Lines>]
      starttime <MMDDYYhhmm[ss]>
      endtime <MMDDYYhhmm[ss]>
```

Description

Displays the system logs containing information and error messages.

Note: *T*he level and display parameters cannot be used simultaneously.

`show syslog clear`

Syntax

```
show syslog clear <all|netlog|servlog|authlog|devlog|diaglog|genlog>
```

Description

Clears one or all of the system logs.

TACACS+ Commands

set tacacs+

Syntax

```
set tacacs+ <one or more parameters>
```

Parameters

```
breakseq <1-10 Chars>
clearports <Port List>
custommenu <Menu Name>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
dataports <Port List>
encrypt <enable|disable>
escapeseq <1-10 Chars>
group <default|power|admin>
listenports <Port List>
permissions <Permission List>
secret <TACACS+ Secret>
server1 <IP Address or Name>
server2 <IP Address or Name>
server3 <IP Address or Name>
state <enable|disable>
```

Description

Configures the SLC console manager to use TACACS+ to authenticate users who log in via the Web, SSH, Telnet, or the console port.

show tacacs+

Syntax

```
show tacacs+
```

Description

Displays TACACS+ settings.

Temperature Commands

set temperature

Syntax

```
set temperature low <Low Temperature in C> high <High Temperature in C>
```

Description

Sets the acceptable range for the internal temperature sensor (an SNMP trap is sent if the temperature is outside of this range).

show temperature

Syntax

```
show temperature
```

Description

Displays the acceptable range and the current reading from the internal temperature sensor.

USB Commands

set usb access

Syntax

```
set usb access <enable | disable>
```

Description

Enables or disables access to USB devices.

set usb modem

Syntax

```
set usb modem <U1> <parameters>
```

Parameters

```
    auth <pap|chap>
    baud <300-115200>
    calleridcmd <Modem Command String>
    calleridlogging <enable|disable>
    cbcpnocallback <enable|disable>
    cbcptype <admin|user>
    chapauth <chaphost|localusers>
    chaphost <CHAP Host or User Name>
    chapsecret <CHAP Secret or User Password>
    databits <7|8>
    dialbackdelay <PPP Dialback Delay>
    dialbacknumber <usernumber|Phone Number>
    dialinlist <Host List for Dial-in>
    dialoutlogin <User Login>
    dialoutnumber <Phone Number>
    dialoutpassword <Password>
    dodauth <pap|chap>
    dodchaphost <CHAP Host or User Name>
    dodchapsecret <CHAP Secret or User Password> restartdelay <PPP
    Restart Delay>
    flowcontrol <none|xon/xoff|rts/cts>
    initscript <Modem Init Script>
    localipaddr <negotiate|IP Address>
    modemmode <text|ppp>
    modemstate <disable | dialin | dialout | dialback | cbcpserver |
    cbcpclient | dialondemand |dialin+ondemand | dialinhostlist>
    modemtimeout <disable|1-9999 sec>
    nat <enable|disable>
    parity <none|odd|even>
    remoteipaddr <negotiate|IP Address>
    service <none|telnet|ssh|tcp>
    sshauth <enable|disable>
    sshport <TCP Port>
    stopbits <1|2>
    tcpauth <enable|disable>
    tcpport <TCP Port>
    telnetauth <enable|disable>
    telnetport <TCP Port>
    timeoutlogins <disable|1-30 minutes>
    usesites <enable|disable>
```

Note: *It is recommended that the initscript be prepended with 'AT' and include 'E1 V1 x4 Q0' so that the SLC console manager may properly control the modem.*

Description

Configures a currently loaded USB modem.

set usb storage dir

Syntax

```
set usb storage dir <U1>
```

Description

Displays a directory listing of a thumb drive.

set usb storage rename

Syntax

```
set usb storage rename <U1> file <Filename> newfile <New Filename>
```

Description

Renames a file on a thumb drive.

set usb storage copy

Syntax

```
set usb storage copy <U1> file <Filename> newfile <New Filename>
```

Description

Copies a file on a thumb drive.

set usb storage delete

Syntax

```
set usb storage delete <U1> file <Current Filename>
```

Description

Removes a file on a thumb drive.

set usb storage format

Syntax

```
set usb storage format <U1> [filesystem <ext2|fat>]
```

Description

Formats a thumb drive.

set usb storage mount

`Syntax`

set usb storage mount <U1>

Description

Mounts a thumb drive for use as a storage device. The thumb drive can be used for saving configurations and device logging.

set usb storage unmount

Syntax

```
set usb storage unmount <U1>
```

Description

Unmounts a thumb drive.

show usb

Syntax

```
show usb
```

Description

Displays currently attached USB devices with their product information and settings.

show usb storage

Syntax

```
show usb storage
```

Description

Display product information and settings for any USB thumb drive.

show usb modem

Syntax

```
show usb modem
```

Description

Display product information and settings for any USB modem.

User Permissions Commands

Each user is a member of a group (default users, power users, administrators) and has a set of user rights associated with the group. Additional user rights which are not defined by the group may also be granted to them using the 'permissions' parameter.

The <Permission List> parameters is a comma-separated list of user rights to be added to or removed from current permissions. Precede the two-letter acronym with a '-' to remove a user right. For example, “nt,dt,-wb” adds Networking and Date/Time rights and removes Web Access rights.

The following parameters assign user rights:

nt - configure Networking

sv - configure Services

dt - configure Date/Time

lu - configure Local Users

ra - configure Remote Authentication methods

rs - Reboot or Shutdown the SLC

fc - manage Firmware and Configurations

ad - full Administrative rights

po - configure Power Outlets

dp - configure Device Ports

do - Device Port operations

pc - configure PC Cards

um - configure User Menus

dr - view Diagnostics & Reports

wb - Web Access

sn - configure Secure Lantronix Network

sk - configure SSH Keys

ub - configure USB

Note: *For remote authentication methods, there is one group and set of user rights defined for all users who login via a remote authentication method.*

Appendix A: Bootloader

The SLC console manager provides a bootload command interface. This interface is only accessible through the SLC console port.

Accessing the Bootloader

To access the bootloader CLI:

1. Power up the SLC console manager.
2. Type **x15** within 10 seconds of power up. The bootloader halts the boot procedure and displays a **Lantronix** command prompt.

Bootloader Commands

Table A-1 User Commands

`help`	Lists and prints the command list and online help.
`?`	An alias for help.
`boot`	Boot default (runs bootcmd).
`bootcheck`	Checks boot bank information.
`bootinfo`	Displays boot bank information.
`bootsel 1|2`	Selects boot bank 1 or boot bank 2.
`IDE`	Accesses the IDE sub-system.
`mtest`	Performs a simple test of the RAM.
`showconf`	Displays hardware configuration.
`su cust|admin`	Switches to another user: from cust (customer) to admin (administrator) and vice versa.
`version`	Prints the bootloader version.
`whoami`	Displays information about the current user.

Administrator Commands

In addition to the commands that the user can issue, the administrator can issue the following commands:

`imagecopy`	Copies an image of the drive from the lower PCMCIA device to the internal CF card.
`passwd`	Provides a new password for user admin. The default password for user admin is admin. User cust does not have a password.
`ping`	Sends a ping request to the network host.
`printeny`	Prints bootloader variables.
`setenv`	Sets environment variables.
`showconf`	Displays hardware configuration parameters.

Appendix B: Security Considerations

The SLC console manager provides data path security by means of SSH or Web/SSL. Do not assume that you have complete security, however. Securing the data path is only one way to ensure security. This appendix briefly discusses some important security considerations.

Security Practice

Develop and document a Security Practice. For example, the Security Practice document should state the rules to maintaining security. For example, do not leave sessions open or advertise passwords because these actions could compromise SSH and SSL. Or, do not speculate about the facility and network infrastructure with reference to how vulnerable the CAT 5 wiring is to tapping.

Factors Affecting Security

External factors affect the security provided by the SLC device, for example:

- Telnet sends the login exchange as clear text across Ethernet. A person snooping on a subnet may read your password.
- A terminal to the SLC console manager may be secure, but the path from the SLC device to the end device may not be secure.
- With the right tools, a person having physical access to open the SLC console manager may be able to read the encryption keys.
- There is no true test for a denial-of-service attack; there is always a legitimate reason to request a storm. A denial-of-service filter locks out some high-performance automated/ scripted requests. The SLC device always attempts to service requests and does not filter out potential denial–of-service attacks.

Appendix C: Safety Information

This appendix describes the safety precautions that should be followed when installing and operating the SLC console manager. It contains the following sections:

- *Cover*
- *Power Plug*
- *Input Supply*
- *Grounding*
- *Fuses*
- *Rack*
- *Port Connections*

Cover

Do not remove the cover of the chassis. There are no user-serviceable parts inside. Opening or removing the cover may expose you to dangerous voltage that could cause fire or electric shock.

Note: *Refer all servicing to Lantronix, Inc.*

Power Plug

- When disconnecting the power cable from the socket, pull on the plug, not the cord.
- Always connect the power cord to a properly wired and grounded power source. Do not use adapter plugs or remove the grounding prong from the cord.
- Only use a power cord with a voltage and current rating greater than the voltage and current rating marked on the unit.
- Install the unit near an AC outlet that is easily accessible.
- Always connect any equipment used with the product to properly wired and grounded power sources.
- To help protect the product from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Do not connect or disconnect this product during an electrical storm.

Input Supply

- This unit may have more than one power supply source. Disconnect all power supply sources before servicing to avoid electric shock.
- Check nameplate ratings to assure there is no overloading of supply circuits that could affect over current protection and supply wiring.

Grounding

- Maintain reliable grounding of this product.
- Pay particular attention to supply connections when connecting to power strips, rather than directly to the branch circuit.
- Install DC-rated equipment only under the following conditions:
  - Connect the equipment to a DC supply source that is electrically isolated from the AC source and reliably connected to ground, or connect it to a DC (SELV) source.
  - Install only in restricted access areas (dedicated equipment rooms, equipment closets or the like) in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
  - Route and secure input wiring to terminal block in such a manner that it is protected from damage and stress. Do not route wiring past sharp edges or moving parts.
  - Incorporate a readily accessible disconnect device, with a 3 mm minimum contact gap, in the fixed wiring.
  - Provide a listed circuit breaker suitable for protection of the branch circuit wiring and rated 60 VDC minimum.

Fuses

For protection against fire, replace the power-input-module fuse with the same type and rating.

Rack

If rack mounted units are installed in a closed or multi-unit rack assembly, they may require further evaluation by Certification Agencies. The following items must be considered:

- Do **not** install the unit in a rack in such a way that a hazardous stability condition results because of uneven loading. A drop or fall could cause injury.
- The ambient temperature (Tma) inside the rack may be greater than the room ambient temperature. Make sure to install the SLC console manager in an environment with an ambient temperature less than the maximum operating temperature of the SLC device. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- Install the equipment in a rack in such a way that the amount of airflow required for safe operation of the equipment is not compromised.
- Maintain reliable earthing of rack-mounted equipment. Give particular attention to supply connections other than direct connections to the branch circuit (e.g. use of power strips) because of the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Before operating the SLC console manager, make sure the SLC unit is secured to the rack.

Port Connections

- Only connect the network port to an Ethernet network that supports 10Base-T/100Base-T.
- Only connect device ports to equipment with serial ports that support EIA-232 (formerly RS-232C).
- Only connect the console port to equipment with serial ports that support EIA-232 (formerly RS-232C).

Appendix D: Sicherheitshinweise

Dieser Anhang beschreibt die Sicherheitshinweise die bei der Installation und Benutzung des SLC Gerätes befolgt werden müssen. Es beinhaltet die folgenden Punkte:

Geräteabdeckung

Entfernen Sie nicht die Abdeckung des Gerätes. Es gibt keine zu wartenden Teile innerhalb des Gerätes. Beim öffnen oder entfernen der Abdeckung könnten Sie gefährlichen Spannungen ausgesetzt werden die unter Umständen Feuer oder elektrischen Schlag zur Folge haben könnten.

Hinweis: *Lassen Sie alle Wartungsarbeiten durch die Firma Lantronix durchführen.*

Netzstecker

- Wenn Sie das Netzkabel von der Steckdose trennen, ziehen Sie am Stecker und nicht am Kabel
- Das Netzkabel muß unter allen Umständen an einer geeigneten sowie geerdeten Netzversorgung angeschlossen werden. Benutzen Sie keine Adapterstecker und entfernen Sie nicht den Schutzleiteranschluss des Netzkabels.
- Benutzen Sie nur ein Netzkabel, das mindestens mit den Anforderungen bezüglich der Spannungs und Stromangaben des Gerätes entsprechen.
- Installieren Sie das Gerät nur an einer leicht zugänglichen Stromversorgung.
- Schließen Sie nur Geräte an das Produkt an, die ensprechend verdrahtet und an einer geerdeten Stromversorgung angeschlossen sind.
- Um das Gerät vor plötzlichen Überspannungsspitzen und Spannungsabfall zu schützen, benutzen Sie entweder einen Überspannungsableiter, Netzleitungsstabilisierer oder eine Unterbrechungsfreie Stromversorgung (UPS).
- Während eines Gewitters sollte das Gerät nicht von der Netzversorgung getrennt oder daran angeschlossen werden.

Stromversorgung

- Dieses Gerät kann mehr als eine Stromversorgung haben. Trennen Sie alle Stromquellen vor Wartungsarbeiten, um elektrischen Schlag zu vermeiden.
- Überprüfen Sie die elektrischen Angaben auf dem Typenschild um sicherzustellen, das die Netzversorgung oder Anschlußkabel nicht überlastet werden.

Anschluß an die Schutzerde

- Stellen Sie sicher, daß das Gerät immer ausreichend mit der Schutzerde verbunden ist.
- Beachten Sie dieses besonders im Falle des Anschlusses an ein Verlängerungskabel oder wenn aus einem anderen Grund das Gerät nicht direkt an eine Steckdose angeschlossen wird.
- Schließen Sie ein ausschließlich für Gleichstrom geeignetes Gerät nur unter folgenden Bedingungen an:
  - Schließen Sie das Gerät nur an eine Gleichstromversorgung an, die elektrisch von einer Wechselstromversorgung getrennt ist und ausreichend geerdet ist, oder verbinden Sie das Gerät mit einer Gleichstromversorgung des Typen SELV
  - Installieren Sie das Gerät nur an einem Ort / Betriebsstätte mit beschränktem Zutritt (speziel dafür vorgesehene IT Räume, Schaltschränke oder ähnliches)
  - Führen und sichern Sie die Anschlussverdrahtung so zu den Anschlussklemmen daß sie vor hoher Beanspruchung und Beschädigung geschützt ist.
  - Beim Anschluß des Gerätes muß eine leicht zugängliche Trennvorrichtung mit einem Kontaktabstand, der mindestens 3mm beträgt, in die Anschlußverkabelung mitinstalliert werden
  - Für die Absicherung des Anschlußstromkreises muß ein geeigneter Schutzschalter benutzt werden, der mindestens für eine Gleichspannung von 60V bemessen ist.

Gerätesicherung

Für den Schutz gegen Feuer ersetzen Sie die Sicherung des Eingangsmodules nur mit einer Sicherung gleichen Typs und Nenngröße.

Rack / Einbauschrank

Falls Geräte für die Installierung in einen Geräteschrank in einen solchen Schrank eingebaut werden, der entweder geschlossen ist oder in dem sich andere Geräte befinden, muß unter Umständen eine weitere Abnahme durch eine Zertifizierungsstelle veranlasst werden. Die folgenden Punkte müssen dabei beachtet werden:

- Installieren Sie das Gerät nicht in einen Einbauschrank oder Rack so daß es zu einer gefährlichen, ungleichgewichtigen Anordnung kommen kann. Das heraus-, hin- oder umfallen kann zu Verletzungen führen.
- Die Umgebungstemperatur (Tma) innerhalb des Einbauschrankes oder Racks kann höher sein als die Raumtemperatur. Stellen Sie sicher, daß das SLC Gerät in einer Umgebung

installiert wird, in der die Temperatur geringer als die für das SLC Gerät angegebene, maximale Betriebstemperatur ist.

- Installieren Sie das Gerät in einen Einbauschrank oder Rack so daß es zu keiner Einschränkung der Luftzufuhr kommt, die einen sicheren Betrieb des Gerätes gewährleistet.
- Installieren Sie das Gerät in einen Einbauschrank oder Rack so daß es zu keiner ungleichen, mechanischen Belastung kommt, die zu einer gefährlichen Situation führen kann. Stellen Sie sicher, daß Geräte, die für den Einbau in einen Geräteschrank oder Rack vorgesehen sind, ausreichend mit der Schutzerde verbunden sind. Beachten Sie dieses besonders im Falle des Anschlusses an eine Steckdosenleiste oder wenn aus einem anderen Grund das Gerät nicht direkt an eine Steckdose angeschlossen wird.
- Bevor Sie das SLC Gerät in Betrieb nehmen stellen Sie sicher, daß es entsprechend und sicher in den Einbauschrank oder Rack installiert ist.

Signalverbindungen

- Verbinden Sie den Netzwerkanschluß nur an einen Ethernetanschluß, der den Typen 10Base-T/100Base-T unterstützt.
- Verbinden Sie die Signalanschlüsse des Gerätes nur an Serielle Anschlüsse, die das Format EIA-232 (früher RS-232C) unterstützten.
- Verbinden Sie die Anschlüsse der Gerätekonsole nur an Serielle Anschlüsse, die das Format EIA-232 (früher RS-232C) unterstützten.

⚠ ***Achtung:*** ***Dieses Gerät kann mehr als eine Stromversorgung haben. Trennen Sie alle Stromquellen vor Wartungsarbeiten, um elektrischen Schlag zu vermeiden.***

Appendix E: Adapters and Pinouts

The serial device ports of the SLC products match the RJ45 pinouts of the console ports of many popular devices found in a network environment. The SLC console manager uses conventional straight-through Category 5 fully pinned network cables for all connections when used with Lantronix adapters. The cables are available in various lengths.

In most cases, you will need an adapter for your serial devices. Lantronix offers a variety of RJ45-to-serial connector adapters for many devices. These adapters convert the RJ45 connection on the SLC console manager to a 9-pin or 25-pin serial connector found on other manufacturers' serial devices or re-route the serial signals for connections to other devices that use RJ45 serial connectors.

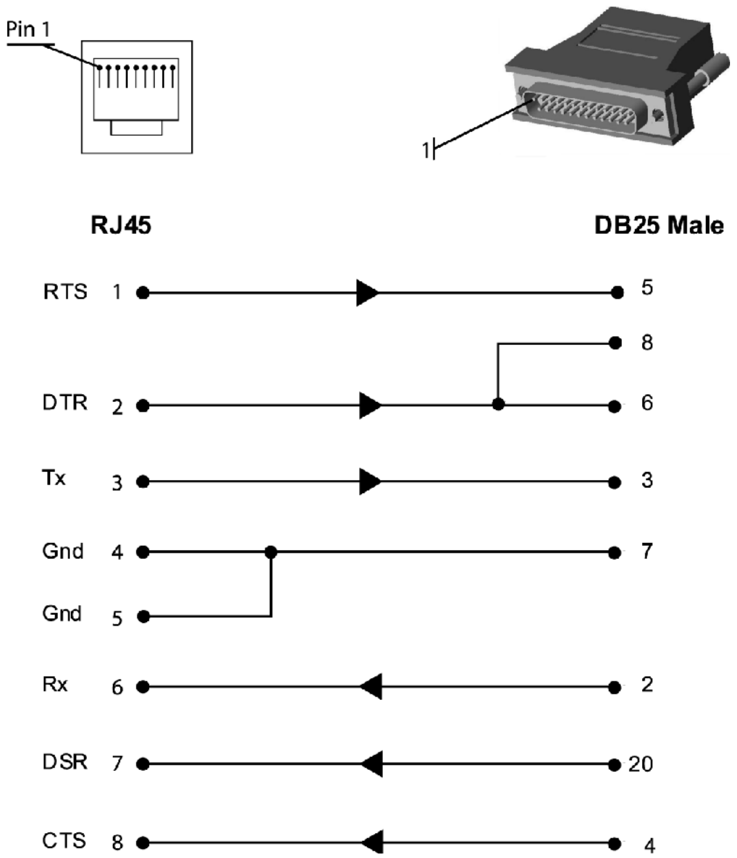
Please check the cabling database on the Lantronix web site at http://www.lantronix.com for suggested cables and adapters for commonly used serial devices.

The console port is wired the same way as the device ports and has the same signal options.

Note: *You can view or change the console port settings using the LCDs and pushbuttons on the front panel, the Console Port web page, or the command line interface* `show console port` *and* `set consoleport` *commands.*

The adapters shown in this chapter are compatible with the Lantronix SLC models.

Figure E-1 RJ45 Receptacle to DB25M DCE Adapter for the SLC Console Manager (PN 200.2066A)



Use PN 200.2066A adapter with a dumb terminal or with many SUN applications.

Figure E-2 RJ45 Receptacle to DB25F DCE Adapter for the SLC Console Manager (PN 200.2067A)

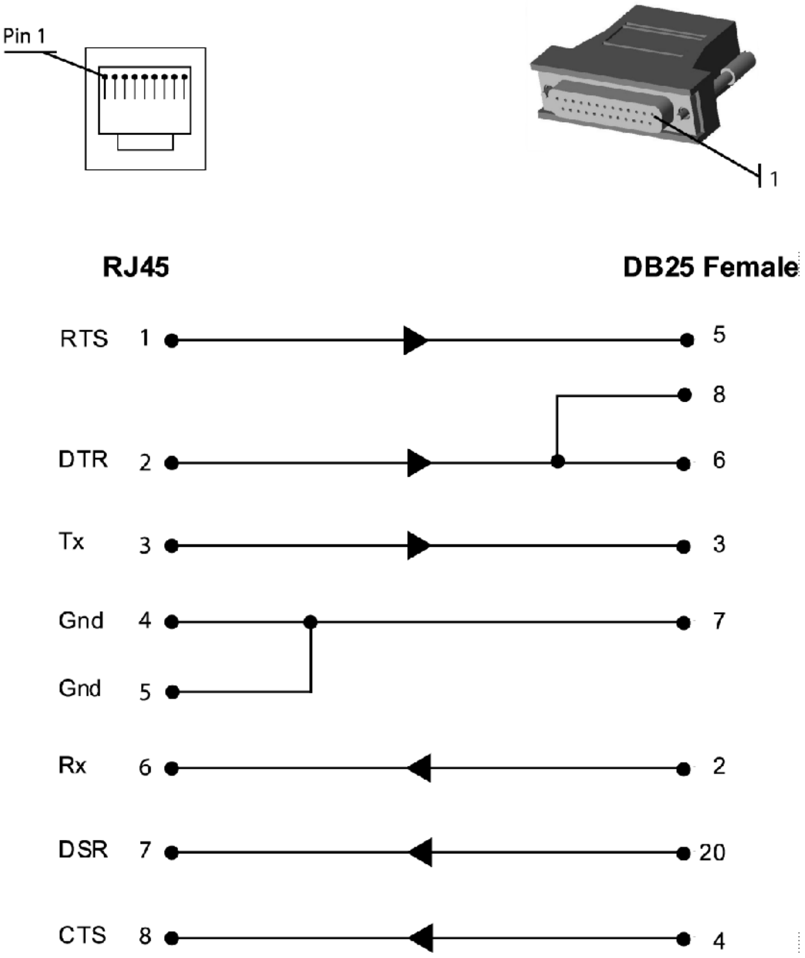


Figure E-3 RJ45 Receptacle to DB9M DCE Adapter for the SLC Console Manager (PN 200.2069A)

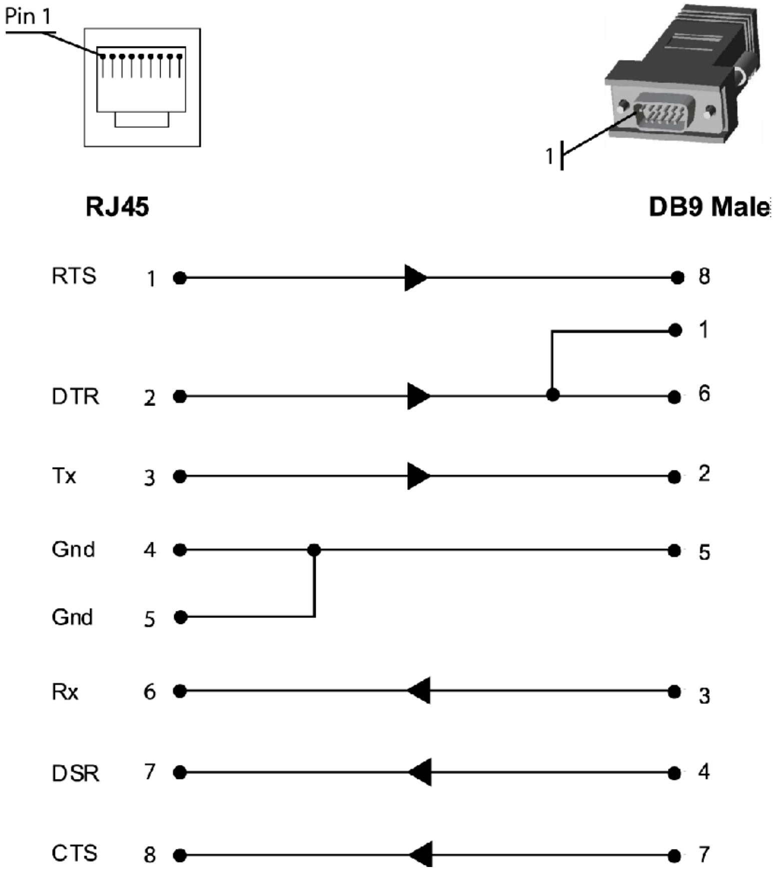
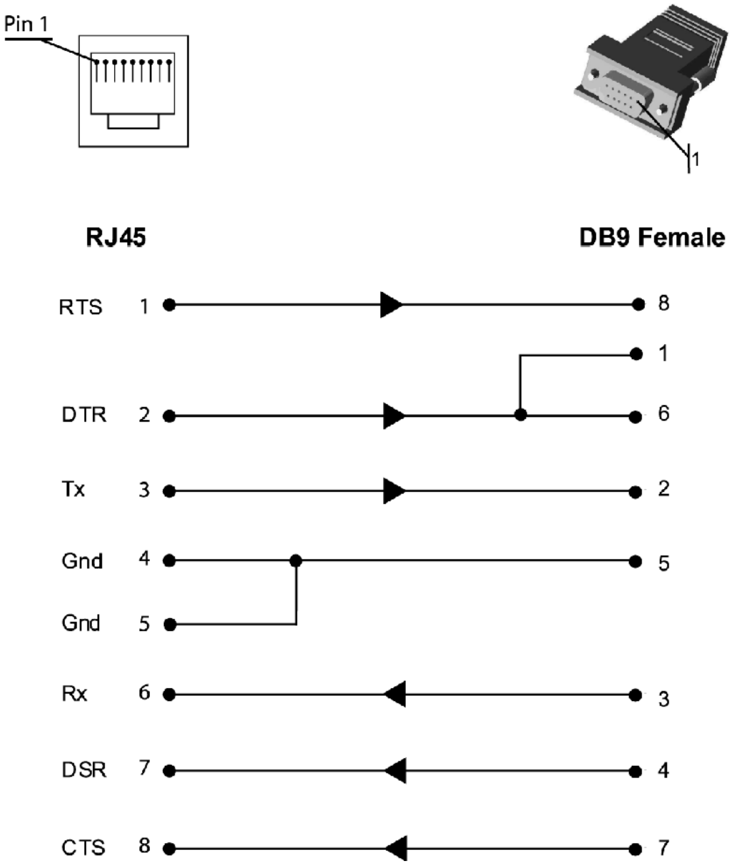
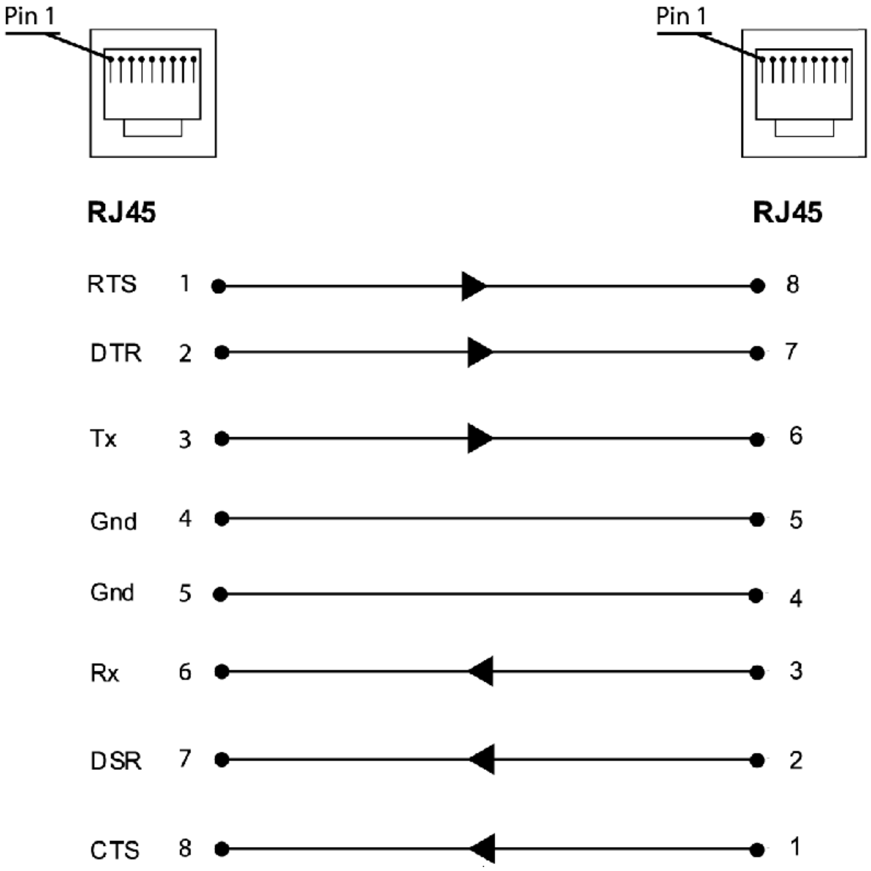


Figure E-4 RJ45 Receptacle to DB9F DCE Adapter for the SLC Console Manager (PN 200.2070A)



Use PN 200.2070A adapter with a PC serial port.

Figure E-5 RJ45 to RJ45 Adapter for Netra/Sun/Cisco and SLP (PNs 200.2225 and ADP010104-01)



Note: *The cable ends of the ADP010104-01 are an RJ45 socket on one end and a RJ45 plug on the other instead of RJ45 sockets on both ends.*

Use this adapter for SLP remote power manager, Netra/SUN/Cisco, and others.

Appendix F: Protocol Glossary

BOOTP (Bootstrap Protocol)

Similar to DHCP, but for smaller networks. Automatically assigns the IP address for a specific duration of time.

CHAP (Challenge Handshake Authentication Protocol)

A secure protocol for connecting to a system; it is more secure than the PAP.

DHCP (Dynamic Host Configuration Protocol)

Internet protocol for automating the configuration of computers that use TCP/IP.

DNS (Domain Name Servers)

A system that allows a network name server to translate text host names into numeric IP addresses.

Kerberos

A network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

LDAP (Lightweight Directory Access Protocol)

A protocol for accessing directory information.

Modem State Parameters

Dial-in—The SLC console manager waits for a peer to call the SLC unit to establish a text (command line) or PPP connection.

- For text connections, the user will be prompted for a login and password, and will be authenticated via the currently the currently enabled authentication methods (Local Users, NIS, LDAP, etc). Once authenticated, a CLI session will be initiated, and the user will remain connected to the SLC console manager until they either logout of the CLI session, or (if **Timeout Logins** is enabled) the CLI session is terminated if it has been idle.
- For PPP connections, the user will be authenticated via PAP or CHAP (configured with the **Authentication** setting). For PAP, the Local User list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the **CHAP Handshake Host/User Name** and **Secret/User Password** will be used to authenticate the login and password sent by the PPP peer. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting).

  Dial-out—The SLC console manager dials a remote peer to establish a PPP connection. The SLC device dials the **Dial-out Number**, and if the remote peer requests PAP or CHAP authentication, provides the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting).

Dial-back—The SLC console manager waits for a peer to call the SLC device, establishes a text (command line) or PPP connection, authenticates the user, and if the SLC console manager is able to determine a dial-back number to use, hangs up and calls the dial-back number to establish either a text or PPP connection.

- For text connections, the user will be prompted for a login and password, and will be authenticated via the currently the currently enabled authentication methods (Local Users, NIS, LDAP, etc). Once authenticated, the SLC device will use the **Dial-back Number** configured for the modem – either a fixed number assigned to the modem, or a number associated with the user that was authenticated (the user must have **Allow Dial-back** enabled and a **Dial-back Number** defined). If the SLC console manager can determine a dial-back number to use, it will hang up and wait **Dial-back Delay** seconds before initiating the dial-back. The SLC device will dial, prompt the user again for a login and password, and a CLI session will be initiated. The user will remain connected to the SLC console manager until they either logout of the CLI session, or (if **Timeout Logins** is enabled) the CLI session is terminated if it has been idle.

- For PPP connections, the user will be authenticated via PAP or CHAP (configured with the **Authentication** setting). For PAP, the Local User list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the **CHAP Handshake Host/User Name** and **Secret/User Password** will be used to authenticate the login and password sent by the PPP peer. Once authenticated, the SLC device will use the **Dial-back Number** configured for the modem – either a fixed number assigned to the modem, or a number associated with the user that was authenticated (the user must have **Allow Dial-back** enabled and a **Dial-back Number** defined). If the SLC console manager can determine a dial-back number to use, it will hang up and wait **Dial-back Delay** seconds before initiating the dial-back. The SLC device will dial, and if the remote peer requests PAP or CHAP authentication, provide the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting).

Dial-on-demand—The SLC console manager automatically dial outs and establishes a PPP connection when IP traffic destined for the peer needs to be sent. It will remain connected until no data packets have been sent to the peer for a specified amount of time. The modem cannot be configured for **Negotiate IP Address –** it must be configured with a **Local IP** and a **Remote IP** as the PPP connection will be established when it sees IP traffic destined for the **Remote IP**. When this occurs, the SLC device dials the **Dial-out Number**, and if the remote peer requests PAP or CHAP authentication, provides the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using the **Local IP** and the **Remote IP**. The PPP connection will stay active until no IP traffic for the **Remote IP** is sent for **Modem Timeout** seconds. Once the timeout has expired, the PPP connection will be terminated and will not be reestablished for at least **Restart Delay** seconds.

Dial-in and Dial-on-demand—A modem is configured to be in two modes: answering incoming calls to establish a PPP connection, and automatically dialing out to establish a PPP connection when IP traffic destined for the peer needs to be sent. When either event occurs (an incoming call or IP traffic destined for the peer), the other mode will be disabled. The modem cannot be configured for **Negotiate IP Address –** it must be configured with a **Local IP** and a **Remote IP** as the PPP connection will be established when it sees IP traffic destined for the **Remote IP**.

- For Dial-in, the user will be authenticated via PAP or CHAP (configured with the **Authentication** setting). For PAP, the Local User list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the **CHAP Handshake Host/User Name** and **Secret/User Password** will be used to authenticate the login and password sent by the PPP peer. Once authenticated, a PPP session will be established using the **Local IP** and the **Remote IP**.

- For Dial-on-Demand, the PPP connection will be established when it sees IP traffic destined for the **Remote IP**. When this occurs, the SLC console manager dials the **Dial-out Number**, and if the remote peer requests PAP or CHAP authentication, provides the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using the **Local IP** and the **Remote IP**. The PPP connection will stay active until no IP traffic for the **Remote IP** is sent for **Modem Timeout** seconds. Once the timeout has expired, the PPP connection will be terminated and will not be reestablished for at least **Restart Delay** seconds.

  Dial-in/Host List—The SLC device waits for a peer to call and establishes a text (command line) connection to the first host in a Host List that connects. A host list of a prioritized list of SSH, Telnet or raw TCP hosts to connect to. If **Authentication** is enabled for the Host List, the user will be prompted for a login and password, and will be authenticated via the currently enabled authentication methods (Local Users, NIS, LDAP, etc). Once authenticated, the SLC console manager will try to connect to each host in the host list until a successful connection is established.

  Callback Control Protocol (CBCP) Server and CBCP Client—CBCP is a PPP option that negotiates the use of callback where the server, after authenticating the client, terminates the connection and calls the client back at a phone number that is determined by the CBCP handshake. For more information on CBCP, see http://technet.microsoft.com/en-us/library/cc957979.aspx. CBCP is used primarily by Microsoft PPP peers. CBCP supports two options for determining the number to dial on callback: the client can specify a user-defined number for the server to dial on callback, or the client can request the server use an administrator-defined number to dial on callback. Optionally, some servers may also allow “no callback” as an option.

- **CBCP Server**—The SLC device waits for a client to call the SLC console manager, establishes a PPP connection, authenticates the user, and negotiates a dial-back number with the client using CBCP.   If the SLC device is able to determine a dial-back number to use, it hangs up and calls the dial-back number.

- When a call is received, a PPP connection is established, and the user will be authenticated via PAP or CHAP (configured with the **Authentication** setting). For PAP, the Local User list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the **CHAP Handshake Host/User Name** and **Secret/User Password** will be used to authenticate the login and password sent by the PPP peer. Once authenticated, the CBCP handshake with the client determines the number to use for dial-back. The SLC console manager will present the client with the available options: if the authenticated user is a Local User with **Allow Dial-back** enabled and a **Dial-back Number** defined, the administrator-defined option is allowed; if this is not the case, the user-defined number is allowed.

- Additionally, if **CBCP Server Allow No Callback** is enabled, the client can also select no callback (the PPP connection established at dial-in will remain up). The client will select from the available callback options.   If the SLC device can determine a dial-back number to use, it will hang up and wait **Dial-back Delay** seconds before initiating the dial-back. The SLC console manager will dial, and if the remote peer requests PAP or CHAP authentication, provide the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting).

- **CBCP Client**—The SLC device will dial out to a CBCP server, establish a PPP connection, negotiate a callback number with the server using CBCP, terminate the connection, and wait for the server to call back. The SLC console manager dials the **Dial-out Number**, and if the remote peer requests PAP or CHAP authentication, provides the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, the CBCP handshake with the server determines the number to use for dial-back.

- The SLC device will request the type of number defined by **CBCP Client Type** - either an Admin-defined Number (the CBCP server determines the number to call) or a User-defined Number (the SLC console manager will provide the **Fixed Dial-back Number** as the number to call). If the CBCP handshake is successful, the SLC device will terminate the PPP connection, hang up, and wait for the server to dial back. When the server dials and the PPP connection is established, the user will be authenticated via PAP or CHAP (configured with the **Authentication** setting).
- For PAP, the Local User list will be used to authenticate the login and password sent by the PPP peer.
- For CHAP, the **CHAP Handshake Host/User Name** and **Secret/User Password** will be used to authenticate the login and password sent by the PPP peer. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting).

Notes:

- In a state where the modem will be answering a call, the modem should always be configured for manual answer, not auto answer.
- When answering a call, the SLC console manager answers after the 2nd ring.
- Any text or PPP connection can be terminated by setting the modem state to disabled.

NAT (Network Address Translation)

An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This enables a company to shield internal addresses from the public Internet.

NFS (Network File System)

A protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer. You can use NFS to mount all or a portion of a file system. Users can access the portion mounted with the same privileges as the user's access to each file.

NIS (Network Information System)

System developed by Sun Microsystems for distributing system data such as user and host names among computers on a network.

NMS (Network Management System)

NMS acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP.

NTP (Network Time Protocol)

A protocol used to synchronize time on networked computers and equipment.

PAP (Password Authentication Protocol)

A method of user authentication in which the username and password are transmitted over a network and compared to a table of name-password pairs.

PPP (Point-to-Point Protocol)

A protocol for creating and running IP and other network protocols over a serial link.

RADIUS (Remote Authentication Dial-In User Service)

An authentication and accounting protocol. Enables remote access servers to communicate with a central server to authenticate dial-in users and their access permissions. A company stores user profiles in a central database that all remote servers can share.

SMB/CIFS

(Server Message Block/Common Internet File System): Microsoft's protocol for allowing all applications as well as Web browsers to share files across the Internet. CIFS runs on TCP/IP and uses the SMB protocol in Microsoft Windows for accessing files. With CIFS, users with different platforms and computers can share files without having to install new software.

SNMP (Simple Network Management Protocol)

A protocol that system administrators use to monitor networks and connected devices and to respond to queries from other network hosts.

SMTP (Simple Mail Transfer Protocol)

TCP/IP protocol for sending email between servers.

SSL (Secure Sockets Layer)

A protocol that provides authentication and encryption services between a web server and a web browser.

SSH (Secure Shell)

A secure transport protocol based on public-key cryptography.

TACACS+ (Terminal Access Controller Access Control System)

A method of authentication used in UNIX networks. It allows a remote access server to communicate with an authentication server to determine whether the user has access to the network.

Telnet

A terminal protocol that provides an easy-to-use method of creating terminal connections to a network host.

Appendix G: Compliance Information

The following information specifies compliance information in accordance with ISO/IEC Guide 22 and EN 45014).

Manufacturer Name and Address

Lantronix Inc., 167 Technology, Irvine, CA 92618 USA

Declares that the following product:

Product Names: Models SLC8, SLC16, SLC32, and SLC48 Console Managers

Conform to the following standards or other normative documents:

Safety: EN60950:1992+A1, A2, A3, A4, A11

Electromagnetic Emissions

EN55022: 1994 (IEC/CSPIR22: 1993)

FCC Part 15, Subpart B, Class B

IEC 1000-3-2/A14: 2000

IEC 1000-3-3: 1994

Electromagnetic Immunity

EN55024: 1998 Information Technology Equipment-Immunity Characteristics

IEC61000-4-2: 1995 Electro-Static Discharge Test

IEC61000-4-3: 1996 Radiated Immunity Field Test

IEC61000-4-4: 1995 Electrical Fast Transient Test

IEC61000-4-5: 1995 Power Supply Surge Test

IEC61000-4-6: 1996 Conducted Immunity Test

IEC61000-4-8: 1993 Magnetic Field Test

IEC61000-4-11: 1994 Voltage Dips & Interrupts Test

Supplementary Information

This Class A digital apparatus complies with Canadian ICES-003 (CSA) and has been verified as being compliant within the Class A limits of the FCC Radio Frequency Device Rules (FCC Title 47, Part 15, Subpart B CLASS A), measured to CISPR 22: 1993 limits and methods of measurement of Radio Disturbance Characteristics of Information Technology Equipment. The product complies with the requirements of the Low Voltage Directive 72/23/EEC and the EMC Directive 89/336/EEC.

Additional Agency Approvals and Certifications

VCCI

TUV

GS Mark

UL/CUL

C-Tick

CB Scheme

NIST-certified implementation of AES as specified by FIPS 197

This product carries the CE mark since it has been tested and found compliant with the following standards:

Safety:EN 60950

Emissions:EN 55022 Class A

Immunity:EN 55024

RoHS Notice

All Lantronix products in are China RoHS-compliant and free of the following hazardous substances and elements:

- Lead (Pb)
- Mercury (Hg)
- Cadmium (Cd)
- Hexavalent Chromium (Cr (VI))
- Polybrominated biphenyls (PBB)
- Polybrominated diphenyl ethers (PBDE)

Table G-1 Lantronix Product Family Names and Toxic/Hazardous Substances and Elements

Product Family Name	Toxic or hazardous Substances and Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr (VI))	Polybrominated biphenyls (PBB)	Polybrominated diphenyl ethers (PBDE)
UDS1100 and 2100	0	0	0	0	0	0
EDS	0	0	0	0	0	0
MSS100	0	0	0	0	0	0
IntelliBox	0	0	0	0	0	0
XPress DR and XPress-DR+	0	0	0	0	0	0
SecureBox 1101 and 2101	0	0	0	0	0	0
WiBox	0	0	0	0	0	0
UBox	0	0	0	0	0	0
MatchPort	0	0	0	0	0	0
SLC	0	0	0	0	0	0
XPort	0	0	0	0	0	0
WiPort	0	0	0	0	0	0
SLB	0	0	0	0	0	0
SLP	0	0	0	0	0	0
SCS	0	0	0	0	0	0
SLS	0	0	0	0	0	0
DSC	0	0	0	0	0	0

0: Toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

x: Toxic or hazardous substance contained in at least one of the homogeneous materials used for this part is above the limit requirement in SJ/T11363-2006.

Manufacturer Contact

Lantronix, Inc.

167 Technology, Irvine, CA 92618 USA

Phone: 949-453-3990

Fax: 949-453-3995

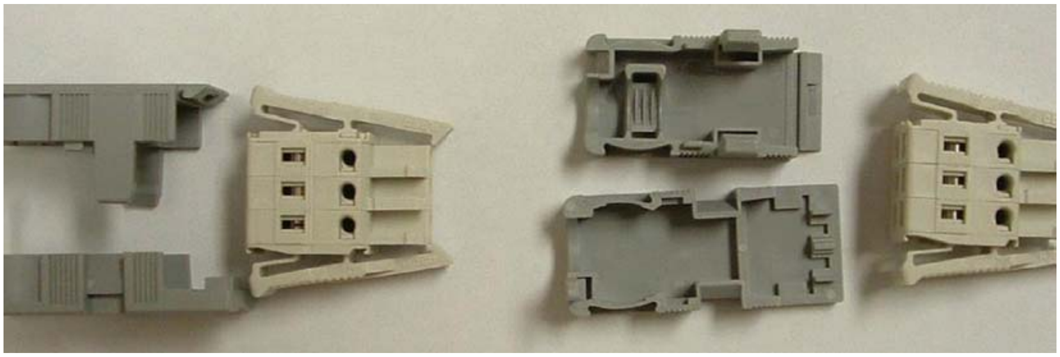
Appendix H: DC Connector Instructions

The -48VDC plug connector is provided to make the input power connectors for your console server. The -48VDC input source should be circuit breaker or fuse protected at 5 amps.

- Input Voltage: -48VDC (acceptable range of -40 to -60 VDC)
- Max. Operating Current: 1.5 amps
- Max. Input Surge Current: 5 amps
- Continuous Power: 100 watts required
- Electrically isolated from any source
- Connected to reliable Earth ground

The connector kit contains 6 pieces that make 2 complete -48VDC connectors as shown in *Figure H-1*.

Figure H-1 Connector Kit Contents

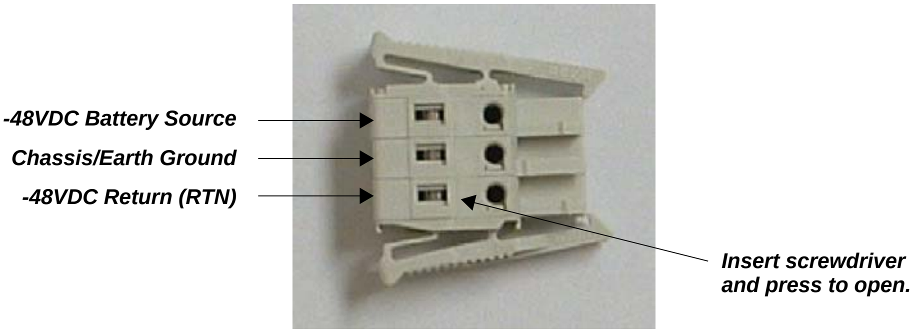


Caution: ***Ensure that the SLC power source is turned off while assembling the connector head.***

To assemble the DC plug connectors:

1. Use 16AWG copper wire to make the connections shown in *Figure H-2*.

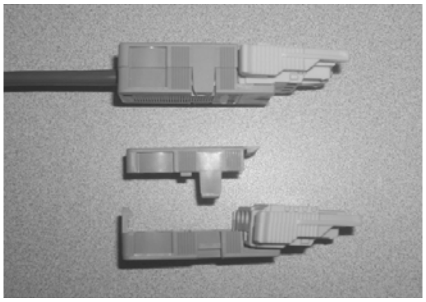
Figure H-2 Wire Connections



2. Strip a suitable amount of wire (~3/8”) from each lead to be inserted into each connector position.

3. Using a small screwdriver, press the slot to release the spring pressure for each conductor (as shown in *Figure H-2*) and insert the wire. When the wire is in position, release the pressure on the screwdriver to securely capture the wire.
4. After the leads are installed as shown in *Figure H-2*, assemble the strain relief (2 gray pieces) to the connector plug and snap the connector together as shown in *Figure H-3*.

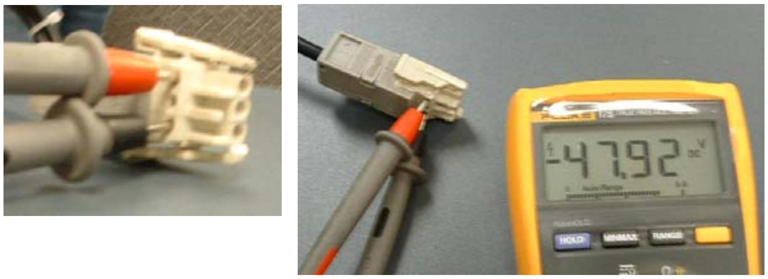
Figure H-3 Plug Parts to Assemble



Caution: ***Verify wiring before connecting to the SLC console manager. If the polarity is reversed, you can damage the SLC internal power supply.***

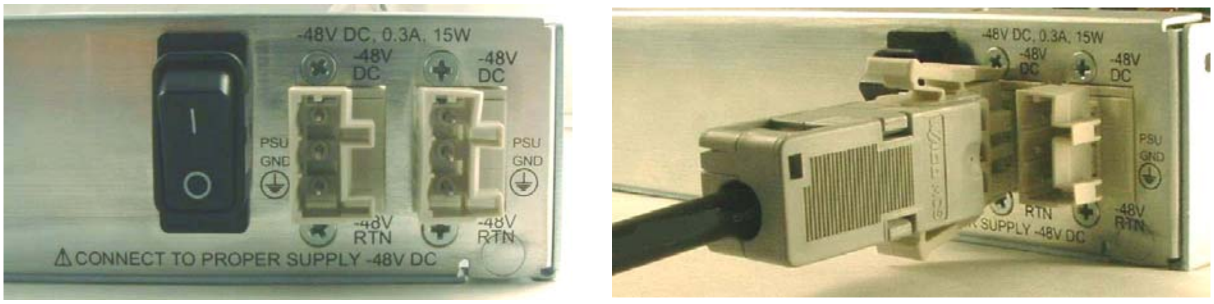
5. Connect a Digital Volt/OHM (DVOM) meter to the power source leads and verify the (-48 VDC) power source.
   a. Insert the **RED** (+) lead of the DVOM into the top hole of the connector for the source power lead.
   b. Then insert the **BLACK** (–) lead of the DVOM into the bottom hole of the connector for the return power lead as shown in *Figure H-4*.

Figure H-4 Verification of the Power Source



   c. Turn on your power source, the voltage should read (-48.00 VDC ±.5 VDC) as shown in the DVOM in *Figure H-4*.
6. With power source off and SLC power switch off, perform the following steps:
   a. Connect the DC power cords to your SLC console server as shown in *Figure H-5*.

Figure H-5 DC Power Cord into the SLC Console Manager



b. Turn on your -48VDC power source.

c. Turn on the power switch of the SLC console server.

7. Follow the setup instructions in your SLC manual to use your product.

Appendix I: LDAP Schemas

This appendix describes the procedure for defining individual user permissions from a Windows Active Directory (AD) server to use with the SLC console manager firmware version 5.4 or greater.

The procedure outlined in this appendix is based on Windows Server 2003 and 2008 and can vary with other Windows versions.

Note: *In this appendix, the terms “rights and permissions” are used interchangeably.*

This appendix contains the following sections:

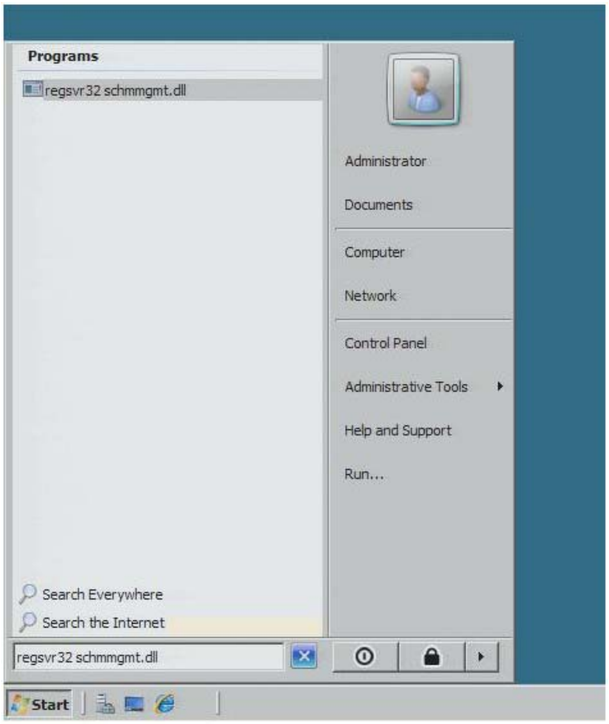
Installing Schema Support in Window AD Server

To install schema support in a Windows AD server for the SLC console manager, follow the steps contained in the document at http://technet.microsoft.com/en-us/library/cc731628.aspx.

Or perform the following steps that were copied from the website above.

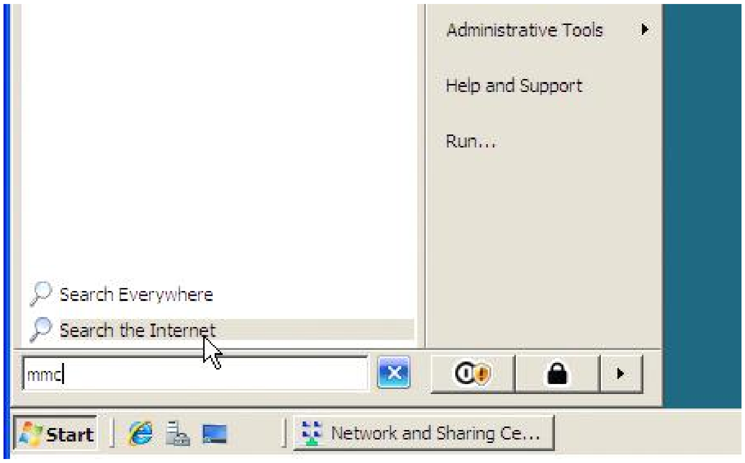
1. Open a command prompt and type **regsvr32 schmmgmt.dll**.
2. Press Enter. *Figure I-1* shows the window that displays.

Figure I-1 Programs Window



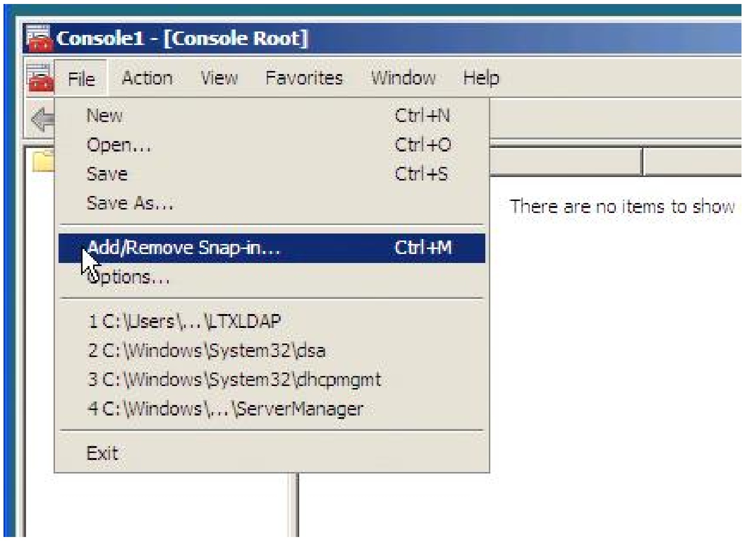
3. Click Start > Run > mmc.
4. Click OK. *Figure I-2* shows the window that displays.

Figure I-2 MMC Window



5. On the **File** menu, click Add/Remove Snap-in. *Figure I-3* shows the window that displays.

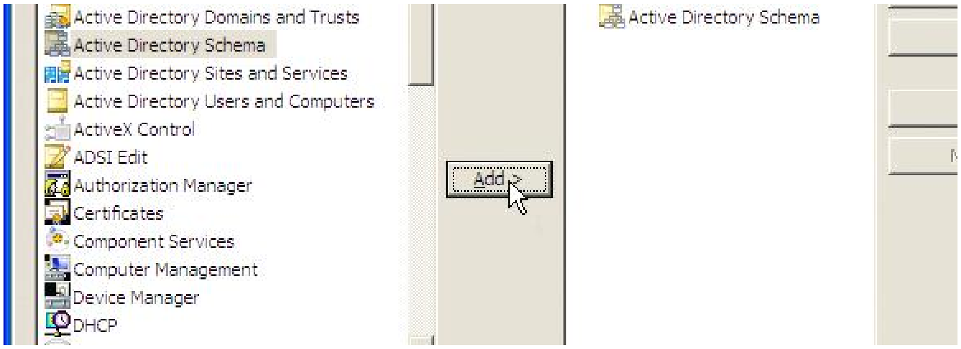
Figure I-3 Snap-In Window



Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Users\...\LTXLDAP
2 C:\Windows\System32\dsa
3 C:\Windows\System32\dhcpmgmt
4 C:\Windows\...\ServerManager
Exit
There are no items to show

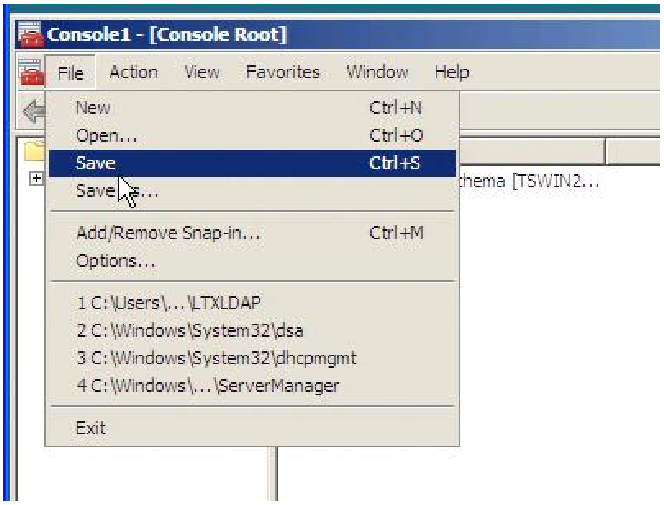
6. Under Available snap-ins, click Active Directory Schema > Add > OK. *Figure I-4* shows the directory that displays.

Figure I-4 Active Directory Schema



7. To save this console, click Save on the **File** menu. *Figure I-5* shows the window that displays.

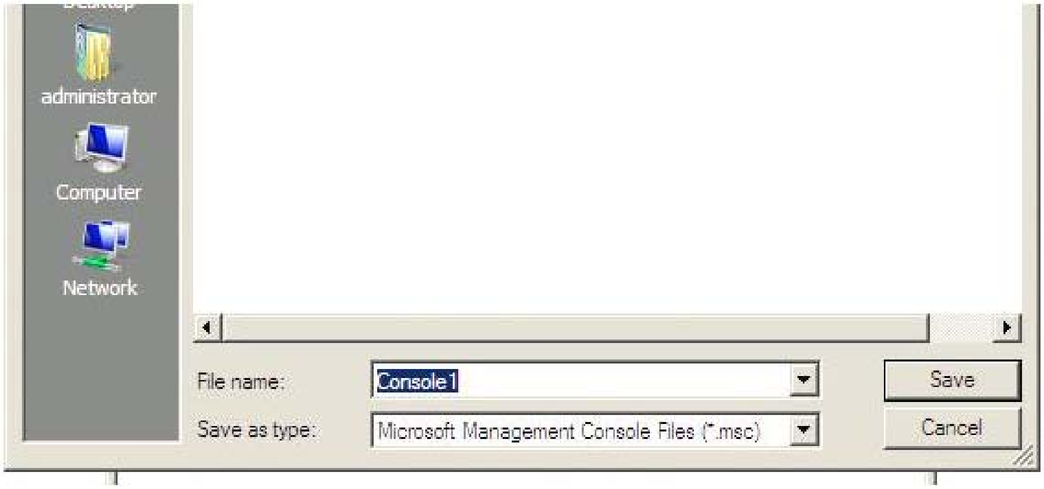
Figure I-5 Console Root


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Users\...\LTXLDAP
2 C:\Windows\System32\dsa
3 C:\Windows\System32\dhcpmgmt
4 C:\Windows\...\ServerManager
Exit
hema [TSWIN2...

8. In the Save As dialog box, do one of the following:

   a. To place the snap-in in the Administrative Tools folder, in File name box, type a name for the snap-in, and then click Save. *Figure I-6* shows the folder that displays.

Figure I-6 Administrative Tools Folder

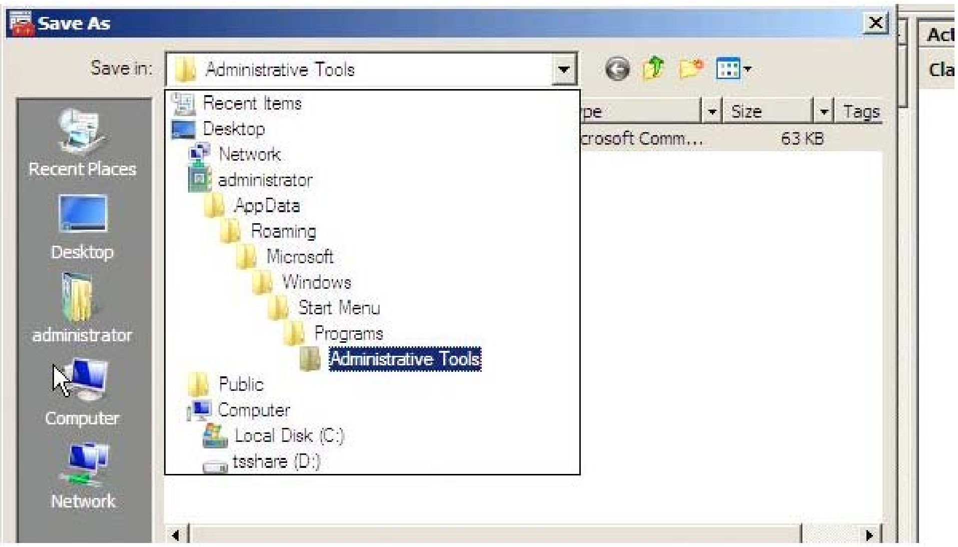


File name: Console1

Save as type: Microsoft Management Console Files (*.msc)

   b. Or, to save the snap-in to a location other than the Administrative Tools folder, in Save in, navigate to a location for the snap-in. In File name, type a name for the snap-in, and then click Save. *Figure I-7* shows the directory that displays.

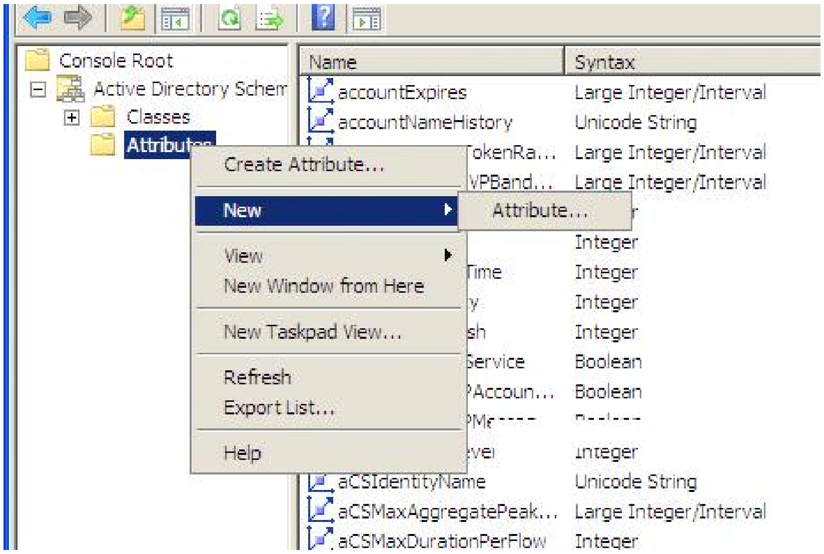
Figure I-7 Save As Window



Creating the SLC Schema Attribute

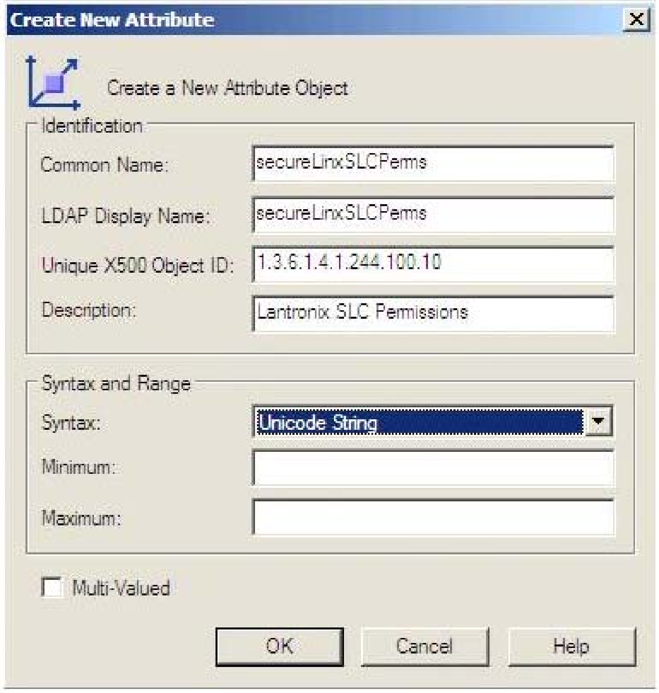
1. Once you have a saved Schema console, open it and right click on Attributes.
2. Mouse over New and left click on Attribute. *Figure I-8* shows the window that displays.

Figure I-8 New Attribute Window



3. Click Continue on the Warning screen.
4. For both the Common Name and LDAP Display Name, use **secureLinxSLCPerms** in exactly that form (case included). *Figure I-9* shows the window that displays.

Figure I-9 Create New Attribute Object Window



Create New Attribute

Create a New Attribute Object

Identification

Common Name: secureLinxSLCPerms

LDAP Display Name: secureLinxSLCPerms

Unique X500 Object ID: 1.3.6.1.4.1.244.100.10

Description: Lantronix SLC Permissions

Syntax and Range

Syntax: Unicode String

Minimum:

Maximum:

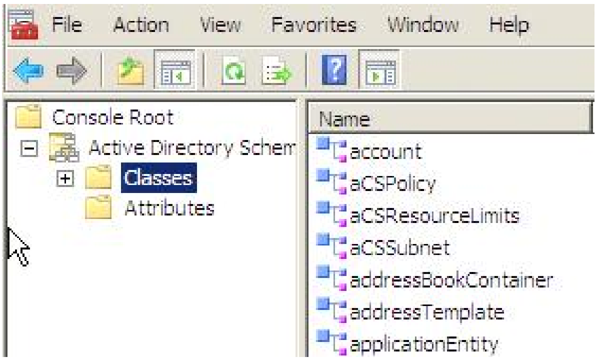
□ Multi-Valued

5. For the OID, enter **1.3.6.1.4.1.244.100.10**.
6. Enter anything for the description.
7. Change the Syntax: pull-down menu to Unicode String.
8. Click on OK.

Adding the Attribute to the Users Group in Windows

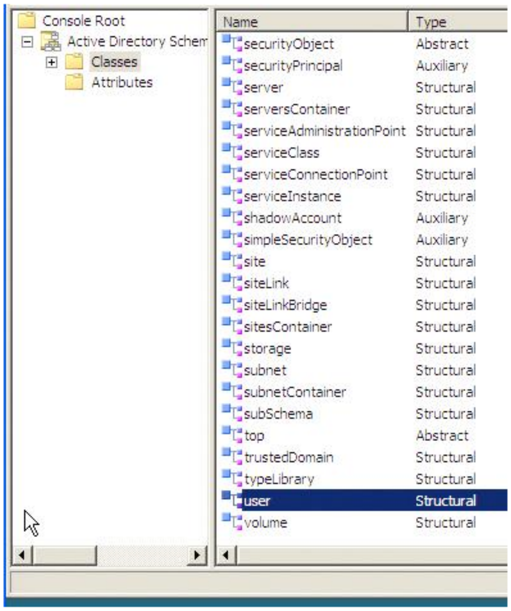
1. Highlight the Classes folder in the console tree on the left. *Figure I-10* shows the files that display.

Figure I-10 Classes Folder



2. In the right pane, scroll down to user. *Figure I-11* shows the window that displays.

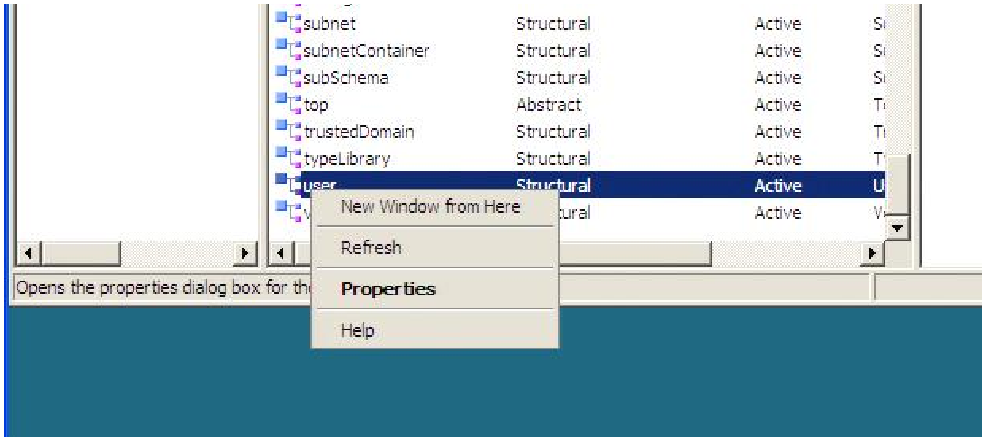
Figure I-11 User Class Window



Name	Type
securityObject	Abstract
securityPrincipal	Auxiliary
server	Structural
serversContainer	Structural
serviceAdministrationPoint	Structural
serviceClass	Structural
serviceConnectionPoint	Structural
serviceInstance	Structural
shadowAccount	Auxiliary
simpleSecurityObject	Auxiliary
site	Structural
siteLink	Structural
siteLinkBridge	Structural
sitesContainer	Structural
storage	Structural
subnet	Structural
subnetContainer	Structural
subSchema	Structural
top	Abstract
trustedDomain	Structural
typeLibrary	Structural
user	Structural
volume	Structural

3. Right click on user and left click on Properties. *Figure I-12* shows the window that displays.

Figure I-12 Class User Properties Window

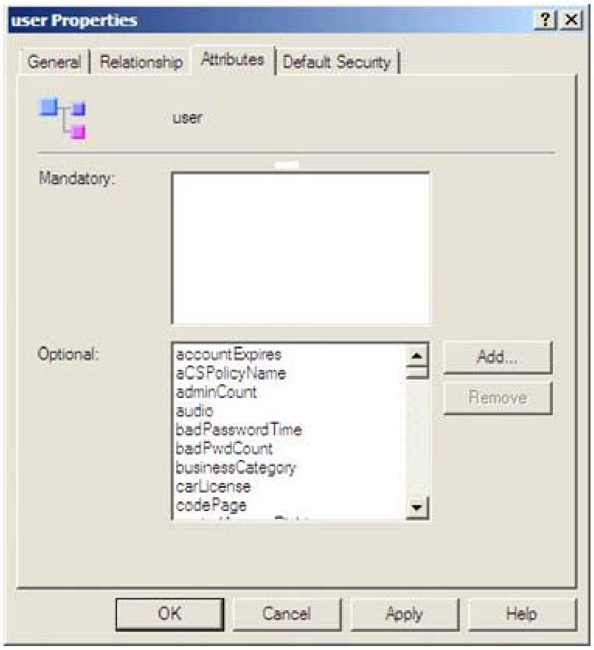


subnet	Structural	Active	S
subnetContainer	Structural	Active	S
subSchema	Structural	Active	S
top	Abstract	Active	T
trustedDomain	Structural	Active	T
typeLibrary	Structural	Active	T
user	Structural	Active	U
v	tural	Active	V

Opens the properties dialog box for th

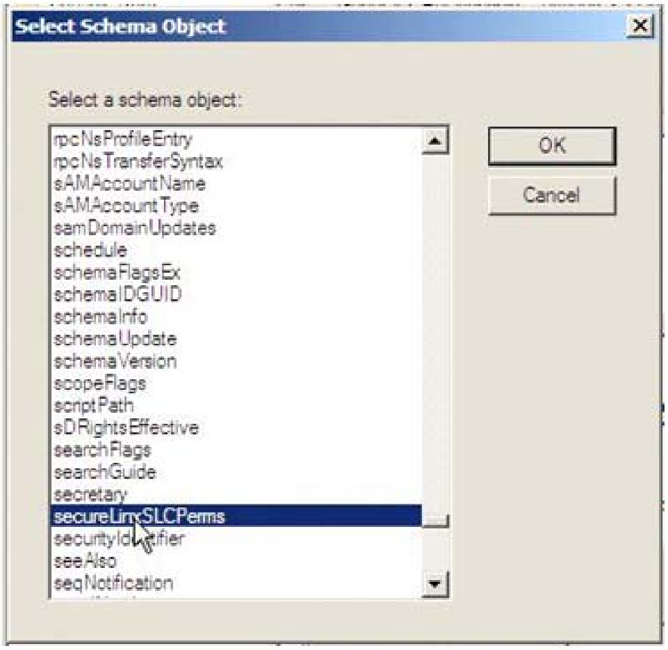
4. Under the Attributes tab, click on Add. *Figure I-13* shows the window that displays.

Figure I-13 User Properties Window



5. Find the **secureLinxSLCPerms** attribute, highlight it, and click on OK.

Figure I-14 Select Schema Object Window

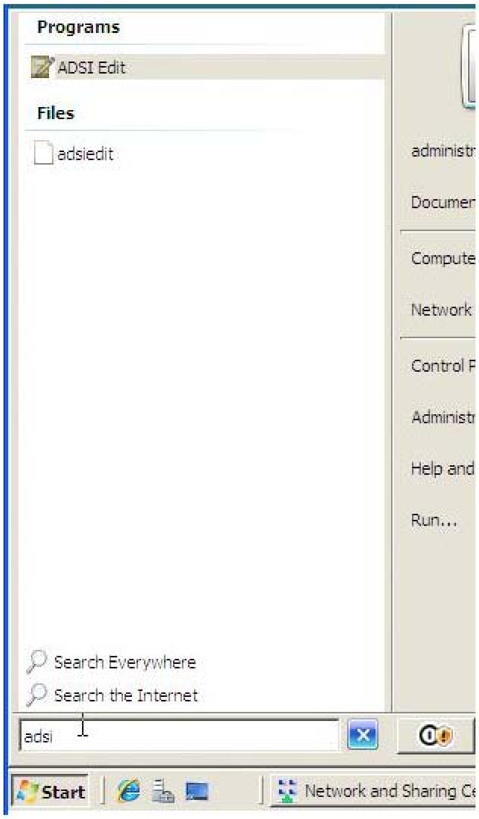


6. Click on OK on the window underneath.
7. Click on File and click on Save.
8. Exit out of MMC.

Adding the Permissions to the Individual User

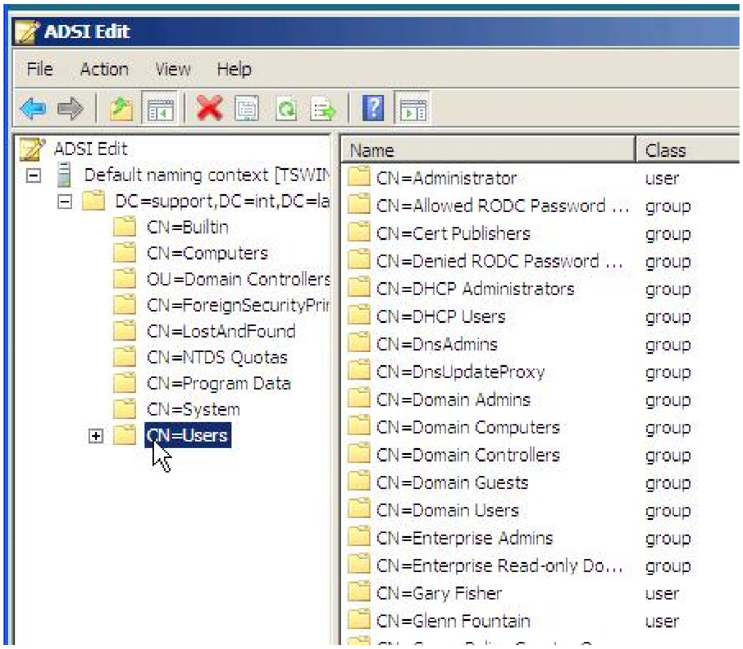
1. Open ADSI Edit (if you start typing adsi in the search line in Windows, it should find it). *Figure I-15* shows the window that displays.

Figure I-15 ADSI Edit Window



2. Expand the console tree until you get to the listing of users. *Figure I-16* shows the folder that displays.

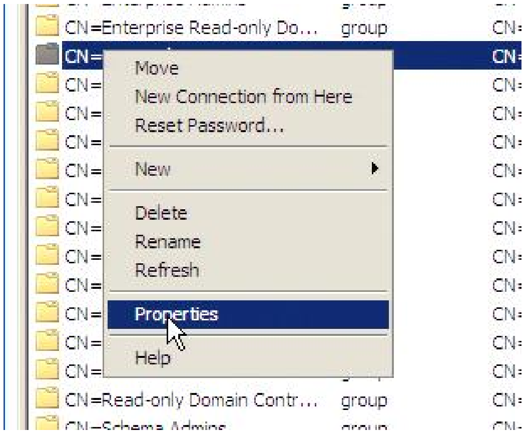
Figure I-16 ADSI Edit Window, CN=Users Folder



Name	Class
CN=Administrator	user
CN=Allowed RODC Password ...	group
CN=Cert Publishers	group
CN=Denied RODC Password ...	group
CN=DHCP Administrators	group
CN=DHCP Users	group
CN=DnsAdmins	group
CN=DnsUpdateProxy	group
CN=Domain Admins	group
CN=Domain Computers	group
CN=Domain Controllers	group
CN=Domain Guests	group
CN=Domain Users	group
CN=Enterprise Admins	group
CN=Enterprise Read-only Do...	group
CN=Gary Fisher	user
CN=Glenn Fountain	user

3. Right click on the user for whom you wish to configure permissions and left click on Properties. *Figure I-17* shows the Properties Window.

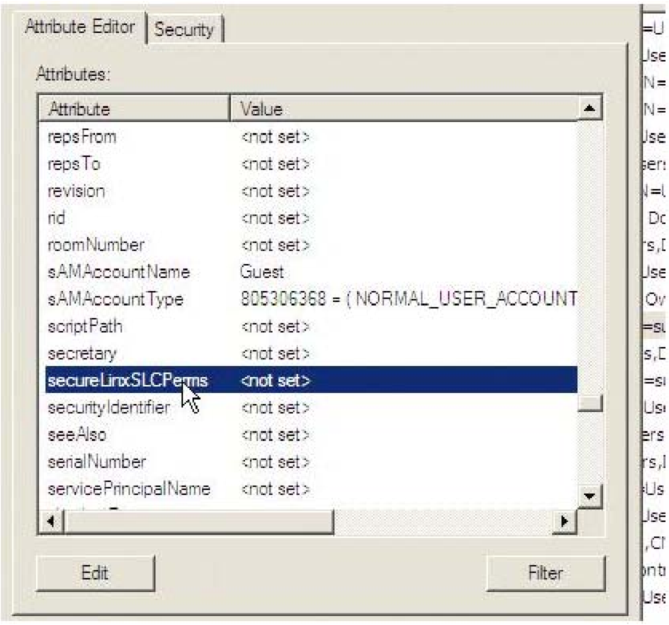
Figure I-17 Properties Window



4. Under the Attribute Editor tab, scroll down to **secureLinxSLCPerms**.

5. Highlight it and click on the Edit button. *Figure I-18* shows the window that displays.

Figure I-18 Attribute Editor Window



Attribute	Value
repsFrom	<not set>
repsTo	<not set>
revision	<not set>
rid	<not set>
roomNumber	<not set>
sAMAccountName	Guest
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
scriptPath	<not set>
secretary	<not set>
secureLinxSLCPerms	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	<not set>

Values to Use

The values that you can use in the **Value:** field that specify the user permissions are as follows:

- **rights**
- **data**
- **listen**
- **clear**
- **outlet** (for the Lantronix SLB™ branch office manager)
- **group**
- **escseq**
- **brkseq**
- **menu**

For **rights**, you can enable the following:

- **fa**: Full Administrative
- **nt**: Networking
- **sv**: Services
- **lu**: Local Users
- **ra**: Remote Authentication
- **dt**: Date/Time
- **sk**: SSH Keys

- **um**: User Menus
- **dp**: Device Ports Configuration
- **do**: Device Ports Operations
- **pc**: PC Cards
- **rs**: Reboot/Shutdown
- **fc**: Firmware/Configuration
- **dr**: Diagnostic Reports
- **sn**: Secure Lantronix Network
- **wb**: Web Access

For **data**, **listen**, and **clear**, you specify ports. Contiguous ports with a dash, non-contiguous with a comma, U1 for the USB port, or U and L for the upper and lower PC Card slots (1-5,8,11,U,L).

For **group**, the options are **admin**, **power**, and **default**.

For **escseq** and **brkseq**, you would specify what key sequence would escape you from a console session and send a break out the current session port, respectively. The default for each is "\x1bA" (esc-A) and "\x1bB" (esc-B), respectively. The \x in the default strings denotes that the next two characters are HEX. With the default, the \x is followed by 1b which equates to ESCAPE.

For **menu**, specify the name of a user menu configured on the SLC console manager that you would like to be displayed when that user logs in.

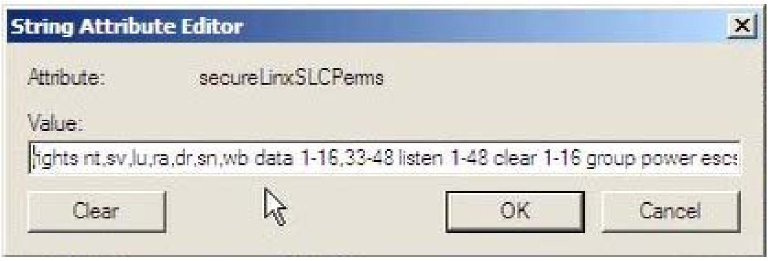
String Format

The string format is the parameter name, followed by a space, followed by the value or values of the parameters. Multiple values for a parameter would be connected with a comma (no spaces in between) or a dash in the case of device ports that are contiguous.

Example: **rights nt,sv,lu,ra,dr,sn,wb data 1-16,33-48 listen 1-48 clear 1-16 group power escseq \x1bE brkseq \x1bZ menu bob**

Enter the string, click **OK** and OK in the next window. *Figure I-19* shows the window that displays.

Figure I-19 String Attribute Editor Window



String Attribute Editor

Attribute: secureLinxSLCPerms

Value:

rights nt,sv,lu,ra,dr,sn,wb data 1-16,33-48 listen 1-48 clear 1-16 group power esc