Copyright and Trademark

© 2014 Lantronix, Inc. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries. SLC, SLB, SLP, SLM, Detector and Spider are trademarks of Lantronix, Inc.

Windows and Internet Explorer are registered trademarks of Microsoft Corporation. Firefox is a registered trademark of the Mozilla Foundation. Chrome is a trademark of Google, Inc. All other trademarks and trade names are the property of their respective holders.

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 may be 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.

All information contained herein is provided “AS IS.” Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all
warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitable or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user’s access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

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 cause 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

<table>
<thead>
<tr>
<th>Date</th>
<th>Rev.</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2006</td>
<td>A</td>
<td>Initial Release</td>
</tr>
<tr>
<td>August 2006</td>
<td>B</td>
<td>Added event configuration, local/remote user authentication precedence,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>firmware update via HTTPS, complex passwords, and port permissions for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>remote users.</td>
</tr>
<tr>
<td>January 2007</td>
<td>C</td>
<td>Added dial-in &amp; dial-on-demand modem state, IP filters, active directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to LDAP section, and additional TACACS+ servers.</td>
</tr>
<tr>
<td>April 2007</td>
<td>D</td>
<td>Added ability to import site-specific SSL certificates and SSH host keys,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to display a list of web sessions, to set an IP filter timer, and to save</td>
</tr>
<tr>
<td></td>
<td></td>
<td>system logs across reboots. Enabled dual boot-up.</td>
</tr>
<tr>
<td>August 2007</td>
<td>E</td>
<td>Added gateway page, phone home; alarm delay; SSH v1 logins; trap</td>
</tr>
<tr>
<td></td>
<td></td>
<td>community; configuration manage option; system logs beginning and end</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dates, device port logging to syslog.</td>
</tr>
<tr>
<td>April 2008</td>
<td>F</td>
<td>New web page design with tabbed menus.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added support for the following: Sensorsoft devices; SecureID over Radius;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>command and status of the SLP expansion chassis; escape and break</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sequences for remote users; password aging, iGoogle Gadget; SNMP v3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>encryption; ability to copy boot bank; host lists for outgoing modem and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>direct connection at the CLI; new option for local users to display a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>custom menu at login.</td>
</tr>
<tr>
<td>Date</td>
<td>Rev.</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------</td>
<td>------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>January 2010</td>
<td>G</td>
<td>Added support for Interface and Batch Scripting, Ethernet Bonding, configurable LCD screens and scrolling, redesigned SLC Network web page, Email Log, Firmware Update via PC Card and NFS, SLC Temperature, and PPP dialback (including CallBack Control Protocol).</td>
</tr>
<tr>
<td>March 2010</td>
<td>H</td>
<td>Updated for USB support that was added in firmware 5.5.</td>
</tr>
<tr>
<td>November 2013</td>
<td>I</td>
<td>Updated product name and trademark information.</td>
</tr>
<tr>
<td>July 2014</td>
<td>J</td>
<td>Updated to firmware release 6.1.0.0.</td>
</tr>
</tbody>
</table>
## Table of Contents

Copyright and Trademark ........................................................................................................... 2  
Warranty ....................................................................................................................................... 2  
Open Source Software .................................................................................................................. 2  
Contacts ....................................................................................................................................... 2  
Disclaimer and Revisions .............................................................................................................. 2  
Revision History ............................................................................................................................ 3  
List of Figures ............................................................................................................................... 14  
List of Tables ................................................................................................................................. 18

1: About This Guide ..................................................................................................................... 19  
  Chapter Summaries .................................................................................................................... 19  
  Conventions ............................................................................................................................... 21  
  Additional Documentation ......................................................................................................... 21

2: Overview .................................................................................................................................. 22  
  SLC Models and Part Numbers ................................................................................................. 22  
  System Features ....................................................................................................................... 24  
    Protocols Supported .............................................................................................................. 25  
    Access Control .................................................................................................................... 25  
    Device Port Buffer ............................................................................................................... 25  
    Configuration Options ......................................................................................................... 25  
  Hardware Features ................................................................................................................... 26  
    Serial Connections ............................................................................................................... 26  
    Network Connections ......................................................................................................... 27  
    PC Card Interface ............................................................................................................... 27  
    USB Port .............................................................................................................................. 28

3: Installation ............................................................................................................................... 29  
  What's in the Box ....................................................................................................................... 29  
    Product Information Label ................................................................................................... 30  
  Technical Specifications .......................................................................................................... 30  
  Physical Installation .................................................................................................................. 31  
    Connecting to Device Ports ................................................................................................. 31  
    Connecting to Network Ports ............................................................................................... 32  
    Connecting to Terminals ....................................................................................................... 32  
    Power ..................................................................................................................................... 32
4: Quick Setup

Recommendations
IP Address
Method #1 Using the Front Panel Display
Front Panel LCD Display and Keypads
Navigating
Entering the Settings
Restoring Factory Defaults
Method #2 Quick Setup on the Web Page
Network Settings
Date & Time Settings
Administrator Settings
Method #3 Quick Setup on the Command Line Interface
Next Step

5: Web and Command Line Interfaces

Web Interface
Logging In
Logging Out
Web Page Help
Command Line Interface
Logging In
Logging Out
Command Syntax
Command Line Help
Tips
General CLI Commands

6: Basic Parameters

Requirements
Eth1 and Eth2 Settings
Gateway
Hostname & Name Servers
DNS Servers
DHCP-Acquired DNS Servers
GPRS-Acquired DNS Servers
TCP Keepalive Parameters
Ethernet Counters
Network Commands
IP Filter
Viewing IP Filters
Enabling IP Filters
Configuring IP Filters ................................................................. 59
Rule Parameters ...................................................................... 60
Updating an IP Filter .............................................................. 62
Deleting an IP Filter ............................................................... 62
Mapping a Ruleset ................................................................. 62
IP Filter Commands ............................................................... 62
Routing ................................................................................. 63
  Dynamic Routing ................................................................ 64
  Static Routing .................................................................... 64
  Equivalent Routing Commands ........................................... 64
VPN ..................................................................................... 65

7: Services .............................................................................. 68
System Logging and Other Services ..................................... 68
SSH/Telnet/Logging .............................................................. 68
  System Logging .................................................................. 69
  Audit Log ......................................................................... 70
  SMTP .............................................................................. 70
  SSH ............................................................................... 70
  Telnet ............................................................................. 71
  Web SSH/Web Telnet Settings .......................................... 71
  Phone Home ..................................................................... 71
SNMP .................................................................................... 72
  Communities .................................................................... 73
  Version 3 .......................................................................... 73
  V3 Read-Only User .......................................................... 74
  V3 Read-Write User .......................................................... 74
  SNMP, SSH, Telnet, and Logging Commands .................. 74
NFS and SMB/CIFS ................................................................. 75
  SMB/CIFS Share .............................................................. 76
  NFS and SMB/CIFS Commands ....................................... 77
Secure Lantronix Network ...................................................... 78
  Secure Lantronix Network Commands ............................. 80
Date and Time ........................................................................ 81
  Date and Time Commands ................................................ 82
Web Server ............................................................................. 83
  Admin Web Commands .................................................... 84
  Services - Web Sessions ................................................... 85
  Services - SSL Certificate ............................................... 86
  Web Server Commands ..................................................... 88
iGoogle Gadgets ................................................................. 88
## 8: Device Ports

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Methods</td>
<td>90</td>
</tr>
<tr>
<td>Permissions</td>
<td>90</td>
</tr>
<tr>
<td>Device Status</td>
<td>91</td>
</tr>
<tr>
<td>Device Port Settings</td>
<td>92</td>
</tr>
<tr>
<td>Telnet/SSH/TCP in Port Numbers</td>
<td>93</td>
</tr>
<tr>
<td>Global Commands</td>
<td>93</td>
</tr>
<tr>
<td>Device Ports - Settings</td>
<td>94</td>
</tr>
<tr>
<td>Device Port Settings</td>
<td>96</td>
</tr>
<tr>
<td>IP Settings</td>
<td>96</td>
</tr>
<tr>
<td>Data Settings</td>
<td>97</td>
</tr>
<tr>
<td>Hardware Signal Triggers</td>
<td>98</td>
</tr>
<tr>
<td>Modem Settings</td>
<td>98</td>
</tr>
<tr>
<td>Modem Settings: Text Mode</td>
<td>99</td>
</tr>
<tr>
<td>Modem Settings: PPP Mode</td>
<td>99</td>
</tr>
<tr>
<td>Port Status and Counters</td>
<td>101</td>
</tr>
<tr>
<td>Device Ports - SLP / ServerTech CDU</td>
<td>101</td>
</tr>
<tr>
<td>Status/Info</td>
<td>102</td>
</tr>
<tr>
<td>SLP Commands</td>
<td>103</td>
</tr>
<tr>
<td>Device Port - Sensorsoft Device</td>
<td>103</td>
</tr>
<tr>
<td>Device Port Commands</td>
<td>104</td>
</tr>
<tr>
<td>Device Commands</td>
<td>106</td>
</tr>
<tr>
<td>Interacting with a Device Port</td>
<td>107</td>
</tr>
<tr>
<td>Device Ports - Logging</td>
<td>108</td>
</tr>
<tr>
<td>Local Logging</td>
<td>108</td>
</tr>
<tr>
<td>NFS File Logging</td>
<td>108</td>
</tr>
<tr>
<td>USB Flash Drive Logging</td>
<td>108</td>
</tr>
<tr>
<td>PC Card Logging</td>
<td>109</td>
</tr>
<tr>
<td>Email/SNMP Notification</td>
<td>109</td>
</tr>
<tr>
<td>Syslogs Logging</td>
<td>109</td>
</tr>
<tr>
<td>Local Logging</td>
<td>110</td>
</tr>
<tr>
<td>Email/SNMP Traps</td>
<td>110</td>
</tr>
<tr>
<td>Log Viewing Attributes</td>
<td>111</td>
</tr>
<tr>
<td>NFS File Logging</td>
<td>111</td>
</tr>
<tr>
<td>USB/PC Card Logging</td>
<td>112</td>
</tr>
<tr>
<td>Syslog Logging</td>
<td>112</td>
</tr>
<tr>
<td>Logging Commands</td>
<td>112</td>
</tr>
<tr>
<td>Console Port</td>
<td>114</td>
</tr>
<tr>
<td>Console Port Commands</td>
<td>115</td>
</tr>
<tr>
<td>Host Lists</td>
<td>115</td>
</tr>
<tr>
<td>Host Parameters</td>
<td>116</td>
</tr>
<tr>
<td>Host Parameters</td>
<td>118</td>
</tr>
<tr>
<td>Host List Commands</td>
<td>119</td>
</tr>
</tbody>
</table>
# Scripts

- User Rights
- Batch Script Syntax
- Interface Script Syntax
- Primary Commands
- Secondary Commands
- Control Flow Commands
- Sample Scripts
- Batch Script—SLC CLI

# Sites

- Modem Dialing States
  - Dial In
  - Dial-back
  - Dial-on-demand
  - Dial-in & Dial-on-demand
  - Dial-back & Dial-on-demand
  - CBCP Server

# 9: PC Cards

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

# 10: USB Port

- Set Up of USB Storage
- Data Settings
- GSM/GPRS Settings
- Modem Settings
- Text Mode
- PPP Mode
- IP Settings
- Manage Firmware and Configuration Files
- USB Commands

# 11: Connections

- Types of Endpoints and Connections
- Typical Setup Scenarios for the SLC Unit
  - Terminal Server
  - Remote Access Server
  - Reverse Terminal Server
  - Multiport Device Server
## 12: User Authentication

- Authentication Commands                                         167
- Local and Remote User Settings                                 168
  - Adding, Editing or Deleting a User                           169
  - Shortcut                                                   173
- Local Users Commands                                          173
- Local User Rights Commands                                    174
- Remote User Commands                                          175
- NIS                                                          176
  - NIS Commands                                               178
- LDAP                                                        179
  - LDAP Commands                                              183
- RADIUS                                                      185
  - RADIUS Commands                                            188
  - User Attributes & Permissions from LDAP Schema or RADIUS VSA 189
- Kerberos                                                    190
  - Kerberos Commands                                          193
- TACACS+                                                     194
  - TACAC + Commands                                           197
- Groups                                                      198
- SSH Keys                                                    201
  - Imported Keys                                              201
  - Exported Keys                                              202
  - Imported Keys (SSH In)                                     203
  - Host & Login for Import                                     204
  - Exported Keys (SSH Out)                                    204
  - Host and Login for Export                                   205
- SSH Commands                                                207
- Custom Menus                                                209
  - Custom User Menu Commands                                  212

## 13: Maintenance

- SLC Maintenance                                              216
  - Internal Temperature                                        218
  - Site Information                                            218
  - SLC Firmware                                               218
  - Boot Banks                                                 219
  - Load Firmware Via Options                                   219
  - Configuration Management                                   219
Administrative Commands
System Logs
System Log Command
Audit Log
Email Log
Diagnostics
Diagnostic Commands
Status/Reports
View Report
Status Commands
Emailing Logs and Reports
Events
Events Commands
LCD/Keypad
LCD/Keypad Commands
Banners
Banner Commands

14: Application Examples
Telnet/SSH to a Remote Device
Dial-in (Text Mode) to a Remote Device
Local Serial Connection to Network Device via Telnet

15: Command Reference
Introduction to Commands
Command Syntax
Command Line Actions and Categories
Tips
Deprecated Commands
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
Group Commands
### Port Connections

Port Connections

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix D: Sicherheitshinweise</td>
<td>321</td>
</tr>
<tr>
<td>Geräteabdeckung</td>
<td>321</td>
</tr>
<tr>
<td>Netzstecker</td>
<td>321</td>
</tr>
<tr>
<td>Stromversorgung</td>
<td>322</td>
</tr>
<tr>
<td>Anschluß an die Schutzerde</td>
<td>322</td>
</tr>
<tr>
<td>Gerätesicherung</td>
<td>322</td>
</tr>
<tr>
<td>Rack / Einbauschrank</td>
<td>322</td>
</tr>
<tr>
<td>Signalverbindungen</td>
<td>323</td>
</tr>
</tbody>
</table>

| Appendix E: Adapters and Pinouts                                     | 324  |
| Appendix F: Protocol Glossary                                        | 329  |
| Appendix G: Compliance Information                                   | 334  |
| Appendix H: DC Connector Instructions                                | 337  |
| Appendix I: LDAP Schemas                                             | 340  |
| Installing Schema Support in Window AD Server                       | 340  |
| Creating the SLC Schema Attribute                                   | 344  |
| Adding the Attribute to the Users Group in Windows                   | 345  |
| Adding the Permissions to the Individual User                       | 348  |
| Values to Use                                                        | 350  |
| String Format                                                        | 351  |
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-2</td>
<td>Lantronix SLC48 Console Manager with PC Card Slots</td>
<td>24</td>
</tr>
<tr>
<td>2-3</td>
<td>Lantronix SLC48 Console Manager with USB Port</td>
<td>24</td>
</tr>
<tr>
<td>2-4</td>
<td>Device Port Connections</td>
<td>26</td>
</tr>
<tr>
<td>2-5</td>
<td>Console Port Connection</td>
<td>27</td>
</tr>
<tr>
<td>2-6</td>
<td>Network Connection</td>
<td>27</td>
</tr>
<tr>
<td>2-7</td>
<td>PC Card Interface</td>
<td>28</td>
</tr>
<tr>
<td>2-8</td>
<td>SLC Console Manager with USB Interface</td>
<td>28</td>
</tr>
<tr>
<td>3-3</td>
<td>CAT 5 Cable Connection</td>
<td>32</td>
</tr>
<tr>
<td>3-4</td>
<td>AC Power Input and Power Switch (SLCxxx2N)</td>
<td>33</td>
</tr>
<tr>
<td>3-5</td>
<td>DC Power Inputs and Power Switch (SLCxxx24T)</td>
<td>33</td>
</tr>
<tr>
<td>4-2</td>
<td>Front Panel LCD Display and Five Button Keypads (Enter, Up, Down, Left, Right)</td>
<td>35</td>
</tr>
<tr>
<td>4-3</td>
<td>Quick Setup</td>
<td>39</td>
</tr>
<tr>
<td>4-4</td>
<td>Beginning of Quick Setup Script</td>
<td>41</td>
</tr>
<tr>
<td>4-7</td>
<td>Completed Quick Setup</td>
<td>42</td>
</tr>
<tr>
<td>5-1</td>
<td>Web Page Layout</td>
<td>45</td>
</tr>
<tr>
<td>6-1</td>
<td>Network &gt; Network Settings</td>
<td>53</td>
</tr>
<tr>
<td>6-2</td>
<td>Network &gt; IP Filter</td>
<td>58</td>
</tr>
<tr>
<td>6-3</td>
<td>Network &gt; IP Filter Ruleset (Adding/Editing Rulesets)</td>
<td>60</td>
</tr>
<tr>
<td>6-4</td>
<td>Network &gt; Routing</td>
<td>63</td>
</tr>
<tr>
<td>6-5</td>
<td>Network &gt; VPN</td>
<td>65</td>
</tr>
<tr>
<td>7-1</td>
<td>Services &gt; SSH/Telnet/Logging</td>
<td>69</td>
</tr>
<tr>
<td>7-2</td>
<td>Services &gt; SNMP</td>
<td>72</td>
</tr>
<tr>
<td>7-3</td>
<td>Services &gt; NFS/CIFS</td>
<td>76</td>
</tr>
<tr>
<td>7-4</td>
<td>Services &gt; Secure Lantronix Network</td>
<td>78</td>
</tr>
<tr>
<td>7-5</td>
<td>Telnet Session</td>
<td>79</td>
</tr>
<tr>
<td>7-6</td>
<td>Services &gt; Secure Lantronix Network &gt; Search Options</td>
<td>80</td>
</tr>
<tr>
<td>7-7</td>
<td>Services &gt; Date &amp; Time</td>
<td>81</td>
</tr>
<tr>
<td>7-8</td>
<td>Services &gt; Web Server</td>
<td>83</td>
</tr>
<tr>
<td>7-9</td>
<td>Web Sessions</td>
<td>86</td>
</tr>
<tr>
<td>7-10</td>
<td>SSL Certificate</td>
<td>87</td>
</tr>
<tr>
<td>7-11</td>
<td>iGoogle Gadget Example</td>
<td>89</td>
</tr>
<tr>
<td>8-1</td>
<td>Devices &gt; Device Status</td>
<td>91</td>
</tr>
<tr>
<td>8-2</td>
<td>Devices &gt; Device Ports</td>
<td>92</td>
</tr>
<tr>
<td>8-3</td>
<td>Device Ports List</td>
<td>94</td>
</tr>
<tr>
<td>8-4</td>
<td>Device Ports &gt; Settings</td>
<td>95</td>
</tr>
</tbody>
</table>
Figure 8-6 Device Ports > SLP
Figure 8-7 Devices > Device Ports > Sensorsoft
Figure 8-8 Devices > Device Ports - Logging
Figure 8-9 Devices > Console Port
Figure 8-10 Devices > Host Lists
Figure 8-11 View Host Lists
Figure 8-12 Devices > Scripts
Figure 8-13 Adding or Editing New Scripts
Figure 9-1 PC Card Page
Figure 9-2 PC Card - Storage Page
Figure 9-3 PC Card - Modem/ISDN Page
Figure 10-1 Devices > USB
Figure 10-2 Devices > USB > Configure
Figure 10-3 Devices > USB > Modem
Figure 10-4 Firmware and Configurations - Manage Files (Top of Page)
Figure 11-1 Terminal Server
Figure 11-2 Remote Access Server
Figure 11-3 Reverse Terminal Server
Figure 11-4 Multiport Device Server
Figure 11-5 Console Server
Figure 11-6 Devices > Connections
Figure 11-7 Current Connections
Figure 12-1 User Authentication > Authentication Methods
Figure 12-2 User Authentication > Local/Remote Users
Figure 12-3 User Authentication > Local/Remote User > Settings
Figure 12-4 User Authentication > NIS
Figure 12-5 User Authentication > LDAP
Figure 12-6 User Authentication > RADIUS
Figure 12-7 User Authentication > Kerberos
Figure 12-8 User Authentication > TACACS+
Figure 12-9 User Authentication > Group
Figure 12-10 User Authentication > SSH Keys
Figure 12-11 Current Host Keys
Figure 12-12 User Authentication > Custom Menus
Figure 13-1 Maintenance > Firmware & Config
Figure 13-2 Manage Configuration Files
Figure 13-3 Maintenance > System Logs
Figure 13-4 System Logs
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-11</td>
<td>User Class Window</td>
<td>346</td>
</tr>
<tr>
<td>I-12</td>
<td>Class User Properties Window</td>
<td>346</td>
</tr>
<tr>
<td>I-13</td>
<td>User Properties Window</td>
<td>347</td>
</tr>
<tr>
<td>I-14</td>
<td>Select Schema Object Window</td>
<td>347</td>
</tr>
<tr>
<td>I-15</td>
<td>ADSI Edit Window</td>
<td>348</td>
</tr>
<tr>
<td>I-16</td>
<td>ADSI Edit Window, CN=Users Folder</td>
<td>349</td>
</tr>
<tr>
<td>I-17</td>
<td>Properties Window</td>
<td>349</td>
</tr>
<tr>
<td>I-18</td>
<td>Attribute Editor Window</td>
<td>350</td>
</tr>
<tr>
<td>I-19</td>
<td>String Attribute Editor Window</td>
<td>351</td>
</tr>
</tbody>
</table>
List of Tables

Table 1-1 Chapter/Appendix and Summary .......................................................... 19
Table 1-2 Conventions Used in This Book .......................................................... 21
Table 2-1 SLC Part Numbers, Models, and Descriptions ...................................... 23
Table 3-1 Component Part Numbers and Descriptions ....................................... 29
Table 3-2 Components and Descriptions ............................................................ 30
Table 4-1 Methods of Assigning an IP Address .................................................... 34
Table 4-3 LCD Arrow Keypad Actions ................................................................. 36
Table 4-4 Front Panel Setup Options with Associated Parameters ....................... 36
Table 5-2 Actions and Category Options ............................................................. 48
Table 8-5 Port Status and Counters ..................................................................... 101
Table 8-14 Definitions ......................................................................................... 124
Table 8-15 Primary Commands .......................................................................... 125
Table 8-16 Secondary Commands ....................................................................... 127
Table 8-17 Control Flow Commands ................................................................... 128
Table 15-1 Actions and Category Options .......................................................... 251
Table A-1 User Commands .................................................................................. 315
Table G-1 Lantronix Product Family Names and Toxic/Hazardous Substances and Elements .............................. 336
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>
<thead>
<tr>
<th>Chapter/Appendix</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2: Overview</td>
<td>Describes the SLC models, main features, and supported protocols.</td>
</tr>
<tr>
<td>Chapter 3: Installation</td>
<td>Provides technical specifications; describes connection formats and power supplies; provides instructions for installing the unit in a rack.</td>
</tr>
<tr>
<td>Chapter 4: Quick Setup</td>
<td>Provides instructions for getting your unit up and running and for configuring required settings.</td>
</tr>
<tr>
<td>Chapter 5: Web and Command Line Interfaces</td>
<td>Describes the web and command line interfaces available for configuring the unit.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: 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.</td>
</tr>
<tr>
<td>Chapter 6: Basic Parameters</td>
<td>Provides instructions for configuring network ports, firewall and routing settings, and date and time.</td>
</tr>
<tr>
<td>Chapter 7: Services</td>
<td>Provides instructions for enabling and disabling system logging, SSH and Telnet logins, SNMP, SMTP, and the date and time.</td>
</tr>
<tr>
<td>Chapter 8: Device Ports</td>
<td>Provides instructions for configuring global device port settings, individual device port settings, and console port settings.</td>
</tr>
<tr>
<td>Chapter 9: PC Cards</td>
<td>Provides instructions for configuring storage (Compact Flash) and modem/ISDN PC cards.</td>
</tr>
<tr>
<td>Chapter/Appendix</td>
<td>Summary</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Chapter 10: USB Port</strong></td>
<td>Provides instructions for configuring USB storage devices (thumb drive) or USB modems.</td>
</tr>
<tr>
<td><strong>Chapter 11: Connections</strong></td>
<td>Provides instructions for configuring connections and viewing, updating, or disconnecting a connection.</td>
</tr>
<tr>
<td><strong>Chapter 12: User Authentication</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Chapter 13: Maintenance</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Chapter 14: Application Examples</strong></td>
<td>Shows how to set up and use the SLC device in three different configurations.</td>
</tr>
<tr>
<td><strong>Chapter 15: Command Reference</strong></td>
<td>Lists and describes all of the commands available on the SLC command line interface.</td>
</tr>
<tr>
<td><strong>Appendix A: Bootloader</strong></td>
<td>Lists and describes the commands available for the bootloader command line interface.</td>
</tr>
<tr>
<td><strong>Appendix B: Security Considerations</strong></td>
<td>Provides tips for enhancing SLC security.</td>
</tr>
<tr>
<td><strong>Appendix C: Safety Information</strong></td>
<td>Lists safety precautions for using the SLC console manager.</td>
</tr>
<tr>
<td><strong>Appendix D: Sicherheitshinweise</strong></td>
<td>Lists safety precautions for using the SLC device in German.</td>
</tr>
<tr>
<td><strong>Appendix E: Adapters and Pinouts</strong></td>
<td>Includes adapter pinout diagrams.</td>
</tr>
<tr>
<td><strong>Appendix F: Protocol Glossary</strong></td>
<td>Lists the protocols supported by the SLC console manager with brief descriptions.</td>
</tr>
<tr>
<td><strong>Appendix G: Compliance Information</strong></td>
<td>Provides information about the SLC compliance with industry standards.</td>
</tr>
<tr>
<td><strong>Appendix H: DC Connector Instructions</strong></td>
<td>Provides -48VDC plug connector instructions for the SLC console manager.</td>
</tr>
<tr>
<td><strong>Appendix I: LDAP Schemas</strong></td>
<td>Provides information about configuring LDAP schemas in Windows active directory.</td>
</tr>
</tbody>
</table>
Conventions

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold text</td>
<td>Default parameters.</td>
</tr>
<tr>
<td>brackets [ ]</td>
<td>Optional parameters.</td>
</tr>
<tr>
<td>angle brackets &lt; &gt;</td>
<td>Possible values for parameters.</td>
</tr>
<tr>
<td>pipe</td>
<td>Choice of parameters.</td>
</tr>
<tr>
<td>Warning</td>
<td>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.</td>
</tr>
<tr>
<td>Note</td>
<td>Note: Means take notice. Notes contain helpful suggestions, information, or references to material not covered in the publication.</td>
</tr>
<tr>
<td>Caution</td>
<td>Caution: Means you might do something that could result in faulty equipment operation, or loss of data.</td>
</tr>
<tr>
<td>Screen Font (Courier New)</td>
<td>CLI terminal sessions and examples of CLI input.</td>
</tr>
</tbody>
</table>

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.
- **SLB and SLC 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, medical 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**
- **System Features**
- **Hardware Features**

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

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).
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 Appendix F: 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 30.

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 Appendix E: Adapters and Pinouts.

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
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.

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.
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
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 318 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>
<thead>
<tr>
<th>Component Part #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapters</td>
<td></td>
</tr>
<tr>
<td>200.2066A</td>
<td>Adapter: DB25M (DCE), Sun w/DB25 female</td>
</tr>
<tr>
<td>200.2067A</td>
<td>Adapter: DB25F (DCE) to RJ45, Sun w/DB25 male and some HP9000s</td>
</tr>
<tr>
<td>200.2069A</td>
<td>Adapter: DB9M (DCE) to RJ45, SGI Onyx</td>
</tr>
<tr>
<td>200.2070A</td>
<td>Adapter: DB9F (DCE) to RJ45, HP9000, SGI Origin, IBM RS6000, and PC-based Linux servers</td>
</tr>
<tr>
<td>ADP010104-01</td>
<td>Adapter: RJ45 rolled serial, Cisco, and Sun Netra</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Cables</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>200.0063</td>
<td>Cable: RJ45 to RJ45, 6.6 ft (2 m)</td>
</tr>
<tr>
<td>500-153</td>
<td>Cable: Loopback</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Power Cords</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>500-041</td>
<td>For single AC models: one AC power cord</td>
</tr>
<tr>
<td></td>
<td>For dual AC models: two AC power cords</td>
</tr>
<tr>
<td>083-011</td>
<td>For dual DC models: one accessory kit, containing DC plug connectors and instructions</td>
</tr>
</tbody>
</table>

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

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 recommend 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 31.

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 32.
   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 32.

4. Connect the power cord, and apply power. See Power on page 32.

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 Appendix E: Adapters and Pinouts on page 324 for more information about Lantronix adapters.*

3. Connect the adapter to the serial console of the serial device as shown in Figure 3-3.
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 324 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 30. 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](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.

Recommendations

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

- Use the front panel LCD display and keypads.
- Complete the Quick Setup 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 unit, 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 . 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.

The following table lists the options for assigning an IP address to your SLC unit.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>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 unit powered up, Eth1 acquires an IP address, viewable on the LCD. At this point, you can use SSH or Telnet to connect to the SLC console manager, or use the web interface.</td>
</tr>
<tr>
<td>BOOTP</td>
<td>Similar to DHCP but for smaller networks.</td>
</tr>
<tr>
<td>DeviceInstaller™</td>
<td>The Lantronix DeviceInstaller is a Windows-based GUI application that provides an easy way to install and configure specific Lantronix device server products. You may utilize DeviceInstaller to assign an IP and other network specific addresses.</td>
</tr>
<tr>
<td>Front panel LCD display and keypads</td>
<td>You manually assign the IP address and other basic network, console, and date/time settings. If desired, you can restore the factory defaults.</td>
</tr>
</tbody>
</table>
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 Keypads**

With the SLC device powered up, you can use the front panel display and keypads to set up the basic parameters.

The front panel display initially shows the hostname (abbreviated to 14 letters) and total current level.

When you click the right-arrow keypad, the SLC console manager's network settings display. Using the five keypads, 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 keypad 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.

The following table lists the SLC navigation actions, buttons, and options.

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

**Table 4-3 LCD Arrow Keypad Actions**

<table>
<thead>
<tr>
<th>Network Settings</th>
<th>Console Settings</th>
<th>Date / Time Settings</th>
<th>Release</th>
<th>Internal Temp</th>
<th>User Strings</th>
<th>Location</th>
<th>Device Ports</th>
<th>Current Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1 IP Address</td>
<td>Baud Rate</td>
<td>Time Zone</td>
<td>Firmware version and date code (display only)</td>
<td>Reading in Celsius &amp; Fahrenheit</td>
<td>Displays configured user string(s), if any.</td>
<td>Indicates the Rack (RK), Row (RW) &amp; Cluster (CW) locations.</td>
<td>Detects the connection state of each port: 0=No serial connection 1=Serial connection detected.</td>
<td>User ID &amp; Current Time</td>
</tr>
<tr>
<td>Eth1 Subnet Mask</td>
<td>Data Bits</td>
<td>Date/Time</td>
<td>Restore Factory Defaults</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>Stop Bits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS1</td>
<td>Parity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS2</td>
<td>Flow Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Note: The individual screens listed from left to right in Table 4-4 can be enabled or disabled for display on the SLC LCD screen. The order of appearance of the screens, if enabled, along with the elected “Home Page” may vary on the LCD monitor according to configuration. See LCD/Keypad (on page 241) for instructions on enabling and disabling screens.

**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. 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.

5. 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.

6. Use the left/right arrow buttons to select **Yes**, and press the **Enter** button.

7. Press the right arrow button to move to the next option, **Console Settings**.

8. Repeat steps 2-7 for each setting.

9. Press the right arrow button to move to the next option, **Date/Time Settings**, and click **Enter** to edit the time zone.

   - 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.
   - 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.

10. 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.

11. Use the left/right arrow buttons to select Yes, and press the Enter button.

12. 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 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 unit reboots.

Method #2 Quick Setup on the Web Page

After the unit has an IP address, you can use the Quick Setup page 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.

To complete the Quick Setup page:

1. Open a web browser (Firefox, Chrome or Internet Explorer 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 unit, the Quick Setup page automatically displays. Otherwise, the Home page displays.

Note: To open the Quick Setup page at another time, click the Quick Setup tab.
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 the Apply button on the Quick Setup page, you can continue using the web interface to configure the SLC console manager further.

5. Enter the following settings:

### Network Settings

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

<table>
<thead>
<tr>
<th>Network Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Eth 1 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. |
4: Quick Setup

Date & Time Settings

**IP Address (if specifying)**
- Enter an IP address that is 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 unit does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).

**Subnet Mask**
- If specifying an IP address, enter the subnet mask for the network on which the SLC console manager 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 unit. 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**

<table>
<thead>
<tr>
<th>Date &amp; Time Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Date/Time</td>
<td>Select the checkbox to manually enter the date and time at the SLC unit’s location.</td>
</tr>
<tr>
<td>Date</td>
<td>From the drop-down lists, select the current month, day, and year.</td>
</tr>
<tr>
<td>Time</td>
<td>From the drop-down lists, select the current hour and minute.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>From the drop-down list, select the appropriate time zone.</td>
</tr>
</tbody>
</table>

**Administrator Settings**

<table>
<thead>
<tr>
<th>Administrator Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sysadmin Password</td>
<td>To change the password (e.g., from the default) enter a Sysadmin Password of up to 64 characters.</td>
</tr>
<tr>
<td>Retype Password</td>
<td>Re-enter the Sysadmin Password above in this field as a confirmation.</td>
</tr>
</tbody>
</table>

6. Click the **Apply** button to save your entries.

**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. (See Connecting to Terminals on page 32.) If the unit has an IP address, you can use SSH or Telnet to connect to the SLC unit.

*Note:* By default, Telnet is disabled and SSH is enabled. To enable Telnet, use the Services > SSH/Telnet/Logging page (see Chapter 7: Services on page 68), a serial terminal connection, or an SSH connection.
To complete the command line interface Quick Setup script:

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 Beginning of Quick Setup Script**

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 information at the prompts:

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

<table>
<thead>
<tr>
<th>CLI Quick Setup Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Eth1</strong></td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>◆ &lt;1&gt; 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 gateway and hostname, depending on its setup.) This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>◆ &lt;2&gt; obtain IP Address from BOOTP: Permits a network node to request configuration information from a BOOTP &quot;server&quot; node.</td>
</tr>
<tr>
<td></td>
<td>◆ &lt;3&gt; static IP Address: Allows you to assign a static IP address manually. The IP address is generally provided by the system administrator.</td>
</tr>
<tr>
<td><strong>IP Address (if specifying)</strong></td>
<td>An IP address that is unique and valid on your network and in the same subnet as your PC. There is no default.</td>
</tr>
<tr>
<td></td>
<td>If you selected DHCP or BOOTP, this prompt does not display.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>IP address of the router for this network. There is no default.</td>
</tr>
</tbody>
</table>
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 SLC32 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 SLC32 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 'GMT'.
Enter time zone: [GMT]

---

### Date/Time

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.*
The current time is Mon Jun  5 02:33:17 2000
Change the current time? [n]

__________________________
Sysadmin Password

Enter new password: [<current password>]

Quick Setup is now complete.

Next Step

After completing quick setup on 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 Chapter 5: Web and Command Line Interfaces.
- To continue configuring the SLC unit, go to Chapter 6: Basic Parameters.
5: Web and Command Line Interfaces

The SLC console manager offers three interfaces for configuring the SLC unit: a command line interface (CLI), a web interface, and an LCD with keypads on the front panel. This chapter discusses the web and command line interfaces. (Chapter 4: Quick Setup includes instructions for using the LCD to configure basic network settings.)

**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 allows the system administrator and other authorized users to configure and manage the SLC console manager using most web browsers (Firefox, Chrome or Internet Explorer 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).

The following figure shows a typical web page:
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 and Power Outlet Bar**:
  - The light green **LCD** button allows you to configure the front panel LCD.
  - The gray **U1** button allows you to configure the USB device (flash drive or modem) plugged into the front panel USB connector. The gray **U2** button allows you to configure the internal USB dial-up modem.
  - The blue **E1** and **E2** buttons display the **Network > 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.
  - The green number buttons allow you to select a port and display its settings. Only ports to which the currently logged-in user has rights are enabled.
Below the bar are options for use with the port buttons. Selecting a port and the **Configuration** option takes you to the **Device Ports > Settings** page. Selecting a port and the **WebSSH** option displays the WebSSH window for the device port --if Web SSH is enabled, and if SSH is enabled for the device port. Selecting the port and the **Connected Device** button allows access to supported devices such as SLPs and/or SensorSoft temperature and humidity probes connected to the device port.

- **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 5 through 12.

- **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 icon bar above the Main Menu has icons that display the following:
  - 🏘️ Home page.
  - 📁 Information about the SLC unit and Lantronix contact information.
  - 🌐 Configuration site map.
  - 📆 Status of the SLC device.

- **Help Button:** Provides online Help for the specific web page.

**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. See Chapter 15: Command Reference for more information.

**To log in to the SLC console manager web interface:**

1. Open a web browser.
2. In the URL field, type `https://` followed by the IP address of your SLC unit.
3. To configure the SLC console manager, use `sysadmin` as the user name and `PASS` as the password. (These are the default values.)

  **Note:** The system administrator may have changed the password using one of the Quick Setup methods 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 Out

To log off the SLC web interface:

1. Click the **Logout** button located on the upper left part of any user interface page. You are brought back to the login screen when logout is complete.

Web Page Help

To view detailed information about an SLC web page:

1. Click the **Help** button to the right of any user interface page. Online Help contents will appear in a new browser.

Command Line Interface

A command line interface (CLI) is available for entering all the commands you can use with the SLC console manager. You can access the command line interface using Telnet, SSH, or a serial terminal connection. 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 *Chapter 15: Command Reference*.

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

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 in to 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:
To log in any other user:

1. Enter your SLC user name and press Enter.
2. Enter your SLC password and press Enter.

Logging Out

To log out of the SLC command line interface, type logout and press Enter.

Command Syntax

Commands have the following format:

```
<action> <category> <parameter(s)>
```

where

- `<action>` is set, show, connect, admin, diag, pccard, or logout.
- `<category>` is a group of related parameters whose settings you want to configure or view. Examples are ntp, deviceport, and network.
- `<parameter(s)>` is one or more name-value pairs in one of the following formats:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`&lt;parameter_name&gt; &lt;aa</td>
<td>bb&gt;`</td>
</tr>
<tr>
<td><code>&lt;parameter_name&gt; &lt;Value&gt;</code></td>
<td>User must specify an appropriate value, for example, an IP address. The parameter values are in mixed case. Square brackets [] indicate optional parameters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 5-2 Actions and Category Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>set</td>
</tr>
</tbody>
</table>
1. USB commands are only accessible on SLC USB part numbers -03.
2. PC Card commands are only accessible on SLC USB part number -02.

Command Line Help

- 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
- For information about the current release, type: help release

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

  ```
  set 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 users and users listed in the remote users list.

<table>
<thead>
<tr>
<th>SCS Commands</th>
<th>SLC Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>info</td>
<td>'show sysstatus'</td>
</tr>
<tr>
<td>version</td>
<td>'admin version'</td>
</tr>
<tr>
<td>reboot</td>
<td>'admin reboot'</td>
</tr>
<tr>
<td>poweroff</td>
<td>'admin shutdown'</td>
</tr>
<tr>
<td>listdev</td>
<td>'show deviceport names'</td>
</tr>
<tr>
<td>direct</td>
<td>'connect direct deviceport'</td>
</tr>
<tr>
<td>listen</td>
<td>'connect listen deviceport'</td>
</tr>
<tr>
<td>clear</td>
<td>'set locallog clear'</td>
</tr>
<tr>
<td>telnet</td>
<td>'connect direct telnet'</td>
</tr>
<tr>
<td>ssh</td>
<td>'connect direct ssh'</td>
</tr>
</tbody>
</table>

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 screenful 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 explains how to set the following basic configuration settings for the SLC console manager using the SLC web interface or the CLI:

- Network parameters that determine how the SLC unit 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. 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

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** (optional)
- IP address: __________ - __________ - __________ - __________
- Subnet mask (optional): __________ - __________ - __________ - __________

**Gateway:** __________ - __________ - __________ - __________

**DNS:** __________ - __________ - __________ - __________
To enter settings for one or both network ports:

1. Click the **Network** tab and select the **Network Settings** option. The following page displays:

   ![Network Settings](image)

---

**Figure 6-1 Network > Network Settings**

**Ethernet Interfaces**

- **E1**: Disabling/Enabling, Obtain from DHCP, Obtain from BOOTP, Specify
- **E2**: Disabling/Enabling, Obtain from DHCP, Obtain from BOOTP, Specify

- **IP Address**: 172.19.100.01, 192.168.1.61
- **Subnet Mask**: 255.255.0.0, 255.255.0.0
- **IPv4 Address**: 198.200.10.1, 198.200.10.1
- **IPv6 Address (link-local)**: fe80:280:100:1f0:fe89:66, fe80:280:100:1f0:fe89:66
- **Mode**: Full Duplex 1000 Mb/s, 1 Gbps
- **MTU**: 1400, 1500

- **E1**
  - **IPv4 Address**: 238.255.255.241, 224.0.0.1
  - **IPv6 Address**: fe80:280:100:1f0:fe89:66, fe80:280:100:1f0:fe89:66

- **Enable IPv6**: Enable (Optional reboot)

**Gateway**

- **Default**: 172.19.0.1
- **Alternate**: 172.18.0.1
- **GPRS Acquired**: 172.18.0.1
- **IP Address to Ring**: 172.18.0.1
- **Ethernet Port for Ring**: E1, E2
- **DHCP Acquired**: DNS, PING, User
- **Delay Between Pings**: 2 seconds
- **Number of Failed Pings**: 5
- **Number of Pings**: 185
- **Interval**: 3000

---

**HostName & Name Servers**

- **Host Name**: slc600d
- **Domain**: lantronix.com
- **DNS Servers**
  - 1: 172.18.1.1
  - 2: 172.18.0.10
  - 3: 172.18.1.2
- **DHCP Acquired DNS Servers**
  - 1: 172.18.1.1
  - 2: 172.18.1.2
  - 3: None
- **GPRS Acquired DNS Servers**
  - 1: None
  - 2: None
  - 3: None

**Enable IP Forwarding**

- **Enable IP Forwarding**: Enabled

---

**IPv6 Parameters**

- **Start Prefix**: 128
- **Number of Prefixes**: 5
- **Interval**: 3000
2. Enter the following information:

**Eth1 and Eth2 Settings**

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

<table>
<thead>
<tr>
<th><strong>Eth 1 Settings</strong> or <strong>Eth 2 Settings</strong></th>
<th><strong>IP Address (if specifying)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled: If selected, disables the network port. 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.</td>
<td>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. <em>Note:</em> Currently, the SLC device does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>If specifying an IP address, enter the network segment on which the SLC resides. There is no default.</td>
</tr>
<tr>
<td><strong>IPv6 Address</strong></td>
<td>Address of the port in IPv6 format. <em>Note:</em> The SLC unit 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.</td>
</tr>
<tr>
<td><strong>IPv6 Address (Link Local)</strong></td>
<td>An IPv6 address that is intended only for communications within the segment of a local network.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>Displays the multicast address of the Ethernet port.</td>
</tr>
<tr>
<td><strong>Enable IPv6</strong></td>
<td>Select this box to enable the IPv6 protocol. Disabled by default.</td>
</tr>
<tr>
<td><strong>Ethernet Bonding</strong></td>
<td>Ethernet 1 and Ethernet 2 can be bonded to support redundancy (Active Backup), aggregation (802.3ad), and load balancing. Disabled by default. Note that if Ethernet Bonding is enabled, assigning individual IP Addresses to Device Ports is not supported.</td>
</tr>
</tbody>
</table>
Note: Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.

**Gateway**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>If you set a default gateway, any network traffic that does not match Eth1 or Eth2 is sent to the default gateway for routing.</td>
</tr>
<tr>
<td>DHCP-Acquired</td>
<td>Gateway acquired by DHCP for Eth1 or Eth2. View only.</td>
</tr>
<tr>
<td>GPRS-Acquired</td>
<td>Displays the IP address of the router if it has been automatically assigned by General Packet Radio Service (GPRS). View only.</td>
</tr>
<tr>
<td>Precedence</td>
<td>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.</td>
</tr>
<tr>
<td>Alternate</td>
<td>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.</td>
</tr>
<tr>
<td>IP Address to Ping</td>
<td>IP address to ping to determine whether to use the alternate gateway.</td>
</tr>
<tr>
<td>Ethernet Port to Ping</td>
<td>Ethernet port to use for the ping.</td>
</tr>
<tr>
<td>Delay between Pings</td>
<td>Number of seconds between pings</td>
</tr>
<tr>
<td>Number of Failed Pings</td>
<td>Number of pings that fail before the SLC unit uses the alternate gateway.</td>
</tr>
<tr>
<td>Enable IP Forwarding</td>
<td>IP forwarding enables network traffic received on one interface (Eth1, Eth2, or an external/USB modem attached to the SLC device 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 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.</td>
</tr>
</tbody>
</table>

**Hostname & Name Servers**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>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.</td>
</tr>
<tr>
<td>Domain</td>
<td>If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLC unit. 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.</td>
</tr>
</tbody>
</table>
DNS Servers

<table>
<thead>
<tr>
<th>DNS Servers #1 - #3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure up to three name servers. #1 is required if you choose to configure DNS (Domain Name Server) servers.</td>
</tr>
<tr>
<td>The first three DNS servers acquired via DHCP through Eth1 and/or Eth2 display automatically.</td>
</tr>
</tbody>
</table>

DHCP-Acquired DNS Servers

<table>
<thead>
<tr>
<th>#1 - #3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the IP address of the name servers if automatically assigned by DHCP.</td>
</tr>
</tbody>
</table>

GPRS-Acquired DNS Servers

<table>
<thead>
<tr>
<th>#1 - #3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the IP address of the name servers if automatically assigned by General Packet Radio Service (GPRS).</td>
</tr>
</tbody>
</table>

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 unit sends before closing a session. The default is 5. |
| Interval | The number of seconds the SLC device waits between probes. The default is 60 seconds. |

3. To save your entries, click the **Apply** button. **Apply** makes the changes immediately and saves them so they will be there when the SLC console manager is rebooted.

Ethernet Counters

The **Network > Network Settings** page displays statistics for each of the SLC unit's Ethernet ports since boot-up. The system automatically updates them.

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

Network Commands

The following CLI commands correspond to the web page entries described above.

**To configure Ethernet port 1 or 2:**

```bash
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>]`
To configure up to three DNS servers:

```
set network dns <1|2|3> ipaddr <IP Address>
```

To set the default and alternate network gateways:

```
set network gateway <parameters>
```

**Parameters:**

- default <IP Address>
- precedence <dhcp|gprs|default>
- alternate <IP Address>
- pingip <IP Address>
- ethport <1 or 2>
- pingdelay <1-250 seconds>
- failedpings <1-25>

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

To set the SLC host name and domain name:

```
set network host <Hostname> [domain <Domain Name>]
```

To set TCP Keepalive and IP Forwarding network parameters:

```
set network <parameters>
```

**Parameters:**

- interval <1-99999 Seconds>
- ipforwarding <enable|disable>
- probes <Number of Probes>
- startprobes <1-99999 Seconds>

To view all network settings:

```
show network all
```

To view Ethernet port settings and counters:

```
show network port <1|2>
```

To view DNS settings:

```
show network dns
```

To view gateway settings:

```
show network gateway
```

To view the host name of the SLC unit:

```
show network host
```
### IP Filter

IP filters (also called a rule set) act as a firewall to allow or deny individual or a range of IP addresses, ports, and protocols. When a network connection is configured to use an IP filter, all network traffic through that connection is compared, in order, to the rules of that filter. 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 rules of that filter rule set.

The administrator uses the **Network > 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.*

### Viewing IP Filters

You can view a list of filters and a table showing how each filter is mapped to an interface.

**To view a list of IP filters:**

1. Click the **Network** tab and select the **IP Filter** option. The following page displays:

   ![Image of Network > IP Filter page](image)

**Figure 6-2  Network > IP Filter**

<table>
<thead>
<tr>
<th>IP Filter RuleSets</th>
<th>Name</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ssh</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ssh-telnet</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ssh-telnet-smtp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IP Filter Status**

- 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.

**Map Rule sets to Interface**

- [ ] Map Rule set to Interface: Ethernet 1

**Delete Mapping**

**IP Filter Mappings**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Ruleset</th>
</tr>
</thead>
</table>
Enabling IP Filters
On the *Network > IP Filter* page, you can enable all filters or disable all filters.

**Note:** There is no way to enable or disable individual filters.

**To enable IP filters:**

1. Enter the following:

<table>
<thead>
<tr>
<th>Enable IP Filter</th>
<th>Select the Enable IP Filter checkbox to enable all filters, or clear the checkbox to disable all filters. Disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Dropped</td>
<td>Displays the number of data packets that the filter ignored (did not respond to). View only.</td>
</tr>
<tr>
<td>Packets Rejected</td>
<td>Displays the number of data packets that the filter sent a “rejected” response to. View.</td>
</tr>
<tr>
<td>Test Timer</td>
<td>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.</td>
</tr>
<tr>
<td>Time Remaining</td>
<td>Indicates how many minutes are left on the timer before it expires and IP Filters disabled. View only.</td>
</tr>
</tbody>
</table>

Configuring IP Filters
The administrator can add, edit, delete, and map IP filters.

**Note:** A configured filter has no effect until it is mapped to a network interface. See Mapping a Ruleset on page 62.

**To add an IP filter:**

1. On the *Network > IP Filter* page, click the Add Ruleset button. The following page displays:
Rulesets can be added or updated on this page.

2. Enter the following:

**Ruleset Name**
Name that identifies a filter; may be composed of letters, numbers, and hyphens only. (The name cannot start with a hyphen.)
Example: FILTER-2

**Rule Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address(es)</strong></td>
<td>Specify a single IP address to act as a filter or specify a range of IP addresses if the range cannot be defined by an IP address and Subnet Mask. Example: 172.19.220.64 – this specific IP address only. 172.19.220.60:172.19.220.68 - a range of IP addresses from 172.19.220.60 through 172.19.220.68.</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Specify a subnet mask to act determine how much of the address should apply to the filter. Example: 255.255.255.255 to specify the whole address should apply.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>From the drop-down list, select the type of protocol through which the filter will operate. The default setting is All.</td>
</tr>
</tbody>
</table>
3. Click the right arrow button to add the new rule to the bottom of the Rules list box on the right. A maximum of 64 rules can be created for each ruleset.

4. To remove a rule from the filter set, highlight that line 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.

5. 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.

6. To save, click the Apply button. The new filter displays in the menu tree.

Note: To add another new filter rule set, click the Back to IP Filter link to return to the Network > IP Filter page.
Updating an IP Filter

To update an IP filter rule set:

1. From the Network > IP Filter page, the administrator selects the IP filter ruleset to be edited and clicks the Edit Ruleset button to return to the Network > IP Filter Ruleset (Adding/Editing Rulesets) page (see Figure 6-3).
2. Edit the information as desired and click the Apply button.

Deleting an IP Filter

To delete an IP filter rule set:

1. On the Network > IP Filter page, the administrator selects the IP filter ruleset to be deleted and clicks the Delete Ruleset button.

Mapping a Ruleset

The administrator can assign an IP Filter Ruleset to a network interface (Ethernet interface) a modem connected to a Device Port.

To map a rule set to a network interface:

1. On the Network > 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 rule set display in the IP Filter Mappings table.

To delete a mapping:

1) On the Network > IP Filter page, select the mapping from the list and click the Delete Mapping button. The mapping no longer displays.
2) Click the Apply button.

IP Filter Commands

The following CLI commands correspond to the web page entries described above.

To enable or disable IP filtering for incoming network traffic:

set ipfilter state

To set IP filter mapping:

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>
state <disable>
state <enable> ruleset <Ruleset Name>

To set IP filter rules:

set ipfilter rules <parameters>

Parameters:

add <Ruleset Name>
delete <Ruleset Name>
edit <Ruleset Name> <Edit Parameters>

Edit Parameters:

append
insert <Rule Number>
replace <Rule Number>
delete <Rule Number>

Routing

The SLC console manager allows you to define static routes and, for networks using Routing Information Protocol (RIP)-capable routes, to enable the RIP protocol to configure the routes dynamically.

To configure routing settings:

1. Click the Network tab and select the Routing option. The following page displays:

Figure 6-4  Network > Routing
2. Enter the following:

**Dynamic Routing**

| 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. |

**Static Routing**

| 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.

**Note:** To display the routing table, status or specific report, see the section, Status/Reports on page 234.

**Equivalent Routing Commands**

The following CLI commands correspond to the web page entries described above.

**To configure static or dynamic routing:**

```
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 IP address, mask, and gateway parameters to 0.0.0.0.

**To set the routing table to display IP addresses (disable) or the corresponding host names (enable):**

```
show routing [resolveip <enable|disable>] [email <Email Address>]
```

**Note:** You can optionally email the displayed information.
VPN

This page can be used to create a Virtual Private Network (VPN) tunnel to the SLC console manager for secure communication between the SLC unit and a remote host or gateway. The SLC device supports IPSec tunnels using Encapsulated Security Payload (ESP). The SLC console manager supports host-to-host, net-to-net, host-to-net, and roaming user tunnels.

**Note:** To allow VPN tunnel access if the SLC firewall is enabled, traffic to UDP ports 500 and 4500 from the remote host should be allowed, as well as protocol ESP from the remote host.

**To complete the VPN page:**

1. Click the **Network** tab and select the **VPN** option. The following page displays:

![Figure 6-5 Network > VPN](image)

- Enable VPN Tunnel: [ ]
- Current VPN Tunnel Status: Down
  
- **Name:**
- **Ethernet Port:** [ ]
- **Remote Host:**
- **Remote Id:**
- **Remote Hop/Router:**
- **Remote Subnet(s):**
- **Local Id:**
- **Local Hop/Router:**
- **Local Subnet(s):**
  
- **IKE Negotiation:** [ ] Main Mode
  - Aggressive Mode
- **IKE Encryption:** [ ] Any Authentication [ ] Any
- **ESP Encryption:** [ ] Any Authentication [ ] Any
  
- **Authentication:** [ ] RSA Public Key [ ] Pre-Shared Key
- **RSA Public Key:**
- **Pre-Shared Key:**
  - **Retype Pre-Shared Key:**
  - **Perfect Forward Secrecy:** [ ]
  - **Mode Configuration Client:** [ ]
  
- **XAUTH Client:**
- **XAUTH Login:**
- **XAUTH Password:**
  - **Retype Password:**

**Apply**
2. Enter the following:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable VPN Tunnel</strong></td>
<td>Select to create a tunnel.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The name assigned to the tunnel. Required to create a tunnel.</td>
</tr>
<tr>
<td><strong>Ethernet Port</strong></td>
<td>Select ethernet port 1 or 2.</td>
</tr>
<tr>
<td><strong>Remote Host</strong></td>
<td>The IP address of the remote host's public network interface. The special</td>
</tr>
<tr>
<td></td>
<td>value of any can be entered if the remote host is a roaming user who may</td>
</tr>
<tr>
<td></td>
<td>not have the same IP address each time a tunnel is created. In this case,</td>
</tr>
<tr>
<td></td>
<td>it is recommended that the <strong>Remote Id</strong> also be configured.</td>
</tr>
<tr>
<td><strong>Remote Id</strong></td>
<td>How the remote host should be identified for authentication. The Id is used</td>
</tr>
<tr>
<td></td>
<td>to select the proper credentials for communicating with the remote host.</td>
</tr>
<tr>
<td><strong>Remote Hop/Router</strong></td>
<td>If the remote host is behind a gateway, this specifies the IP address of</td>
</tr>
<tr>
<td></td>
<td>the gateway's public network interface.</td>
</tr>
<tr>
<td><strong>Remote Subnet(s)</strong></td>
<td>One or more subnets behind the remote host, expressed in CIDR notation</td>
</tr>
<tr>
<td></td>
<td>(IP address/mask bits). If multiple subnets are specified, the subnets</td>
</tr>
<tr>
<td></td>
<td>should be separated by a comma.</td>
</tr>
<tr>
<td><strong>Local Id</strong></td>
<td>How the SLC console manager should be identified for authentication. The</td>
</tr>
<tr>
<td></td>
<td>Id is used by the remote host to select the proper credentials for</td>
</tr>
<tr>
<td></td>
<td>communicating with the SLC device.</td>
</tr>
<tr>
<td><strong>Local Hop/Router</strong></td>
<td>If the SLC console manager is behind a gateway, this specifies the IP</td>
</tr>
<tr>
<td></td>
<td>address of the gateway's public network interface.</td>
</tr>
<tr>
<td><strong>Local Subnet(s)</strong></td>
<td>One or more subnets behind the SLC unit, expressed in CIDR notation (IP</td>
</tr>
<tr>
<td></td>
<td>address/mask bits). If multiple subnets are specified, the subnets should</td>
</tr>
<tr>
<td></td>
<td>be separated by a comma.</td>
</tr>
<tr>
<td><strong>IKE Negotiation</strong></td>
<td>The Internet Key Exchange (IKE) protocol is used to exchange security</td>
</tr>
<tr>
<td></td>
<td>options between two hosts who want to communicate via IPSec. The first</td>
</tr>
<tr>
<td></td>
<td>phase of the protocol authenticates the two hosts to each other and</td>
</tr>
<tr>
<td></td>
<td>establishes the Internet Security Association Key Management Protocol</td>
</tr>
<tr>
<td></td>
<td>Security Association (ISAKMP SA). The second phase of the protocol</td>
</tr>
<tr>
<td></td>
<td>establishes the cryptographic parameters for protecting the data passed</td>
</tr>
<tr>
<td></td>
<td>through the tunnel, which is the IPSec Security Association (IPSec SA). The</td>
</tr>
<tr>
<td></td>
<td>IPSec SA can periodically be renegotiated to ensure security. The IKE</td>
</tr>
<tr>
<td></td>
<td>protocol can use one of two modes: Main Mode, which provides identity</td>
</tr>
<tr>
<td></td>
<td>protection and takes longer, or Aggressive Mode, which provides no identity</td>
</tr>
<tr>
<td></td>
<td>protection but is quicker. With Aggressive Mode, there is no negotiation</td>
</tr>
<tr>
<td></td>
<td>of which cryptographic parameters will be used; each side must give the</td>
</tr>
<tr>
<td></td>
<td>correct cryptographic parameters in the initial package of the exchange,</td>
</tr>
<tr>
<td></td>
<td>otherwise the exchange will fail. If Aggressive Mode is used, the **IKE</td>
</tr>
<tr>
<td></td>
<td>Encryption, IKE Authentication, and IKE DH Group must be specified.</td>
</tr>
<tr>
<td><strong>IKE Encryption</strong></td>
<td>The type of encryption, <strong>3DES</strong> or <strong>AES</strong>, used for IKE negotiation. <strong>Any</strong></td>
</tr>
<tr>
<td></td>
<td>can be selected if the two sides can negotiate which type of encryption to</td>
</tr>
<tr>
<td></td>
<td>use.</td>
</tr>
<tr>
<td><strong>Authentication (Ike)</strong></td>
<td>The type of authentication, <strong>SHA1</strong> or <strong>MD5</strong>, used for IKE negotiation. <strong>Any</strong></td>
</tr>
<tr>
<td></td>
<td>can be selected if the two sides can negotiate which type of authentication</td>
</tr>
<tr>
<td></td>
<td>to use.</td>
</tr>
<tr>
<td><strong>DH Group (Ike)</strong></td>
<td>The Diffie-Hellman Group, <strong>2</strong> or <strong>5</strong>, used for IKE negotiation. <strong>Any</strong></td>
</tr>
<tr>
<td></td>
<td>can be selected if the two sides can negotiate which Diffie-Hellman Group</td>
</tr>
<tr>
<td></td>
<td>to use.</td>
</tr>
<tr>
<td><strong>ESP Encryption</strong></td>
<td>The type of encryption, <strong>3DES</strong> or <strong>AES</strong>, used for encrypting the data</td>
</tr>
<tr>
<td></td>
<td>sent through the tunnel. <strong>Any</strong> can be selected if the two sides can</td>
</tr>
<tr>
<td></td>
<td>negotiate which type of encryption to use.</td>
</tr>
<tr>
<td><strong>Authentication (Ike)</strong></td>
<td>The type of authentication, <strong>SHA1</strong> or <strong>MD5</strong>, used for authenticating data</td>
</tr>
<tr>
<td></td>
<td>sent through the tunnel. <strong>Any</strong> can be selected if the two sides can</td>
</tr>
<tr>
<td></td>
<td>negotiate which type of authentication to use.</td>
</tr>
</tbody>
</table>
To save, click **Apply** button.

4. To see the details of the VPN tunnel connection, including the cryptographic algorithms used, select the **View Detailed Status** link.

5. To see the last 100 lines of the logs associated with the VPN tunnel, select the **View VPN Logs** link.

6. To see the RSA public key for the SLC console manager (required for configuring the remote host if RSA Public Keys are being used), select the **View SLC RSA Public Key** link.
7: Services

System Logging and Other Services

Use the Services > SSH/Telnet/Logging page to:

- Configure the amount of data sent to the logs.
- Enable or disable SSH and Telnet logins.
- Enable a Simple Network Management Protocol (SNMP) agent.

Note: The SLC console manager supports both MIB-II (as defined by RFC 1213) and a private enterprise MIB. The private enterprise MIB provides read-only access to all statistics and configurable items provided by the SLC unit. It provides read-write access to a select set of functions for controlling the SLC device and device ports. See the MIB definition file for details.

- 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 managers on the Secure Lantronix network.
- Set the date and time.

SSH/Telnet/Logging

To configure SSH, Telnet, and Logging settings:

1. Click the Services tab and select the SSH/Telnet/Logging option. The following page displays.
Figure 7-1 Services > SSH/Telnet/Logging

2. Enter the following settings:

**System Logging**

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

- **Off**: Disables this type of logging.
- **Error**: Saves messages that are output because of an error.
- **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.
- **Info**: Saves informative message, in addition to warning and error messages.
- **Debug**: Saves extraneous detail that may be helpful in tracking down a problem, in addition to information, warning, and error messages.

<table>
<thead>
<tr>
<th>Network Level</th>
<th>Messages concerning the network activity, for example about Ethernet and routing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>Messages concerning services such as SNMP and SMTP.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Messages concerning user authentication.</td>
</tr>
<tr>
<td>Device Ports</td>
<td>Messages concerning device ports and connections.</td>
</tr>
</tbody>
</table>

2. Enter the following settings:
Diagnostics | Messages concerning system status and problems.
--- | ---
General | Any message not in the categories above.
Remote Servers (#1 and #2) | IP address of the remote server(s) where system logs are stored. The system log is always saved to local SLC storage. It is retained through SLC unit 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.

### 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 console manager reboots.
--- | ---
**Size** | The log has a default maximum size of 50 Kbytes (approximately 500 entries). You can set the maximum size of the log from 1 to 500 Kbytes.
--- | ---
**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** | If enabled, the contents of the audit log are added to the system log (under the General/Info category/level). Disabled by default.

### 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.

### SSH

**Enable Logins** | Enables or disables SSH logins to the SLC unit 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 - Settings (on page 94) 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** | If you enable SSH logins, you can cause an idle connection to disconnect after a specified number of minutes. Select Yes and enter a value of from 1 to 30 minutes.
*Note:* You must reboot the unit before a change will take effect.
--- | ---
**SSH Port** | Allows you to change the SSH login port to a different value in the range of 1 - 65535. The default is 22.
*Note:* You must reboot the unit before a change will take effect.
--- | ---
**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 Network > Network Settings page. Also, you must reboot the SLC 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 - Settings (on page 94) 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** | If you enable Telnet logins, you can cause an idle connection to disconnect after a specified number of minutes. 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. |

### Web SSH/Web Telnet Settings

| **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. |

### Phone Home

| **Enable** | If enabled, allows SLC unit to directly contact an SLM and request addition to the database |
| **IP Address** | IP address of the SLM unit. |
| **Last Attempt** (view only) | Displays the date and time of last connection attempt. |
| **Results** (view only) | Indicates whether the SLC console manager successfully generated a phone home UDP packet. This status is not an acknowledgement of successful receipt by the SLM unit. |

3. To save, click the **Apply** button.
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. The following page displays:

   **Figure 7-2 Services > SNMP**

   - **Enable Agent**: Enables or disables SNMP agent, which allows read-only access to the system. Disabled by default.
   - **Enable Traps**: Allows the agent to generate traps.
   - **Location**: Lomita, CA 93942 USA
   - **Contact**: Technical Support US
   - **Version 3 Security**: 
     - No Authentication
     - Authentication
     - No Encryption
     - Encryption
   - **V3 Read/Write User**
     - **Username**: slc191248
     - **Password**: ************
     - **Re-type Password**: ************
     - **Secret**: ************
     - **Re-type Secret**: ************
   - **V3 Read/Write User**
     - **Username**: slc191248
     - **Password**: ************
     - **Re-type Password**: ************
     - **Secret**: ************
     - **Re-type Secret**: ************

2. Enter the following:
   - **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 unit sends the traps to the host identified in the **NMS** field.

### NMS #1 (or #2)

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 console manager and receive traps from the SLC unit. Enter the IP address of the NMS server. Required if you selected Enable Traps.

### Location

Physical location of the SLC unit (optional). Useful for managing the SLC unit using SNMP. Up to 20 characters.

### Contact

Description of the person responsible for maintaining the SLC console manager, for example, a name (optional). Up to 20 characters.

## Communities

### Read-Only

A string that the ACS 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**.

### Enable v1/v2

If checked, SNMP version 1 and version 2 (which use the Read-Only and Read-Write Communities) is enabled. Uncheck to only allow the more secure version 3 to be used to access the SLC unit via SNMP. The default is enabled.

### Alarm Delay

Number of seconds delay between outgoing SNMP traps.

## Version 3

### Security

Levels of security available with SNMP v. 3.

- **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

<table>
<thead>
<tr>
<th>User Name</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password/Retype</td>
<td>Password for a user with read-only authority to use to access SNMP v3. The default is SNMPPASS. Up to 20 characters.</td>
</tr>
<tr>
<td>Password/Retype</td>
<td>Passphrase associated with the password for a user with read-only authority. Up to 20 characters.</td>
</tr>
</tbody>
</table>

V3 Read-Write User

<table>
<thead>
<tr>
<th>User Name</th>
<th>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 snmpuser. Up to 20 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password/Retype</td>
<td>Password for the user with read-write authority to use to access SNMP v3. The default is SNMPRPWPASS. Up to 20 characters.</td>
</tr>
<tr>
<td>Password/Retype</td>
<td>Passphrase associated with the password for a user with read-write authority. Up to 20 characters.</td>
</tr>
</tbody>
</table>

3. To save, click the Apply button.

SNMP, SSH, Telnet, and Logging Commands

The following CLI commands correspond to the web page entries described above.

To configure services (system logging, SSH and Telnet access, SSH and Telnet timeout, SNMP agent, email (SMTP) server, and audit log):

```
set services <one or more services parameters>
```

Parameters:

- `alarmdelay <1-6000 Seconds>`
- `auditlog <enable|disable>`
- `auditsize <Size in Kbytes>`
  
  Range is 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>`
- `location <Physical Location>`
- `netlog <off|error|warning|info|debug>`
- `nms1 <IP Address or Name>`
- `nms2 <IP Address or Name>`
- `phonehome <enable|disable>`
- `phoneip <IP Address>`
- `portssh <TCP Port>`
- `rocommunity <Read-Only Community Name>`
- `rwcommunity <Read-Write Community Name>`
servlog <off|error|warning|info|debug>
smtptserver <IP Address or Hostname>
snmp <enable|disable>
ssh <enable|disable>
syslogserver1 <IP Address or Name>
syslogserver2 <IP Address or Name>
telnet <enable|disable>
timeoutssh <disable or 1-30>
timeouttelnet <disable or 1-30>
traps <enable|disable>
trapcommunity <Trap Community>
v1ssh <enable|disable>
v1v2 <enable|disable>
v3user <V3 RO User>
v3password <V3 RO User Password>
v3phrase <V3 RO User Passphrase>
v3rwuser <V3 RW User>
v3rwpassword <V3 RW User Password>
v3rphrase <V3 RW User Passphrase>
v3security <noauth|auth|authencrypt>
v3auth <md5|sha>
v3encrypt <des|aes>
v3password <Password for v3 auth>
v3user <User for v3 auth>
webssh <enable|disable>
webtelnet <enable|disable>

To view current services:

```
show services
```

**NFS and SMB/CIFS**

Use the Services > NFS/CIFS page if you want to save configuration and logging data onto a remote NFS server, or export configuration 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 unit available for the logging file(s). You may also save SLC configurations on the network server.

Similarly, use SMB/CIFS (Server Message Block/Common Internet File System), Microsoft's file-sharing protocol, to export a directory on the SLC device as an SMB/CIFS share. The SLC unit exports a single read-write CIFS share called "public," with the subdirectory The 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.
To configure NFS and SMB/CIFS:

1. Click the Services tab and select the NFS/CIFS option. The following page displays:

   **Figure 7-3 Services > NFS/CIFS**

   ![Services > NFS/CIFS](image)

   - **NFS Mounts**
     - Remote Directory:
       - #1: 172.19.38.22:/home/glenn/nfs1
       - #2: 172.19.38.22:/home/glenn/nfs2
       - #3: 172.19.38.22:/home/glenn/nfs3
     - Local Directory:
       - /slc Scarborough
     - Read-Write:
       - [ ]
     - Mount:
       - [ ]

   - **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 (172.19.168.61)
       - Eth2 (192.168.1.61)
     - CIFS User Password:
       - [ ]
     - CIFS Password:
       - [ ]
     - Workgroup:
       - workgroup
     - The SMB/CIFS share can be accessed by the 'slicuser' login.

2. Enter the following for up to three directories:

   **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 unit creates the local directory automatically.
   - **Read-Write**
     - If enabled, indicates that the SLC device 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 unit to mount the file to the NFS server. Enabled by default.

3. Enter the following:

   **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 both network ports.
4. To save, click the **Apply** button.

### NFS and SMB/CIFS Commands

The following CLI commands correspond to the web page entries described above.

**To mount a remote NFS share:**

```
set nfs mount <one or more parameters>
```

**Parameters:**

- `locdir <Directory>`
- `mount <enable|disable>`
- `remdir <Remote NFS Directory>`
- `rw <enable|disable>`

*Enables read/write access to remote directory.*

**Note:** The `remdir` and `locdir` parameters are required, but if you specified them previously, you do not need to provide them again.

**To unmount a remote NFS share:**

```
set nfs unmount <1|2|3>
```

**To view NFS share settings:**

```
show nfs
```

**To configure the SMB/CIFS share, which contains the system and device port logs:**

```
set cifs <one or more parameters>
```

**Parameters:**

- `eth1 <enable|disable>`
- `eth2 <enable|disable>`
- `state <enable|disable>`
- `workgroup <Windows workgroup>`

*Note:* The `admin config` command saves SLC configurations on the SMB/CIFS share.

**To change the password for the SMB/CIFS share login (default is cifsuser):**

```
set cifs password
```

**To view SMB/CIFS settings:**

```
show cifs
```
Secure Lantronix Network

Use the **Secure Lantronix Network** option to view and manage Secure Lantronix Managers and 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 access Secure Lantronix Managers and Spider devices on the local network:**

1. Click the **Services** tab and select the **Secure Lantronix Network** option. The following page displays.

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.
To directly access the CLI interface for a device:

1. Click the **SSH** or **Telnet** link in the SSH/Telnet to CLI column directly beside the port you would like to access. A ssh or telnet popup window appears depending on what is clicked.

![Telnet Session](image)

To configure how Secure Lantronix devices are searched for on the network:

1. Click the **Search Options** link on the top right of the **Services > Secure Lantronix Network** page. The following web page displays:
2. Enter the following:

<table>
<thead>
<tr>
<th>Secure Lantronix Network Search</th>
<th>Select the type of search you want to conduct.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Local Subnet performs a broadcast to detect Secure Lantronix devices on the local subnet.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Both is the default selection.</td>
</tr>
</tbody>
</table>

**IP Address**

If you selected Manually Entered IP Address List or Both, enter the IP address of the Secure Lantronix 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 **Services > Secure Lantronix Network** page displays the Secure Lantronix devices resulting from the search. You can now manage these devices.

**Secure Lantronix Network Commands**

The following commands for the command line interface correspond to the web page entries described above.

To detect and view all SLC console manager or user-defined IP addresses on the local network:

```
set slcnetwork <one or more parameters>
```

**Parameters:**

- add <IP Address>
- delete <IP Address>
- search <localsubnet|ipaddrlist|both>
To detect and display all secure Lantronix managers and Spider devices on the local network:

```
show slcnetwork [ipaddrlist <all|Address Mask>]
```

**Note:** Without the `ipaddrlist` parameter, the command searches the network according to the search setting. 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).

**Date and Time**

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

**To set the local date, time, and time zone:**

1. Click the **Services** tab and select the **Date & Time** option. The following page displays:

   ![Figure 7-7  Services > Date & Time](image)

   **Change Date/Time**
   - **Date:** Select the current month, day, and year.
   - **Time:** Select the current hour, minute, and second.
   - **Time Zone:** Select the time zone.

   **Enable NTP:** Check to enable NTP synchronization.

   **Current NTP Status:**
   - **remote:**
   - **reloid:**
   - **st:**
   - **t:**
   - **when reach:**
   - **delay:**
   - **offset:**
   - **jitter:**

   **Synchronize With:**
   - **Broadcast from NTP Server**
   - **Peer NTP Server(s)**
   - **Local:**
   - **Public:**

2. Enter the following:

   **Change Date/Time** Select the checkbox to manually enter the date and time at the SLC device’s location.

   **Date** From the drop-down lists, select the current month, day, and year.
3. To save, click the **Apply** button.

**To synchronize the SLC unit with a remote timeserver using NTP:**

1. Enter the following:

<table>
<thead>
<tr>
<th>Enable NTP</th>
<th>Select the checkbox to enable NTP synchronization. NTP is disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize via</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Broadcast from NTP Server:</strong> Enables the SLC console manager to accept time information periodically transmitted by the NTP server. This is the default if you enable NTP.</td>
</tr>
<tr>
<td></td>
<td><strong>Poll NTP Server:</strong> Enables the SLC unit to query the NTP Server for the correct time. If you select this option, complete one of the following:</td>
</tr>
<tr>
<td></td>
<td>&gt; <strong>Local:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>&gt; <strong>Public:</strong> 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 <a href="http://www.ntp.org">www.ntp.org</a> 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.</td>
</tr>
</tbody>
</table>

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

**Date and Time Commands**

The following CLI commands correspond to the web page entries described above.

**To set the local date, time, and local time zone (one parameter at a time):**

```plaintext
set datetime <one date/time parameter>
```

**Parameters:**

```plaintext
date <MMDDYYhhmm[ss]>
timezone <Time Zone>
```

**Note:** If you type an invalid time zone, the system guides you through the process of selecting a time zone.

**To view the local date, time, and time zone:**

```plaintext
show datetime
```

**To synchronize the SLC console manager with a remote time server using NTP:**

```plaintext
set ntp <one or more ntp parameters>
```

**Parameters:**

```plaintext
localserver1 <IP Address or Hostname>
localserver2 <IP Address or Hostname>
```
To view NTP settings:

```plaintext
show ntp
```

## 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 units.

### To configure the Web Server:

1. Click the **Services** tab and select the **Web Server** option. The following page appears:

   ![Web Server Page](image-url)

   **Figure 7-8  Services  > Web Server**

   - **Timeout**: (Yes, minutes (5-120)) 30
   - **Enable iGoogle Gadget Web Content**: 
   - **Allow SSLv2 Protocol**: (in addition to SSLv3/TLSv1)
   - **Cipher**: High (256, 168, 128), Medium (128), Low (64, 56)
   - **Group Access**: 
   - **Banner**:

   **Note**: Changing Protocol or Cipher requires a reboot.

   **Network Interfaces**: ETH1 ETH2 PPP

   [Apply]
2. Enter the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Timeout**                  | - **Select No** to disable Timeout.  
                              - **Select Yes, minutes (5-120)** to enable timeout.  
                              Enter the number of minutes (must be between 30 and 120 minutes) after which the SLC web session times out. The default is 5.  
                              
                              *Note:* If a session times out, refresh the browser page and login to a new web session.                                           |
| **Enable iGoogle Gadget**    | Select the check box to enable an SLC iGoogle gadget. The iGoogle gadget allows an iGoogle user to view the port status of many SLC units on one web page.  
                              (See iGoogle Gadgets on page 88.)                                                                                                     |
| **Web Content**              |                                                                                                                                              |
| **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. |
| **Group Access**             | If undefined, any group can access the web. If one or more groups are specified (groups are delimited by the characters ‘,’ (comma) or ‘;’ (semicolon)), then any user who logs into the web must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the SLC or SLB unit. A group provided by a remote server must be either a single group or multiple groups delimited by the characters ‘,’ (comma), ‘;’ (semicolon), or ‘=' (equals) - for example "group=group1,group2;" or "group1,group2,group3". |
| **Banner**                   | The text to display on the web manager home page after the user logs in. May contain up to 1024 characters (single quote and double quote characters are not supported). Blank by default.  
                              *Note:* To create additional lines in the banner use the \n character sequence.                                                  |
| **Network Interfaces**       | The interfaces that the web server is available on. By default, Eth1, Eth2 and PPP interfaces on modems are enabled.                          |
| **Web Sessions**             | Click the Web Sessions link to view or terminate a web session. (See Services - Web Sessions on page 85.)                                      |
| **SSL Certificate**          | Click the SSL Certificate link to view, import or reset the SSL Certificate. ()                                                             |

3. Click the **Apply** button to save.

**Admin Web Commands**

The following CLI commands correspond to the webg page entries described above.

To configure the timeout for web sessions:

```
admin web timeout <disable|5-120 minutes>
```

To configure the web server to use SSLv2 in addition to SSLv3 and TLSv1:

```
admin web protocol <sslv2|nossalv2>
```
To configure 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 cipher <himed|himedlow>

To enable or disable iGoogle Gadget web content:
admin web gadget <enable|disable>

To configure the group that can access the web:
admin web group <Local or Remote Group Name>

To configure the banner displayed on the web home page:
admin web banner <Banner Text>

To define a list of network interfaces the web is available on:
admin web iface <none,eth1,eth2,ppp>

To terminate a web session:
admin web terminate <Session ID>

To view the current sessions and their ID:
admin web show

To import an SSL certificate or reset the web server certificate to the default:
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>]
admin web certificate reset
admin web certificate show

admin web show [viewslmsessions <enable|disable>]

Services - Web Sessions

The Services > Web Server page enables you to view and terminate current web sessions.

To view or terminate current web sessions:

1. On the Services tab, click the Web Server page and click the Web Sessions link to the right. The following page displays:
2. To terminate, click the check box in the row of the session you want to terminate.

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

**Services - SSL Certificate**

The Services > Web Server page enables you to view and update SSL certificate information. The SSL certificate, consisting of a public/private key pair used to encrypt HTTP data, is associated with the web server. You can import a site-specific SSL certificate, if desired.

**To view, reset, import, or change an SSL Certificate:**

1. On the Services tab, click the Web Server page and click the SSL Certificate link. The following page displays the current SSL certificate.
2. If desired, enter the following:

- **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**: From the drop-down list, select the method of importing the certificate (SCP or SFTP). The default is **SCP**.
- **Certificate Filename**: Filename of the certificate.
- **Key Filename**: Filename of the private key for the certificate.
- **Passphrase / Retype Passphrase**: Enter the passphrase associated with the SSL certificate if the private key is encrypted protected with a passphrase.
- **Host**: Host name or IP address of the host from which to import the file.
- **Path**: Path of the directory where the certificate 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.
Note: You must reboot the SLC console manager for the update to take effect.

4. To return to the Services > Web Server page, click the Back to Web Server link.

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

- admin web certificate
- admin web certificate reset
- admin web cipher
- admin web gadget
- admin web protocol
- admin web timeout
- admin web terminate
- admin web show

iGoogle Gadgets
You can create an iGoogle gadgets that enables you to view the status of the ports of many SLCs on one web page.

Anyone with a Google email account (gmail.com) can create an iGoogle gadget for viewing web pages. There are two types of iGoogle gadgets: public gadgets and private gadgets. The public gadgets are listed for import on iGoogle web pages. The SLC gadget is a private gadget, whose location is not publicly advertised.

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
<?xml version="1.0" encoding="UTF-8" ?>
- <Module>
  <ModulePrefs title="__UP_model__ Devport Status" title_url="http://www.lantronix.com"
    directory_title="SLC 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="SLC" display_value="SLC" />
  </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" />
```
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.
You should see an iGoogle gadget similar to the following:

**Figure 7-11  iGoogle Gadget Example**

![iGoogle Gadget Example](image)
8: **Device Ports**

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

### 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 in to the command line interface. At the command line interface, issue the connect direct or connect listen commands.

2. If Telnet is enabled for a device port, Telnet to <Eth1 IP address>:<telnet port number> or <Eth2 IP address>:<telnet port number>, where 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>, where 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 <Eth1 IP address>:<tcp port number> or <Eth2 IP address>:<tcp port number>, where tcp port number is uniquely assigned for each device port.

6. Connect a terminal or a terminal emulation program directly to the device port. If logins are enabled, the user is prompted for a username and password and logs in to 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:

1. **Direct (or data) mode**: The user can interact with and monitor the device port (connect direct command).

2. **Listen mode**: The user can only monitor the device port (connect listen command).

3. **Clear mode**: The user can clear the contents of the device port buffer (set locallog <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 *Devices > Device Status* page displays the status of the SLC console manager's ports, and power outlets.

1. Click the **Devices** tab and select the **Device Status** option. The following page displays:

**Figure 8-1 Devices > Device Status**

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>DSR</th>
<th>Bytes</th>
<th>Input/Output</th>
<th>Errors</th>
<th>Connection Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>StdPort.1</td>
<td>Yes</td>
<td>1391306596</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>2</td>
<td>StdPort.2</td>
<td>Yes</td>
<td>650084724</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>3</td>
<td>StdPort.3</td>
<td>Yes</td>
<td>2772519774</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>4</td>
<td>StdPort.4</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>5</td>
<td>Port-6</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>6</td>
<td>Port-8</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>7</td>
<td>Port-10</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>8</td>
<td>Port-11</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>9</td>
<td>Port-12</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>10</td>
<td>Port-13</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>11</td>
<td>Port-14</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>12</td>
<td>Port-15</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>13</td>
<td>Port-16</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>14</td>
<td>Port-17</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>15</td>
<td>Port-18</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>16</td>
<td>Port-19</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>17</td>
<td>Port-20</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>18</td>
<td>Port-21</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>19</td>
<td>Port-22</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>20</td>
<td>Port-23</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>21</td>
<td>Port-24</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>22</td>
<td>Port-25</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>23</td>
<td>Port-26</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>24</td>
<td>Port-27</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>25</td>
<td>Port-28</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>26</td>
<td>Port-29</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>27</td>
<td>Port-30</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>28</td>
<td>Port-31</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
<tr>
<td>29</td>
<td>Port-32</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Live</td>
</tr>
</tbody>
</table>
Device Port Settings

On the Devices > Device Ports page, you can set up the numbering of Telnet, SSH, and TCP ports, view a summary of current port modes, establish the maximum number of direct connections for each device port, and select individual ports to configure.

1. Click the Devices tab and select the Device Ports option. The following page displays:

**Figure 8-2 Devices > Device Ports**

Current port numbering schemes for Telnet, SSH, and TCP ports display on the left. The list of ports 1-16 on the right includes the individual ports and their current mode.

**Note:** For units with more ports, click the buttons above the table to view additional ports.

Icons that represent some of the possible modes include:

- **Idle** The port is not in use.
  - The port is in data/text mode.
  - **Note:** You may set up ports to allow Telnet access using the IP Setting per Device Ports - Settings (on page 94).

- 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 (a user has logged in).
To set up Telnet, SSH, and TCP port numbering:

1. Enter the following:

**Telnet/SSH/TCP in Port Numbers**

<table>
<thead>
<tr>
<th>Starting Telnet Port</th>
<th>Each port is assigned a number for connecting via Telnet. Enter a number (1025-65528) 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting SSH Port</td>
<td>Each port is assigned a number for connecting via SSH. Enter a number (1025-65528) 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.</td>
</tr>
<tr>
<td>Starting TCP Port</td>
<td>Each port is assigned a number for connecting through a raw TCP connection. Enter a number (1025-65528) 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 situations where a TCP/IP connection is to communicate 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.</td>
</tr>
</tbody>
</table>

*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).

2. Click the **Apply** button to save the settings.

**To set limits on direct connections:**

1. Enter the maximum number (1-10) of simultaneous direct connections for each device port. The default is 1.

2. Click the **Apply** button to save the settings.

**To configure a specific port:**

1. You have two options:
   - Select the port from the ports list and click the **Configure** button. The Device Ports > Settings page for the port displays.
   - Click the port number on the green bar at the top of each page.

2. Continue with directions in the section, Device Ports - Settings (on page 94).

**Global Commands**

The following CLI commands correspond to the web page entries described above.

**To configure settings for all or a group of device ports:**

```
set deviceport global <one or more parameters>
```
Parameters:

sshport <TCP Port>
tcpport <TCP Port>
telnetport <TCP Port>

*Port is a port number between 1025 and 65528.*

To view global settings for device ports:

show deviceport global

Device Ports - Settings

On the *Device Ports > Settings* page, configure IP and data (serial) settings for individual ports, and if the port connects to an external modem, modem settings as well.

To open the *Device Ports - Settings* page:

1. You have two options:
   - In the *Device Ports List* page (described in the previous section), select the port from the ports list and click the *Configure* button.
   - Click the desired port number in the green bar (shown below) at the top of any page:

   ![Figure 8-3 Device Ports List](image)

   The following page displays:
Figure 8-4  Device Ports > Settings

Device Ports - Settings

Data Settings
- Baud: 9600
- Data Bits: 8
- Stop Bits: 1
- Parity: None
- Flow Control: RTS/CTS
- Enable DTR: Yes
- Max Direct Connects: 1
- Show Lines On Connecting: Yes, # of lines: 24

Hardware Signal Triggers
- Check DSR on Connect: No
- Disconnect on DSR: No

Port Status and Counters
- DSR/CD: No
- DTR: Yes
- CTS: No
- RTS: Yes
- Synch input: 0
- Synch output: 0
- Framing errors: 0
- Parity errors: 0
- Overrun errors: 0
- Flow Control errors: 0
- Seconds since zeroed: 11:34

IP Settings
- Telnet In: Yes, timeout: 600
- SSH In: Yes, timeout: 600
- TCP In: Yes, timeout: 600
- IP Address/Netmask Bits: 24
- Web SSM/Resize Column: 80
- Rows: 24

Modem Settings
- State: Disabled
- PPP Logging: No
- Use Sites: None
- Initialization Script: None
- Dial-back Number: None
- Dial-back Delay: 15 seconds
- Dial-back Retries: 3

Text Mode
- Timeout Digits: No, timeout: 30 minutes
- Dial-in Host List: None

PPP Mode
- Negotiate IP Address: Yes
- Local IP: None
- Remote IP: None
- Authentication: PAP, CHAP
- CHAP Handshake: None
- CHAP Auth User: None
- Same authentication for Dial-in & Dial-out (DDC): None
- Dial-in Authentication: None
- Dial-out Authentication: None
- Secret User Password: None
- Enable NAPT: No
- Dial-out Number: None
- Remote/Dial-out Login: None
- Remote/Dial-out Password: None
- RDP: None
- Restart Delay: 20 seconds
- CPSEC Server: None
- Allow No Callback: None
- CPSEC Client Type: Admin-defined Number

Apply
- Apply Settings: None
- to Device Ports: None

Notes: In addition to applying settings to the currently selected Device Port, all or some of these settings can also be applied to other Device Ports.
2. Enter the following:

**Device Port Settings**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays number of port; displays automatically.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>The status of the port; displays automatically.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the port. Valid characters are letters, numbers, dashes (-), periods, and underscores (_).</td>
</tr>
<tr>
<td>Group Access</td>
<td>If undefined, any group can access the device port. If one or more groups are specified (groups are delimited by the characters ' ' (space), ',' (comma), or ';' (semicolon)), then any user who logs into the device port must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the SLC unit. A group provided by a remote server must be either a single group or multiple groups delimited by the characters ' ' (space), ',' (comma), ',' (semicolon), or '=' (equals) - for example &quot;group=group1,group2,&quot; or &quot;group1,group2,group3&quot;.</td>
</tr>
<tr>
<td>Banner</td>
<td>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.</td>
</tr>
<tr>
<td>Break Sequence</td>
<td>A series of one to ten 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.</td>
</tr>
<tr>
<td>View Port Log Seq</td>
<td>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 (\x1bV).</td>
</tr>
<tr>
<td>View Port Log</td>
<td>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.</td>
</tr>
<tr>
<td>Zero Port Counters</td>
<td>Resets all of the numerical values in the Port Counters table at the bottom of the page to zero (0).</td>
</tr>
<tr>
<td>Logging</td>
<td>Click the Settings link to configure file logging, email logging, and local logging.</td>
</tr>
<tr>
<td>Connected to</td>
<td>The type of device connected to the device port. Presently, the SLC console manager supports Lantronix’s Secure Lantronix Remote Power Manager (SLP8 and SLP16), SserverTech CDUs and Sensorsoft devices. If the type of device is not listed, select undefined. If you select anything other than undefined, click Device Commands. The appropriate web page displays.</td>
</tr>
</tbody>
</table>

**IP Settings**

| Telnet In | Enables access to this port through Telnet. Disabled by default. |
| SSH In | Enables access to this port through SSH. Disabled by default. |
| TCP in | Enables access to this port through a raw TCP connection. Disabled by default:  
**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). |
| Port | Automatically assigned Telnet, SSH, and TCP port numbers. You may override this value, if desired. |
### Data Settings

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td>If selected, the SLC unit requires user authentication before granting access to the port. <strong>Authenticate</strong> is selected by default for Telnet in and SSH in, but not for TCP in.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>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 no timeout.</td>
</tr>
<tr>
<td><strong>Seconds</strong></td>
<td>Number of seconds before a timeout.</td>
</tr>
<tr>
<td><strong>IP Address /Netmask Bits</strong></td>
<td>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. The optional netmask bits specify the netmask to use for the IP address. For example, for a netmask of 255.255.255.0 specify 24 bits. If the netmask bits are not specified, a default netmask used for the class of network that the IP address falls in will be used. 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. <strong>Note:</strong> If Ethernet Bonding is enabled, assigning individual IP Addresses to Device Ports is not supported. Note that the IP address will be bound to Eth1 only, so if Eth2 is connected and configured, and Eth1 is not, this feature will not work.</td>
</tr>
<tr>
<td><strong>Web SSH/Telnet Columns</strong></td>
<td>Number of columns in the Web SSH/Telnet applet when this device port is accessed via the applet.</td>
</tr>
<tr>
<td><strong>Rows</strong></td>
<td>Number of rows in the Web SSH/Telnet applet when this device port is accessed via the applet.</td>
</tr>
<tr>
<td><strong>Baud</strong></td>
<td>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 the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate.</td>
</tr>
<tr>
<td><strong>Data Bits</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Stop Bits</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Parity</strong></td>
<td>Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is none.</td>
</tr>
<tr>
<td><strong>Flow Control</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enable Logins</strong></td>
<td>For serial devices connected to the device port, displays a login prompt and authenticates users. Successfully authenticated users are logged into the command line interface. The default is disabled. This is the correct setting if the device port is the endpoint for a network connection.</td>
</tr>
<tr>
<td><strong>Max Direct Connects</strong></td>
<td>Enter the maximum number (1-10) of simultaneous connections for the device port. The default is 1.</td>
</tr>
</tbody>
</table>
### Show Lines on Connecting

If enabled, when the user either does a connect direct from the CLI or connects directly to the port using Telnet or SSH, the SLC console manager outputs up to 24 lines of buffered data as soon as the serial port is connected.

For example, an SLC user issues a connect direct device 1 command to connect port 1 to a Linux server.

Then the SLC user ls command to display a directory on the Linux server, then exits the connection. When the SLC user issues another direct connect device 1, the last 24 lines of the ls command is displayed so the user can see what state the server was left in.

### Hardware Signal Triggers

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check DSR on Connect</td>
<td>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 transitioning to, when a connection attempt is made. Disabled by default unless dial-in, dial-out, or dial-back is enabled for the device port.</td>
</tr>
<tr>
<td>Disconnect on DSR</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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, dial-back & dial-on-demand, or dial-in/host list. For more information on the different dialing types, see *Modem Dialing States (on page 136)*. Disabled by default.

**Mode**

The format in which the data flows back and forth:

- **Text**: In this mode, the SLC unit 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 in dial-out mode (e.g., the SLC console manager connects to an external network), dial-in mode (e.g., the external computer connects to the network that the SLC device is part of), or dial-on-demand.

**Use Sites**

Enables the use of site-oriented modem parameters which can be activated by various modem-related events (authentication, outbound network traffic for dial-on-demand connections, etc.). Sites can be used with the following modem states: dial-in, dial-back, dial-on-demand, dial-in & dial-on-demand, dial-back & dial-on-demand, and CBCP server.

**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 device 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. For information on **AT** commands, refer to the modem user guide, or do a web search for **at command set**.
### 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 console manager 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 unit 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/User Name** (for UNIX systems) or **Secret/User Password** (for Windows systems) used for CHAP authentication. May have up to 128 characters.
3. To save settings for just this port, click the **Apply** button.

4. To save selected settings to ports other than the one you are configuring:
   - From the **Apply Settings** drop-down box, select none, a group of settings, or All.
   - 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.

<table>
<thead>
<tr>
<th>Device Ports</th>
<th>Description</th>
</tr>
</thead>
</table>
| **CHAP Auth Uses** | Select the method of CHAP Authorization:  
  - Through the CHAP Host user name and password established under CHAP Handshake.  
  - Through the username and password established under Local/Remote User database. |
| **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/User Name 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 ) basis. Users dialing into the SLC unit access the network connected to Eth1 and/or Eth2.  
  **Note:** IP forwarding must be enabled on the Network > Network Settings page for NAT to work. See Chapter 6: Basic Parameters on page 52. |
| **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. |
| **Remote/Dial-out Login** | User ID for authentication when dialing out to a remote system, or if a remote system requests authentication from the SLC when it dials in. May have up to 32 characters. |
| **Remote/Dial-out Password** | Password for authentication when dialing out to a remote system, or if a remote system requests authentication from the SLC when it dials in. May have up to 64 characters. |
| **Retype** | Re-enter remote/dial-out 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. |
| **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. |
Port Status and Counters

Port Counters describe 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.

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.

<table>
<thead>
<tr>
<th>Table 8-5 Port Status and Counters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Status and Counters</td>
</tr>
<tr>
<td>DSR/CD</td>
</tr>
<tr>
<td>DTR</td>
</tr>
<tr>
<td>CTS</td>
</tr>
<tr>
<td>RTS</td>
</tr>
<tr>
<td>Bytes input</td>
</tr>
<tr>
<td>Bytes output</td>
</tr>
<tr>
<td>Framing errors</td>
</tr>
<tr>
<td>Parity errors</td>
</tr>
<tr>
<td>Overrun errors</td>
</tr>
<tr>
<td>Flow Control errors</td>
</tr>
<tr>
<td>Seconds since zeroed</td>
</tr>
</tbody>
</table>

Device Ports - SLP / ServerTech CDU

On the *Device Ports > SLP* page, configure commands to send to a ServerTech CDU, SLP or SLP 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 Port Settings* page, select an SLP, SLPEXP or ServerTech CDU.
2. Click the **Device Commands** link. The following page displays:
To enter SLP commands:

1. Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Outlets</td>
<td>Enter the number of outlets for a ServerTech CDU. This setting is not applicable for an SLP unit.</td>
</tr>
<tr>
<td>Number of Expansion Outlets</td>
<td>Enter the number of outlets for a ServerTech CDU expansion unit. This setting is not applicable for an SLP device.</td>
</tr>
<tr>
<td>Login</td>
<td>User ID for logging into the SLP or ServerTech CDU.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter password for logging into the SLP or ServerTech CDU.</td>
</tr>
<tr>
<td>Retype Password</td>
<td>Re-enter password for logging into the SLP or ServerTech CDU.</td>
</tr>
<tr>
<td>Prompt</td>
<td>Enter the prompt displayed by the SLP unit or ServerTech CDU device. This will default to a typical prompt for an SLP power manager or ServerTech CDU. If you are unable to control the SLP unit or ServerTech CDU device, verify that the prompt is set to the right value.</td>
</tr>
</tbody>
</table>

Status/Info

Note: If there is an SLP and an SLP Expansion chassis, the SLP is Tower A and the Expansion chassis is Tower B. This is also applicable to a or ServerTech CDU.

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. If you select Single Outlet, enter a value of 1-8 for the SLP8 or 1-16 for the SLP16. For the ServerTech CDU, the valid range of outlets is specified by the Number of Outlets setting (for Tower A) or the Number of Expansion Outlets setting (for Tower B).

Click the Outlet Status link to see the status of the selected outlet(s).
Device Port - Sensorsoft Device

Devices made by Sensorsoft are used to monitor environmental conditions.

1. In the Connected to field above the IP Settings section of the Device Port Settings page, select Sensorsoft.

2. Click the Device Commands link. The following page displays:

3. Select a port and enter or view the following information:

- **Dev Port**: Displays the number of the SLC port.
- **Device Port Name**: Displays the name of the SLC port.
- **Temp**: Current temperature (degrees Celsius) on the device the sensor is monitoring.
- **Low Temp**: Enter the temperature (degrees Celsius) permitted on the monitored device below which the SLC console manager sends a trap.
- **High Temp**: Enter the temperature (degrees Celsius) permitted on the monitored device above which the SLC unit sends a trap.
- **Use °F**: Display and set the temperature for this device in degrees Fahrenheit, instead of Celsius, which is the default.
- **Humidity (%)**: Current relative humidity on the device the sensor is monitoring.
4. Click the **Apply** button.

5. To view the status detected by the Sensorsoft, click the **Sensorsoft Status** link to the right of the table.

### Device Port Commands

The following CLI commands correspond to the web page entries described above.

*To configure a single port or a group of ports (for example, set deviceport port 2-5,6,12,15-16 baud 2400):*

```
set deviceport port <Device Port List or Name> <one or more device port parameters>
```

**Parameters:**

- `auth <pap|chap>`
- `banner <Banner Text>`
- `baud <300-115200>`
- `breakseq <1-10 Chars>`
- `calleridcmd <Modem Command String>`
- `calleridlogging <enable|disable>`
- `chapauth <chaphost|localusers>`
- `chaphost <CHAP Host or User Name>`
- `chapsecret <CHAP Secret or User Password>`

*The user defines the secret.*

- `checkdsr <enable|disable>`
- `closedsr <enable|disable>`
- `databits <7|8>`
- `device <none|slp8|slp16|slp8exp8|slp8exp16|slp16exp8|slp16exp16|sensorsoft|servertech>`
- `dialbackretries <1-10>`
- `dialbackdelay <PPP Dial-back Delay>`
- `dialinlist <Host List for Dial-in>`
- `dialoutnumber <Phone Number>`
- `dialoutlogin <User Login>`
- `dialoutpassword <Password>`
- `dialbacknumber <usernumber|Phone Number>`
- `dodauth <pap|chap>`
- `dodchaphost <CHAP Host or User Name>`
- `dodchapsecret <CHAP Secret or User Password>`
- `flowcontrol <none|xon/xoff|rts/cts>`
- `group <Local or Remote Group Name>`
- `idletimeout <disable|1-9999 seconds>`
- `ipaddr <IP Address>`
- `initscript <Initialization Script>`
A script that initializes a modem.

localipaddr <negotiate|IP Address>
logins <enable|disable>
modemmode <text|ppp>
modemstate <disable|dialout|dialin|dialback|dialondemand|
dialin+dialondemand|dialinhostlist>
modemtimeout <disable|1-9999 seconds>
name <Device Port Name>
nat <enable|disable>
parity <none|odd|even>
remoteipaddr <negotiate|IP Address>
restartdelay <PPP Restart Delay>
showlines <enable|disable>
sshauth <enable|disable>
sshin <enable|disable>
sshort <TCP Port>
stopbits <1|2>
tcpauth <enable|disable>
tcpin <enable|disable>
tcpport <TCP Port>
telnetauth <enable|disable>
telnetin <enable|disable>
telnetport <TCP Port>
timeoutlogins <disable or 1-30>
usesites <enable|disable>
webcolumns <Web SSH/Telnet Cols>
webrows <Web SSH/Telnet Rows>

To view the settings for one or more device ports:

show deviceport port <Device Port List or Name>

To view a list of all device port names:

show deviceport names

To view the modes and states of one or more device port(s):

Note: You can optionally email the displayed information.

show portstatus [deviceport <Device Port List or Name>] [email <Email Address>]

To view device port statistics and errors for one or more ports:

Note: You can optionally email the displayed information.

show portcounters [deviceport <Device Port List or Name>] [email <Email Address>]

To zero the port counters for one or more device ports:

show portcounters zerocontainers <Device Port List or Name>
Device Commands

The following CLI commands correspond to the web page entries described above.

To send 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, ServerTech CDU and Sensorsoft devices.

```
set command
```

**Syntax**

```
set command <Device Port # or Name or List> <one or more parameters>
```

**Parameters**

```
slp|servertech auth login <User Login>
Establishes the authentication information to log into the SLP or ServerTech CDU attached to the device port.
```

```
slp|servertech restart
Issues the CLI command the SLP or ServerTech CDU uses to restart itself.
```

```
slp|servertech outletcontrol state <on|off|cyclepower> [outlet <Outlet #>][tower <A|B>]
Outlet # is 1-8 for SLP8 and 1-16 for SLP16. For the ServerTech CDU, the valid range of outlets is specified by the number of outlets settings (for Tower A) or number of expansion outlets settings (for Tower B) - see below.
The outletcontrol parameters control individual outlets.
```

```
slp|servertech outletstate [outlet <Outlet #>][tower <A|B>]
The outletstate parameter shows the state of all outlets or a single outlet.
```

```
slp|servertech envmon
Displays the environmental status (e.g., temperature and humidity) of the SLP or ServerTech CDU.
```

```
slp|servertech infeedstatus
Displays the infeed status and load of the SLP or ServerTech CDU.
```

```
slp|servertech system
Displays the system configuration information, such as firmware, revision and uptime.
```

```
slp|servertech config [prompt <Command Prompt>]
Enter the prompt displayed by the SLP or ServerTech CDU device. This will default to a typical prompt for an SLP or ServerTech CDU. If you are unable to control the SLP or ServerTech CDU device, verify that the prompt is set to the right value.
```

```
[numoutlets <Number of Outlets>]
[numexpoutlets <Number of Expansion Outlets>]
Enter the number of outlets for a ServerTech CDU main unit or the number of outlets for a Server Tech CDU expansion unit. This setting is not applicable for an SLP.
```

```
sensorsoft lowtemp <Low Temperature in C.>
```

```
Sets the lowest temperature permitted for the port.
sensorsoft hightemp <High Temperature in C.>

Sets the highest temperature permitted for the port.
sensorsoft lowhumidity <Low Humidity %>

Sets the lowest humidity permitted for the port.
sensorsoft highhumidity <High Humidity %>

Sets the lowest humidity permitted for the port.
sensorsoft traps <enable|disable>

Enables or disables temperature settings as celsius or fahrenheit.
sensorsoft degrees <celsius|fahrenheit>

Enables or disables traps when specified conditions are met.
sensorsoft status

Displays the status of the port.

Interacting with a Device Port

Once a device port has been configured and connected to an external device such as the console port of an external server, the data received over the device port can be monitored at the command line interface with the connect listen command, as follows:

To connect to a device port to monitor it:
connect listen deviceport <Port # or Name>

In addition, you can send data out the device port (for example, commands issued to an external server) with the connect direct command, as follows:

To connect to a device port to monitor and/or interact with it, or to establish an outbound network connection:
connect direct <endpoint>

endpoint is one of:

   deviceport <Port # or Name>
   ssh <IP Address> [port <TCP Port>] [<SSH flags>]

   where:

   <SSH flags> is one or more of:
   user <Login Name>
   version <1|2>
   command <Command to Execute>
   tcp <IP Address> port <TCP Port>
   telnet <IP Address> [port <TCP Port>]
   udp <IP Address> port <UDP Port>
   hostlist <Host List>

   Note: To escape from the connect direct command when the endpoint of the command is deviceport, tcp, or udp and return to the command line interface, type the
escape sequence assigned to the currently logged in user. If the endpoint is telnet or SSH, logging out returns the user to the command line prompt.

**Note:** To escape from the connect listen command, press any key.

Setting up a user with an escape sequence is optional. For any NIS, LDAP, RADIUS, Kerberos, or TACACS+ user, or any local user who does not have an escape sequence defined, the default escape sequence is Esc+A.

### 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, or USB port) 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 Devices > Device Ports - Logging 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 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`

#### USB Flash Drive Logging

Data can be logged to a USB flash drive that is loaded into the USB port on the front of the SLC unit (see **USB Port on page 148**). Data logged locally to the SLC device is limited to 256 Kbytes and may be lost in the event of a power loss. Data logged to a USB flash drive 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

PC Card Logging

Data can be logged to a PC card that is loaded into PC card slot on the front of the SLC unit (see PC Cards on page 140). Data logged locally to the SLC device is limited to 256 Kbytes and may be lost in the event of a power loss. Data logged to a PC card 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

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 on page 68). 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 - SLP / ServerTech CDU (on page 101) to set logging parameters on individual ports.

Sylogs 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 on page 68.)

To set logging parameters:

1. In the top section of the Device Port Settings page, click the Settings link in the Logging field. The following page displays:
2. Enter the following:

### Local Logging

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Logging</strong></td>
<td>If you enable local logging, each device port stores 256 Kbytes (approximately 400 screens) of I/O data in a true FIFO buffer. Disabled by default.</td>
</tr>
<tr>
<td><strong>Clear Local Log</strong></td>
<td>Select the checkbox to clear the local log.</td>
</tr>
<tr>
<td><strong>View Local Log</strong></td>
<td>Click this link to see the local log in text format.</td>
</tr>
</tbody>
</table>

### Email/SNMP Traps

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email/Traps</strong></td>
<td>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 Chapter 7: Services on page 68) when alert criteria are met. Disabled by default.</td>
</tr>
<tr>
<td><strong>Send</strong></td>
<td>If you enabled email and SNMP logging, select what type of notification log to send:</td>
</tr>
<tr>
<td></td>
<td>• Email (default)</td>
</tr>
<tr>
<td></td>
<td>• SNMP Trap</td>
</tr>
<tr>
<td></td>
<td>• Both</td>
</tr>
</tbody>
</table>

---

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

---

**NFS Log to View**: **Most Recent**

**Directory to Log to**: **select one**

**Max Number of Files**: 10

**Max Size of Files**: 2048 bytes

---

**USB Log to View**: **Most Recent**

**Log to**: **Part 01**

**Max Number of Files**: 10

**Max Size of Files**: 2048 bytes

---

**Syslog Logging**: **on**

**Apply settings to Device Ports**: **on**

**Notes**: In addition to applying settings to the currently selected Device Port, the settings can also be applied to other Device Ports.
### 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 the SLC unit’s performance, particularly when regular expressions are used.

### Byte Threshold
The number of bytes of data the port receives before the SLC console manager captures log data and sends a notification regarding this port. 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 unit 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 console manager receives 30 bytes of data, it captures log data and sends an email regarding this port.

### Text String
The specific pattern of characters the SLC unit 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 abcdeg, abceg, abcfeg.

The SLC console manager supports GNU regular expressions; for more information, see:
- [http://www.delorie.com/gnu/docs/regex/regex.html](http://www.delorie.com/gnu/docs/regex/regex.html)

### Email Delay
A time limit of how long (in seconds), after the SLC unit 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
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
The complete email address of the message recipient(s) for each device port(s). 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
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

<table>
<thead>
<tr>
<th>Displays</th>
<th>Select to view either the beginning (head) or end (tail) of the log.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Lines</td>
<td>Number of lines from the head or tail of the log to display.</td>
</tr>
</tbody>
</table>
8: Device Ports

NFS File Logging

<table>
<thead>
<tr>
<th>NFS File Logging</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Log to View</td>
<td>Available log files in the selected NFS Directory to view.</td>
</tr>
</tbody>
</table>
| 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 unit. 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. |

USB/PC Card Logging

| USB/PC Card Logging | Select to enable USB/PC Card logging.  
  | ◆ A PC Card Compact Flash must be loaded into one of the PC Card slots of the SLC unit and properly mounted.  
  | ◆ A USB flash drive must be loaded into the SLC unit.  
  | ◆ Disabled by default. |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------|
| USB/PC Card Log to View | Available log files in the selected USB port or PC card slot to view.                                                                |
| Log To | Select the USB port or PC card slot to use for logging.                                                                                 |
| 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 unit 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 > SSH/Telnet/Logging page. |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|
| Apply settings to Device Ports | Check checkbox to apply settings to other device ports in addition to the currently selected port, 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. |

3. To save, click the Apply button.

Logging Commands

The following CLI commands correspond to the web page entries described above.

To configure logging settings for one or more device ports:

set deviceport port <Device Port List or Name> <one or more deviceport parameters>
**Note:** Local logging must be enabled for a device port for the `locallog` commands to be executed. To use the `set locallog clear` command, the user must have permission to clear port buffers (see Chapter 12: User Authentication on page 165).

**Example:**

set deviceport port 2-5,6,12,15-16 baud 2400 locallogging enable

**Parameters:**

- `emaildelay <Email Delay>`
- `emaillogging <disable|bytecnt|charstr>`
- `emailrestart <Restart Delay>`
- `emailsend <email|trap|both>`
- `emailstring <Regex String>`
- `emailsubj <Email Subject>`
- `emailthreshold <Byte Threshold>`
- `emailto <Email Address>`
- `filedir <Logging Directory>`
- `filelogging <enable|disable>`
- `filemaxfiles <Max # of Files>`
- `filemaxsize <Max Size of Files>`
- `locallogging <enable|disable>`
- `name <Device Port Name>`
- `nfsdir <Logging Directory>`
- `nfslogging <enable|disable>`
- `nfsmaxfiles <Max # of Files>`
- `nfsmaxsize <Size in Bytes>`
- `sysloglogging <enable|disable>`
- `usblogging <enable|disable>`
- `usbmaxfiles <Max # of Files>`
- `usbmaxsize <Size in Bytes>`
- `usbport <U1>`
- `pccardlogging <enable|disable>`
- `pccardmaxfiles <Max # of Files>`
- `pccardmaxsize <Size in Bytes>`
- `pccardslot <upper|lower>`

**To view a specific number of bytes of data for a device port:**

show locallog <Device Port # or Name> [bytes <Bytes To Display>]

1 Kbyte is the default.

**To clear the local log for a device port:**

set locallog clear <Device Port # or Name>

**Note:** The `locallog` commands can only be executed for a device port if local logging is enabled for the port. The `set locallog clear` command can only be executed if the user has permission to clear port buffers (see Chapter 12: User Authentication on page 165).
Console Port

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

To set console port parameters:

1. Click the Devices tab and select Console Port. The following page displays:

![Console Port Page](image)

2. Change the following as desired:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Baud</strong></td>
<td>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 the console port defaults to this value.</td>
</tr>
<tr>
<td><strong>Data Bits</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Stop Bits</strong></td>
<td>The number of stop bits that indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is 1.</td>
</tr>
<tr>
<td><strong>Parity</strong></td>
<td>Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is none.</td>
</tr>
<tr>
<td><strong>Flow Control</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>The number of minutes (1-30) after which an idle session on the console is automatically logged out. Disabled by default.</td>
</tr>
<tr>
<td><strong>Show Lines on Connecting</strong></td>
<td>If selected, when you connect to the console port with a terminal emulator, you will see the last lines output to the console, for example, the SLC boot messages or the last lines output during a CLI session on the console.</td>
</tr>
</tbody>
</table>
3. Click the **Apply** button to save the changes.

### Console Port Commands

The following CLI commands correspond to the web page entries described above.

**To configure console port settings:**

```
set consoleport <one or more parameters>
```

**Parameters:**

- `baud` `<300->`
- `databits` `<7|8>`
- `stopbits` `<1|2>`
- `group` `<Local or Remote Group Name>`
- `parity` `<none|odd|even>`
- `flowcontrol` `<none|xon/xoff|rts/cts>`
- `showlines` `<enable|disable>`
- `timeout` `<disable|1-30>`

**To view console port settings:**

```
show consoleport
```

### 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 select the **Host Lists** option. The following page displays:
2. Enter the following:

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host List Id</td>
<td>Displays after a host list is saved.</td>
</tr>
<tr>
<td>Host List Name</td>
<td>Enter a name for the host list.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of times the SLC console manager should attempt to retry connecting to the host list.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select to require authentication when the SLC unit connects to a host.</td>
</tr>
</tbody>
</table>

3. You have the following options:
   - To save the host list without adding hosts at this time, click the **Add Host List** button.
   - To add hosts, enter the following:

**Host Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Name or IP address of the host.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol for connecting to the host (TCP, SSH, or Telnet).</td>
</tr>
</tbody>
</table>
4. Click the right arrow. The host displays in the Hosts box.

5. 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.

6. You have the following options:
   - To remove a host from the host list, select the host in the Hosts box and click the left arrow.
   - To give the host a higher precedence, select the host in the Hosts box and click the up arrow.
   - To give the host a lower precedence, select the host in the Hosts box and click the down arrow.

7. Click the Add Host List button. After the process completes, a link back to the Device Ports > Settings page displays.

**To view or update a host list:**

1. In the Host Lists table, select the host list and click the View Host List button. The list of hosts display in the Hosts box.
2. View, add, or update the following:

- **Host List Id**: 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 unit connects to a host.

### Host Parameters

- **Host**: Name or IP address of the host.
- **Protocol**: Protocol for connecting to the host (TCP, SSH, or Telnet).
- **Port**: Port on the host to connect to SLC console manager.
- **Escape Sequence**: The escape character used to get the attention of the SSH or Telnet client. It is optional, and if not specified, Telnet and SSH use their default escape character. For Telnet, the escape character is either a 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. For SSH, the escape character is a single character.

3. You have the following options:

- To add a host to the host list, click the right arrow. The host displays in the Hosts box.
To remove a host from the host list, select the host in the Hosts box and click the left  arrow.

To give the host a higher precedence, select the host in the Hosts box and click the up  arrow.

To give the host a lower precedence, select the host in the Hosts box and click the down  arrow.

4. Click the Edit Host List button. After the process completes, a link back to the Device Ports > Settings page displays.

**To delete a host list:**

1. Select the host list in the Host Lists table.
2. Click the Delete Host List button. After the process completes, a link back to the Device Ports > Settings page displays.

**Host List Commands**

The following CLI commands correspond to the web page entries described above.

**To configure a prioritized list of hosts to be used for modem dial-in connections:**

```plaintext
set hostlist add|edit <Host List Name> [parameters]
```

**Parameters:**

- name <Host List Name> (edit only)
- retrycount <1-10>

*Default is 3.*

- auth <enable|disable>

**To add a new host entry to a list or edit an existing entry:**

```plaintext
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>

**To move a host entry to a new position in the host list:**

```plaintext
set hostlist edit <Host List Name> move <Host Number> position <Host Number>
```

**To delete a host list, or a single host entry from a host list:**

```plaintext
set hostlist delete <Host List> [entry <Host Number>]
```

**To display the members of a host list:**

```plaintext
show hostlist <all|names|Host List Name>
```
Scripts

The SLC console manager supports 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.

- **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 utilize scripts at the CLI. For a description of the syntax allowed in Interface Scripts, see Interface Script Syntax at the end of this page.

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

**To add a script:**

1. Click the Devices tab and select the Scripts option. This page displays.

![Figure 8-12 Devices > Scripts](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Grp</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test1</td>
<td>Batch</td>
<td>Def</td>
<td></td>
</tr>
<tr>
<td>Test2</td>
<td>Interface</td>
<td>Def</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Full Administrative</th>
<th>Networking</th>
<th>Services</th>
<th>Secure Lantronix Network</th>
<th>Date/Time</th>
<th>Local Users</th>
<th>Remote Authentication</th>
<th>SSH Keys</th>
<th>User Names</th>
<th>Web Access</th>
<th>Diagnostics &amp; Reports</th>
<th>Power Users</th>
<th>Administrators</th>
<th>USB</th>
<th>Device Port Configuration</th>
<th>Device Port Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>

*Images and text from the provided page have been transcribed and formatted into a plain text representation.*
2. Click the **Add Scripts** button. The page for editing script attributes displays.

![Figure 8-13 Adding or Editing New Scripts](image)

3. Enter the following:

   **Scripts**

<table>
<thead>
<tr>
<th>Script Name</th>
<th>A unique identifier for the script.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select <strong>Interface</strong> for a script that utilizes Expect/Tcl to perform pattern detection and action generation on Device Port output. Select <strong>Batch</strong> for a script of CLI commands.</td>
</tr>
</tbody>
</table>

4. In the **User Rights** section, select the user **Group** to which NIS users will belong:
User Rights

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default Users</strong></td>
<td>This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td><strong>Power Users</strong></td>
<td>This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</td>
</tr>
<tr>
<td><strong>Administrators</strong></td>
<td>This group has all possible rights.</td>
</tr>
</tbody>
</table>

5. Assign or unassign **User Rights** for the specific user by checking or unchecking the following boxes:

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Administrative</strong></td>
<td>Right to add, update, and delete all editable fields.</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td><strong>Secure Lantronix Network</strong></td>
<td>Right to view and manage Secure Lantronix units (e.g., SLP, Spider, SLC and SLB units) on the local subnet.</td>
</tr>
<tr>
<td><strong>Date/Time</strong></td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td><strong>Local Users</strong></td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td><strong>Remote Authentication</strong></td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td><strong>SSH Keys</strong></td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td><strong>User Menus</strong></td>
<td>Right to create a custom user menu for the CLI for NIS users.</td>
</tr>
<tr>
<td><strong>Web Access</strong></td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td><strong>Diagnostics &amp; Reports</strong></td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td><strong>Reboot &amp; Shutdown</strong></td>
<td>Right to use the CLI or shut down the SLC console manager and then reboot it.</td>
</tr>
<tr>
<td><strong>Firmware &amp; Configuration</strong></td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot &amp; Shutdown.</td>
</tr>
<tr>
<td><strong>Device Port Operations</strong></td>
<td>Right to control device ports.</td>
</tr>
<tr>
<td><strong>Device Port Settings</strong></td>
<td>Right to enter device port settings.</td>
</tr>
<tr>
<td><strong>USB</strong></td>
<td>Right to enter modem settings for USB. The USB checkbox is available for certain SLC and SLB models.</td>
</tr>
<tr>
<td><strong>PC Card</strong></td>
<td>Right to enter modem settings for PC cards. Includes managing storage PC cards. The PC card checkbox is available for certain SLC and SLB models.</td>
</tr>
</tbody>
</table>

6. To save, click the **Apply** button. If the type of script is Interface, the script will be validated before it is saved. Once the script is saved, the main **Scripts** page is displayed.

**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 (see **Figure 8-13**).
2. Update the script **attributes** (see **To add a script**: above).
3. To save, 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 will be renamed and the **Devices > Scripts** page redisplays.

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 will be deleted and the **Devices > Scripts** page redisplays.

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 updates and the **Devices > Scripts** page redisplays.

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 runcli <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>
```

The `while` command allows a loop containing CLI commands to be executed. Syntax:

```
while {<Boolean expression>} {
   CLI command 1
   CLI command 2
   ...
   CLI command n
}
```

**Note:** The closing left brace `{}` must be on a line without any other characters. To support a `while` command, the `set command`, variables, and secondary commands are also supported.
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.

**Table 8-14 Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Word</strong></td>
<td>A contiguous group of characters delimited on either side by spaces. Not enclosed by double quotes.</td>
</tr>
<tr>
<td><strong>Primary Command</strong></td>
<td>One of the primary commands listed in this section.</td>
</tr>
<tr>
<td><strong>Secondary Command</strong></td>
<td>One of the secondary commands defined in this section.</td>
</tr>
<tr>
<td><strong>Quoted String</strong></td>
<td>A group of characters enclosed by double quote (&quot;) 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 ('').</td>
</tr>
<tr>
<td><strong>Variable Reference</strong></td>
<td>A word (as defined above) preceded by a dollar sign character ('$').</td>
</tr>
<tr>
<td><strong>CLI Command</strong></td>
<td>A quoted string containing a valid CLI show command.</td>
</tr>
<tr>
<td><strong>Arithmetic Operator</strong></td>
<td>A single character representing a simple arithmetic operation. The character may be one of the following:</td>
</tr>
<tr>
<td></td>
<td>◆ A plus sign (+) representing addition</td>
</tr>
<tr>
<td></td>
<td>◆ A minus sign (-) representing subtraction</td>
</tr>
<tr>
<td></td>
<td>◆ An asterisk sign (*) representing multiplication</td>
</tr>
<tr>
<td></td>
<td>◆ A forward slash (/) representing division</td>
</tr>
<tr>
<td></td>
<td>◆ A percent sign (%) representing a modulus</td>
</tr>
<tr>
<td><strong>Boolean Expression</strong></td>
<td>An expression which evaluates to TRUE or FALSE. A Boolean expression has the following syntax:</td>
</tr>
<tr>
<td></td>
<td>◆ <code>&lt;value&gt; &lt;Boolean operator&gt; &lt;value&gt;</code></td>
</tr>
<tr>
<td></td>
<td>Each can be either a word or a variable reference.</td>
</tr>
<tr>
<td><strong>Boolean Operator</strong></td>
<td>A binary operator which expresses a comparison between two operands and evaluates to TRUE or FALSE. The following Boolean operators are valid:</td>
</tr>
<tr>
<td></td>
<td>◆ `&lt;' less than</td>
</tr>
<tr>
<td></td>
<td>◆ `&gt;' greater than</td>
</tr>
<tr>
<td></td>
<td>◆ `=&lt;' less than or equal to</td>
</tr>
<tr>
<td></td>
<td>◆ `&gt;=' greater than or equal to</td>
</tr>
<tr>
<td></td>
<td>◆ `=' equal to</td>
</tr>
<tr>
<td></td>
<td>◆ <code>!=</code> not equal to</td>
</tr>
</tbody>
</table>
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 ("{")

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 `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>` is 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. |
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:

```plaintext
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.

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

```plaintext
return <value>
```

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>expect, expect_user, expect_before, expect_after, expect_background</td>
<td>The <code>expect</code> 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 <code>expect</code> commands have the same syntax: <code>expect {&lt;string 1&gt; {command 1} &lt;string 2&gt; {command 2} ... &lt;string n&gt; {command n}}</code> where <code>&lt;string x&gt;</code> will either be a quoted string, a variable reference or the reserved word 'timeout.' The command <code>x</code> is optional, but the curly braces (<code>{</code> and <code>}</code>) are required. If present it must be a primary command.</td>
</tr>
<tr>
<td>return</td>
<td>The <code>return</code> command terminates execution of the script and returns an optional value to the calling environment. Syntax: <code>return &lt;value&gt;</code> where <code>&lt;value&gt;</code> can be a word or a variable reference.</td>
</tr>
</tbody>
</table>


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 ("]").

### Table 8-16  Secondary Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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'
|
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.

Table 8-17  Control Flow Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| 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 } |
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:

```plaintext
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 $sleepTime
#Log in or check for Command Prompt
```
expect {
    #Did not capture "oain" or Command Prompt
    timeout { send_user "Time out login......\n"; return }
    #Got login prompt
    "login" {
        send_user "Logging in....\n"
        send "$login\n"
        expect {
            timeout { send_user "Time out waiting for pwd
                 prompt......\n"; return }
            #Got password prompt
            "password" {
            #Send Password
            send "$pwd\n"
            expect {
                timeout { send_user "Time out waiting for prompt......\n"; return }
                $prompt {}
            }
        }
        
        #Already Logged in got Command Prompt
        $prompt {
            send_user "Already Logged....\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 "\n\n\n\n\n"
    send_user "Device [string toupper $hostname]\r\n"
    send_user 
    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:

```plaintext
slb247glenn]> conn script ex4 deviceport 7
login: Logging in....
sysadmin
sysadmin
Password: PASS
Welcome to the Secure Lantronix Console Manager
Model Number: SLC 48
For a list of commands, type 'help'.
[SLC251glen]> show network port 1 host
show network port 1 host
  _Current Hostname
Settings___________________________________________________
Hostname: SLC251glen
Domain: support.int.lantronix.com
[SLC251glen]
Device HOSTNAME: SLC 251GLEN

  -----------------------------------------------
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
[SLC251glen]> [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
[SLC251glen]> Port Counter Monitor Script Ending......

Login Out.......
logout
Returning to command line
[slb247glen]>```

**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 Secure Lantronix Console Manager
Model Number: slc 48
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: SLC 251GLENN

  _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]>
```
8: Device Ports

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

Port Counter Monitor Script Ending......

________________________________________________________________________
Login Out.......
logout
Returning to command line

[slbvz249_glenn]> show script
___Interface Scripts________Group/
Permissions____________________
test3                     Def/do
___Batch Scripts__________Group/
Permissions____________________
test1                     Adm/
ad,nt,sv,dt,lu,ra,um,dp,ub,rs,fc,dr,sn,wb,sk,po,do

Sites

A site is a group of site-oriented modem parameters that can be activated by various modem-related events (authentication on dial-in, outbound network traffic for a dial-on-demand connection, etc.). The site parameters will override parameters that are configured for a modem.

To use sites with a modem, create one or more sites (described below), then enable Use Sites for the modem. Sites can be used with the following modem states: dial-in, dial-back, CBCP Server, dial-on-demand, dial-in & dial-on-demand, and dial-back & dial-on-demand. For more information on how sites are used with each modem state, see Modem Dialing States on page 136.

To add a site:

1. Click the Devices tab and select the Sites option. The Sites page displays:
2. In the lower section of the page, enter the following:

<table>
<thead>
<tr>
<th>Site Id (view only)</th>
<th>Displays after a site is created.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>Enter a name for the site.</td>
</tr>
<tr>
<td>Port</td>
<td>Select the device port, UPC card slot, or USB port the site is assigned to. For dial-on-demand sites, a port must be selected. For any other sites, the port selection can be set to None. See Modem Dialing States on page 136.</td>
</tr>
<tr>
<td>Login/CHAP Host</td>
<td>The login name (for PAP authentication) or CHAP host (for CHAP authentication) associated with this site. If a modem has sites enabled and the authentication is successful at dial-in (for modem states dial-in, dial-back, CBCP server, dial-in &amp; dial-on-demand, or dial-back &amp; dial-on-demand), and the name that was authenticated matches the Login/CHAP Host, the site parameters will be used for the remainder of the modem connection.</td>
</tr>
</tbody>
</table>
**CHAP Secret**
The CHAP secret associated with this site. If a modem has sites enabled and CHAP authentication enabled, then at dial-in, if the remote server sends a name in the CHAP challenge response that matches the CHAP host of a site, the CHAP secret for the site will be used to authenticate the CHAP challenge response sent by the remote server.

**Authentication**
The type of authentication, **PAP** or **CHAP**, for which this site is applicable. On dial-in authentication, only sites with the authentication type that matches the authentication type configured for the modem will be used to try to find a matching site.

**Timeout Logins**
For text dial-in connections, the connection can time out after the connection is inactive for a specified number of minutes.

**Negotiate IP Address**
If the SLC console manager and the remote server should negotiate the IP addresses for each side of the PPP connection, select **Yes**. Select **No** if the address of the SLC unit (**Local IP**) and remote server (**Remote IP**) need to be specified.

**Static Route IP Address**
The Static Route IP Address, Subnet Mask and Gateway must be configured for dial-on-demand sites. The SLC device will automatically dial-out and establish a PPP connection when IP traffic destined for the network specified by the static route needs to be sent.

*Note: Static Routing must be enabled on the Network - Routing page for dial-on-demand connections.*

**Static Route Subnet Mask**
The subnet mask for a dial-on-demand connection.

**Static Route Gateway**
The gateway for a dial-on-demand connection.

**Dial-out Number**
The dial-out number must be specified for dial-on-demand sites. This indicates the phone number to dial when the SLC console manager needs to send IP traffic for a dial-on-demand connection.

**Dial-out Login**
User ID for authentication when dialing out to a remote system. May have up to 32 characters. This ID is used for authenticating the SLC unit during the dial-out portion of a dial-back (including CBCP server) and dial-on-demand.

**Dial-out Password**
Enter the password for authentication when dialing out to a remote system. May have up to 64 characters. This password is used for authenticating the SLC device during the dial-out portion of a dial-back (including CBCP server) and dial-on-demand.

**Retype Password**
Re-enter the password for authentication when dialing out to a remote system. May have up to 64 characters. This password is used for authenticating the SLC console manager during the dial-out portion of a dial-back (including CBCP server) and dial-on-demand.

**Dial-back Number**
The phone number to dial on callback for text or PPP dial-back connections. A site must successfully authenticate, have **Allow Dial-back** enabled and have a Dial-back Number defined in order for the site to be used for callback.

**Allow Dial-back**
If enabled, the site is allowed to be used for dial-back connections.

**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.

**Dial-back Retries**
For dial-back and CBCP Server, the number of times the SLC unit will retry the dial-out portion of the dialing sequence if the first attempt to dial-out fails.

**Modem Timeout**
Timeout for dial-in and dial-on-demand PPP 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.
3. Click the **Add Site** button.

**To view or update a site:**

1. In the **Sites** table, select the site and click the **View Site** button. The site attributes are displayed in the bottom half of the page.

2. Update any of the site attributes.

3. Click the **Edit Site** button.

**To delete a site:**

1. Select the site in the **Sites** table.

2. Click the **Delete Site** button.

Configures a set of site-oriented modem parameters that can be activated by various modem-related events (authentication, outbound network traffic for DOD connections, etc.).

The site parameters will override any parameters configured for the modem.

Uses sites with a modem, enable 'usesites'. Sites can be used with the following modem states: dialin, dialback, cbcpserver, dialondemand, dialin+ondemand, and dialback+ondemand.

**To create or edit a site:**

```
set site add|edit <Site Name> [parameters]
```

**Parameters:**

- **name**: `<Site Name>` (edit only)
- **deviceport**: `<Device Port # or Name or none>`
- **usbport**: `<U1|U2>`
- **pccardslot**: `<upper|lower>`
- **auth**: `<pap|chap>`
- **loginhost**: `<User Login/CHAP Host>`
- **chapsecret**: `<CHAP Secret>`
- **localipaddr**: `<negotiate|IP Address>`
- **remoteipaddr**: `<negotiate|IP Address>`
- **routeipaddr**: `<IP Address>`
- **restartdelay**: `<PPP Restart Delay>`
- **routegateway**: `<Gateway>`
- **modemtimeout**: `<disable|1-9999 secs>`
- **routemask**: `<Mask>`
- **cbcpnocallback**: `<enable|disable>`
- **cbcpdelay**: `<disable|1-10>`
- **allowdialback**: `<enable|disable>`
- **dialoutnumber**: `<Phone Number>`
- **dialoutlogin**: `<User Login>`
- **dialoutpassword**: `<Password>`
- **dialbacknumber**: `<Phone Number>`
- **dialbackdelay**: `<Dial-back Delay>`
- **dialbackretries**: `<1-10>`
- **timeoutlogins**: `<disable|1-30 minutes>`
- **nat**: `<enable|disable>`

**To delete a site:**

```
set site delete <Site Name>
show site <all|names|Site Name>
```
Modem Dialing States

This section describes how each modem state that supports sites operates when sites are enabled.

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 enabled authentication methods (Local Users, NIS, LDAP, etc). The site list will be searched for a site that (a) the Login/CHAP Host matches the name that was authenticated, (b) Authentication is set to PAP, and (c) the Port is set to None or matches the port the modem is on.

If a matching site is found, the Timeout Logins parameter configured for the site will be used for the rest of the dial-in connection instead of the Timeout Logins parameter configured for the modem. 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 (determined by the Authentication setting for the modem). For PAP, the Local/Remote User list will be used to authenticate the login and password sent by the PPP peer, and the site list will be searched for a site that (a) the Login/CHAP Host matches the name that was authenticated, (b) Authentication is set to PAP, and (c) the Port is set to None or matches the port the modem is on. For CHAP, the site list will be searched for a site that (a) the Login/CHAP Host and CHAP Secret match the name and secret sent in the CHAP Challenge response by the PPP peer, (b) Authentication is set to CHAP, and (c) the Port is set to None or matches the port the modem is on. If the remote peer requests PAP or CHAP authentication from the SLC unit, the Remote/Dial-out Login and Remote/Dial-out Password configured for the modem (not the site) will be provided as authentication tokens.

If a matching site is found, its Negotiate IP Address, NAT, and Modem Timeout parameters will be used for the rest of the dial-in connection instead of the parameters configured for the modem. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the Negotiate IP Address setting). The PPP connection will stay active until no IP traffic is sent for Modem Timeout seconds.

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 unit 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 enabled authentication methods (Local Users, NIS, LDAP, etc). The site list will be searched for a site that (a) the Login/CHAP Host matches the name that was authenticated, (b) Authentication is set to PAP, and (c) the Port is set to None or matches the port the modem is on.

If a matching site is found, its Timeout Logins, Dial-back Number, Allow Dial-back, and Dial-back Delay parameters will be used for the rest of the dial-back connection instead of the parameters configured for the modem. Once the remote server is authenticated, if Allow Dial-back is enabled for the site and a Dial-back Number is defined, the SLC console manager will hang up and wait Dial-back Delay seconds before initiating the dial-back. The SLC unit 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 device 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 (determined by the Authentication setting for the modem). For PAP, the Local/Remote User list will be used to authenticate the login and password sent by the PPP peer, and the site list will be searched for a site that (a) the Login/CHAP Host matches the name that was authenticated, (b) Authentication is set to PAP, and (c) the Port is set to None or matches the port the modem is on. For CHAP, the site list will be searched for a site that (a) the Login/CHAP Host and CHAP Secret match the name and secret sent in the CHAP Challenge response by the PPP peer, (b) Authentication is set to CHAP, and (c) the Port is set to None or matches the port the modem is on. If the remote peer requests PAP or CHAP authentication from the SLC console manager, the Remote/Dial-out Login and Remote/Dial-out Password configured for the modem (not the site) will be provided as authentication tokens.

If a matching site is found, its Dial-back Number, Allow Dial-back, Dial-back Delay, Dial-out Login, Dial-out Password, Negotiate IP Address, NAT, and Modem Timeout parameters will be used for the rest of the dial-back connection instead of the parameters configured for the modem. Once the remote server is authenticated, if Allow Dial-back is enabled for the site and a Dial-back Number is defined, the SLC unit 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 a remote network needs to be sent. It will remain connected until no data packets have been sent to the peer for a specified amount of time.

When this modem state is initiated, the SLC unit searches the site list for all sites that (a) have a Dial-out Number defined, (b) have a Static Route IP Address, Static Route Subnet Mask and Static Route Gateway defined, and (c) the Port matches the port the modem is on. A dial-on-demand connection will be started for each, waiting for IP traffic destined for a remote network. When IP traffic needs to be sent, the SLC device dials the appropriate Dial-out Number for the site, 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). The PPP connection will stay active until no IP traffic 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 & 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 a remote network needs to be sent. When either event occurs (an incoming call or IP traffic destined for the remote network), the other mode will be disabled.

- For Dial-in, the user will be authenticated via PAP or CHAP (determined by the Authentication setting for the modem). For PAP, the Local/Remote User list will be used to authenticate the login and password sent by the PPP peer, and the site list will be searched for a site that (a) the Login/CHAP Host matches the name that was authenticated, (b) Authentication is set to PAP, and (c) the Port is set to None or matches the port the modem is on. For CHAP, the site list will be searched for a site that (a) the Login/CHAP Host and
8: Device Ports

CHAP Secret match the name and secret sent in the CHAP Challenge response by the PPP peer, (b) Authentication is set to CHAP, and (c) the Port is set to None or matches the port the modem is on. If the remote peer requests PAP or CHAP authentication from the SLC console manager, the Remote/Dial-out Login and Remote/Dial-out Password configured for the modem (not the site) will be provided as authentication tokens. If a matching site is found, its Negotiate IP Address, NAT, and Modem Timeout parameters will be used for the rest of the dial-in connection instead of the parameters configured for the modem. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the Negotiate IP Address setting). The PPP connection will stay active until no IP traffic is sent for Modem Timeout seconds.

- For Dial-on-Demand, the SLC unit searches the site list for all sites that (a) have a Dial-out Number defined, (b) have a Static Route IP Address, Static Route Subnet Mask and Static Route Gateway defined, and (c) the Port matches the port the modem is on. A dial-on-demand connection will be started for each, waiting for IP traffic destined for a remote network. When IP traffic needs to be sent, the SLC device dials the appropriate Dial-out Number for the site, 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). The PPP connection will stay active until no IP traffic 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-back & Dial-on-demand

A modem is configured to be in two modes: answering incoming calls to initiate a dial-back, and automatically dialing out to establish a PPP connection when IP traffic destined for a remote network needs to be sent. When either event occurs (an incoming call or IP traffic destined for the remote network), the other mode will be disabled.

- For Dial-back, the user will be authenticated via PAP or CHAP (determined by the Authentication setting for the modem). For PAP, the Local/Remote User list will be used to authenticate the login and password sent by the PPP peer, and the site list will be searched for a site that (a) the Login/CHAP Host matches the name that was authenticated, (b) Authentication is set to PAP, and (c) the Port is set to None or matches the port the modem is on. For CHAP, the site list will be searched for a site that (a) the Login/CHAP Host and CHAP Secret match the name and secret sent in the CHAP Challenge response by the PPP peer, (b) Authentication is set to CHAP, and (c) the Port is set to None or matches the port the modem is on. If the remote peer requests PAP or CHAP authentication from the SLC console manager, the Remote/Dial-out Login and Remote/Dial-out Password configured for the modem (not the site) will be provided as authentication tokens. If a matching site is found, its Dial-back Number, Allow Dial-back, Dial-back Delay, Dial-out Login, Dial-out Password, Negotiate IP Address, NAT, and Modem Timeout parameters will be used for the rest of the dial-back connection instead of the parameters configured for the modem. Once the remote server is authenticated, if Allow Dial-back is enabled for the site and a Dial-back Number is defined, the SLC unit 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).

- For Dial-on-Demand, the SLC console manager searches the site list for all sites that (a) have a Dial-out Number defined, (b) have a Static Route IP Address, Static Route Subnet Mask and Static Route Gateway defined, and (c) the Port matches the port the modem is on. A
dial-on-demand connection will be started for each, waiting for IP traffic destined for a remote network. When IP traffic needs to be sent, the SLC unit dials the appropriate **Dial-out Number** for the site, 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). The PPP connection will stay active until no IP traffic 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.

**CBCP Server**

Callback Control Protocol (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](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.

For CBCP Server, the SLC console manager waits for a client to call the unit, establishes a PPP connection, authenticates the user, and negotiates a dial-back number with the client using CBCP. If the SLC unit 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 (determined by the **Authentication** setting for the modem). For PAP, the Local/Remote User list will be used to authenticate the login and password sent by the PPP peer, and the site list will be searched for a site that (a) the **Login/CHAP Host** matches the name that was authenticated, (b) **Authentication** is set to PAP, and (c) the **Port** is set to **None** or matches the port the modem is on. For CHAP, the site list will be searched for a site that (a) the **Login/CHAP Host** and **CHAP Secret** match the name and secret sent in the CHAP Challenge response by the PPP peer, (b) **Authentication** is set to CHAP, and (c) the **Port** is set to **None** or matches the port the modem is on. If the remote peer requests PAP or CHAP authentication from the SLC console manager the **Remote/Dial-out Login** and **Remote/Dial-out Password** configured for the modem (not the site) will be provided as authentication tokens.

If a matching site is found, its **CBCP Server Allow No Callback**, **Dial-back Number**, **Allow Dial-back**, **Dial-back Delay**, **Dial-out Login**, **Dial-out Password**, **Negotiate IP Address**, **NAT**, and **Modem Timeout** parameters will be used for the rest of the dial-back connection instead of the parameters configured for the modem. Once the remote server is authenticated, the CBCP handshake with the client determines the number to use for dial-back. The SLC unit will present the client with the available options: if **Allow Dial-back** is enabled for the site and a **Dial-back Number** is 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 call back the previously authenticated remote peer, 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).
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**

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.
4. Enter the following fields.

<table>
<thead>
<tr>
<th>Slot (view only)</th>
<th>Slot on the SLC console manager where the PC Card is inserted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device (view only)</td>
<td>Type of PC Card (modem or storage).</td>
</tr>
<tr>
<td>Type (view only)</td>
<td>Information read from PC Card.</td>
</tr>
<tr>
<td>State (view only)</td>
<td>Applies to storage cards.</td>
</tr>
<tr>
<td>Mount</td>
<td>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.</td>
</tr>
<tr>
<td>Unmount</td>
<td>Click the checkbox to eject the compact flash from the SLC console manager after unmounting it.</td>
</tr>
<tr>
<td>Format</td>
<td>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.</td>
</tr>
<tr>
<td>Filesystem</td>
<td>Select ext2 or FAT, the file systems the SLC console manager supports.</td>
</tr>
</tbody>
</table>

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

![Figure 9-3  PC Card - Modem/ISDN Page](image)
5. Enter the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Slot</strong></td>
<td>Displays the slot position.</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td>Displays the device type.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Displays the card type.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Displays the state of the device.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Enables the modem to use dial-out, dial-in, dial-back, CBCP server, CBCP client, dial-on-demand, dial-in &amp; dial-on-demand, dial-back &amp; dial-on-demand, or dial-in/ host list. Disabled by default. For more information on the different dialing types, see <strong>Modem State Parameters on page 329</strong>.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>PPP Logging</strong></td>
<td>Check checkbox to turn on PPP logging.</td>
</tr>
<tr>
<td><strong>PPP Debug</strong></td>
<td>Check checkbox to include debugger information in the PPP log.</td>
</tr>
<tr>
<td><strong>Use Sites</strong></td>
<td>Enables the use of site-oriented modem parameters which can be activated by various modem-related events (authentication, outbound network traffic for dial-on-demand connections, etc.). Sites can be used with the following modem states: dial-in, dial-back, dial-on-demand, dial-in &amp; dial-on-demand, dial-back &amp; dial-on-demand, and CBCP server. For more information see <strong>Sites on page 133</strong>.</td>
</tr>
<tr>
<td><strong>Group Access</strong></td>
<td>If undefined, any group can access the modem (text login only). If one or more groups are specified (groups are delimited by the characters ',' (comma) or ';' (semicolon)), then any user who logs into the modem must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the SLC or SLB unit. A group provided by a remote server must be either a single group or multiple groups delimited by the characters ',' (comma), ';' (semicolon), or '=' (equals) - for example &quot;group=group1,group2,&quot; or &quot;group1,group2,group3&quot;.</td>
</tr>
<tr>
<td><strong>Initialization Script</strong></td>
<td>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 &amp;D2 &amp;c1 E1 Q0. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td><strong>Modem Timeout</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Caller ID Logging</strong></td>
<td>Select to enable the SLC console manager to log caller IDs on incoming calls. Disabled by default. <strong>Note:</strong> For the Caller ID AT command, refer to your Modem User Guide.</td>
</tr>
</tbody>
</table>
### 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 Modern State Parameters on page 329.

### Dial-back Retries

For dial-back and CBCP Server, the number of times the SLC or SLB unit will retry the dial-out portion of the dialing sequence if the first attempt to dial-out fails.

### Data Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Baud</strong></td>
<td>The speed with which the device port exchanges data with the attached serial device.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Data Bits</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Parity</strong></td>
<td>Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is none.</td>
</tr>
<tr>
<td><strong>Stop Bits</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Flow Control</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

### ISDN Settings

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Channel</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Phone #</strong></td>
<td>Phone number associated with the B channel. May have up to 20 characters. Any format is acceptable.</td>
</tr>
</tbody>
</table>

### 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.)

<table>
<thead>
<tr>
<th>Dial-out Mode</th>
<th>Select the type of dial-out connection:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✷ GPRS: (General Packet Radio Service)</td>
</tr>
<tr>
<td></td>
<td>✷ GSM: (Global System for Mobile communication)</td>
</tr>
</tbody>
</table>

| PIN / Retype PIN | PIN (personal identification number) for accessing the GSM/GPRS card. |

| PPP Compression | Select to enable negotiation of data compression over PPP links. Disabled by default. |

| 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 (view only) | IP address associated with the GPRS connection. |

| GPRS Context | Command to specify the protocol data packet (PDP) context parameter values. |

| GSM Bearer Svc. | Command to select the bearer service, data rate, and connection element to use when data call originate. |

**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. |
### CHAP Auth Uses
Select the method of CHAP Authorization:
- Through the CHAP Host user name and password established under CHAP Handshake.
- Through the username and password established under Local/Remote User database.

### 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.

### Remote/Dial-out Login
User ID for authentication when dialing out to a remote system, or if a remote system requests authentication from the SLC or SLB device when it dials in. May have up to 32 characters.

### Remote/Dial-out Pwd and Retype
Password for authentication when dialing out to a remote system, or if a remote system requests authentication from the SLC or SLB unit when it dials in. 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 329*.

### 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 329*.

---

### IP Settings

<table>
<thead>
<tr>
<th>Service</th>
<th>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 <strong>None</strong>.</th>
</tr>
</thead>
</table>
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 296)
- `pccard storage delete` (on page 296)
- `pccard storage dir` (on page 296)
- `pccard storage format` (on page 296)
- `pccard storage mount` (on page 296)
- `pccard storage rename` (on page 297)
- `pccard storage unmount` (on page 297)
- `show pccard storage` (on page 297)
- `pccard modem` (on page 294)
- `show pccard modem` (on page 297)
- `show pccard` (on page 297)
- `set log clear modem` (on page 287)
- `set log modem pppdebug` (on page 288)
- `show log modem` (on page 288)
10: USB Port

This chapter describes how to configure storage by using the Devices > USB page and CLI. This 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 Port Settings (on page 96).

This chapter describes the Web Manager pages and available CLI commands that configure the SLC console manager 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 Devices > USB page has an USB Access checkbox. USB Access is a security feature that ensures that access to any USB device is disabled if the box is unchecked. The SLC unit ignores any USB device plugged into the port.

To set up USB storage in the SLC console manager perform the following steps.

1. Insert any of the supported thumb drives into the USB port on the front of the SLC unit. 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 in if you have inserted it. If it does not display and you have inserted it, refresh the web page.

![Figure 10-1 Devices > USB](image)

To configure the USB port, from the USB Ports table,

1. Click the radio button (on the far right) for Port U1.

2. Click Configure. Figure 10-2 shows the page that displays if a USB storage device is inserted in Port U1.
3. Enter the following fields.

**Mount**

Enables the first partition of the USB device (if not currently mounted). Once mounted, a device is used for device port logging and 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 unit 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, FAT16 or FAT32)
- Mount the USB device

**Filesystem**

Select Ext2, FAT16 or FAT32, the file systems the SLC unit supports.

**Filesystem Check**

Select to run a filesystem integrity check on the thumb drive. This is recommended if the filesystem does not mount or if the filesystem has errors.

4. Click **Apply**.

**To configure the USB Modem port, from the Modem USB Ports table:**

1. Click the radio button (on the far right) for Port U1 or U2.
2. Click **Configure.** Figure 10-3 shows the page that displays if a USB modem is inserted in Port U1, or if Port U2 is selected.
3. Enter the following fields.
Data Settings

*Note:* Check the modem’s equipment settings and documentation for the proper settings. The attached modem must have the same 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 the device port defaults to this value. 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**.

GSM/GPRS Settings

**Dial-out Mode**
Select either GPRS or GSM (Global System for Mobile communication) as the type of dial-out connection.

**PIN**
Enter PIN (personal identification number) for accessing the GSM/GPRS card.

**Retype PIN**
Re-enter PIN (personal identification number) for accessing the GSM/GPRS card.

**PPP Compression**
Select to enable negotiation of data compression over PPP links. Disabled by default.

**Auto-acquire DNS**
Select to enable the SLC console manager to acquire up to three DNS servers by means of GPRS (General Packet Radio Service). Enabled by default.

**Negotiated IP**
IP address associated with the GPRS connection.

**GPRS Context**
Command to specify the protocol data packet (PDP) context parameter values.

**GSM Bearer Svc**
Command to select the bearer service, data rate, and connection element to use when data call originate.

Modem Settings

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

**State**
If enabling, set the modem to dial-out, dial-in, dial-back, CBICP server, CBICP client, dial-on-demand, dial-in & dial-on-demand, dial-back & dial-on-demand, or dial-in/host list. Disabled by default. For more information on the different dialing types, see *Modem Dialing States (on page 136)*.

**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 in dial-out mode (e.g., the SLC unit connects to an external network), dial-in mode (e.g., the external computer connects to the network that the SLC device is part of), or dial-on-demand.
### Use Sites
Enables the use of site-oriented modem parameters which can be activated by various modem-related events (authentication, outbound network traffic for dial-on-demand connections, etc.). Sites can be used with the following modem states: dial-in, dial-back, dial-on-demand, dial-in & dial-on-demand, dial-back & dial-on-demand, and CBCP server.

### Group Access
If undefined, any group can access the modem (text login only). If one or more groups are specified (groups are delimited by the characters ' ' (space), ',' (comma), or ';' (semicolon)), then any user who logs into the modem must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the SLC console manager. A group provided by a remote server must be either a single group or multiple groups delimited by the characters ',' (space), ',' (comma), ',' (semicolon), or '=' (equals) - for example "group=group1,group2;" or "group1,group2,group3".

### 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 unit 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 device may properly control the modem.*

### Modem Timeout
Timeout for all modem connections. Select Yes (default) for the SLC console manager 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 unit 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 console manager and enter their login and password. Once the SLC unit 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. See Device Ports - Settings (on page 94) for more information.

### 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.

### Dial-back Retries
For dial-back and CBCP Server, the number of times the SLC or SLB unit will retry the dial-out portion of the dialing sequence if the first attempt to dial-out fails.

### Text Mode

<table>
<thead>
<tr>
<th>Text Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout Logins</td>
<td>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.</td>
</tr>
</tbody>
</table>

---

**SLC™ Console Manager User Guide**

152
## PPP Mode

### 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 console manager successfully connects to one.

To establish and configure host lists, click the **Host Lists** link.

### Negotiate IP Address
If the SLC unit 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 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/User Name** (for UNIX systems) or **Secret/User Password** (for Windows systems) used for CHAP authentication. May have up to 128 characters.

### CHAP Auth Uses
For CHAP authentication, determines what is used to validate the CHAP host/user sent by the remote peer: either the **CHAP Host** defined for the modem, or any of the users in the **Local Users** list.

### 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/User Name** 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 USB port) basis. Users dialing into the SLC unit access the network connected to Eth1 and/or Eth2. **Note**: IP forwarding must be enabled on the Network > Network Settings page for NAT to work. See Chapter 6: Basic Parameters on page 52.

### 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.

### Remote/Dial-out Login
User ID for authentication when dialing out to a remote system, or if a remote system requests authentication from the SLC or SLB device when it dials in. May have up to 32 characters.

### Remote/Dial-out Pwd
Password for authentication when dialing out to a remote system, or if a remote system requests authentication from the SLC or SLB unit when it dials in. May have up to 64 characters.

### Retype
Re-enter password for dialing out to a remote system. May have up to 64 characters.
10: USB Port

<table>
<thead>
<tr>
<th><strong>Restart Delay</strong></th>
<th>The number of seconds after the timeout and before the SLC console manager attempts another connection. The default is 30 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CBCP Server Allow No Callback</strong></td>
<td>For CBCP Server state, allows &quot;No Callback&quot; as an option in the CBCP handshake in addition to User-defined Number and Admin-defined Number.</td>
</tr>
<tr>
<td><strong>CBCP Client Type</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**IP Settings**

<table>
<thead>
<tr>
<th><strong>Service</strong></th>
<th>The available connection services for this modem port (Telnet, SSH, or TCP). Only one can be active at a time. The default is None.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Telnet Port</strong></td>
<td>Telnet Port Telnet session port number to use if you selected Telnet. Defaults:</td>
</tr>
<tr>
<td></td>
<td>USB Port U1: 2049</td>
</tr>
<tr>
<td></td>
<td>USB Port U2: 2050</td>
</tr>
<tr>
<td></td>
<td>Range: 1025-65535</td>
</tr>
<tr>
<td><strong>SSH Port</strong></td>
<td>The SSH session port number to use if you selected SSH. Defaults:</td>
</tr>
<tr>
<td></td>
<td>USB Port U1: 3049</td>
</tr>
<tr>
<td></td>
<td>USB Port U2: 3050</td>
</tr>
<tr>
<td></td>
<td>Range: 1025-65535</td>
</tr>
<tr>
<td><strong>TCP Port</strong></td>
<td>The TCP (raw) session port number to use if you selected TCP. Defaults:</td>
</tr>
<tr>
<td></td>
<td>USB Port U1: 4049</td>
</tr>
<tr>
<td></td>
<td>USB Port U2: 4050</td>
</tr>
<tr>
<td></td>
<td>Range: 1025-65535</td>
</tr>
<tr>
<td><strong>Authenticate (checkbox)</strong></td>
<td>If selected, the SLC unit requires user authentication before granting access to the port. <strong>Authenticate</strong> is selected by default for <strong>Telnet Port</strong> and <strong>SSH Port</strong>, but not for <strong>TCP Port</strong>.</td>
</tr>
</tbody>
</table>

4. Click **Apply**.
Manage Firmware and Configuration Files

To manage any firmware and configuration files stored on a USB thumb drive, perform the following steps.

1. Click the **Manage Files on the Thumb Drive** link on the **Devices > USB > Configure** page.

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 File** 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** field.

5. Click **Rename File**.

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

<table>
<thead>
<tr>
<th>Files - USB Port U1</th>
<th>Date/Time Saved</th>
<th>SSH Keys</th>
<th>SSL Certificate</th>
<th>Scripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>slmodem-6b-6.1.0.0.tgz</td>
<td>06/21/14 18:00:52</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>sl48_252-61_all-600.tgz</td>
<td>06/24/14 03:08:06</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
USB Commands

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

- set usb access
- set usb modem
- set usb storage mount
- set usb storage unmount
- set usb storage dir
- set usb storage fsck
- set usb storage rename
- set usb storage copy
- set usb storage delete
- set usb storage format
- show usb
- show usb storage
- show usb modem
Chapter 8: Device Ports described how to configure and interact with an SLC device port connected to an external device. This chapter describes how to use the Devices > Connections page to connect external devices and outbound network connections (such as Telnet or SSH) in various configurations.

Types of Endpoints and Connections

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

- 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

This enables the user to set up connections such as those described in the next section. You can establish a connection at various times:

- Immediately. These connections are always re-established 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 re-established until the specified data passes through the connection.

Typical Setup Scenarios for the SLC Unit

Following are typical configurations in which SLC connections can be used, with references to settings on the Devices > Connections and Device Ports > Settings web pages.

Terminal Server

In this setup, the SLC console manager acts as a single server computer. Terminal devices are connected to the serial ports of the SLC unit and configured as a Device Port to Telnet out type connection on the Devices > 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.
Remote Access Server

In this setup, the SLC console manager is 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 unit 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 unit and connect to the command line interface.

Reverse Terminal Server

In this scenario, the SLC console manager has 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 device. To configure the SLC unit, select the Enable Telnet In or Enable SSH In option on the Device Ports > Settings page.
Multiport Device Server

A PC can use 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. To use the SLC unit in this setup, the PC requires special software, for example, Com Port Redirector (available on www.lantronix.com or similar software).

![Figure 11-4 Multiport Device Server](image)

Console Server

For this situation, the SLC console manager is configured so that the user can manage a number of servers or pieces of network equipment using their console ports. The device ports on the SLC unit are connected to the console ports of the equipment that the user would like to manage.

To manage a specific piece of equipment, the user can Telnet or SSH to a specific port or IP address on the SLC console manager and be connected directly to the console port of the end server or device.

To configure this setup, set the Enable Telnet In or Enable SSH In option on the Device Ports > Settings page for the device port in question. The user 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. A user could then dial into the SLC unit 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 select the Connections option. The following page displays:
2. For a device port, enter the following:

**Outgoing Connection Timeout**
- Select to turn on or turn off the connection timeout:
  - **No** for no timeout
  - **Yes** for a timeout. Specify the number of seconds in the seconds field.

**Port**
- The number of the device port you are connecting.
- This 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.
11: Connections

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

**To view, update, or disconnect a current connection:**

The bottom of the **Current Connections** page displays current connections.

**Figure 11-7 Current Connections**

<table>
<thead>
<tr>
<th>Current Connections</th>
<th>Configure</th>
<th>Terminate</th>
<th>Keep Connection</th>
<th>Restart</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port/Service</strong></td>
<td><strong>Flow</strong></td>
<td><strong>User</strong></td>
<td><strong>Time</strong></td>
<td></td>
</tr>
<tr>
<td>Device Port 5</td>
<td>Tel Out 172 19:39:22</td>
<td>N/A</td>
<td>0:00:58</td>
<td></td>
</tr>
<tr>
<td>Console Port</td>
<td>Command Line</td>
<td>N/A</td>
<td>4:24:30</td>
<td></td>
</tr>
<tr>
<td>Device Port 6</td>
<td>SSH Out 172 19:39:22</td>
<td>N/A</td>
<td>6:59:46</td>
<td></td>
</tr>
</tbody>
</table>

1. To view details about a connection, hold the mouse over the arrow icon in the **Flow** column.
2. To disconnect (delete) a connection, select the connection in the **Select** column and click the **Terminate** button.
3. To reestablish the connection, create the connection again in the top part of the page.
4. To view information about Web connections, click the here link in the text above the table. The **Maintenance > Firmware & Config** page displays.
Connection Commands
These commands for configuring connections correspond to the web page entries described above.

To connect to a device port to monitor and/or interact with it, or to establish an outbound network connection:

```
connect direct <endpoint>
```

**Endpoint is one of:**

```
deviceport <Port # or Name>
ssh <IP Address or Name> [port <TCP Port>] [<SSH flags>]
```

where <SSH flags> is one or more of:

```
user <Login Name>
version <1|2>
command <Command to Execute>
tcp <IP Address> [port <TCP Port>]
telnet <IP Address or Name> [port <TCP Port>]
udp <IP Address> [port <UDP Port>]
hostlist <Host List>
```

To configure initial timeout for outgoing connections:

```
connect global outgoingtimeout <disable|1-9999 seconds>
```

**Note:** This is not a TCP timeout.

To monitor a device port:

```
connect listen deviceport <Device Port # or Name>
```

To connect a device port to another device port or an outbound network connection (data flows in both directions):

```
connect bidirection <Port # or Name> <endpoint>
```

**Endpoint is one of:**

```
charcount <# of Chars>
charseq <Char Sequence>
charxfer <toendpoint|fromendpoint>
deviceport <Device Port # or Name>
date <MMDDYYhhmm[ss]>
exclusive <enable|disable>
ssh <IP Address or Name> [port <TCP Port>] [<SSH flags>]
```

where <SSH flags> is one or more of:

```
user <Login Name>
version <1|2>
command <Command to Execute>
tcp <IP Address> [port <TCP Port>]
telnet <IP Address or Name> [port <TCP Port>]
trigger <now|datetime|chars>
udp <IP Address> [port <UDP Port>]
```
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.

To connect a device port to another device port or an outbound network connection (data flows in one direction):

connect unidirection <Device Port # or Name> dataflow <toendpoint|fromendpoint> <endpoint>

Endpoint is one of:

- charcount <# of Chars>
- charseq <Char Sequence>
- datetime <MMDDYYhhmm[ss]>
- deviceport <Port # or Name>
- exclusive <enable|disable>
- ssh <IP Address or Name> [port <TCP Port>] >
  <SSH flags>

where <SSH flags> is one or more of:

- user <Login Name>
- version <1|2>
- command <Command to Execute>
- tcp <IP Address> [port <TCP Port>]
- telnet <IP Address or Name> [port <TCP Port>]
- trigger <now|datetime|chars>
- udp <IP Address> [port <UDP Port>]

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.

To terminate a bidirectional or unidirectional connection:

connect terminate <Connection ID>

To view connections and their IDs:

show connections [email <Email Address>].

You can optionally email the displayed information.

Note: The connection IDs are in the left column of the resulting table. The connection ID associated with a particular connection may change if connection times out and is restarted.

To display details for a single connection:

show connections connid <Connection ID> [email <Email Address>]

You can optionally email the displayed information.

To display global connections:

connect global show
12: User Authentication

Users who attempt to log in to the SLC console manager by means of Telnet, SSH, the console port, or one of the device ports are granted access by one or more authentication methods.

The User Authentication page provides a submenu of methods (Local Users, NIS, LDAP, RADIUS, Kerberos, and TACACS+) for authenticating users attempting to log in. Use this page to assign the order in which the SLC unit will use the methods. By default, local user authentication is enabled and is the first method the SLC console manager uses to authenticate users. If desired, you can disable local user authentication or assign it a lower precedence.

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

Authentication can occur using all methods, in the order of precedence, until a successful authentication is obtained, or using only the first authentication method that responds (in the event that a server is down).

If you have the same user name defined in multiple authentication methods, the result is unknown.

Example:
There is an LDAP user "joe" and an NIS user "joe" and the order of authentication methods is:
1. Local Users
2. LDAP
3. NIS

User "joe" tries to log in. Because there is an LDAP user "joe," the SLC unit tries to authenticate him against his LDAP password first. If he fails to log in, then the SLC device may (or may not) try to authenticate him against his NIS "joe" user password.

To enable, disable, and set the precedence of authentication methods:
1. From the main menu, select User Authentication. The following page displays:
2. To enable a method currently in the **Disabled methods** list, select the method and press the left arrow to the left of the list. The methods include:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NIS</strong> (Network Information System)</td>
<td>A network naming and administration system developed by Sun Microsystems for smaller networks. Each host client or server computer in the system has knowledge about the entire system. 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).</td>
</tr>
<tr>
<td><strong>LDAP</strong> (Lightweight Directory Access Protocol)</td>
<td>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.</td>
</tr>
<tr>
<td><strong>RADIUS</strong> (Remote Authentication Dial-In User Service)</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Kerberos</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
3. To disable a method currently in the **Enabled methods** list, select the method and click the right ► arrow between the lists.

4. To set the order in which the SLC unit will authenticate users, use the up ↑ and down ↓ arrows to the left of the **Enabled methods** list.

5. For **Attempt next method on authentication rejection**, you have the following options:
   - To enable the SLC console manager to use all methods, in order of precedence, until it obtains a successful authentication, select the check box. This is the default.
   - To enable the SLC device to use only the first authentication method that responds (in case a server is down or unavailable), clear the check box.

6. Click **Apply**.

Now that you have enabled one or more authentication methods, you must configure them.

### Authentication Commands

The following command for the command line interface corresponds to the web page entries described above.

#### To set ordering of authentication methods:

**Note:** Local Users authentication is always the first method used. Any methods omitted from the command will be disabled.

```
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>`

#### To view authentication methods and their order of precedence:

```
show auth
```
Local and Remote User Settings

The system administrator can configure the SLC console manager to use local accounts and remote accounts to authenticate users.

1. Click the User Authentication tab and select the Local/Remote Users option. The following page displays.

![Figure 12-2 User Authentication > Local/Remote Users]

The top of the page has entry fields 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.

The top of the page has entry fields 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/or remote users:

2. Enter the following:

<table>
<thead>
<tr>
<th>Enable Local Users</th>
<th>Select to enable all local users except sysadmin. The sysadmin is always available regardless of how you set the check box. Enabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Sysadmin Web Logins</td>
<td>Select to allow the sysadmin to have multiple simultaneous logins to the web interface. Disabled by default.</td>
</tr>
<tr>
<td>Sysadmin Access Limited to Console Port</td>
<td>Select to limit sysadmin logins to the Console Port only. Disabled by default.</td>
</tr>
<tr>
<td>Authenticate only remote users who are in the remote users list</td>
<td>Select the check box to authenticate users listed in the Remote Users list in the lower part of the page. Disabled by default.</td>
</tr>
</tbody>
</table>

3. Continue to set **Local User Passwords**:

<table>
<thead>
<tr>
<th>Complex Passwords</th>
<th>Select to enable the SLC unit to enforce rules concerning the password structure (e.g., alphanumeric requirements, number of characters, punctuation marks). Disabled by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity rules:</td>
<td>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 ( [ )-!@#$%^&amp;*+-={}[;]&quot;'&lt;&gt;,.?/_).</td>
</tr>
<tr>
<td>Allow Reuse</td>
<td>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.</td>
</tr>
<tr>
<td>Reuse History</td>
<td>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.</td>
</tr>
<tr>
<td>Password Lifetime (days)</td>
<td>The number of days until the password expires. The default setting is 90.</td>
</tr>
<tr>
<td>Warning Period (days)</td>
<td>The number of days ahead that the system warns that the user's password will expire. The default setting is 7.</td>
</tr>
<tr>
<td>Max Login Attempts</td>
<td>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).</td>
</tr>
<tr>
<td>Lockout Period (minutes)</td>
<td>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).</td>
</tr>
</tbody>
</table>

4. Click the **Apply** button.

**Adding, Editing or Deleting a User**

Through this **User Authentication > Local/Remote Users** page, you can delete a user listed in the table or open a page for adding or editing a user.

**To add a user:**

1. On the **User Authentication > Local/Remote Users**, click the **Add/Edit User** button. The **User Authentication > Local/Remote User > Settings** page displays.
2. Enter the following information for the user:

<table>
<thead>
<tr>
<th>Login</th>
<th>User ID of selected user.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td>Select the type of authenticated user:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Local</strong>: User listed in the SLC database.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Remote</strong>: User not listed in the SLC database.</td>
</tr>
<tr>
<td><strong>UID</strong></td>
<td>A unique numeric identifier the system administrator assigns to each user. Valid UIDs are 101-4294967295.</td>
</tr>
<tr>
<td>Note: The UID must be unique. If it is not, SLC console manager automatically increments it. Starting at 101, the SLC unit finds the next unused UID.</td>
<td></td>
</tr>
<tr>
<td><strong>Listen Ports</strong></td>
<td>The device ports that the user may access to view data using the <code>connect listen</code> command. Enter the port numbers or the range of port numbers (for example, 1, 5, 8, 10-15).</td>
</tr>
<tr>
<td><strong>Data Ports</strong></td>
<td>The device ports with which the user may interact using the <code>connect direct</code> command. Enter the port numbers or the range of port numbers.</td>
</tr>
<tr>
<td><strong>Clear Port Buffers</strong></td>
<td>The device port buffers the users may clear using the <code>set locallog clear</code> command. Enter the port numbers or the range of port numbers.</td>
</tr>
</tbody>
</table>
### 12: User Authentication

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable for Dial-back</strong></td>
<td>Select to grant a local user dial-back access. Users with dial-back access can dial into the SLC console manager and enter their login and password. Once the SLC unit authenticates them, the modem hangs up and dials them back. Disabled by default.</td>
</tr>
<tr>
<td><strong>Dial-back Number</strong></td>
<td>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 Port - Settings page), or on a number that is associated with the user's login (specified here).</td>
</tr>
<tr>
<td><strong>Escape Sequence</strong></td>
<td>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 &quot;A&quot; performed quickly but not simultaneously). You would specify this value as <code>\x1bA</code>, 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.</td>
</tr>
<tr>
<td><strong>Break Sequence</strong></td>
<td>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 &quot;B&quot; performed quickly but not simultaneously). You would specify this value as <code>\x1bB</code>, which is hexadecimal (\x) character 27 (1B) followed by a B.</td>
</tr>
<tr>
<td><strong>Custom Menu</strong></td>
<td>If custom menus have been created, you can assign a default custom menu to the user. The custom menu will display at login. <strong>Note:</strong> In the Local Users table, if the menu assigned to a local user no longer exists, it is marked with an asterisk (*).</td>
</tr>
<tr>
<td><strong>Display Menu at Login</strong></td>
<td>If custom menus have been created, select to enable the menu to display when the user logs into the CLI.</td>
</tr>
<tr>
<td><strong>Password / Retype Password</strong></td>
<td>When a user logs into the SLC console manager, the unit prompts for a password (up to 64 characters). The sysadmin establishes that password here.</td>
</tr>
<tr>
<td><strong>Password Expires</strong></td>
<td>If not selected, allows the user to keep a password indefinitely. If selected the user keeps the password for a set period. (See the section, Local and Remote User Settings (on page 168) for information on specifying the length of time before the password expires.)</td>
</tr>
<tr>
<td><strong>Allow Password Change</strong></td>
<td>Select to allow the user to change password.</td>
</tr>
<tr>
<td><strong>Change Password on Next Login</strong></td>
<td>Indicate whether the user must change the password at the next login.</td>
</tr>
<tr>
<td><strong>Lock Account</strong></td>
<td>Select to lock the account indefinitely.</td>
</tr>
</tbody>
</table>
| **Account Status**               | Displays the current account status:  
  - Active  
  - Locked  
  - 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.
12: User Authentication

4. Click the **Apply** button.

5. Click the **Back to Local/Remote Users** link to return to the Local/Remote User Settings page.

6. Add another user or click the **Back to Local/Remote Users** link. The Local/Remote Users page displays with the new user(s) listed in the table.

**Note:** The logged-in user’s name displays at the top of the web page. Only the tabs and options for which the user has rights display.

---

<table>
<thead>
<tr>
<th>Group</th>
<th>Select the group to which the user will belong:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td> <strong>Default Users:</strong> This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td></td>
<td> <strong>Power Users:</strong> This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td></td>
<td> <strong>Administrators:</strong> This group has all possible rights.</td>
</tr>
<tr>
<td></td>
<td> <strong>Custom Group:</strong> Select a custom group from the drop-down menu.</td>
</tr>
<tr>
<td>Full Administrative</td>
<td>Right to perform any function on the SLC console manager.</td>
</tr>
<tr>
<td>Networking</td>
<td>Right to enter network and routing settings.</td>
</tr>
<tr>
<td>Services</td>
<td>Right to enable and disable system and audit logging, SSH and Telnet logins, SNMP, and SMTP. Includes NFS and CIFS.</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>Right to view and manage Secure Lantronix units (e.g., SLP, Spider, and SLC units) on the local subnet.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td>Local Users</td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td>Remote Authentication</td>
<td>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.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td>User Menus</td>
<td>Right to create or edit a custom user menu for the CLI.</td>
</tr>
<tr>
<td>Web Access</td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td>Diagnostics &amp; Reports</td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td>Reboot &amp; Shutdown</td>
<td>Right to shutdown or reboot the SLC console manager.</td>
</tr>
<tr>
<td>Firmware &amp; Configuration</td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings).</td>
</tr>
<tr>
<td>Device Port Operations</td>
<td>Right to control device ports.</td>
</tr>
<tr>
<td>Device Port Configuration</td>
<td>Right to enter device port settings.</td>
</tr>
<tr>
<td>USB</td>
<td>Right to enter modem settings for USB. The USB checkbox is available for certain SLC and SLB models.</td>
</tr>
<tr>
<td>PC Card</td>
<td>Right to enter modem settings for PC cards. Includes managing storage PC cards. The PC card checkbox is available for certain SLC and SLB models.</td>
</tr>
</tbody>
</table>
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 Users Commands

The following CLI commands correspond to the web page entries described above.

To configure local accounts (including sysadmin) who log in to the SLC console manager by means of SSH, Telnet, the Web, or the console port:

```
set localusers add|edit <User Login> <parameters>
```

Parameters:

- `accessoutlets <Outlet List>`
- `allowdialback <enable|disable>`
- `breakseq <1-10 Chars>`
- `changenextlogin <enable|disable>`
- `changepassword <enable|disable>`
- `clearports <Port List>`
- `custommenu <Menu Name>`
To set whether a complex login password is required:
set localusers complexpasswords <enable|disable>

To enable or disable authentication of local users:
set localusers state <enable|disable>

To set a login password for the local user:
set localusers password <User Login>

To delete a local user:
set localusers delete <User Login>

To view settings for all users or a local user:
show localusers [user <User Login>]

To block (lock out) a user's ability to log in:
set localusers lock <User Login>

Note: This capability is not available on the web page.

To allow (unlock) a user's ability to log in:
set localusers unlock <User Login>

Note: This capability is not available on the web page.

Local User Rights Commands
The following CLI commands correspond to the web page entries described above.

To add a local user to a user group or to change the group the user belongs to:
set localusers add|edit <user> group <default|power|admin>

To set a local user's permissions (not defined by the user group):
set localusers add|edit <user> permissions <Permission List>

where
<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, ub, rs, rc, dr, wb, sn, ad, po, pc

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

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

show user

Remote User Commands

The following CLI commands correspond to the web page entries described above.

To configure whether remote users who are not part of the remote user list will be authenticated:

set remoteusers listonlyauth <enable|disable>

To configure attributes for users who log in by a remote authentication method:

set remoteusers add|edit <User Login> [parameters]

Parameters
accessoutlets <Outlet List>
breakseq <1-10 Chars>
clearports <Port List>
dataports <Port List>
escapeseq <1-10 Chars>
group <default|power|admin|Custom Group Name>
listenports <Port List>
permissions <Permissions List>

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, ub, rs, rc, dr, wb, sn, ad, po, pc

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

To remove a remote user:

set remoteusers delete <User Login>

To view settings for all remote users:

show remoteusers

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

show user
12: User Authentication

NIS

The system administrator can configure the SLC console manager to use NIS to authenticate users attempting to log in to the SLC unit 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 unit to use NIS to authenticate users:

1. Click the User Authentication tab and select the NIS option.

Figure 12-4  User Authentication > NIS

The SLC can be configured to use NIS to authenticate users who log in to the SLC via SSH, Telnet, the Web or the Console Port. NIS users are granted Device Port access through the port permissions below:

- NIS Master Server
- NIS Slave Server #1
- NIS Slave Server #2
- NIS Slave Server #3
- NIS Slave Server #4
- NIS Slave Server #5

Data Ports 7, U, L

Escape Sequence \x1B a
Break Sequence \x1B b

Enable for Dial-back

Dial-back Number

User Rights

Full Administrative
Networking
Services
Secure Lantronix 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:

<table>
<thead>
<tr>
<th>Enable NIS</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIS Domain</td>
<td>The NIS domain of the SLC console manager must be the same as the NIS domain of the NIS server.</td>
</tr>
<tr>
<td>Broadcast for NIS Server</td>
<td>If selected, the SLC unit sends a broadcast datagram to find the NIS Server on the local network.</td>
</tr>
<tr>
<td>NIS Master Server (required)</td>
<td>The IP address or host name of the master server.</td>
</tr>
<tr>
<td>NIS Slave Servers #1-5</td>
<td>The IP addresses or host names of up to five slave servers.</td>
</tr>
<tr>
<td>Custom Menu</td>
<td>If custom menus have been created, you can assign a default custom menu to NIS users.</td>
</tr>
<tr>
<td>Escape Sequence</td>
<td>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 \x1bA (escape key, then uppercase &quot;A&quot; 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.</td>
</tr>
<tr>
<td>Break Sequence</td>
<td>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 \x1bB (escape key, then uppercase &quot;B&quot; performed quickly but not simultaneously). You would specify this value as \x1bB, which is hexadecimal (\x) character 27 (1B) followed by a B.</td>
</tr>
<tr>
<td>Enable for Dial-back</td>
<td>Select to grant a user Dial-back (on page 136). 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.</td>
</tr>
<tr>
<td>Dial-back Number</td>
<td>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).</td>
</tr>
<tr>
<td>Data Ports</td>
<td>The ports users are able to monitor and interact with using the connect direct command.</td>
</tr>
<tr>
<td>Listen Ports</td>
<td>The ports users are able to monitor using the connect listen command.</td>
</tr>
<tr>
<td>Clear Port Buffers</td>
<td>The ports whose port buffer users may clear using the set locallog clear command.</td>
</tr>
</tbody>
</table>

3. In the User Rights section, select the user Group to which NIS users will belong:

<table>
<thead>
<tr>
<th>Group</th>
<th>Select the group to which the NIS users will belong:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Users</td>
<td>This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td>Power Users</td>
<td>This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</td>
</tr>
<tr>
<td>Administrators</td>
<td>This group has all possible rights.</td>
</tr>
</tbody>
</table>
4. Assign or unassign **User Rights** for the specific user by checking or unchecking the following checkboxes:

<table>
<thead>
<tr>
<th>Full Administrative</th>
<th>Right to add, update, and delete all editable fields.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td>Services</td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>Right to view and manage Secure Lantronix units (e.g., SLP, Spider, SLC, and SLB units) on the local subnet.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td>Local Users</td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td>Remote Authentication</td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td>User Menus</td>
<td>Right to create a custom user menu for the CLI for NIS users.</td>
</tr>
<tr>
<td>Web Access</td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td>Diagnostics &amp; Reports</td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td>Reboot &amp; Shutdown</td>
<td>Right to use the CLI or shut down the SLC console manager and then reboot it.</td>
</tr>
<tr>
<td>Firmware &amp; Configuration</td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot &amp; Shutdown.</td>
</tr>
<tr>
<td>Device Port Operations</td>
<td>Right to control device port settings.</td>
</tr>
<tr>
<td>Device Port Configuration</td>
<td>Right to enter device port settings.</td>
</tr>
<tr>
<td>USB</td>
<td>Right to enter modem settings for USB. The USB checkbox is available for certain SLC and SLB models.</td>
</tr>
<tr>
<td>PC Card</td>
<td>Right to enter modem settings for PC cards. Includes managing storage PC cards. The PC card checkbox is available for certain SLC and SLB models.</td>
</tr>
</tbody>
</table>

5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

**NIS Commands**

These commands for the CLI correspond to the web page entries described above.

To configure the SLC unit to use NIS to authenticate users who log in via the Web, SSH, Telnet, or the console port:

```
set nis <one or more parameters>
```

**Parameters:**

- `accessoutlets <Outlet List>`
- `breakseq <1-10 Chars>`
- `broadcast <enable|disable>`
- `clearports <Port List>`
- `dataports <Port List>`
- `domain <NIS Domain Name>`
To set group and permissions for NIS users:

```
set nis group <default|power|admin>
```

To set permissions for NIS users not already defined by the user rights group:

```
set nis permissions <Permission List>
```

where

```
<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, ub, rs, rc, dr, wb, sn, ad, po, pc
```

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

To set a default custom menu for NIS users:

```
set nis custommenu <Menu Name>
```

To view NIS settings:

```
show nis
```

**LDAP**

The system administrator can configure the SLC console manager to use LDAP to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

LDAP allows SLC users to authenticate 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.

Users who are authenticated through LDAP are granted device port access through the port permissions on this page.

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.

To configure the SLC unit to use LDAP to authenticate users:

1. Click the **User Authentication** tab and select **LDAP**. The following page displays.
2. Enter the following:

<table>
<thead>
<tr>
<th>Enable LDAP</th>
<th>Displays selected if you enabled this method on the first User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The IP address or host name of the LDAP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Number of the TCP port on the LDAP server to which the SLC talks. The default is 389.</td>
</tr>
<tr>
<td>Base</td>
<td>The name of the LDAP search base (e.g., dc=company, dc=com). May have up to 80 characters.</td>
</tr>
</tbody>
</table>

If port permissions are not provided via LDAP Schema, LDAP users are granted Device Port access through the port permissions below.
<table>
<thead>
<tr>
<th><strong>Bind Name</strong></th>
<th>The name for a non-anonymous bind to an LDAP server. This item has the same format as LDAP Base. One example is cn=admin,ou=Users,dc=domain,dc=com</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bind Password / Retype Password</strong></td>
<td>Password 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.</td>
</tr>
<tr>
<td><strong>Bind with Login</strong></td>
<td>Select to bind with the login and password that a user is authenticating with. This requires that the Bind Name contain the $login token, which will be replaced with the current login. For example, if the Bind Name is <code>uid=$login,ou=People,dc=lantronix,dc=com</code>, and user roberts logs in to the SLC, LDAP will bind with <code>uid=roberts,ou=People,dc=lantronix,dc=com</code> and the password entered by roberts.</td>
</tr>
<tr>
<td><strong>User Login Attribute</strong></td>
<td>The attribute used by the LDAP server for user logins. If nothing is specified for the user filter, the SLC unit will use &quot;uid&quot;. For AD LDAP servers, the attribute for user logins is typically &quot;sAMAccountName&quot;.</td>
</tr>
<tr>
<td><strong>Group Filter Objectclass</strong></td>
<td>The objectclass used by the LDAP server for groups. If nothing is specified for the group filter, the SLC device will use &quot;posixGroup&quot;. For AD LDAP servers, the objectclass for groups is typically &quot;Group&quot;.</td>
</tr>
<tr>
<td><strong>Group Member Attribute</strong></td>
<td>The attribute used by the LDAP server for group membership. This attribute may be used to search for a name (ie, &quot;msmith&quot;) or a Distinguished Name (ie, &quot;uid=msmith,ou=People,dc=lantronix,dc=com&quot;). Select either Name or DN as appropriate for the LDAP server. If nothing is specified for the group membership attribute, the SLC console manager will use &quot;memberUID&quot; for name and &quot;uniqueMember&quot; for DN. For AD LDAP servers, the Group Membership Value is typically DN, with the Group Membership Attribute of &quot;member&quot;.</td>
</tr>
<tr>
<td><strong>Group Member Value</strong></td>
<td>The attribute used by the LDAP server for group membership. This attribute may be used to search for a name (ie, &quot;msmith&quot;) or a Distinguished Name (ie, &quot;uid=msmith,ou=People,dc=lantronix,dc=com&quot;). Select either Name or DN as appropriate for the LDAP server. If nothing is specified for the group membership attribute, the SLC unit will use &quot;memberUID&quot; for name and &quot;uniqueMember&quot; for DN. For AD LDAP servers, the Group Membership Value is typically DN, with the Group Membership Attribute of &quot;member&quot;.</td>
</tr>
<tr>
<td><strong>Use LDAP Schema</strong></td>
<td>Select the check box to obtain remote user attributes (group/permissions and port access) from an Active Directory server's scheme via the user attribute 'SecureLinxSLCPerms'. See <strong>User Attributes &amp; Permissions from LDAP Schema or RADIUS VSA on page 189</strong>. Disabled by default.</td>
</tr>
<tr>
<td><strong>Active Directory Support</strong></td>
<td>Select 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.</td>
</tr>
</tbody>
</table>
### Encrypt Messages
Select Start TLS or SSL to encrypt messages between the SLC or SLB unit and the LDAP server. If Start TLS is selected, the port will automatically be set to 389 and the StartTLS extension will be used to initiate a secure connection; if SSL is selected, the port will automatically be set to 636 and a SSL tunnel will be used for LDAP communication. The port number can be changed to a non-standard LDAP port; if the port number is set to anything other than 636, Start TLS will be used as the encryption method. Disabled by default.

A certificate can be uploaded to the SLC or SLB unit for peer authentication. The certificate file is a file of CA certificates in PEM format. The file can contain several CA certificates identified by:

```
-----BEGIN CERTIFICATE-----
(CA certificate in base64 encoding)
-----END CERTIFICATE-----
```

sequences. Before, between, and after the certificates text is allowed which can be used e.g. for descriptions of the certificates.

### Custom Menu
If custom menus have been created, you can assign a default custom menu to LDAP users. (See Custom Menus on page 209.)

### Escape Sequence
A single character or a two-character sequence that causes the SLC unit 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 console manager and enter their login and password. Once the SLC unit 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.

### 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 locallog clear command.

3. In the **User Rights** section, select the user group to which LDAP users will belong:

### Group
Select the group to which the LDAP users 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.
- **Administrators:** This group has all possible rights.
4. Select or clear the checkboxes for the following rights:

<table>
<thead>
<tr>
<th>Right Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Administrative</td>
<td>Right to add, update, and delete all editable fields.</td>
</tr>
<tr>
<td>Networking</td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td>Services</td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>Right to view and manage Secure Lantronix units (e.g., SLP, Spider, SLB, and SLC units) on the local subnet.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td>Local Users</td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td>Remote Authentication</td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td>User Menus</td>
<td>Right to create a custom user menu for the CLI for LDAP users.</td>
</tr>
<tr>
<td>Web Access</td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td>Diagnostics &amp; Reports</td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td>Reboot &amp; Shutdown</td>
<td>Right to use the CLI or shut down the SLC console manager and then reboot it.</td>
</tr>
<tr>
<td>Firmware &amp; Configuration</td>
<td>Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot &amp; Shutdown.</td>
</tr>
<tr>
<td>Device Port Operations</td>
<td>Right to control device ports.</td>
</tr>
<tr>
<td>Device Port Configuration</td>
<td>Right to enter device port settings.</td>
</tr>
<tr>
<td>USB</td>
<td>Right to enter modem settings for USB. The USB checkbox is available for certain SLC and SLB models.</td>
</tr>
<tr>
<td>PC Card</td>
<td>Right to enter modem settings for PC cards. Includes managing storage PC cards. The PC card checkbox is available for certain SLC and SLB models.</td>
</tr>
</tbody>
</table>

5. Click the **Apply** button.

*Note:* You must reboot the unit before your changes will take effect.

**LDAP Commands**

These commands for the command line interface correspond to the web page entries described above.

To configure the SLC unit to use LDAP to authenticate users who log in via the Web, SSH, Telnet, or the console port:

set ldap <one or more parameters>

**Parameters:**

accessoutlets <Outlet List>
adsupport <enable|disable>

Enables or disables active directory.

base <LDAP Base>
bindname <Bind Name>
breakseq <1-10 Chars>
dataports <Ports List>
listenports <Port List>
clearports <Port List>
escapeseq <1-10 Chars>
bindpassword <Bind Password>
encrypt <starttls|ssl|disable>
filteruser <User Login Attribute>
filtergroup <Group Objectclass>
grmemberattr <Group Membership Attribute>
grmembervalue <dn|name>
port <TCP Port>

**Default is 389.**

server <IP Address or Hostname>
state <enable|disable>

**To set user group and permissions for LDAP users:**

group <default|power|admin>

**To set permissions for LDAP users not already defined by the user rights group:**

permissions <Permission List>

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, ub, rs, rc, dr, wb, sn, ad, po, pc

**To remove a permission, type a minus sign before the two-letter abbreviation for a user right.**

**To set a default custom menu for LDAP users:**

custommenu <Menu Name>

**To view LDAP settings:**

show ldap
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 unit to use RADIUS to authenticate users:

1. Click the User Authentication tab and select RADIUS. The following page displays.

![User Authentication > RADIUS](image)

Enable RADIUS: ☑️
RADIUS Server #1: 172.19.30.20
Server #1 Port: 1812
Server #1 Secret: 1234
RADIUS Server #2:
Server #2 Port: 1845
Server #2 Secret: 1234
Timeout: 5 seconds
Use VSA: ☑️

User Methods: LDAP
Local/Remote Users: 
NIS
LDAP
RADIUS
Kerberos
TACACS+
Groups
SSH Keys
Custom Menus

![User Rights](image)

Group:
- Default Users
- Power Users
- Administrators

Full Administrative: ☑️
Networking: ☑️
Services: ☑️
Secure Lantronix Network: ☑️
DateTime: ☑️

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:

<table>
<thead>
<tr>
<th><strong>Enable RADIUS</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RADIUS Server #1</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Server #1 Port</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Server #1 Secret</strong></td>
<td>Text that serves as a shared secret between a RADIUS client and the server (SLC). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.</td>
</tr>
<tr>
<td><strong>RADIUS Server #2</strong></td>
<td>IP address or host name of the secondary RADIUS server. This server can be used as a SecurID proxy.</td>
</tr>
<tr>
<td><strong>Server #2 Port</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Server #2 Secret</strong></td>
<td>Text that serves as a shared secret between a RADIUS client and the server (SLC). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>The number of seconds (1-30) after which the connection attempt times out. The default is 30 seconds.</td>
</tr>
<tr>
<td><strong>Use VSA</strong></td>
<td>Select the check box to obtain remote user attributes (group/permissions and port access) from the RADIUS server via the Vendor-Specific Attribute (VSA). For details on the format of the VSA, see User Attributes &amp; Permissions from LDAP Schema or RADIUS VSA on page 189.</td>
</tr>
<tr>
<td><strong>Custom Menu</strong></td>
<td>If custom menus have been created, you can assign a default custom menu to RADIUS users.</td>
</tr>
<tr>
<td><strong>Escape Sequence</strong></td>
<td>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 &quot;A&quot; 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.</td>
</tr>
<tr>
<td><strong>Break Sequence</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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 unit 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.

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 locallog 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 will belong.

<table>
<thead>
<tr>
<th>Group</th>
<th>Select the group to which the RADIUS users will belong:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Users</td>
<td>This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td>Power Users</td>
<td>This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</td>
</tr>
<tr>
<td>Administrators</td>
<td>This group has all possible rights.</td>
</tr>
</tbody>
</table>

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 Lantronix units (e.g., SLP, Spider, SLC and SLB unit) 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. |
| Web Access | Right to access Web-Manager. |
| Diagnostics & Reports | Right to obtain diagnostic information and reports about the unit. |
| Reboot & Shutdown | Right to use the CLI or shut down the SLC 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. |
| Device Port Operations | Right to control device ports. |
| Device Port Configuration | Right to access to port settings. |
5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

### RADIUS Commands

These commands for the command line interface correspond to the web page entries described above.

**To configure the SLC console manager to use RADIUS to authenticate users who log in via the Web, SSH, Telnet, or the console port:**

```
set radius <one or more parameters>
```

**Parameters:**

- `accessoutlets <Outlet List>`
- `breakseq <1-10 Chars>`
- `clearports <Port List>`
- `dataports <Port List>`
- `escapeseq <1-10 Chars>`
- `listenports <Port List>`
- `state <enable|disable>`

**To identify the RADIUS server(s), the text secret, and the number of the TCP port on the RADIUS server:**

```
set radius server <1|2> host <IP Address or Hostname> secret <Secret> [port <TCP Port>]
```

*The default port is **1812**.*

**To set the number of seconds after which the connection attempt times out:**

```
set radius timeout <disable|1-30>
```

*May be 1-30 seconds.*

**To set user group and permissions for RADIUS users:**

```
set radius group <default|power|admin>
```

**To set permissions for RADIUS users not already defined by the user rights group:**

```
set radius permissions <Permission List>
```

*where*

- `<Permission List>` is one or more of `nt, sv, dt, lu, ra, sk, um, dp, ub, rs, rc, dr, wb, sn, ad, po, pc`
To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

To set a default custom menu for RADIUS users:

set radius custommenu <Menu Name>

To view RADIUS settings:

show radius

User Attributes & Permissions from LDAP Schema or RADIUS VSA

Remote user attributes (group/permissions and port access) can be obtained from an Active Directory server's schema via the user attribute 'secureLinxSLCPerms', or from a RADIUS server's Vendor-Specific Attribute (see below). 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. Whitespace is not supported in the value strings. The parameters that are supported are:

- **rights** - User rights. The value string is a comma-separated list of two letter user permissions. Example: "nt,wb,ra".
- **data** - Data port access. The value string specifies the list of ports the user has 'direct' access to. Example: "2,4-18,U,L".
- **listen** - Listen port access. The value string specifies the list of ports the user has 'listen' access to.
- **clear** - Clear port access. The value string specifies the list of port buffers the user has the right to clear.
- **group** - User group. Valid values for the value string are "default", "power", and "admin", and any SLC or SLB custom group name. If a custom group name is specified and it matches a current SLC custom group name, any rights attribute will be ignored, and the custom group's rights (permissions) will be used instead. A group name with spaces cannot be specified.
- **escseq** - Escape sequence. The value string specifies the user's escape sequence. Use "\x" to specify non-printable characters. For example, "\x1bA" specifies the sequence "ESC-A".
- **brkseq** - Break sequence. The value string specifies the user's break sequence.
- **menu** - Custom user menu. The value string specifies the user's custom user menu.
- **display** - Display custom user menu when a user logs into the CLI. Valid values for the value string are "yes" and "no".
- **dbnumber** - Dial-back number. The value string specifies the user's dial-back number for modem dial-back connections.
- **allowdb** - Allow a user to have dial-back access. Valid values for the value string are "yes" and "no".

RADIUS servers will need to be configured to support the Lantronix Vendor-Specific Attribute. For example, on a FreeRADIUS server, the dictionary will need be updated with the Lantronix definition by including the contents below in a file named `dictionary.lantronix`, and including it in the RADIUS server dictionary definitions by adding the appropriate `$INCLUDE` directive to the main dictionary file.
Once this is complete, the users file can be updated to include the Lantronix VSA for any user:

```
myuser    Auth-Type := Local, User-Password == "myuser_pwd"
          Reply-Message = "Hello, %u",
          Lantronix-User-Attributes = "data 1-4 listen 1-6 clear 1-4 group power"
```

### 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 unit to use Kerberos to authenticate users:**

1. Click the **User Authentication** tab and select the **Kerberos** option. The following page displays.
2. Enter the following:

**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).
## 12: User Authentication

| **KDC Port** | Port on the KDC listening for requests. Enter an integer with a maximum value of 65535. The default is **88**. |
| **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. |
| **Custom Menu** | If custom menus have been created, 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 unit 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, 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. |
| **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 locallog clear` command. |

### 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 Lantronix units (e.g., SLP, Spider, SLC and SLB units) 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.

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. 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.  
**Administrators:** This group has all possible rights. |

4. Select or clear the checkboxes for the following rights:
5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

**Kerberos Commands**

These commands for the command line interface correspond to the web page entries described above.

To configure the SLC unit to use Kerberos to authenticate users who log in via the Web, SSH, Telnet, or the console port:

```
set kerberos <one or more parameters>
```

**Parameters:**

- `accessoutlets <Outlet List>
- `breakseq <1-10 Chars>
- `clearports <Port List>
- `dataports <Port List>
- `escapeseq <1-10 Chars>
- `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>

To set user group and permissions for Kerberos users:

```
set kerberos group <default|power|admin>
```
To set permissions for Kerberos users not already defined by the user rights group:

```
set kerberos permissions <Permission List>
```

where

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, ub, rs, rc, dr, wb, sn, ad, po, pc

To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

To set a default custom menu for Kerberos users:

```
set kerberos custommenu <Menu Name>
```

To view Kerberos settings:

```
show kerberos
```

**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+**. The following page displays.
2. Enter the following:

**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 unit 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.
12: User Authentication

3. In the **User Rights** section, select the user group to which TACACS+ users will belong.

<table>
<thead>
<tr>
<th>Group</th>
<th>Select the group to which the TACACS+ users will belong:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◆ <strong>Default Users</strong>: This group has only the most basic rights. You can specify additional rights for the individual user.</td>
</tr>
<tr>
<td></td>
<td>◆ <strong>Power Users</strong>: This group has the same rights as Default Users plus Networking, Date/Time, Reboot &amp; Shutdown, and Diagnostics &amp; Reports.</td>
</tr>
<tr>
<td></td>
<td>◆ <strong>Administrators</strong>: This group has all possible rights.</td>
</tr>
</tbody>
</table>

4. Select or clear the checkboxes for the following rights:

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Administrative</strong></td>
<td>Right to add, update, and delete all editable fields.</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td>Right to enter Network settings.</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td><strong>Secure Lantronix Network</strong></td>
<td>Right to view and manage Secure Lantronix units (e.g., SLP and Spider units) on the local subnet.</td>
</tr>
<tr>
<td><strong>Date/Time</strong></td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td><strong>Local Users</strong></td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td><strong>Remote Authentication</strong></td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td><strong>SSH Keys</strong></td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td><strong>User Menus</strong></td>
<td>Right to create a custom user menu for the CLI for TACACS+ users.</td>
</tr>
<tr>
<td><strong>Web Access</strong></td>
<td>Right to access Web-Manager.</td>
</tr>
</tbody>
</table>
5. Click the **Apply** button.

**Note:** You must reboot the unit before your changes will take effect.

**TACACS+ Commands**

These commands for the command line interface correspond to the web page entries described above.

To configure the SLC console manager to use TACACS+ to authenticate users who log in via the Web, SSH, Telnet, or the console port:

```plaintext
set tacacs+ <one or more parameters>
```

**Parameters:**

accessoutlets <Outlet List>
breakseq <1-10 Chars>
clearports <Port List>
dataports <Port List>
encrypt <enable|disable>
escapeseq <1-10 Chars>
listenports <Port List>
secret <TACACS+ Secret>
server1 <IP Address or Name>
server2 <IP Address or Name>
server3 <IP Address or Name>
state <enable|disable>

To set user group and permissions for TACACS+ users:

```plaintext
set tacacs+ group <default|power|admin>
```

To set permissions for TACACS+ users not already defined by the user rights group:

```plaintext
set tacacs+ permissions <Permission List>
```

**where**

<Permission List> is one or more of nt, sv, dt, lu, ra, sk, um, dp, ub, rs, rc, dr, wb, sn, ad, po, pc
To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

To set a default custom menu for TACACS+ users:

set tacacs+ custommenu <Menu Name>

To view TACACS+ settings:

show tacacs+

Groups

The SLC console manager has 3 pre-defined groups: Administrators, Power Users, and Default Users. Custom groups can also be created; each custom group is a set of user attributes and permissions. Local Users and Remote Users defined on the SLC unit can be assigned to one of the pre-defined groups or a custom group. When a user authenticates, if they belong to custom group, they will be granted the custom group attributes and permissions, rather than their individual attributes and permissions. The SLC device supports querying a LDAP server for groups that a LDAP user is a member of; if any of the LDAP group names match a (Custom Group Name), the LDAP user will be granted the rights of the custom group.

A custom group cannot be given the name of one of the pre-defined groups: "Admin", "Power" or "Default" (or any version of these names where the case of the letters is different) since these names are used for the SLC pre-defined groups. Any LDAP group that matches one of these pre-defined group names will be ignored and not used to assign rights to a user.

To configure Groups in the SLC console manager:

1. From the main menu, select User Authentication - Groups. The following page displays.

Note: If the fields in the lower part of the page have been populated by viewing another group, the fields can be cleared by selecting the Reset Group button.
2. Enter the following:

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Enter a name for the group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen Ports</td>
<td>The ports users are able to monitor using the <code>connect listen</code> command.</td>
</tr>
</tbody>
</table>
3. Select or clear the checkboxes for the following rights:

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Administrative</td>
<td>Right to add, update, and delete all editable fields.</td>
</tr>
<tr>
<td>Networking</td>
<td>Right to enter network settings.</td>
</tr>
<tr>
<td>Services</td>
<td>Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.</td>
</tr>
<tr>
<td>Secure Lantronix Network</td>
<td>Right to view and manage Secure Lantronix units (e.g., SLP, Spider, or SLC units) on the local subnet.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Right to set the date and time.</td>
</tr>
<tr>
<td>Local Users</td>
<td>Right to add or delete local users on the system.</td>
</tr>
<tr>
<td>Remote Authentication</td>
<td>Right to assign a remote user to a user group and assign a set of rights to the user.</td>
</tr>
<tr>
<td>SSH Keys</td>
<td>Right to set SSH keys for authenticating users.</td>
</tr>
<tr>
<td>User Menus</td>
<td>Right to create or edit a custom user menu for the CLI.</td>
</tr>
<tr>
<td>Web Access</td>
<td>Right to access Web-Manager.</td>
</tr>
<tr>
<td>Diagnostics &amp; Reports</td>
<td>Right to obtain diagnostic information and reports about the unit.</td>
</tr>
<tr>
<td>Reboot &amp; Shutdown</td>
<td>Right to use the CLI or shut down the SLC device and then reboot it.</td>
</tr>
</tbody>
</table>
4. Click the Add Group button.

To view or update a group:

1. In the Groups table, select the group and click the View Group button. The group attributes and permissions will be displayed in the lower section of the page.
2. Modify the group attributes and permissions and click the Edit Group button.

To delete a group:

1. Select the group in the Groups table.
2. Click the Delete Group button.

**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 unit 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 device 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 console manager can generate SSH keys for SSH connections out of the SLC device 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 unit for the designated host/user combination uses the SSH key for authentication.

To configure the SLC unit to use SSH keys to authenticate users:

1. From the main menu, select User Authentication - SSH Keys. The following page displays.
2. Enter the following:

**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, or
- The imported key file contains multiple keys; in this case, each key must include the user name and host at the end of the line in the standard "<key> <user name>@<host>" format.

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-rsa AAAAB3NzaC1yc2EAAAABAIAwAAAEEAepUHCX9EwsHt+jmUGXa1YC3usABYxIXUhSU1N+NU9HNaUADUFPfd8LYz8/gUnUSH4Ksm8GRT7/8/Sn9jCVfGPhUQ== asallaway@winserver
```

<table>
<thead>
<tr>
<th>Host</th>
<th>The host name or IP address which will be associated with the SSH Key, typically the host that the key was generated on. Once imported, the key can be used to access the SLC unit from any host, not just the host associated with the key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The User ID of the user being given secure access to the SLC console manager.</td>
</tr>
</tbody>
</table>

**Host & Login for Import**

<table>
<thead>
<tr>
<th>Import via</th>
<th>Select SCP, FTP, HTTPS and Copy/Paste as the method for importing the SSH keys. SCP is the default. If SCP or FTP are selected, the Filename, Host, Path, Login, and Password fields are filled in. If HTTPS is selected, the Upload File link will become active to upload a file containing a public key to the SLC. If Copy/Paste is selected, the public key will be entered into the Filename/Public Key field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename/Public Key</td>
<td>The name of the file that was uploaded via HTTPS, or to be copied via SCP or FTP (may contain multiple keys); or the public key (optionally including &quot;user@host&quot; at the end) if Copy/Paste is used.</td>
</tr>
<tr>
<td>Host</td>
<td>IP address of the remote server from which to SCP or FTP the public key file.</td>
</tr>
<tr>
<td>Path</td>
<td>Optional pathname to the public key file.</td>
</tr>
<tr>
<td>Login</td>
<td>User ID to use to SCP or FTP the file.</td>
</tr>
<tr>
<td>Password / Retype Password</td>
<td>Password to use to SCP or FTP the file.</td>
</tr>
</tbody>
</table>

**Exported Keys (SSH Out)**

<table>
<thead>
<tr>
<th>Export</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User ID of the person given secure access to the remote server.</td>
</tr>
<tr>
<td>Key Name</td>
<td>Name of the key. This will generate the public key filename (e.g., &lt;keyname&gt;.pub),</td>
</tr>
<tr>
<td>Key Type</td>
<td>Select either the RSA or the DSA encryption standard. RSA is the default.</td>
</tr>
<tr>
<td>Number of Bits</td>
<td>Select the number of bits in the key (1024 or 2048). The default is 1024.</td>
</tr>
<tr>
<td>Passphrase / Retype Passphrase</td>
<td>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.</td>
</tr>
<tr>
<td>SECSH Format</td>
<td>Indicate whether the keys will be exported in SECSH format (by default the key is exported in OpenSSH format).</td>
</tr>
<tr>
<td>Public Key Filename</td>
<td>Filename of the public host key.</td>
</tr>
</tbody>
</table>
Host and Login for Export

<table>
<thead>
<tr>
<th>Export via</th>
<th>Select the method (SCP, FTP, HTTPS, or Cut and Paste) of exporting the key to the remote server. Cut and Paste, the default, requires no other parameters for export.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address of the remote server to which the SLC console manager will SCP or FTP the public key file.</td>
</tr>
<tr>
<td>Path</td>
<td>Optional path of the file on the host to SCP or FTP the public key too.</td>
</tr>
<tr>
<td>Login</td>
<td>User ID to use to SCP or FTP the public key file.</td>
</tr>
<tr>
<td>Password /</td>
<td>Password to use to SCP or FTP the public key file.</td>
</tr>
<tr>
<td>Retype Password</td>
<td></td>
</tr>
</tbody>
</table>

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 AAAAB3NzaC1yc2EAAAABIwAAAIAEAxGxPGY9HsG9VqroDo98B89Cf haqB6jG//0tTMKkb3zrpPu0HHAXaixVXHAVv71Ate31VToXdLAXN0uCvuJLf aL/LvvGmoEWBuBSu5051qZnL70ijxZWOEvTJGFqUQTSq8Ls3/v31kJUJEX51n 2A1Qx0F40I5wNCE0+m3dQE+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. The following page displays the current host keys. In the example below, the current keys are the defaults.

![Current Host Keys](image)

**SSH Server/Host Keys**

**Current Host RSA Public Key (Default Key)**

```
```

**Current Host RSA Public Key (Default Key)**

```
ssh-rsa AAAAAB33zC1ycZBAAAABImnl1iF/86E0e9CRv3b10+P0vevAPH1+4sh0brX1LXnJ8nc
EnvVDeemVvLsawVZcZ94vWV7F8Lgo3qQW8ghvZ7105kZvWQuQAig/OK9L1cO/3NV08pXaANMVXKC
IAYVIG quiltxx5QyPwOcropz2ElDBSFGtqW199qCCCFPP64ozrr+eCq4je72KLMXvHawuFpdp14ldt331
D7YtvakRMJ3C6/mLZItXmnnb1iCTvevqd7kVhV7Ah7uS8L0d1NqAvAA/PgJhNC5N3M35E7YAdLcK7d
0qgW9Wkypuji32kvWcFf1r62zjAhnuC6rXKC+ajrX831K9sy56pYw== root@eic0737?
```

Fingerprint:

**Current Host DSA Public Key (Default Key)**

```
ssh-dss AAAAAB33zC1ycZBAAAABImnl1iF/86E0e9CRv3b10+P0vevAPH1+4sh0brX1LXnJ8nc
EnvVDeemVvLsawVZcZ94vWV7F8Lgo3qQW8ghvZ7105kZvWQuQAig/OK9L1cO/3NV08pXaANMVXKC
IAYVIG quiltxx5QyPwOcropz2ElDBSFGtqW199qCCCFPP64ozrr+eCq4je72KLMXvHawuFpdp14ldt331
D7YtvakRMJ3C6/mLZItXmnnb1iCTvevqd7kVhV7Ah7uS8L0d1NqAvAA/PgJhNC5N3M35E7YAdLcK7d
0qgW9Wkypuji32kvWcFf1r62zjAhnuC6rXKC+ajrX831K9sy56pYw== root@eic0737?
```

Fingerprint:

**Reset to Default Host Key**

- **All Keys**
- **RSA**
- **DSA**

**Note:** changing a host key requires a reboot for the update to take effect.

**Import Host Key**

- **Type:** RSA1
- **Import via:** SCP

**Host:**

**Path:**

**Login:**

**Password:**

**Re-type Password:**

**Back to SSH Keys**

**Apply**
2. View or enter the following:

| 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.
4. Repeat steps 2-3 for each key you want to import.
5. To return to the SSH Keys page, click the Back to SSH Keys link.

**SSH Commands**

These commands for the command line interface correspond to the web page entries described above.

**To import an SSH key:**

```
set sshkey import <ftp|scp> <one or more parameters>
```

**Parameters:**

- [keyhost <SSH Key IP Address or Name>]
- [keyuser <SSH Key User>]
- [path <Path to Public Key File>]
- file <Public Key File>
- host <IP Address or Name>
- login <User Login>

**To export a key:**

```
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 <1024|2048>
- keyname <SSH Key Name>
- keyuser <SSH Key User>
- type <rsa|dsa>
To export the public keys of all previously created SSH keys:

set sshkey all export <ftp|scp|copypaste> [pubfile <Public Key File>] [host <IP Address or Name>] [login <User Login>] [path <Path to Copy Keys>]

To delete a key:

set sshkey delete <one or more parameters>

Parameters:
keyhost <SSH Key Host>
keyname <SSH Key Name>
keyuser <SSH Key User>

Note: Specify the key user and key host to delete an imported key; specify the keyuser and keyname to delete an exported key.

To import an SLC host key or to reset a SLC host key to the default:

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>]

To reset defaults for all or selected host keys:

set sshkey server reset [type <all|rsa1|rsa|dsa>]

To display SSH keys that have been imported:

show sshkey import <one or more parameters>

Parameters:
[keyhost <SSH Key IP Address or Name>] [keyuser <SSH Key User>] [viewkey <enable|disable>]

To display SSH keys that have been exported:

show sshkey export <one or more parameters>

Parameters:
[keyhost <SSH Key IP Address or Name>] [keyuser <SSH Key User>] [viewkey <enable|disable>]

To display host keys (public key only):

show sshkey server [type <all|rsa1|rsa|dsa>]

1. Click the Apply button. New entries display in the Imported SSH Keys table and Exported SSH Keys table, as applicable.
Custom Menus

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. The command `returncli` can be used to break out of a menu and return to the regular CLI.

**To add a custom menu:**

1. Click the User Authentication tab and select the Custom Menus option. The Custom Menus page displays:
2. In the lower section of the page, enter the following:
Note: To clear fields in the lower part of the page, click the Clear Custom Menu button.

<table>
<thead>
<tr>
<th>Menu Name</th>
<th>Enter a name for the custom menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Enter an optional title which will be displayed about the menu at the CLI.</td>
</tr>
<tr>
<td>Nicknames</td>
<td>Select to enable nicknames to be displayed in the menu instead of the commands. If the custom menu will have nicknames, this should also be selected prior to entering the commands in the web page, as this will facilitate entry of the nicknames.</td>
</tr>
<tr>
<td>Redisplay Menu</td>
<td>Select to redisplay the custom menu each time before the CLI prompt is displayed.</td>
</tr>
</tbody>
</table>

3. You have the following options:

   - To save the custom menu without any more commands than the default logout command, click the Add Custom Menu button.

   - To add menu commands, select the QuickEdit Mode box. This will move the cursor from Command to Nickname and back to Command (if Nicknames is selected), or keep the cursor on Command (if Nicknames is not selected). Commands (and the optional nicknames) are added to the Menu Commands/Nicknames list when carriage return is entered at the Command field (if Nicknames is not selected) or the Nickname field (if Nicknames is selected). Most browsers have a "Select All" keystroke (such as Control-A) which allow you to select all of the text in a field; this can be used in conjunction with the Delete key to clear the contents of a field before entering a new command or nickname. The Clear Command & Nickname button can also be used to delete the contents of the Command and Nickname fields.

     Commands can also be added to the list when QuickEdit Mode is not selected. Enter the command and the optional nickname and click the right arrow. The command will be added before the logout command (if a command/nickname is not selected in the list) or will replace the currently selected command/nickname in the list. The Unselect Command & Nickname button can be used to unselect the currently selected command/nickname in the list.

4. To add more commands to the custom menu, repeat step 3.

5. You also have the following options:

   - To edit a command/nickname in the custom menu, select the command in the Commands/Nicknames List box and select the left arrow button. Change the command and/or the nickname, and with the same command still selected in the list, select the right arrow button.

   - To remove a command/nickname from the custom menu, select the command in the Commands/Nicknames List box and select the Delete Command & Nickname button.

   - To move a command higher up in the menu (the commands are shown in the order they will be presented in the custom menu, with command #1 listed first), select the command in the Commands/Nicknames List box and click the up arrow.

   - To move a command further down in the menu, select the menu in the Commands/Nicknames List box and click the down arrow.

6. Click the Add Custom Menu button.
To view or update a custom menu:

1. In the **Custom Menus** table, select the custom menu and click the **View Custom Menu** button. The custom menu attributes appear in the lower part of the page.
2. Update the menu attributes following the instructions for adding a menu above.
3. Click the **Edit Custom Menu** button.

To delete a custom menu:

1. Select the custom menu in the **Custom Menus** table.
2. Click the **Delete Custom Menu** button.

To create a new custom menu from an existing custom menu:

1. Select the custom menu in the **Custom Menus** table.
2. Enter a name for the new menu in the **New Menu Name** field.
3. Click the **Copy Custom Menu** button.

**Custom User Menu Commands**

From the current menu, a user can display another menu, thus allowing menus to be nested. The special command `showmenu <Menu Name>` displays a specified menu. The special command `returnmenu` redisplays the parent menu if the current menu was displayed from a `showmenu` 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.

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.)

To assign a custom user menu to a local or remote user:

```shell
set localusers add|edit <User Login> menu <Menu Name>
```

To create a new custom user menu or add a command to an existing custom user menu:

```shell
set menu add <Menu Name> [command <Command Number>]
```

To change a command or nickname within an existing custom user menu:

```shell
set menu edit <Menu Name> command <Command Number>
set menu edit <Menu Name> nickname <Command Number>
```
To set the optional title for a menu:

set menu edit <Menu Name> title <Menu Title>

To enable or disable the display of command nicknames instead of commands:

set menu edit <Menu Name> shownicknames <enable|disable>

To enable or disable the redisplay of the menu before each prompt:

set menu edit <Menu Name> redisplaymenu <enable|disable>

To delete a custom user menu or one command within a custom user menu:

set menu delete <Menu Name> [command <Command Number>]

To view a list of all menu names or all commands for a specific menu:

show menu <all|Menu Name>

Example

The system administrator creates two custom user menus, with menu1 having a nested menu (menu2):

[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

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

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 4 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 Server
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...
13: Maintenance

The system administrator performs maintenance activities and operates the SLC using the options for the Maintenance tab and additional commands on the command line interface.

SLC Maintenance

The Maintenance > Firmware & Config 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, PC card, or USB). Update the version of the firmware running on the SLC console manager.

◆ Save a snapshot of all settings on the SLC unit (save a configuration).

◆ Restore the configuration, either to a previously saved configuration, or to the factory defaults.

◆ View and terminate current web sessions.

◆ 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. The Maintenance > Firmware & Config page displays.
Figure 13-1  Maintenance > Firmware & Config

**General**
- Reboot: □
- Shutdown: □

**Internal Temperature**
- Current: 43 °C / 109 °F
- Low: 25 °C / 77 °F
- High: 45 °C / 113 °F
- Calibrate Offset: 5 °C / 9 °F

**Site Information**
- Data Center Rack Row: 2
- Data Center Rack Cluster: 3
- Data Center Rack: 4

Note: Temperatures can be entered in either Celsius or Fahrenheit. To indicate a temperature in Fahrenheit, append the degrees with an "F", e.g. "55°F".

**SLC Firmware**
- Current Version: 6.1.0.0
- Update Firmware: □
- Firmware Filename: □
- Key: □
- Load Firmware via: □ FTP

**Load Firmware Via Options**
- HTTPS: Upload File □
- NFS Mounted Dir: select one □
- PC Card Slot: □ Upper Slot □ Lower Slot
- FTP Server Path: /cfgdir
- Login: root
- Password: *******
- Retype Password: *******

**Boot Banks**
- Bank 1: 5.4
- Bank 2: 6.1.0.0 (current)
- Next Boot 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 □

Files will be uploaded to Local Disk.

Apply
2. Enter the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 unit. The default is No.              |

**Internal Temperature**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>Displays current temperature.</td>
</tr>
<tr>
<td>Low (°C)</td>
<td>Sets the acceptable minimum for the internal temperature of the SLC console manager. If the temperature of the SLC device changes to be outside of this range, the unit will issue an SNMP trap.</td>
</tr>
<tr>
<td>High (°C)</td>
<td>Sets the acceptable maximum for the internal temperature of the SLC device. If the temperature of the SLC unit changes to be outside of this range, the SLC device will issue an SNMP trap.</td>
</tr>
<tr>
<td>Calibrate Offset (°C)</td>
<td>An offset for calibrating the internal temperature of the SLC console manager. The offset will be applied one hour after setting the calibration value. Zeroing the offset will take effect immediately and will cancel any current and/or pending calibration.</td>
</tr>
</tbody>
</table>

**Site Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Rack Row</td>
<td>Set these fields to define the rack row the SLC unit is located within a large data center. The default for these fields is 1.</td>
</tr>
<tr>
<td>Data Center Rack Cluster</td>
<td>Set these fields to define the rack cluster the SLC device is located within a large data center. The default for these fields is 1.</td>
</tr>
<tr>
<td>Data Center Rack</td>
<td>Set these fields to define the rack the SLC console manager is located within a large data center. The default for these fields is 1.</td>
</tr>
</tbody>
</table>

**SLC Firmware**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Version</td>
<td>Displays the current firmware version.</td>
</tr>
</tbody>
</table>
| Update Firmware | ✦ To update the SLC firmware, select the checkbox. If you select this option, the SLC unit reboots after you apply the update. The first time boot for each bank may take up to 5 minutes. Subsequent boot times will be approximately 2 minutes.  
  ✦ To view a log of all prior firmware updates, click the Firmware Update Log link.  
  *Note: For dual boot units, 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.* |
| Firmware Filename | The name of the firmware update file downloaded from the Lantronix web site. |
| Key           | A key for validating the firmware file. The key is provided with the firmware file (32 hex characters). |
| Load Firmware via | From the drop-down list, select the method of loading the firmware. Options are FTP, SFTP, TFTP, HTTP, NFS, USB and PC Card. FTP is the default. For NFS, the mount directory must be specified. For PC Card, the slot must be selected. Connections available depend on the model of the SLB or SLC unit. |
Boot Banks

Note: The first time boot for each bank may take up to 5 minutes. Subsequent boot times will be approximately 2 minutes.

<table>
<thead>
<tr>
<th>Bank 1</th>
<th>Displays the version of SLC firmware in bank 1. Note: The word “current” displays next to the bank from which the SLC unit booted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank 2</td>
<td>Displays the version of SLC firmware in bank 2.</td>
</tr>
<tr>
<td>Next Boot Bank</td>
<td>Displays the current setting for bank to boot from at next reboot.</td>
</tr>
<tr>
<td>Switch to Bank 1</td>
<td>If desired, select the alternate bank to boot from at next reboot.</td>
</tr>
<tr>
<td>Copy configuration from Bank 2 to Bank 1 during firmware update</td>
<td>If checked, will copy the configuration from the current bank to the bank being updated. The two numbers are automatically generated so that the first number is the current bank.</td>
</tr>
<tr>
<td>Copy contents of Bank 2 to Bank 1</td>
<td>If checked, enables you to copy the current boot bank to the alternate boot bank. This process takes a few minutes to complete.</td>
</tr>
</tbody>
</table>

Load Firmware Via Options

HTTPS | Click on Upload File to upload the firmware patch. Enter the key in the Key: field of the main webpage. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Mounted Dir</td>
<td>Select the NFS mounted directory from the drop-down menu.</td>
</tr>
<tr>
<td>USB Port</td>
<td>Click to select USB port. USB ports are available on certain models of SLC or SLB units.</td>
</tr>
<tr>
<td>PC Card Slot</td>
<td>Click to select the Upper Slot or Lower Slot if PC Card. PC Cards are available on certain models of SLC or SLB units</td>
</tr>
<tr>
<td>FTP/SFTP/TFTP Server</td>
<td>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.</td>
</tr>
<tr>
<td>Path</td>
<td>The default path on the server for obtaining firmware update files and getting and putting configuration save files.</td>
</tr>
<tr>
<td>Login</td>
<td>The userid for accessing the FTP server. May be blank.</td>
</tr>
<tr>
<td>Password / Retype Password</td>
<td>The FTP user password.</td>
</tr>
</tbody>
</table>

Configuration Management

<table>
<thead>
<tr>
<th>Configuration Management</th>
<th>From the option list, select one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Save/Restore</td>
<td>Does not save or restore a configuration.</td>
</tr>
<tr>
<td>Save Configuration</td>
<td>Saves all settings to file, which can be backed up to a location that is not on the SLC unit.</td>
</tr>
<tr>
<td>Restore Factory Defaults</td>
<td>Restores factory defaults. If you select this option, the SLC console manager reboots after you apply the update.</td>
</tr>
<tr>
<td>Restore Saved Configuration</td>
<td>Returns the SLC settings to a previously saved configuration. If you select this option, the SLC unit reboots after you apply the update.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Save with Config or Preserve with Restore</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Keys</td>
<td>Select the SSH Keys checkbox to save any imported or exported SSH keys.</td>
</tr>
<tr>
<td>SSL Certificate</td>
<td>Select the SSL Certificate checkbox to save an imported certificate.</td>
</tr>
<tr>
<td>Scripts</td>
<td>Select the Scripts checkbox to save any interface or batch scripts. Disabled by default.</td>
</tr>
</tbody>
</table>
3. Click **Apply**.

**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 set the acceptable range for the internal temperature sensor (an SNMP trap is sent if the temperature is outside of this range):

```
set temperature <one or more parameters>
```

**Parameters:**

- `low <Low Temperature in C.>`
- `high <High Temperature in C.>`
- `calibrate <Temperature Calibration in C.>`

**Note:** the calibration offset will be applied one hour after setting the value.
To display the acceptable range and the current reading from the internal temperature sensor:

```
show temperature
```

To set the acceptable range for the internal temperature sensor (an SNMP trap is sent if the temperature is outside of this range):

```
set temperature <one or more parameters>
```

**Parameters:**

- low <Low Temperature in C. or F.>
- high <High Temperature in C. or F.>
- calibrate <Temperature Calibration in C. or F.|cancel>

**Note:** the calibration offset will be applied one hour after setting the value.

To display the acceptable range and the current reading from the internal temperature sensor:

```
show temperature
```

To save the current SLC configuration to a selected location:

```
admin config save <Config Name> location
    <local|ftp|sftp|nfs|cifs|usb|pccard>
    [nfsdir <NFS Mounted Directory>] [usbport <U1>]
    [pccardslot <upper|lower>]
    [savesshkeys <enable|disable>] [savesslcert <enable|disable>]
    [savecripts <enable|disable>]
```

To restore a saved configuration to the SLC:

```
admin config restore <Config Name> location
    <local|ftp|sftp|nfs|cifs|usb|pccard>
    [nfsdir <NFS Mounted Directory>] [usbport <U1>]
    [pccardslot <upper|lower>]
    [savesshkeys <enable|disable>] [savesslcert <enable|disable>]
    [savecripts <enable|disable>]
    [preserveconfig <Config Params to Preserve>]
```

To restore the SLC to factory default settings:

```
admin config factorydefaults [savesshkeys <enable|disable>]
    [savesslcert <enable|disable>] [savecripts <enable|disable>]
    [preserveconfig <Config Params to Preserve>]
```

<Config Params to Preserve> is a comma separated list of current configuration parameters to retain after the config restore or factorydefaults:

- nt - Networking
- sv - Services
- dt - Date/Time
- lu - Local Users
- ra - Remote Authentication
- dp - Device Ports
- ub - USB / pc - PC Card
To delete or rename a configuration (the user is prompted for the new name for renames):

```
admin config rename|delete <Config Name> location
[local|nfs|cifs|usb|pccard> [nfsdir <NFS Mounted Directory>] [usbport <U1>] [pccardslot <upper|lower>]
```

To copy the current configuration (or optionally, a configuration from another location) to the other bank (for dual-boot SLB/SLC units):

```
admin config copy <current|Config Name>
[location <local|nfs|cifs|usb|pccard> [nfsdir <NFS Mounted Directory>] [usbport <U1>] [pccardslot <upper|lower>]
```

To list the configurations saved to a location:

```
admin config show <local|ftp|sftp|nfs|cifs|usb|pccard>
[nfsdir <NFS Mounted Directory>] [usbport <U1>] [pccardslot <upper|lower>]
```

**Note:** A reboot will automatically be done after a successful config restore or factory defaults.

To update the SLB/SLC firmware to a new revision (the firmware file should be accessible via the settings displayed by `admin ftp show`):

```
admin firmware update <ftp|tftp|sftp|nfs|usb|pccard> file
<Firmware File> key <Checksum Key>
[nfsdir <NFS Mounted Directory>] [usbport <U1>] [pccardslot <upper|lower>]
```

To set the boot bank to be used at the next SLB/SLC reboot (for dual-boot SLB/SLC units):

```
admin firmware bootbank <1|2>
```

To copy the boot bank from the currently booted bank to the alternate bank (for dual-boot SLB/SLC units):

```
admin firmware copybank
```

To list the current firmware revision, the boot bank status (for dual-boot SLB/SLC units), and optionally displays the log containing details about firmware updates:

```
admin firmware show [viewlog <enable|disable>]
```

**Note:** A reboot will automatically be done after a successful firmware update.

To manage configuration files:

The Manage option on the Maintenance > Firmware & Config page allows you to view all configurations saved to the selected location and delete any of the configurations. This feature is available for the default, CIFS Share, and USB locations.

1. On the Maintenance > Firmware & Config page, click the Manage link. The following page displays the name and the time and date the file was saved:
2. To delete files, select one or more files and click the **Delete File** button.

3. To download a new firmware file, click the **Delete File** button.

4. To rename a listed file, select the file, type the new file name into the **New File Name** field, and click the **Rename File** button.

**Administrative Commands**

These commands for the command line interface correspond to the web page entries described above.

*To copy the boot bank from the currently booted bank to the alternate bank (for dual-boot SLB/SLC units):*

```
admin firmware copybank
```

*To reboot the SLC:*

```
admin reboot
```

**Note:** The front panel LCD displays the “Rebooting the SLC” message, and the normal boot sequence occurs.

*To prepare the SLC console manager to be powered off:*

```
admin shutdown
```

**Note:** When you use this command to shut down the SLC unit, the LCD front panel displays “Shutting down the SLC console manager,” followed by a pause, and then “Shutdown complete.” When “Shutdown complete” displays, it is safe to power off the SLC unit. This command is not available on the web page.

*To list current hardware and firmware information:*

```
admin version
```
To update SLC firmware to a new revision:

Note: The firmware file should be accessible via the settings displayed by admin ftp show. The SLC console manager automatically reboots after successful update.

admin firmware update <ftp|tftp|sftp|nfs|pccard|usb> file <Firmware File> key <Checksum Key> [nfsdir <NFS Mounted Directory>] [usbport <U1>] [pccardslot <upper|lower>]

To set the boot bank to be used at the next SLC unit reboot:

admin firmware bootbank <1|2>

Applies to dual-boot SLB/SLC units only

To list the current firmware revision:

admin firmware show [viewlog <enable|disable>]

Lists the current firmware revision, the boot bank status (for dual-boot SLB/SLC units), and optionally displays the log containing details about firmware updates

To set the FTP/TFTP/SFTP server used for firmware updates and configuration save/restore:

admin ftp server <IP Address or Hostname> [login <User Login>] [path <Directory>]

To view FTP settings:

admin ftp show

To set the FTP server password and prevent it from being echoed:

admin ftp password

To restore the SLC console manager to factory default settings:

admin config factorydefaults [savesshkeys <enable|disable>] [savesslcrt <enable|disable>] [preserveconfig <Config Params to Preserve>]

<Config Params to Preserve> is a comma-separated list of current configuration parameters to retain after the config restore or factorydefaults:

- nt - Networking
- sv - Services
- dt - Date/Time
- lu - Local Users
- ra - Remote Authentication
- dp - Device Ports
- ub - USB

To restore a saved configuration to the SLC unit:

admin config restore <Config Name> location <default|ftp|sftp|nfs|cifs> [nfsdir <NFS Mounted Dir>] [ <>] [keepconfig <Config Params to Keep>]

[preserveconfig <Config Params to Prserve>]

<Config Params to Preserve> is a comma-separated list of current configuration parameters to retain after the config restore or factory defaults:

- nt - Networking
- sv - Services
- dt - Date/Time
- lu - Local Users
- ra - Remote Authentication
- dp - Device Ports
- ub - USB

**To save the current SLC configuration to a selected location:**

```
admin config save <Config Name> location <default|ftp|sftp|nfs|cifs|usb|pccard> [nfsdir <NFS Mounted Dir>] [usbport <u1>] [pccardslot <upper|lower>]
```

**To delete a saved configuration:**

```
admin config delete <Config Name> location <default|cifs|usb> [usbport <u1>] [pccardslot <upper|lower>]
```

**To list the configurations saved to a location:**

```
admin config show <default|ftp|sftp|nfs|cifs|usb|pccard> [nfsdir <NFS Mounted Dir>] [usbport <u1>] [pccardslot <upper|lower>]
```

**To run the quick setup script:**

```
admin quicksetup
```

**System Logs**

The Maintenance > System Logs page allows you to view various system logs. (See Chapter 7: Services on page 68 for more information about system logs.) You can also clear logs on this page.

**To view system logs:**

1. Click the Maintenance tab and select the System Logs option. The following page displays:
2. Enter the following to define the parameters of the log you would like to view:

**Log**
Select the type(s) of log you want to view:
- All
- Network
- Services
- Authentication
- Device Ports
- Diagnostics
- General
- Software

**Level**
Select the alert level you want to view for the selected log:
- Error
- Warning
- Info
- Debug

**Starting at**
Select the starting point of the range you want to view:
- **Beginning of Log**: to view the log from the earliest available beginning time and date.
- **Date**: to view the log starting from a specific starting date and time.

**Ending at**
Select the endpoint of the range you want to view:
- **End of Log**: to view the log from the latest available ending time and date.
- **Date**: to view the log up to the last available log ending date and time.

3. Click the **View Log** button. Your specified system log displays. For example, if you select the type **All** and the level **Error**, the SLC console manager displays a log similar to this:
Figure 13-4 System Logs

From a queried system log (i.e., Figure 13-4), you may email this information to a specific individual or to Lantronix Technical Support. See Emailing Logs and Reports (on page 236).

To clear system logs:

1. From the Maintenance > System Logs page, select SLC Maintenance - System Logs.
2. Click the Clear Log button to clear all log information.

System Log Command

The following command for the command line interface corresponds to the web page entries described above.

To view the system logs containing information and error messages:

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>]
startingtime <MMDDYYhhmm [ss]]
endtime <MMDDYYhhmm [ss]]

Note: The level and time parameters cannot be used simultaneously.
13: Maintenance

To clear one or all of the system logs:

```plaintext
show syslog clear
<all|netlog|servlog|authlog|devlog|diaglog|genlog>
```

Audit Log

The Maintenance > Audit Log 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 > SSH/Telnet/Logging 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 unit reboots.

1. Click the Maintenance tab and select the Audit Log option. The following page displays:

```
Figure 13-5 Maintenance > Audit Log
```

2. To select a sort option, click the appropriate button:
   - To sort by date and time, click the Sort by Date/Time button (this is the default.)
   - To sort by user, click the Sort by User button.
   - To sort by command/action, click the Command button.

3. To email this log, follow the instructions in Emailing Logs and Reports (on page 236).
4. To clear the log, click the **Clear Log** button.

5. To freeze or stop automatic refreshing of the log, click the **Stop Refresh** button.

### Email Log

The **Maintenance > Email Log** page displays a log of all attempted emails. The log file can be cleared from here. The email log is saved through SLC unit reboots.

1. Click the Maintenance tab and select the Email Log option. The following page displays:

   ![Figure 13-6 Maintenance > Email Log](image)

   **Email Log**

   Send Failures: 1
   Emails Sent: 6
   Bytes Sent: 338075

   06/10/14 14:27 gfooteam@lantronix.com | update.lantronix.com: soft Port error
   06/10/14 16:28 gfooteam@lantronix.com | Message Sent [Temperature out of range]
   06/13/14 22:44 gfooteam@lantronix.com | Message Sent [Report]

   2. To email this log, follow the instructions in *Emailing Logs and Reports (on page 236)*.

   3. To clear the log, click the **Clear Log** button.
Diagnostics

The Maintenance > Diagnostics 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. The following page displays:

![Figure 13-7 Maintenance > Diagnostics](image)

Select Diagnostics:  
- All
- Arp Table
- Netstat
- Host Lookup
- Ping
- Send Packet
- Loopback
- SLC Internals

Protocol:  
- TCP
- UDP

Hostname:

Port:

String:

Count:

IPv6:  
- Both
- IPv4
- IPv6

Device Port:  
- Internal
- External

Select Diagnostics from checklist (one or more diagnostic methods you want to run, or select All to run them all):

<table>
<thead>
<tr>
<th>ARP Table</th>
<th>Address Resolution Protocol (ARP) table used to view the IP address-to-hardware address mapping.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netstat</td>
<td>Displays network connections. If you select the checkbox, select the TCP or UDP protocol, or select All for both protocols to control the output of the Netstat report.</td>
</tr>
<tr>
<td>Host Lookup</td>
<td>Select to verify that the SLC console manager can resolve the host name into an IP address (if DNS is enabled). If selected, also enter a host name in the corresponding Hostname field.</td>
</tr>
</tbody>
</table>
3. Click the Run Diagnostics button. The Diagnostics Report page displays.

3. Click the Run Diagnostics button. The Diagnostics Report page displays.

<table>
<thead>
<tr>
<th>Diagnostic Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To display the ARP table of IP address-to-hardware address mapping:</strong></td>
</tr>
<tr>
<td><code>diag arp [email &lt;Email Address&gt;]</code></td>
</tr>
</tbody>
</table>
You can optionally email the displayed information.

**To display a report of network connections:**

```bash
diag netstat [protocol <all|tcp|udp>] [email <Email Address>]
```

You can optionally email the displayed information.

**To resolve a host name into an IP address:**

```bash
diag lookup <Hostname> [email <Email Address>]
```

You can optionally email the displayed information.

**To test a device port by transmitting data out the port and verifying that it is received correctly:**

```bash
diag loopback <Device Port Number or Name>[<parameters>]
```

**Parameters:**

- `test <internal|external>`
- `xferdatasize <Size In Kbytes to Transfer>

*Default is 1 Kbyte.*

**Note:** A special loopback cable comes with the SLC unit. 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.

**To display the route that packets take to get to a network host:**

```bash
diag traceroute <IP Address or Hostname>
```

**To verify that the host is up and running:**

```bash
diag ping <IP Address or Name> [<parameters>]
```

**Parameters:**

- `count <Number of Times to Ping>
  
  *The default is 5.*
- `packetsize <Size in Bytes>
  
  *The default is 64.*

**To display performance statistics for an Ethernet port or a device port (averaged over the last 5 seconds):**

```bash
diag perfstat [ethport <1|2>] [deviceport <Device Port # or Name>]
```

**To generate and send Ethernet packets:**

```bash
diag sendpacket host <IP Address or Name> port <TCP or UDP Port Number> [string <Packet String>] [protocol <tcp|udp>] [count <Number of Packets>]
```
The default is 1.

**To display all network traffic, applying optional filters:**

*Note:* This command is not available on the web interface.

`diag nettrace <one or more parameters>`

Parameters:
- `ethport <1|2>`
- `host <IP Address or Name>`
- `numpackets <Number of Packets>`
- `protocol <tcp|udp|icmp>`
- `verbose <enable|disable>`

**To display information on the internal memory, storage and processes of the SLC unit:**

`diag internals [email <Email Address>]`

*Note:* This command is available the web interface as SLC Internals under **Maintenance > Diagnostics**.
Status/Reports

On this 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 following page displays:

   ![Figure 13-9 Maintenance > Status/Reports](image)

   The top half of the page displays the status of each port, power supply, and power outlet:

   - **Green** indicates that the port connection or power supply is active and functioning correctly.
   - **Red** indicates an error or failure or that the device is off.

2. Select the desired reports to view under **View Report**:

   **View Report**

   | All | Port Status | Port Counters | IP Routes | Connections | System Configuration - Complete | System Configuration - Basic | System Configuration - Authentication | System Configuration - Devices |

   The top half of the page displays the status of each port, power supply, and power outlet:

   - **Green** indicates that the port connection or power supply is active and functioning correctly.
   - **Red** indicates an error or failure or that the device is off.

2. Select the desired reports to view under **View Report**:

   **View Report**

   | All | Displays all reports. |
   | 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. |
3. Click the **Generate Report** button. In the upper left of the *Generated Status/Reports* page displays a list of reports generated.

4. To email these report(s), follow the instructions in *Emailing Logs and Reports (on page 236)*.

**Status Commands**

These commands for the command line interface correspond to the web page entries described above.

*To display device port modes and states for one or more ports:*

```
show portstatus [deviceport <Device Port List or Name>] [email <Email Address>]
```

You can optionally email the displayed information.
To display a snapshot of configurable parameters:

```
show sysconfig [display <basic|auth|devices>] [email <Email Address>]
```

You can optionally email the displayed information.

Displays a report of all configurable parameters or a shorter report with basic system settings, authentication settings, or device settings.

To generate a report for one or more ports: You can optionally email the displayed information.

```
show portcounters [deviceport <Device Port List or Name>] [email <Email Address>]
```

To display the overall status of all SLC devices:

```
show sysstatus [email <Email Address>]
```

You can optionally email the displayed information.

To display a list of all current connections:

```
show connections [email <Email Address>]
```

You can optionally email the displayed information.

To provide details, e.g., endpoint parameters and trigger, for a specific connection:

```
show connections connid <Connection ID> [email <Email Address>]
```

You can optionally email the displayed information.

**Note:** Use the basic show connections command to obtain the Connection ID.

**Emailing Logs and Reports**

The following logs and reports can be directly emailed to a specific individual or to Lantronix Technical Support directly from the log page:

- System Log (i.e., *Figure 13-4*)
- Audit Log (i.e., *Figure 13-5*)
- Email Log (i.e., *Figure 13-6*)
- Diagnostic Reports (i.e., *Figure 13-8*)
- Status/Reports (i.e., *Figure 13-10*)

**To email a log to an individual:**

1. In the Comment field of a particular log or report page, enter a comment (if desired).
2. Select the to field beside the empty field where you then enter the person's email address.
3. Press the Email Output button. An email is immediately sent out and a confirmation appears on the screen.
To email a log to Lantronix Technical Support:

1. Click the question mark icon on the upper right corner to access SLC console manager device and setup information as well as contact information for Lantronix Technical Support (see Figure 13-12).
2. Call Lantronix Tech Support with the contact information provided and obtain a case number.

3. Press the **Email Output** button to send Lantronix Tech Support the log along with the identifying support number.

4. Click **OK** in the confirmation popup that appears.
Events

On this Maintenance > Events page, you can define what action you want to take for events that may occur in the SLC console manager.

1. Click the Maintenance tab and select the Events option. The following page displays:

![Figure 13-13 Maintenance > Events](image)

2. Enter the following:

   - **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)
     - Device Port Data Drop
     - Current Over Threshold

   Note: Certain event triggers are available on some SLC and SLB models.

   - **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(s) 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.
You have 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 Maintenance > 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) To save, click Apply.

**Events Commands**

**To manage the response to events that occur in the SLC unit:**

```
admin events add <trigger> <response>
<trigger> is one of:
    |receivetrap|templimit|humidlimit|overcurrent|dpdatadrop
    |inletstatus|nomodemdial
<response> is one of:
    action <syslog>
    action <fwdalltrapseth|fwdseltrapseth> 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> usbport <U1> pccardslot <upper|lower> nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap OID>]
    action <emailalert> emailaddress <destination email address>
```

**To update event definitions:**

```
admin events edit <Event ID> <parameters>
```

**Parameters:**

- community <SNMP Community>
- deviceport <Device Port # or Name>
- ethport <1|2>

---

<table>
<thead>
<tr>
<th>Modem Connection on</th>
<th>For actions that require a modem connection (for example, Forward All Traps to a Modem Connection, select which device port or USB port/PC Card with a modem connection to use.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMS/Host to forward trap to</td>
<td>For actions that forward a trap, enter the IP address of the computer to forward the trap to. The computer does not have to be an SNMP NMS; it just has to be capable of receiving SNMP traps.</td>
</tr>
<tr>
<td>SNMP Community</td>
<td>Forwarded traps are sent with this SNMP community value There is no default.</td>
</tr>
<tr>
<td>SNMP Trap OID</td>
<td>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 &quot;get&quot; 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.</td>
</tr>
<tr>
<td>Email Addresses</td>
<td>Enter an email address to receive email alerts.</td>
</tr>
</tbody>
</table>
To delete an event:
admin events delete <Event ID>

To view events:
admin events show

**LCD/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.
To configure the LCD:

The screens that are currently enabled are displayed in order in the left Enabled screens list.

1. Select a screen to be removed from the **Enabled Screens** and click the ➡️ button. The screen moves to the **Disabled Screens** list to the right.

2. Select a screen to be added from the **Disabled Screens** list and click the ➡️ button. The screen is added to the **Enabled Screens** to the left.

3. Select a screen in the **Enabled Screens** list and click the ⬆️ or ⬇️ button to change the order of the screens.

**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.

4. Click **Apply** to save.

To configure the Keypad:

1. Enter the following fields.

<table>
<thead>
<tr>
<th>Keypad Locked</th>
<th>Select this to lock out any input to the keypad. The default is for the keypad to be unlocked.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Factory Defaults Password / Retype Password</td>
<td>Enter the 6 digit key sequence entered at the keypad to restore the SLC unit to factory defaults. The default is 999999.</td>
</tr>
</tbody>
</table>

2. Click **Apply** to save.

LCD/Keypad Commands

The following CLI commands correspond to the **Maintenance > LCD/Keypad** page. For more information, see Chapter 15: Command Reference.

- admin keypad lock
- admin keypad password
- admin keypad show
- admin lcd reset
- admin lcd default
- admin lcd screens
- admin lcd line1
- admin lcd scrolling
- admin lcd show
Banners

The Maintenance > Banners page allows the system administrator to customize text messages that display to users.

To configure banner settings:

1. Click the Maintenance tab and select Banners option.

![Figure 13-15 Maintenance > Banners]

2. Enter the following fields.

<table>
<thead>
<tr>
<th>Banner Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome Banner</td>
<td>The text to display on the command line interface before the user logs in. May contain up to 1024 characters (single quote and double quote characters are not supported). Welcome to the SLC unit is the default. <strong>Note:</strong> To create more lines use the \n character sequence.</td>
</tr>
<tr>
<td>Login Banner</td>
<td>The text to display on the command line interface after the user logs in. May contain up to 1024 characters (single quote and double quote characters are not supported). Default is blank. <strong>Note:</strong> To create more lines, use the \n character sequence.</td>
</tr>
<tr>
<td>Logout Banner</td>
<td>The text to display on the command line interface after the user logs out. May contain up to 1024 characters (single quote and double quote characters are not supported). Default is blank. <strong>Note:</strong> To create more lines use, the \n character sequence.</td>
</tr>
<tr>
<td>SSH Banner</td>
<td>The text to display when a user logs into the SLC device via SSH, prior to authentication. May contain up to 1024 characters (single quote and double quote characters are not supported). Blank by default. <strong>Note:</strong> To create more lines use the \n character sequence.</td>
</tr>
</tbody>
</table>

3. Click Apply to save.
Banner Commands

The following CLI commands correspond to the Maintenance > Banners page. For more information, see Chapter 15: Command Reference.

- admin banner login
- admin banner logout
- admin banner show
- admin banner ssh
- admin banner welcome
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.

   ![Setting display](image)

   - Modem Settings: Modem State: disabled, Modem Mode: text
   - Data Settings: Baud Rate: 9600, Data Bits: 8, Parity: none
   - IP Settings: Telnet: disabled, Telnet Port: 2002

2. Change the baud to 57600 and disable flow control by using the `baud` and `flowcontrol` parameters.

   ![Baud and flowcontrol change](image)

3. Connect to the device port y using the `connect direct` command.

   ![Connect direct](image)

4. View messages from the SUN server console.

   ![Message view](image)

5. Reboot the SUN server by using the `reboot` command.

   ![Reboot](image)

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.

   ```plaintext
   [SLC]> set deviceport port 1 modemmode text
   Device Port settings successfully updated.
   [SLC]> set deviceport port 1 initscript "ATzF&K3xCl&d2%0A"
   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.

   ```plaintext
   [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
Authentication: PAP  Login: 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-back Number: usernumber
Initialization Script: <none>

Logging Settings-----------------------------------------------
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
```

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
- Deprecated Commands
- Device Commands
- Device Port Commands
- Diagnostic Commands
- Email Log Commands
- Events Commands
- Group 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
- Site Commands
- SLC Network Commands
- SSH Key Commands
- Status Commands
- System Log Commands
- TACACS+ Commands
- Temperature Commands
- USB Commands
- User Permissions Commands
- VPN 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>
<thead>
<tr>
<th>Action</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>auth</td>
</tr>
<tr>
<td>show</td>
<td>auth</td>
</tr>
<tr>
<td>connect</td>
<td>bidirection</td>
</tr>
<tr>
<td>diag</td>
<td>arp</td>
</tr>
<tr>
<td>pcard2</td>
<td>modem</td>
</tr>
<tr>
<td>admin</td>
<td>banner</td>
</tr>
<tr>
<td>logout</td>
<td>terminates CLI session</td>
</tr>
</tbody>
</table>

1 USB commands are only accessible on SLC USB part number -03.
2 PC Card commands are only accessible on SLC USB part number -02.

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
  
  set 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 for parameters which accept the CLEAR command. CLI parameters which accept CLEAR are listed at the beginning of each section.

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 287))
- show locallog (replaced by show log local (on page 288))

### 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.
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 | usb | pccard> [nfsdir <NFS Mounted Directory>] [usbport <U1>] [pccardslot <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>] [savesscripts <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>] [savesscripts <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>] [savesscripts <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.

The following list includes options which accept the CLEAR command:
**Note:** CLEAR must be in all caps.

```
admin ftp login, path
```

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.

Syntax
admin lcd default

Description
Restores the LCD screens to their factory default settings.

Syntax
admin lcd reset

Description
Restarts the program that controls the LCD.

Syntax
admin lcd line1

Description
Sets the strings displayed on the LCD user string screen.

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.

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 memory

Syntax
admin memory

Description
Displays information about SLC memory usage and allows configuration of a swap space if available memory is low. Creates a swap space on the SLC disk or an external storage device:

admin memory swap add <Size of Swap in MB> [usbport <U1>]

Deletes the swap space from the SLC disk or an external storage device:

admin memory swap delete
admin memory show

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>]

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

| admin web | group, banner |

**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 iface

**Syntax**
admin web iface <none,eth1,eth2,ppp>

**Description**
Defines a list of network interfaces the web is available on:

admin web group

**Syntax**
admin web group <Local or Remote Group Name>

**Description**
Configures the group that can access the web:

admin web banner

**Syntax**
admin web banner <Banner Text>

**Description**
Configures the banner displayed on the web home page:

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 [viewsessions <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.

cconnect direct

Syntax
cconnect 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.

cconnect listen

Syntax
cconnect 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>
group <Local or Remote Group Name>
parity <none|odd|even>
showlines <disable|1-50 lines>
stopbits <1|2>
timeout <disable|1-30 minutes>
The following list includes options which accept the **CLEAR** command:

**Note:** CLEAR must be in all caps.

```
set consoleport group
```

**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>

The following list includes options which accept the **CLEAR** command:

**Note:** CLEAR must be in all caps.

| set menu edit | nickname |

**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|servertech auth login <User Login>
slp|servertech config [prompt <Command Prompt>]
    [numoutlets <Number of Outlets>]
    [numexpoutlets <Number of Expansion Outlets>]
slp|servertech restart
slp|servertech outletcontrol state <on|off|cyclepower>
    [outlet <Outlet #>] [tower <A|B>]
slp|servertech outletstate [outlet <Outlet #>] [tower <A|B>]
slp|servertech envmon
slp|servertech infeedstatus
slp|servertech system

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, ServerTech CDU 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>
cbcnpocallback <enable|disable>
chapauth <chaphost|localusers>
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 | servertech>
dialbackdelay <PPP Dial-back Delay>
dialbacknumber <usernumber|Phone Number>
dialbackretries <1-10>
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 | dialback+ondemand|
dialinhostlist | cbcpserver | cbcpclient>

modemtimeout <disable|1-9999 seconds>
name <Device Port Name>
nat <enable|disable>
nfsdir <Logging Directory>
nfslogging <enable|disable>
nfsmmaxfiles <Max # of Files>
nfsmmaxsize <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>
slnms <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>
usesites <enable|disable>
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’.

The following list includes options which accept the `CLEAR` command:

**Note:** `CLEAR` must be in all caps.

<table>
<thead>
<tr>
<th>Command</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>set deviceports</td>
<td>dialinlist, nfsdir, nfsdir, breakseq, banner, group, portlogseq, chaphost, chapsecret, dodchaphost, dodchapsecret, initscript, dialoutlogin, dialoutpassword, dialbacknumber, emailsubj, emailstring, emailto</td>
</tr>
</tbody>
</table>

**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 [email <Email Address>]

**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|fwdseltrapseth> 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>
- usbport <U1>
- pccardslot <upper|lower>
- emailaddress <destination email address>

**Description**

Edits event definitions.

admin events show

**Syntax**

admin events show

**Description**

Displays event definitions.

**Group Commands**

set groups add|edit <Group Name> [ <parameters> ]

**Syntax**

set groups add|edit <Group Name> [ <parameters> ]

**Parameters:**

- dataports <Port List>
- listenports <Port List>
- clearports <Port List>
- access outlets <Outlet List>
- escapeseq <1-10 Chars>
- breakseq <1-10 Chars>
- custommenu <Menu Name>
- displaymenu <enable|disable>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
permissions <Permission List>

Note: See 'help user permissions' for information on user rights.

set groups rename

Syntax
set groups rename <Group Name> newname <New Group Name>

Description
Renames the name of the group.

set groups delete

Syntax
set groups delete <Group Name>

Description
Deletes a group. All members must be removed from a group before it can be deleted.

show group

Syntax
show groups [name <Group Name>] members <enable|disable>

Description
Displays all groups or a specific group. The members of the group(s) can optionally be displayed.

The following list includes options which accept the CLEAR command.

Note: CLEAR must be in all caps.

set groups custommenu, escapeseq, breakseq, dialbacknumber, outletlist, listenports, dataports, clearports

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**
- accessoutlets <Outlet List>
- 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>

The following list includes options which accept the CLEAR command:

Note: CLEAR must be in all caps.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>set kerberos</td>
<td>realm, kdc, custommenu, escapeseq, breakseq, dialbacknumber, accessoutlets, listenports, dataports, clearports</td>
</tr>
</tbody>
</table>

**Description**
Configures the SLC console manager to use Kerberos to authenticate users who log in via the Web, SSH, Telnet, or the console port.

**Syntax**
show kerberos

**Description**
Displays Kerberos settings.

**LDAP Commands**

set ldap

**Syntax**
set ldap <one or more parameters>

**Parameters**
accessoutlets <Outlet List>
adsupport <enable|disable>
base <LDAP Base>
bindname <Bind Name>
bindpassword <Bind Password>
bindwithlogin <enable|disable>
useldapschema <enable|disable>
brakeseq <1-10 Chars>
clearports <Port List>
custommenu <Menu Name>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
dataports <Ports List>
encrypt <starttls|ssl|disable>
escapeseq <1-10 Chars>
filteruser <User Login Attribute>
filtergroup <Group Objectclass>
grmemberattr <Group Membership Attribute>
grmembervalue <dn|name>
group <default|power|admin>
listenports <Port List>
permissions <Permission List>
port <TCP Port> (Default is 389.)
server <IP Address or Hostname>
state <enable|disable>

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

| set ldap | custommenu, escapeseq, breakseq, dialbacknumber, base, bindname, bindpassword, filteruser, filtergroup, grmemberattr, accessoutlets, listenports, dataports, clearports |

**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>
accessoutlets <Outlet List>
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|Custom Group Name>
listenports <Port List>

passwordexpires <enable|disable>
permissions <Permission List>

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures local accounts including sysadmin who log in to the SLC console manager by means of the Web, SSH, Telnet, or the console port.</td>
</tr>
<tr>
<td>set localusers allowreuse</td>
</tr>
</tbody>
</table>

**Syntax**

set localusers allowreuse <enable|disable>

**Description**

Sets whether a login password can be reused.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>set localusers complexpasswords</td>
</tr>
</tbody>
</table>

**Description**

Sets whether a complex login password is required.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>set localusers consoleonlyadmin</td>
</tr>
</tbody>
</table>

**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.

```plaintext
set log modem pppdebug
```

**Syntax**

```plaintext
set log modem pppdebug <enable|disable>
```

**Description**

Enables PPP debugging in the modem log. When enabled, performance could be impacted.

```plaintext
show log files
```

**Syntax**

```plaintext
show log files nfs | pccard | usb [local <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.

```plaintext
show log local
```

**Syntax**

```plaintext
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.

```plaintext
show log modem
```

**Syntax**

```plaintext
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>

The following list includes options which accept the CLEAR command:

Note: CLEAR must be in all caps.

| set network | domain |

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.

display 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>

The following list includes options which accept the `CLEAR` command:

**Note:** **CLEAR** must be in all caps.

| set cifs | 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 remdir and locdir parameters are required. Once specified, the parameters do not need to be re-specified.

The following list includes options which accept the CLEAR command:

Note: CLEAR must be in all caps.

| set nfs | remdir, locdir |

**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
accessoutlets <Outlet List>
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>
escapeeq <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>

The following list includes options which accept the CLEAR command:
Note: CLEAR must be in all caps.

| set nis          | custommenu, escapeseq, breakseq, dialbacknumber, domain, accessoutlets, listenports, dataports, clearports |

**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>`
- `chapauth <chaphost|localusers>`
- `chapsecret <CHAP Secret or User Password>`
- `databits <7|8>`
- `dialbackdelay <PPP Dialback Delay>`
- `dialbacknumber <usernumber|Phone Number>`
- `dialbackretries <1-10>`
- `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 | dialback+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.

The following list includes options which accept the CLEAR command:
**Note:** CLEAR must be in all caps

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pccard modem</td>
<td>dialinlist, chaphost, chapsecret, dodchaphost, dodchapsecret, initscript, dialoutlogin, dialoutpassword, dialbacknumber, group</td>
</tr>
</tbody>
</table>

**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**
- `accessoutlets <Outlet List>`
- `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>
usevsa <enable|disable>

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

| set radius | custommenu, escapeseq, breakseq, dialbacknumber, secret, accessoutlets, listenports, dataports, clearports |

**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**
- accessoutlets <Outlet List>
- 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|Custom Group Name>
- 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, po

**Note:** To remove a permission, type a minus sign before the two-letter abbreviation for a user right.

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

| set remoteusers add|edit <User Login> [<parameters>] | custommenu, escapeseq, breakseq, dialbacknumber, accessoutlets, listenports, dataports, clearports |

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rip</td>
<td>&lt;enable</td>
</tr>
<tr>
<td>route</td>
<td>&lt;1-64&gt; ipaddr &lt;IP Address&gt; mask &lt;Netmask&gt; gateway &lt;IP Address&gt;</td>
</tr>
<tr>
<td>static</td>
<td>&lt;enable</td>
</tr>
<tr>
<td>version</td>
<td>&lt;1</td>
</tr>
</tbody>
</table>

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>
- nms1 <IP Address or Name>
- nms2 <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>
v1v2 <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>
webssh <enable|disable>
webtelnet <enable|disable>

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

| set services | location, contact, v3phrase, v3rwphrase, phonenumber |

**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.

---

**Site Commands**
To create or edit a site:

```bash
set site add|edit <Site Name> [<parameters>]
```

**Parameters:**

- `name <Site Name>` (edit only)
- `dialoutnumber <Phone Number>`
- `deviceport <Device Port # or Name or none>`
- `dialoutlogin <User Login>`
- `usbport <U1|U2>`
- `auth <pap|chap>`
- `pccardslot <upper|lower>`
- `dialbacknumber <Phone Number>`
- `dialbackdelay <Dial-back Delay>`
- `dialbackretries <1-10>`
- `timeoutlogins <disable|1-30 minutes>`
- `modemtimeout <disable|1-9999 secs>`
- `restartdelay <PPP Restart Delay>`
- `cbcpnocallback <enable|disable>`
- `loginhost <User Login/CHAP Host>`
- `chapsecret <CHAP Secret>`
- `remoteipaddr <negotiate|IP Address>`
- `localipaddr <negotiate|IP Address>`
- `routeipaddr <IP Address>`
- `routemask <Mask>`
- `routegateway <Gateway>`
- `dialoutpassword <Password>`
- `allowdialback <enable|disable>`
- `allowdialback <enable|disable>`
- `pap|chap>`
- `allowdialback <enable|disable>`
- `validate | disable>`
- `enable|disable>`
- `dialoutpassword <Password>`
- `allowdialback <enable|disable>`
- `loginhost <User Login/CHAP Host>`
- `chapsecret <CHAP Secret>`
- `remoteipaddr <negotiate|IP Address>`
- `localipaddr <negotiate|IP Address>`
- `routeipaddr <IP Address>`
- `routemask <Mask>`
- `routegateway <Gateway>`
- `dialoutpassword <Password>`
- `allowdialback <enable|disable>`
- `loginhost <User Login/CHAP Host>`
- `chapsecret <CHAP Secret>`
- `remoteipaddr <negotiate|IP Address>`
- `localipaddr <negotiate|IP Address>`
- `routeipaddr <IP Address>`
- `routemask <Mask>`
- `routegateway <Gateway>`

To delete a site:

```bash
set site delete <Site Name>
show site <all|names|Site Name>
```

The following list includes options which accept the `CLEAR` command:

**CLEAR must be in all caps.**

<table>
<thead>
<tr>
<th>set sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>loginhost, chapsecret, dialoutlogin, dialoutpassword, dialbacknumber</td>
</tr>
</tbody>
</table>

SLC Network Commands

**set slcnetwork**

**Syntax**

```bash
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**

```bash
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**

```plaintext
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**

```plaintext
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**

```plaintext
set sshkey export <ftp|scp|copypaste> <one or more parameters>
```

**Parameters**

- `[format <openssl|secsh>]`
- `[host <IP Address or Name>]`
- `[login <User Login>]`
- `[path <Path to Copy Key>]`
- `[bits <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**

```bash
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**

```bash
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**

```bash
set sshkey server reset [type <all|rsa1|rsa|dsa>]
```

**Description**
Resets defaults for all or selected host keys.

**show sshkey export**

**Syntax**

```bash
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**

```bash
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: The 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**
accessoutlets <Outlet List>
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>

The following list includes options which accept the CLEAR command:

**Note:** CLEAR must be in all caps.

| set tacacs+ | custommenu, escapeseq, breakseq, dialbacknumber, secret, accessoutlets, listenports, dataports, clearports |
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
low <Low Temperature in C. or F.>  
high <High Temperature in C. or F.>
calibrate <Temperature Calibration in C. or F.|cancel>

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>
cbcctype <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 <username|Phone Number>
dialbackretries <1-10>
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|rtsc/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>
sshort <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.

The following list includes options which accept the **CLEAR** command:

**Note:** **CLEAR** must be in all caps.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set usb modem</td>
<td>Configures a currently loaded USB modem.</td>
</tr>
<tr>
<td>set usb storage dir</td>
<td>Displays a directory listing of a thumb drive.</td>
</tr>
<tr>
<td>set usb storage rename</td>
<td>Renames a file on a thumb drive.</td>
</tr>
<tr>
<td>set usb storage copy</td>
<td>Copies a file on a thumb drive.</td>
</tr>
<tr>
<td>set usb storage delete</td>
<td>Removes a file on a thumb drive.</td>
</tr>
<tr>
<td>set usb storage format</td>
<td>Formats a thumb drive. (Options: ext2, fat16, fat32)</td>
</tr>
</tbody>
</table>

**set usb modem**

- dialinlist, chaphost, chapsecret, dodchaphost, dodchapsecret, initscript, dialoutlogin, dialoutpassword, dialbacknumber, group
**Description**

Formats a thumb drive. Runs a filesystem check on a thumb drive (recommended if it does not mount):

```
set usb storage fsck <U1>
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.

```
show user
```

**Description**

Displays information about the currently logged in user, including a list of groups retrieved from a remote authentication server and the actual group the user has inherited rights and attributes from. The `viewremoteperm` option also displays user attributes retrieved from a LDAP or RADIUS server.
show user [viewremoteperm <enable|disable>]

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.

VPN Commands

Configure an IPsec VPN tunnel:

set vpn <parameters>

Parameters

- tunnel <enable|disable>
- name <VPN Tunnel Name>
- ethport <1|2>
- auth <rsa|psk>
- remotehost <Remote Host IP Address or Name>
- remoteid <Authentication Name>
- remotehop <IP Address>
- remotesubnet <one or more subnets in CIDR notation>
- localid <Authentication Name>
- localhop <IP Address>
- localsubnet <one or more subnets in CIDR notation>
ikenegotiation <main|aggressive>  
ikeenc <any|3des|aes>  
ikeauth <any|sha1|md5>  
ikedhgroup <any|dh2|dh5>  
espenc <any|3des|aes>  
espauth <any|sha1|md5>  
espdhgroup <any|dh2|dh5>  
pfs <enable|disable>  
modeconfig <enable|disable>  
xauthclient <enable|disable>  
xauthlogin <User Login>

The following list includes options which accept the CLEAR command:

**CLEAR** must be in all caps.

| set vpn       | name, remoteid, localid, remotesubnet, localsubnet, xauthlogin |

Enter RSA public key or Pre-Shared Key of remote host:

set vpn key

**Enter XAUTH** password:

set vpn xauthpassword

Display all VPN settings and current status:

show vpn [email <Email Address>]

Display detailed VPN status:

show vpn status [email <Email Address>]

Display VPN logs:

show vpn viewlog [numlines <Number of Lines] [email <Email Address>]

Display RSA public key of the SLC:

show vpn rsakey
Appendix A: Bootloader

The SLC console manager provides a bootloader 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>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Lists and prints the command list and online help.</td>
</tr>
<tr>
<td>?</td>
<td>An alias for help.</td>
</tr>
<tr>
<td>boot</td>
<td>Boot default (runs bootcmd).</td>
</tr>
<tr>
<td>bootcheck</td>
<td>Checks boot bank information.</td>
</tr>
<tr>
<td>bootinfo</td>
<td>Displays boot bank information.</td>
</tr>
<tr>
<td>bootsel 1</td>
<td>2</td>
</tr>
<tr>
<td>IDE</td>
<td>Accesses the IDE sub-system.</td>
</tr>
<tr>
<td>mtest</td>
<td>Performs a simple test of the RAM.</td>
</tr>
<tr>
<td>showconf</td>
<td>Displays hardware configuration.</td>
</tr>
<tr>
<td>su cust</td>
<td>admin</td>
</tr>
<tr>
<td>version</td>
<td>Prints the bootloader version.</td>
</tr>
<tr>
<td>whoami</td>
<td>Displays information about the current user.</td>
</tr>
</tbody>
</table>
### Administrator Commands

In addition to the commands that the user can issue, the administrator can issue the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>imagecopy</code></td>
<td>Copies an image of the drive from the USB port or from the lower PCMCIA device to the internal CF card.</td>
</tr>
<tr>
<td><code>passwd</code></td>
<td>Provides a new password for user admin. The default password for user admin is admin. User cust does not have a password.</td>
</tr>
<tr>
<td><code>ping</code></td>
<td>Sends a ping request to the network host.</td>
</tr>
<tr>
<td><code>printenv</code></td>
<td>Prints bootloader variables.</td>
</tr>
<tr>
<td><code>setenv</code></td>
<td>Sets environment variables.</td>
</tr>
<tr>
<td><code>showconf</code></td>
<td>Displays hardware configuration parameters.</td>
</tr>
</tbody>
</table>
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
- Netzstecker
- Netzversorgung
- Anschluß an die Schutzerde
- Gerätesicherung
- Rack / Einbauschrank
- Signalverbindungen

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
- 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 entsprechend 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.
Appendix D: Sicherheitshinweise

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 (speziell 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 Eingangsmoduls 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 Einbauschränk 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)

<table>
<thead>
<tr>
<th>RJ45</th>
<th>DB25 Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTS</td>
<td>5</td>
</tr>
<tr>
<td>DTR</td>
<td>8</td>
</tr>
<tr>
<td>Tx</td>
<td>6</td>
</tr>
<tr>
<td>Gnd</td>
<td>3</td>
</tr>
<tr>
<td>Gnd</td>
<td>7</td>
</tr>
<tr>
<td>Rx</td>
<td>2</td>
</tr>
<tr>
<td>DSR</td>
<td>20</td>
</tr>
<tr>
<td>CTS</td>
<td>4</td>
</tr>
</tbody>
</table>
Figure E-3  RJ45 Receptacle to DB9M DCE Adapter for the SLC Console Manager (PN 200.2069A)
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.

**IPsec (Internet Protocol Security)**
A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

**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 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 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). 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 dialback. 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](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 2\textsuperscript{nd} 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.
Appendix F: Protocol Glossary

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
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 China 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

<table>
<thead>
<tr>
<th>Product Family Name</th>
<th>Toxic or hazardous Substances and Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lead (Pb)</td>
</tr>
<tr>
<td>UDS1100 and 2100</td>
<td>0</td>
</tr>
<tr>
<td>EDS</td>
<td>0</td>
</tr>
<tr>
<td>MSS100</td>
<td>0</td>
</tr>
<tr>
<td>IntelliBox</td>
<td>0</td>
</tr>
<tr>
<td>XPress DR and XPress-DR+</td>
<td>0</td>
</tr>
<tr>
<td>SecureBox 1101 and 2101</td>
<td>0</td>
</tr>
<tr>
<td>WiBox</td>
<td>0</td>
</tr>
<tr>
<td>UBox</td>
<td>0</td>
</tr>
<tr>
<td>MatchPort</td>
<td>0</td>
</tr>
<tr>
<td>SLC</td>
<td>0</td>
</tr>
<tr>
<td>XPort</td>
<td>0</td>
</tr>
<tr>
<td>WiPort</td>
<td>0</td>
</tr>
<tr>
<td>SLB</td>
<td>0</td>
</tr>
<tr>
<td>SLP</td>
<td>0</td>
</tr>
<tr>
<td>SCS</td>
<td>0</td>
</tr>
<tr>
<td>SLS</td>
<td>0</td>
</tr>
<tr>
<td>DSC</td>
<td>0</td>
</tr>
</tbody>
</table>

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](image)

**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](image)

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.
Appendix H: DC Connector Instructions

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
- Creating the SLC Schema Attribute
- Adding the Attribute to the Users Group in Windows
- Adding the Permissions to the Individual User
- Values to Use
- String Format

Installing Schema Support in Window AD Server


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.
3. Click **Start > Run > mmc**.

4. Click **OK**. *Figure I-2* shows the window that displays.

5. On the **File** menu, click **Add/Remove Snap-in**. *Figure I-3* shows the window that displays.
6. Under Available snap-ins, click **Active Directory Schema > Add > OK**. Figure I-4 shows the directory that displays.

7. To save this console, click Save on the **File** menu. Figure I-5 shows the window that displays.
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](image)

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.
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.
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.
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.

2. In the right pane, scroll down to user. Figure I-11 shows the window that displays.
3. Right click on a user and left click on **Properties**. *Figure I-12* shows the window that displays.

4. Under the **Attributes** tab, click on **Add**. *Figure I-13* shows the window that displays.
5. Find the secureLinxSLCPerms attribute, highlight it, and click on **OK**.

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](image)

2. Expand the console tree until you get to the listing of users. **Figure I-16** shows the folder that displays.
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.

![ADSI Edit Window, CN=Users Folder](image1)

*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.
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**
- **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
Appendix I: LDAP Schemas

- **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**, and any SLC or SLB custom group name. If a custom group name is specified and it matches a current SLC custom group name, any rights attribute will be ignored, and the custom group’s rights (permissions) will be used instead. A group name with spaces cannot be specified.

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**