

SLC™ 9000
Advanced Console Server
User Guide

Part Number PMD-00347
Revision A July 2026

Intellectual Property

© 2026 Lantronix, Inc. All rights reserved. No part of the contents of this publication 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.

Patented: lantronix.com/legal/patents/; additional patents pending.

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 policy, please go to our Web site at lantronix.com/technical-support/warranty/.

Contacts

Lantronix Corporate Headquarters

48 Discovery, Suite 250
Irvine, CA 92618, USA

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

Technical Support

Online: lantronix.com/technical-support/

Sales Offices

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

Disclaimer & Revisions

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, suitability 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.

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.

Note: *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.

User Information

Class A Equipment (Broadcasting and communication equipments for office work)

Seller and user shall be noticed that this equipment is suitable for electromagnetic equipments for office work (Class A) and it can be used outside home.

Changes or modifications made to this device that are not explicitly approved by Lantronix will void the user's authority to operate this device.

Open Source Software

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

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

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

Revision History

Date	Rev.	Comments
July 2026	A	Initial release

Table of Contents

1: About this Guide 20

Purpose and Audience 20
Summary of Chapters 20
Additional Documentation 21

2: Introduction 22

SLC 9000 Models 22
Features 23
- Console Management 23
- Power 23
- Integration with Other Secure Lantronix Products 23

Hardware Overview 24
- SLC 9000 Hardware 24

System Features 27
- Protocols Supported 28
- Access Control 28
- Device Port Buffer 28
- Configuration Options 28
- Network Connections 29
- Integration with Lantronix Percepxion™ 29
- Product Label 29

3: Installation 30

What's in the Box 30
Technical Specifications 30
Physical Installation 32
- Connecting to a Device Port 32
- Connecting to Network Ports 33
- Connecting Terminals 33
- Power Input 34

LEDs 35

4: Quick Setup 36

Recommendations 36
IP Address 36
Lantronix Provisioning Manager 37
Method #1 Quick Setup on the Web Page 37
- Network Settings 38
- Date & Time Settings 39

Administrator Settings 39
Method #2 Quick Setup on the Command Line Interface 40
Next Step 43

5: Web and Command Line Interfaces 44

Web Manager 44
Logging In 46
Logging Out 46
Web Page Help 46
Command Line Interface 47
Logging In 47
Logging Out 47
Command Syntax 47
Command Line Help 48
Tips 48

6: Networking 51

Requirements 51
Network Port Settings 51
Ethernet Interfaces (Eth1 and Eth2) 54
TCP Keepalive Parameters 55
Gateway 56
Fail-Over Settings 57
Fail-Over Cellular Gateway Configuration 59
Advanced Cellular Gateway Configuration 61
Fail-Over Cellular Gateway Firmware 62
Load Cellular Gateway Firmware Options 62
Ethernet Counters 62
Network Commands 63
SFP Port Settings 63
Ethernet Interfaces 65
Hostname and Name Servers 66
Hostname & Name Servers 67
FQDN List 69
Virtual Interfaces 70
Ethernet Switch 72
Port Statistics 74
DHCP 76
DHCP Server Settings 77
DHCP Relay Settings 78
IP Filter 78
Viewing IP Filters 78
Mapping Rulesets 79

Enabling IP Filters 79
Configuring IP Filters 80
Rule Parameters 81
Updating an IP Filter 83
Deleting an IP Filter 83
IP Filter Commands 83
Routing 83
Dynamic Routing 84
Static Routing and IPv4 Static Routes 84
IPv6 Static Routing 85
Routing Commands 85
Forwarding 86
Forwarding Connections Commands 87
VPN Settings 87
Sample ipsec.conf Files 98
VPN Commands 103
Security 103
Performance Monitoring 106
Performance Monitoring - Add/Edit Probe 108
Performance Monitoring - Results 111
Performance Monitoring Commands 115

7: Services 116

System Logging and Other Services 116
SSH/Telnet/Logging 117
System Logging 118
SSH 119
Telnet 119
Audit Log 120
SMTP 120
Web SSH/Web Telnet Settings 120
Discovery Server 121
SSH/Telnet/Logging Commands 121
SNMP 121
v1/v2c Communities 125
Version 3 126
V3 User Read-Only 126
V3 User Read-Write 126
V3 User Trap 126
Version 3 TLS (over TCP) 127
Services Commands 128
NFS 129
NFS Commands 130

Secure Lantronix Network 131
Web SSH/Telnet Copy and Paste 134
Secure Lantronix Network Commands 135
Date and Time 135
Date and Time Commands 139
Web Server 140
Web Server - Web Sessions 142
Web Server - SSL Certificate 142
Web Server - Ciphers 145
Admin Web Commands 146
REST API 147

8: Percepxion 149
Before You Begin 149
Connect the SLC 9000 Unit to Percepxion 149
How Percepxion Connects (Connection Sequence) 151
Zero-Touch Deployment via Percepxion 152
Percepxion Commands 154

9: USB Port 155
USB Storage 155
Manage Files on Storage Device 157
USB Modem Settings 158
Data Settings 160
Modem Settings 160
Text Mode 162
PPP Mode 162
IP Settings 163
USB Serial Settings 163
Data Settings 165
IP Settings 166
USB Commands 166

10: Device Ports 167
Connection Methods 167
Permissions 167
Device Status 168
Device Ports 169
Telnet/SSH/TCP in Port Numbers 170
Device Port Global Commands 170
Device Ports - Settings 171
Device Port Settings 173

IP Settings 175
Data Settings 176
Hardware Signal Triggers 177
Modem Settings (Device Ports) 178
Modem Settings: Text Mode 179
Modem Settings: PPP Mode 180
Port Status and Counters 181
Device Ports - Power Management 181
Device Ports - RPMs - Add Device 184
Device Port - Sensorsoft Device 186
Device Port Commands 187
Interacting with a Device Port 187
Device Ports - Logging and Events 188
Local Logging 188
NFS File Logging 188
USB Logging 188
Token/Data Detection 189
Syslog Logging 189
Token & Data Detection 190
Local Logging 192
Log Viewing Attributes 192
NFS File Logging 192
USB Logging 192
Syslog Logging 192
Logging Commands 193
Console Port 193
Console Port Commands 194
Xmodem 194
Host Lists 197
Host Parameters 198
Host Parameters 199
Host List Commands 200
Scripts 200
Scripts 203
Script Commands 206
Batch Script Syntax 206
Interface Script Syntax 207
Primary Commands 208
Secondary Commands 209
Control Flow Commands 211
Custom Script Syntax 212
Example Scripts 213
Sites 229

Site Commands 232
Access Lists 232
Access List Commands 234
Modem Dialing States 234
Dial In 234
Dial-back 235
Dial-on-demand 236
Dial-in & Dial-on-demand 236
Dial-back & Dial-on-demand 237
CBCP Server and CBCP Client 237
CBCP Server 237
CBCP Client 238
Key Sequences 238

11: Managed Devices Automation 240

12: Containers (Docker) 245

13: Power Management 247

Integrated PDU Management 247
Power Commands 250
Remote Power Managers 250
Devices - RPMs 250
RPMs - Add Device 254
RPMs - Manage Device 257
RPMs - Outlets 260
RPM Shutdown Procedure 261
Optimizing and Troubleshooting RPM Behavior 262
RPM Commands 263

14: Connections 264

Typical Setup Scenarios for the SLC Unit 264
Terminal Server 264
Remote Access Server 265
Reverse Terminal Server 265
Multiport Device Server 266
Console Server 266
Connection Configuration 267
Connection Commands 269

15: User Authentication 270

Authentication Methods 270

Authentication Commands 272
User Rights 272
Local and Remote Users 274
Sysadmin Account Default Login Values 276
Limiting Sysadmin User Access 277
Local/Remote User Settings 277
Shortcuts 281
Local Users Commands 281
Remote User Rights Commands 281
LDAP 282
LDAP Commands 286
RADIUS 287
RADIUS Commands 290
User Attributes & Permissions from LDAP Schema or RADIUS VSA 290
TACACS+ 291
TACACS+ Groups 291
TACACS+ Commands 296
Groups 296
Group Commands 299
SSH Keys 299
Overview 299
Imported Keys 299
Exported Keys 299
Create an SSH Key 300
Imported Keys (SSH In) 302
Host & Login for Import 303
Exported Keys (SSH Out) 303
Host and Login for Export 304
SSH Server/Host Keys 304
SSH Commands 306
Custom Menus 306
Custom User Menu Commands 309

16: Maintenance 310

Firmware & Configurations 310
Internal Temperature 312
Site Information 312
SLC Firmware 312
Boot Banks and Bootloader Settings 313
Load Firmware Via Options 314
Configuration Management 314
Administrative Commands 316
HTTPS Push Configuration Restore 316

Factory Reset with External Storage Device 316
Factory Reset with Reset Button 317
Zero Touch Provisioning and Bootstrapping 317
Provision via Zero Touch Provisioning 319
Creating a Certificate 320
Provision via Bootstrap Server 323
System Logs 324
System Log Commands 326
Audit Log 326
Audit Log Commands 327
Email Log 327
Logging Commands 328
Diagnostics 328
Diagnostic Commands 332
Status/Reports 333
View Report 333
Status Commands 334
Emailing Logs and Reports 335
Events 336
Events Commands 338
Banners 339
Administrative Banner Commands 340
System Info 340
Manage Files 341

17: Application Examples 343

Telnet/SSH to a Remote Device 343
Dial-in (Text Mode) to a Remote Device 345
Local Serial Connection to Network Device via Telnet 346

18: Command Reference 348

Introduction to Commands 348
Command 348
Command Line Help 349
Tips 349
Access List Commands 350
Administrative Commands 351
Audit Log Commands 366
Authentication Commands 367
LDAP Commands 368
Local Users Commands 369
RADIUS Commands 373
TACACS+ Commands 374

User Permissions Commands 376
Remote User Commands 377
CLI Commands 379
Cellular Modem Commands 381
Connection Commands 382
Console Port Commands 385
Container Commands 386
Custom User Menu Commands 388
Date and Time Commands 390
Device Commands 392
Device Port Commands 393
DHCP Commands 397
Diagnostic Commands 398
Events Commands 403
Group Commands 405
Host List Commands 405
IP Filter Commands 406
Logging Commands 408
Managed Device (Automation) Commands 411
Network Commands 415
NFS Commands 418
Percepxion Commands 419
Performance Monitoring Commands 423
Power Commands 427
Routing Commands 427
RPM Commands 428
Script Commands 430
Security Commands 433
Services Commands 433
Site Commands 435
SLC Network Commands 436
SNMP Commands 437
SSH Key Commands 438
Status Commands 441
Switch Commands 443
System Log Commands 445
Temperature Commands 446
USB Access Commands 447
USB Device Commands 447
USB Modem Commands 448
USB Serial Commands 449
USB Storage Commands 450
Virtual Interface Commands 452

VPN Commands 452
Xmodem Commands 455

Appendix A: Security Considerations 456
Security Practice 456
Factors Affecting Security 456
Security Best Practices 456

Appendix B: Safety Information 458
Safety Precautions 458
Fuse Caution Statement 458
Cover 458
Power Plug 458
Input Supply 459
Grounding 459
Rack 459
Port Connections 459

Appendix C: Adapters and Pinouts 461

Appendix D: Protocol Glossary 464

Appendix E: Compliance Information 466
RoHS, REACH and WEEE Compliance Statement 467

Appendix F: Ansible Interoperability 468
Ansible Installation 468
Ansible Setup 469
Pinging Hosts and Running Playbooks 471

List of Figures

Figure 2-1 SLC 9000 Overview 24
Figure 2-2 SLC 9000, front view. 24
Figure 2-3 SLC 9000 back view, AC model 24
Figure 2-4 SLC 9000, back view, DC model 24
Figure 2-5 SLC 9000, front, network ports 25
Figure 2-6 RJ45 console port pinout 25
Figure 2-7 RJ45 serial module 26
Figure 2-9 USB serial module 26
Figure 2-10 Ethernet switch module 27
Figure 3-4 AC and DC Power Input connections 34
Figure 3-5 SLC 9000 LEDs 35
Figure 4-2 Quick Setup 38
Figure 4-3 Quick Setup Completed in Web Manager 40
Figure 4-4 Home 40
Figure 4-5 Beginning of Quick Setup Script 41
Figure 4-6 Quick Setup Completed in CLI 42
Figure 5-1 Web Page Layout 44
Figure 5-2 Sample Dashboard 45
Figure 6-1 Network > Network Settings (1 of 2) 52
Figure 6-2 Network > Network Settings (2 of 2) 53
Figure 6-3 Hostname and Name Serverst 69
Figure 6-4 Network > Ethernet Switch 73
Figure 6-5 Network > DHCP 77
Figure 6-6 Network > IP Filter 79
Figure 6-7 Network > IP Filter Ruleset (Adding/Editing Rulesets) 81
Figure 6-8 Network > Routing 84
Figure 6-9 Network > Forwarding Connections 86
Figure 6-10 Network > VPN 90
Figure 6-11 Network > Perf Monitoring 107
Figure 6-12 Performance Monitoring - Add/Edit Probe 109
Figure 6-14 Performance Monitoring - Operations 114
Figure 7-1 Services > SSH/Telnet/Logging 117
Figure 7-2 Services > SNMP (1 of 2) 122
Figure 7-3 Services > SNMP (2 of 2) 123
Figure 7-4 Services > NFS 129
Figure 7-5 Services > Secure Lantronix Network 131

Figure 7-6 IP Address Login Page 132
Figure 7-7 SSH or Telnet CLI Session 132
Figure 7-8 Disabled Port Number Popup Window 133
Figure 7-9 Services > Secure Lantronix Network > Search Options 134
Figure 7-10 Services > Date & Time 137
Figure 7-11 Services > Web Server 140
Figure 7-12 Web Sessions 142
Figure 7-13 Web Server - SSL Certificate 143
Figure 7-14 Web Server - Ciphers List 146
Figure 8-1 Services > Percepxion 154
Figure 9-1 Devices > USB 156
Figure 9-2 Devices > USB > USB - Storage 156
Figure 9-3 Firmware and Configurations - Manage Files 158
Figure 9-4 Devices > USB > USB - Modem 159
Figure 9-5 Devices > USB - Serial Port 164
Figure 9-6 Devices > USB > USB - Serial 165
Figure 10-1 Devices > Device Status 168
Figure 10-2 Devices > Device Ports 169
Figure 10-3 Device Ports > Settings (1 of 2) 172
Figure 10-4 Device Ports > Settings (2 of 2) 173
Figure 10-6 Device Ports - Power Management 183
Figure 10-7 Device Ports > RPMs - Add Device 185
Figure 10-8 Devices > Device Ports > Sensorsoft 186
Figure 10-9 Devices > Device Ports - Logging & Events 190
Figure 10-10 Devices > Console Port 193
Figure 10-11 Devices > Host Lists 197
Figure 10-12 View Host Lists 199
Figure 10-13 Devices > Scripts 201
Figure 10-14 Adding or Editing New Scripts 202
Figure 10-19 Devices > Sites 230
Figure 10-20 Devices > Access Lists. 233
Figure 13-1 Devices > Power Outlets: 248
Figure 13-2 Devices > RPMs 251
Figure 13-3 RPM Shutdown Order 252
Figure 13-4 RPM Notifications 253
Figure 13-5 RPM Raw Data Log 253
Figure 13-6 RPM Logs 254
Figure 13-7 RPM Environmental Log 254

Figure 13-8 Device Ports > RPMs - Add Device 255
Figure 13-9 RPMs - Managed Device 258
Figure 13-10 RPMs - Outlets 261
Figure 14-1 Terminal Server 265
Figure 14-2 Remote Access Server 265
Figure 14-3 Reverse Terminal Server 265
Figure 14-4 Multiport Device Server 266
Figure 14-5 Console Server 266
Figure 14-6 Devices > Connections 267
Figure 14-7 Current Connections 268
Figure 15-1 User Authentication > Authentication Methods 271
Figure 15-3 User Authentication > Local/Remote Users 275
Figure 15-4 User Authentication > Local/Remote User > Add/Edit User 278
Figure 15-5 User Authentication > LDAP 283
Figure 15-6 User Authentication > RADIUS 287
Figure 15-7 User Authentication > TACACS+ 293
Figure 15-8 User Authentication > Groups 297
Figure 15-9 User Authentication > SSH Keys 302
Figure 15-10 Current Host Keys 305
Figure 15-11 User Authentication > Custom Menus 307
Figure 16-1 Maintenance > Firmware & Configurations 311
Figure 16-2 Network > Firmware/Config > Manage 315
Figure 16-3 ZTP/Bootstrap Flowchart 319
Figure 16-4 Maintenance > System Logs 324
Figure 16-5 System Logs 325
Figure 16-6 Maintenance > Audit Log 326
Figure 16-7 Maintenance > Email Log 327
Figure 16-8 Maintenance > Diagnostics 329
Figure 16-9 Maintenance > Diagnostics 332
Figure 16-10 Maintenance > Status/Reports 333
Figure 16-11 Generated Status/Reports 334
Figure 16-12 About SLC 336
Figure 16-13 Maintenance > Events 337
Figure 16-14 Maintenance > Banners 339
Figure 16-15 System Info 340
Figure 17-1 SLC - Console Manager Configuration 343
Figure 17-2 Remote User Connected to a UNIX Server via the SLC unit 343
Figure 17-3 Dial-in (Text Mode) to a Remote Device 345

Figure 17-4 Local Serial Connection to Network Device via Telnet _____346

List of Tables

Table 2-8 RJ45 serial port default pinout ____ 26
Table 3-1 SLC 9000 Technical Specifications ____ 30
Table 3-2 Console Port and Device Port - Reverse Pinout Disabled ____ 33
Table 3-3 Device Port - Reverse Pinout Enabled (Default) ____ 33
Table 4-1 Methods of Assigning an IP Address ____ 36
Table 5-3 SCS Commands ____ 49
Table 5-4 CLI Keyboard Shortcuts ____ 50
Table 6-13 Error Conditions ____ 113
Table 10-5 Port Status and Counters ____ 181
Table 10-15 Definitions ____ 207
Table 10-16 Primary Commands ____ 208
Table 10-17 Secondary Commands ____ 210
Table 10-18 Control Flow Commands ____ 211
Table 15-2 User Types and Rights ____ 272
Table 18-1 Actions and Category Options ____ 348

1: About this Guide

Purpose and Audience

This guide provides the information needed to install, configure, and use the Lantronix SLC™ 9000 advanced console server. The SLC unit 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 for facilities that are typically remote branch offices or "distributed" IT locations.

If you are setting up the SLC 9000 for the first time, start with *Chapter 3: Installation* and *4: Quick Setup*.

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
Chapter 2: Introduction	Describes the SLC 9000 models, their main features, and the protocols they support.
Chapter 3: Installation	Provides technical specifications; describes connection form factors and power supplies; provides instructions for installing the SLC 9000 advanced console server in a rack.
Chapter 4: Quick Setup	Provides instructions for getting your SLC unit up and running and for configuring required settings.
Chapter 5: Web and Command Line Interfaces	Describes the web and command line interfaces available for configuring the SLC 9000 advanced console server. The configuration chapters (6-12) provide detailed instructions for using the web interface and include equivalent command line interface commands.
Chapter 6: Networking	Provides instructions for configuring network ports, firewall and routing settings, and VPN.
Chapter 7: Services	Provides instructions for enabling and disabling system logging, SSH and Telnet logins, SNMP, SMTP, and the date and time.
Chapter 9: USB Port	Provides instructions for using the USB port.
Chapter 10: Device Ports	Provides instructions for configuring global device port settings, individual device port settings, and console port settings.
Chapter 13: Power Management	Provides instructions for using RPMs and integrated PDU management.
Chapter 14: Connections	Provides instructions for configuring connections and viewing, updating, or disconnecting a connection.
Chapter 15: User Authentication	Provides instructions for enabling or disabling methods that authenticate users who attempt to log in via the web, SSH, Telnet, or the console port. Provides instructions for creating custom menus.
Chapter 16: Maintenance	Provides instructions for upgrading firmware, viewing system logs and diagnostics, generating reports, and defining events. Includes information about web pages and commands used to shut down and reboot the SLC 9000 advanced console server.

Chapter (continued)	Description
Chapter 17: Application Examples	Shows how to set up and use the SLC unit in three different configurations.
Chapter 18: Command Reference	Lists and describes all of the commands available on the SLC command line interface
Appendix A: Security Considerations	Provides tips for enhancing SLC security.
Appendix B: Safety Information	Lists safety precautions for using the SLC 9000 advanced console server.
Appendix C: Adapters and Pinouts	Includes adapter pinout diagrams.
Appendix D: Protocol Glossary	Lists the protocols supported by the SLC unit with brief descriptions.
Appendix E: Compliance Information	Provides information about the SLC 9000 advanced console server's compliance with industry standards.

Additional Documentation

Visit the Lantronix web site for the latest documentation and resources.

Document	Description
SLC 9000 Advanced Console Server Quick Start Guide	Provides accessories and part number information, hardware installation instructions, directions to connect the SLC unit, and network IP configuration information.
SLC 9000 Advanced Console Server Product Brief	Provides product overview information and specifications.

2: Introduction

The Lantronix SLC 9000 with Percepxion™ transforms out-of-band management from a collection of manual tasks into an automated, policy-driven platform. New sites can be deployed with true zero-touch provisioning of the SLC 9000, allowing field technicians to install and connect equipment without requiring an engineer to perform initial configuration. When an SLC 9000 powers on, it automatically connects to Percepxion using DHCP or cellular, downloads its approved configuration, enrolls connected devices, and appears in inventory. This approach reduces deployment time, eliminates configuration errors, and helps organizations scale remote infrastructure without increasing administrative overhead.

Percepxion is Lantronix's cloud management platform for SLC 9000 deployments. When connected to Percepxion, admins can access any device's console port from anywhere without a VPN, monitor fleet health across all SLC 9000 units, push firmware and configuration updates to the entire fleet, and set up new devices to self-configure when they come online.

The platform also strengthens network resiliency by providing secure, always-available console access when the production network is unavailable. With integrated cellular failover, administrators maintain access to critical infrastructure during outages, misconfigurations, or security incidents. Beyond connectivity, Percepxion continuously monitors device state, automates configuration backups, and enforces firmware and configuration compliance across the fleet. Admins can quickly identify devices that fall outside policy and remediate them through centralized management rather than relying on individual SSH sessions and manual tracking.

SLC 9000 Models

This document applies to the SLC 9000 advanced console server.

The following model numbers are defined:

Model	Description
SLC9016	SLC9000 Console Server, 16 RJ45 serial ports, 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
SLC9016-16U	SLC9000 Console Server, 32 serial ports (16 RJ45, 16 USB Type-A), 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
SLC9016-32U	SLC9000 Console Server, 48 serial ports (16 RJ45, 32 USB Type-A), 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
SLC9016-16E	SLC9000 Console Server, 16 RJ45 serial ports, 16x 1GbE switch ports, 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
SLC9016-16U-16E	SLC9000 Console Server, 32 serial ports (16 RJ45, 16 USB Type-A), 16x 1GbE switch ports, 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
SLC9016-32E	SLC9000 Console Server, 16 RJ45 serial ports, 32x 1GbE switch ports, 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
SLC9024-24E	SLC9000 Console Server, 24 RJ45 serial ports, 24x 1GbE switch ports, 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
SLC9032	SLC9000 Console Server, 32 RJ45 serial ports, 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
SLC9032-16U	SLC9000 Console Server, 48 serial ports (32 RJ45, 16 USB Type-A), 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU

Model	Description
SLC9032-16E	SLC9000 Console Server, 32 RJ45 serial ports, 16x 1GbE switch ports, 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
SLC9048	SLC9000 Console Server, 48 RJ45 serial ports, 2x 1GbE, 2x SFP+, TPM 2.0, dual AC PSU
AC Power Cord Options	The default part numbers above ship without power cords. For North American power cords (NEMA 5-15P), add “-NA” to the end of the part number. For example: SLC9016-NA
DC Power	The SLC 9000 is also available with dual DC power inputs. Add “-DC” to the end of the part number to order. For example: SLC9016-DC
Accessories	
NTC-501-SLC9	NTC-501 (North America) kit to deploy as the 5G cellular OOB component of an SLC 9000
NTC-502-SLC9	NTC-502 (EMEA, APAC excl. Japan & China (Telstra)) kit to deploy as the 5G cellular OOB component of an SLC 9000
SFPs	Lantronix offers a variety of fiber and copper SFPs. See the Lantronix website.

Features

Console Management

- Up to 48 serial RJ45 RS-232 and/or USB type A ports for console connectivity

  Note: *USB ports are generally intended to connect directly to USB console ports. It is also possible to connect a USB to serial adapter to them to connect to serial console ports, if needed.*

- Enables system administrators to remotely manage devices with serial and/or USB console ports, e.g., Linux, Unix, and recent versions of Windows servers, routers, telecom, and switches with RS-232C or USB compatible serial consoles in a 1U-tall rack space.
- Provides data logging, monitoring, and secure access control via the Internet
- Managed Ethernet switch (16 or 32 ports)

Power

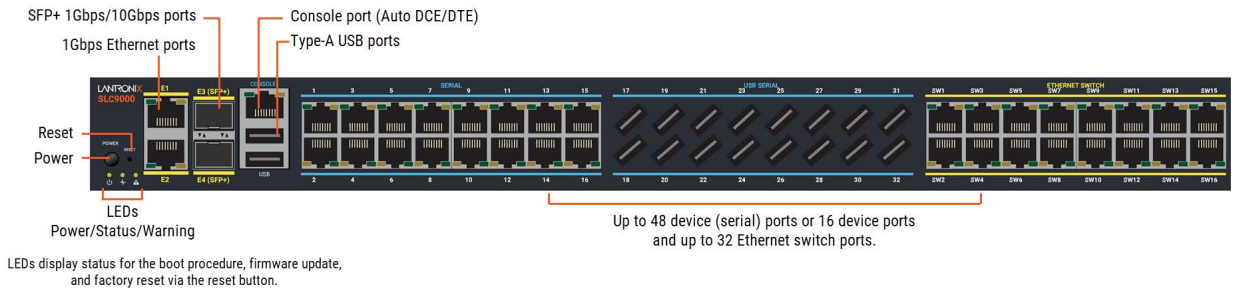
- AC model: Dual input, (100-240V, 50/60 Hz, 60 W)
- DC model: Dual input, -20 to -72 VDC
- Convection cooled, silent operation, low power consumption

Integration with Other Secure Lantronix Products

The SLC 9000 can integrate seamlessly with the Percepxion™ for a complete end-to-end Out-of-Band (OOB) management solution. Percepxion is the recommended way to manage SLC 9000 devices at scale. It enables Zero Touch Provisioning, remote console access, fleet firmware management, and telemetry. Connect your SLC9000 to Percepxion as part of initial deployment.

Hardware Overview

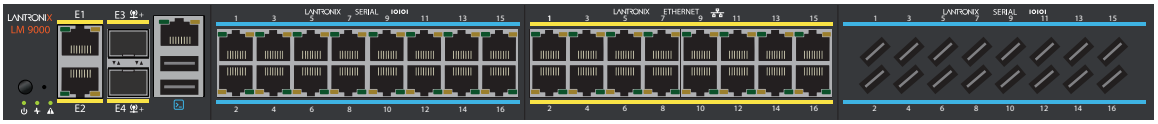
Figure 2-1 SLC 9000 Overview



SLC 9000 Hardware

The SLC 9000 hardware has 3 bays which can be populated with up to 48 device (serial) ports or 16 device ports and up to 32 Ethernet switch ports. The ports are located on the front of the unit. The device ports can be any combination of RJ45 or USB serial ports. Any empty slots must be to the right. The image below shows an SLC 9000 unit with a 16 port RJ45 serial module, a 16 port USB serial module, and a 16 port Ethernet switch module.

Figure 2-2 SLC 9000, front view.



The back of the unit has a slot for an optional cellular modem on the right, and dual AC or DC power supplies on the left (when facing the back of the unit the PS2 power supply is on the left and the PS1 power supply is on the right). Immediately after boot (for approximately one minute), the PS1 and PS2 Power Supply status (OK or Failed) displayed in the Web UI Status/Reports page and the CLI show sysstatus command may not be accurate until the PS status becomes available to the system.

Figure 2-3 SLC 9000 back view, AC model



Figure 2-4 SLC 9000, back view, DC model

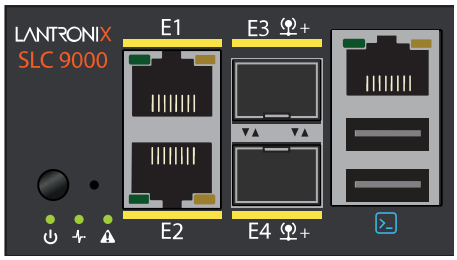


Ensure that the installation site ambient temperature is between 32°F to 122°F (0°C to 50°C).

In addition to a software watchdog, the SLC 9000 has a hardware watchdog that will reset the unit if the hardware watchdog is unable to reset an internal CPU state timer for 128 seconds.

The left side of the front of the unit contains 2 standard RJ45 ports, 2 SFP network ports, a console port, two type-A USB ports, LEDs, the power button and a pinhole factory reset button:

Figure 2-5 SLC 9000, front, network ports



The pinout for the RJ45 console port is DCE (see pinout table below), but is also auto-sensing and can detect the port pinout of the connected device. The default settings are 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control.

Figure 2-6 RJ45 console port pinout

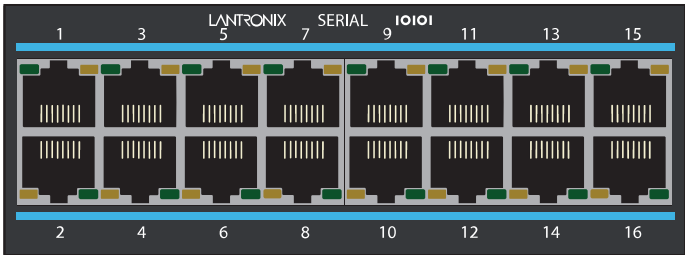
SLC 9000 Console RJ45 Port Pinout		
Pin Number	**Description**	**Male RJ45 8-pin**
1	CTS (input)	
2	DSR (input)	
3	RxD (input)	
4	Ground	
5	Ground	
6	TxD (output)	
7	DTR (output)	
8	RTS (output)	

The pinhole button can be used to reset the unit to factory defaults.

If power to the unit is lost or turned off, the power up behavior can be configured with the CLI command `admin system powerstate`: the device will either always power on when power is applied (without using the power button), or remember the last power state and either remain off or turn on.

RJ45 Serial Module

Figure 2-7 RJ45 serial module



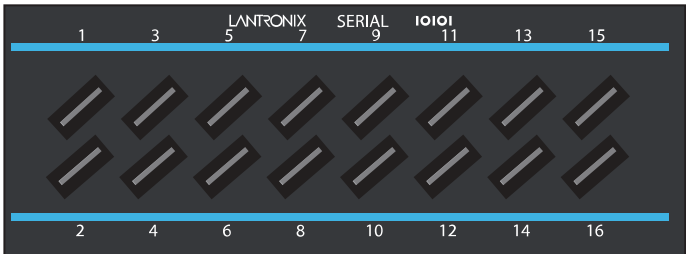
RJ45 serial ports are reversed by default so that straight-through RJ45 patch cables may be used to connect to Cisco and similar RJ45 serial console ports. The pinout is software reversible, to easily connect to devices with non-reversed pinouts. The default serial settings are 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control.

Table 2-8 RJ45 serial port default pinout

SLC 9000 RJ45 Serial Port Pinout		
Pin Number	**Description**	**Male RJ45 8-pin**
1	CTS (input)	
2	DSR (input)	
3	RxD (input)	
4	Ground	
5	Ground	
6	TxD (output)	
7	DTS (output)	
8	RTS (output)	

USB Serial Module

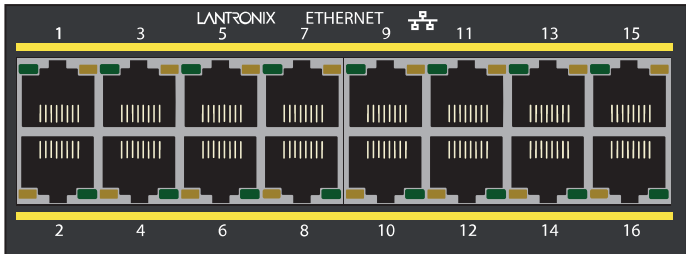
Figure 2-9 USB serial module



USB serial ports support the following types of USB to serial device drivers: Prolific-PL2303, Prolific-PL2303GS, FTDI, CDC ACM, CP210X and MCT U232.

Ethernet Switch Module

Figure 2-10 Ethernet switch module



System Features

The SLC 9000 firmware has the following basic capabilities:

- Software reversible device port pinouts (serial RJ45 ports only)
- Connects up to 48 serial RJ45 RS-232 and/or USB type A consoles
- Support use of simple straight-through cables for use with Cisco and other devices that use the “Cisco” RJ-45 serial pinouts
- 10/100/1000 Base-T Ethernet network compatibility and SFP+ ports to support single mode or multi-mode 1 or 10 Gigabit SFP transceiver modules
- Managed Device Automation for onboarding Cisco, Arista, and other network devices connected to the serial ports, then automating monitoring and management of the device.
- Support for Docker containers to run pre-built applications for automation and monitoring on the SLC.
- Buffer logging to file
- Email and SNMP notification
- ID/Password security, configurable access rights
- Secure shell (SSH) security; supports numerous other security protocols
- 2FA (two factor authentication) with RADIUS and LDAP
- Network File System (NFS)
- RAW TCP, 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
- Break-safe
- Simultaneous access on the same port - “listen” and “direct” connect mode
- Remote power manager (RPM) control of UPS and PDU devices
- Local access through a dedicated front panel serial console port
- Web administration (using most browsers)
- Integrated PDU management for Snyaccess SP-1004A/B and APC APC7900B PDUs

- High availability access with network fail-over and fail-back via an integrated cellular modem or an external dial-up modem
- REST API for querying, configuring, updating, and monitoring the SLC 9000

Protocols Supported

The SLC 9000 advanced console server supports the TCP/IP network protocol as well as:

- SSH, Telnet, PPP, and NFS 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
- SCP, FTP and SFTP for file transfers and firmware upgrades
- TFTP for firmware upgrades
- DHCP and BOOTP for IP address assignment
- HTTPS/TLS for secure browser-based configuration
- NTP for time synchronization
- LDAP with Group support, RADIUS with VSA support, CHAP, PAP, and TACACS+ with Group support for user authentication
- Callback Control Protocol (CBCP)
- IPSec for VPN access

For brief descriptions of these protocols, see *Appendix D: Protocol Glossary on page 464*.

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 RADIUS, TACACS+, and LDAP. Groups are supported in LDAP, RADIUS (using VSA), and TACACS+ (using priv_lvl).

2FA (two factor authentication) is supported with LDAP and RADIUS, if the remote authentication server is configured for 2FA to request an OTP (one-time password) from the user. 2FA is supported for web UI, SSH, Telnet, and console port logins.

Device Port Buffer

The SLC 9000 unit 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

Both a web interface viewed through a standard browser and a command line interface (CLI) are available for configuring the SLC 9000 settings and monitoring performance.

An OpenAPI 3.1 compliant REST API is available for status queries, configuration and firmware updates, and monitoring the SLC 9000.

Network Connections

The SLC 9000 offers the option of four network management connections between the 2 10/100/100 Base-T Ethernet ports and 2 1-10 Gbps SFP+ ports. 2 Eth 1G and SFP+ 1/10/Gb ports. The 10/100/1000 Base-T Ethernet are for use with a conventional Ethernet network. Use standard RJ45-terminated cables, like Category 5 or 6 patch cable. CAT5E or better cables are recommended for 1000 Base Ethernet. CAT6 or better cables are recommended for SFP+ 10G Base Ethernet.

Integration with Lantronix Percepxion™

The SLC 9000 is compatible with Lantronix Percepxion management software for an end-to-end Out-of-Band (OOB) management solution. The Percepxion cloud-based platform provides comprehensive device life cycle management, application integration, remote access, and data analytics.

Product Label

The product label on the underside of the SLC 9000 advanced console server contains the following information about each SLC unit:

- Part Number
- Product Revision
- Country of Manufacturing Origin
- Serial Number
- Device ID (Percepxion)
- Manufacturing Date Code
- Bar Code

3: Installation

This chapter provides a high-level procedure for installing the SLC advanced console server.

Caution: ***To avoid physical and electrical hazards, please read Appendix B: Safety Information before installing the SLC 9000 advanced console server.***

What's in the Box

The following components come in the box:

The package contains the following:

- SLC 9000 advanced console server, model numbers vary
- (2) Rack mount brackets, and (4) mounting screws
- Product registration card and promotional flyer
- North American AC models (SKUs ending in "-NA"): (2) two NEMA 5-15P power cables, AC Shielded, 6ft. US. Other AC SKUs do not come with power cables.
- DC models: DC Plug Connector Accessory Kit

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

For Lantronix SFP modules, visit https://lantronix.com/products-class/sfps/

For accessories and ordering information, visit https://lantronix.com/products/slc9000/

Technical Specifications

Table 3-1 SLC 9000 Technical Specifications

Component	Description
Serial Interface (Device)	◆ Up to 48 RJ45-type 8-conductor connectors in 16-port increments. These connectors have individually configurable standard and reversible pinouts, ◆ Speed software selectable (300 to 115200 baud) ***Note:*** *Serial RJ45 device ports for the SLC 9000 advanced console server are reversed by default.*
USB 2.0 Interface (Device)	◆ Up to 48 USB type A (Host). ◆ HS, FS, and LS ◆ Capable of providing VBUS 5V up to 100 mA per port, but not to exceed 600 mA total per 16-port USB I/O module. ◆ May be used with a USB-to-serial adapter to connect a serial device, if needed. Please contact Lantronix for the list of tested adapters. ***Caution:*** ***USB ports are designed for data traffic only. They are not designed for charging or powering devices. Over-current conditions on VBUS 5V may disrupt operations.***

Component (continued)	Description
Serial Interface (Console)	◆ (1) RJ45-type 8-pin connector (DCE, auto-sensing) ◆ Speed software selectable (300 to 115200 baud) ◆ LEDs: ➢ Green light ON indicates data transmission activities ➢ Yellow light ON indicates data receiving activities
Ethernet Switch Interface	◆ (1) Ethernet Switch module can be installed, providing up to 32 LAN ports.
Network Interface	◆ (2) 10/100/1000 Base-T RJ45 Ethernet with LED indicators: ➢ Green light ON indicates a link at 1000 Base-T. ➢ Green light OFF indicates a link at other speeds or no link. ➢ Yellow/Orange light ON indicates a link is established. ➢ Yellow/Orange light blinking indicates activity. **AND** ◆ (2) SFP+ 1G/10G ports to support standard fiber or copper SFP transceiver modules (single or multi-mode) at speed 1 Gigabit. LED indicators: ➢ Green light ON indicates a link is established. ➢ Green light OFF indicates no link. ➢ Yellow/Orange light steady ON indicates no activity. ➢ Yellow/Orange light blinking indicates activity.
Rear option slot for External Modem Support	◆ USB type-C 5V 2A power support and 2-way 12V termination block
Power Supply AC (dual)	◆ Universal AC power input: 100-240 VAC ◆ 50 or 60 Hz IEC 60320/C14
Power Supply DC (dual)	-24/-48/-60VDC
Power Consumption	◆ Less than 25W with 48 RS232 serial ports ◆ Less than 45W with 48 USB ports
Dimensions	44.5 mm x 444.5 mm x 267 mm (1.75 in x 17.5 in x 10.5 in) 1 Rack Unit (1RU)
Weight	◆ 2.7 Kg (6 pounds)
Temperature	◆ Operating: 0 to 50°C (32 to 122°F) at mean sea level ◆ Storage: -30 to 80°C (-22 to 176°F) at mean sea level
Relative Humidity	◆ Operating: 20% to 80% non-condensing ◆ Storage: 10% to 90% non-condensing
Front USB Ports	◆ (2) USB type-A 3.0 ports
Operating Atmosphere ***Caution: EQUIPMENT IS FOR INDOOR USE ONLY!***	 For use at altitudes no more than 2000 meters above sea level only. 仅适用于海拔 2000m 以下地区安全使用  For use in non-tropical conditions only. 仅适用于非热带气候条件下安全使用

Physical Installation

Install the SLC 9000 advanced console server in an EIA-standard 19-inch rack (1U tall) or as a desktop unit. The SLC module uses convection cooling to dissipate excess heat.

To install the SLC 9000 advanced console server in a rack:

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

Warning: ***Do not to block the air vents on the sides of the SLC module. If you mount the SLC advanced console server in an enclosed rack, we recommend that the rack have a ventilation fan to provide adequate airflow through the SLC unit.***

2. Connect the serial device(s) to the SLC unit ports. See the section, *Connecting to a Device Port (on page 32)*.
3. Choose one of the following options:
   - To configure the SLC 9000 advanced console server 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 33)*.
   - To configure the SLC unit using a dumb terminal or a computer with terminal emulation, connect the terminal or PC to the front panel SLC console port. See *Connecting Terminals (on page 33)*.
4. For AC supply model, connect the power cord, and apply power. For DC supply model, the plug connectors must be assembled according to the DC Plug Connector Kit instructions prior to installation. Connect the power cord to the power supply before applying power.
5. Wait approximately one minute for the boot process to complete. The status (center) LED flashes once every 2 seconds when the system is loaded and ready.

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

Connecting to a Device Port

You can connect almost any device that has a serial console port to a device port on the SLC 9000 unit for remote administration. The console port must support the RS-232C interface.

Note: *Many servers must either 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 serial RJ45 device port:

1. Connect one end of the Ethernet cable to the device port.
2. Connect the other end of the Ethernet cable to an RJ45 serial console port or to other port types using a Lantronix serial console adapter.

Notes:

- *See Device Port Commands to enable or disable reverse pinouts through the CLI.*
- *Table 3-2 and Table 3-3 provide additional information on reverse pinouts.*
- *See Appendix C: Adapters and Pinouts for information about Lantronix adapters.*

3. Connect the adapter to the serial console port on the serial device.

Table 3-2 Console Port and Device Port - Reverse Pinout Disabled

Pin Number	Description
1	RTS (output)
2	DTR (output)
3	TXD (output)
4	Ground
5	Ground
6	RXD (input)
7	DSR (input)
8	CTS (input)

Table 3-3 Device Port - Reverse Pinout Enabled (Default)

Pin Number	Description
1	CTS (input)
2	DSR (input)
3	RXD (input)
4	Ground
5	Ground
6	TXD (output)
7	DTR (output)
8	RTS (output)

To connect to a USB device port:

1. Connect the USB type A connector of a USB cable to a device port.
2. Connect the other end of the USB cable to a USB console port.

Connecting to Network Ports

The SLC network ports, 10/100/1000 Base-T Ethernet and SFP+ 1G/10G, 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. CAT5E or better cables are recommended for 1000 Base Ethernet. CAT6 or better cables are recommended for SFP+ 10G Base Ethernet.

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 Terminals

The console port is for local access to the SLC 9000 advanced console server 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 serial settings are 9600 baud, 8 bit data, No parity, 1 stop bit with no flow control.

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 DCE but is also auto-sensing. See *Appendix C: Adapters and Pinouts on page 461* for more information.

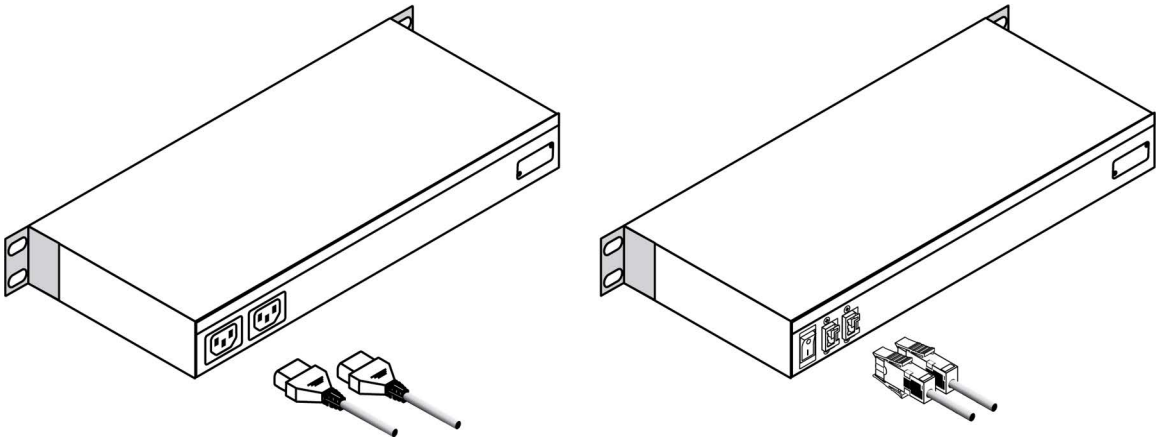
To connect a terminal:

1. Attach the Lantronix adapter to your terminal (typically a PN 200.2066A adapter - see *Figure C-1*) or your PC's serial port (use PN 200.2070A adapter - see *Figure C-4*).
2. Connect the Ethernet 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., PuTTY or TeraTerm Pro).
4. Once the SLC 9000 advanced console server is running, press **Enter** to establish connection. You should see the model name and a login prompt on your terminal.
5. On a factory default SLC you may log in using `sysadmin` as the user name and the last 8 characters of the Device ID as the password.

Power Input

Warning: ***Risk of serious electric shock! Disconnect all power cords before servicing the SLC.***

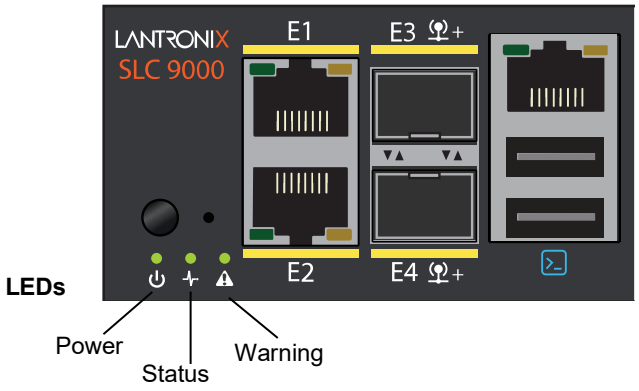
Figure 3-4 AC and DC Power Input connections



LEDs

The SLC 9000 has three LEDs on the front, to the left of the console port. These LEDs display status for the boot procedure, firmware update, and factory reset via the reset button.

Figure 3-5 SLC 9000 LEDs



Power LED: solid green when the system is powered on.

Status LED: blinks green periodically during the following events:

- Unit Boot Process - flashing (4 times per second) when the BIOS is loading, flashing (once per second) when the operating system is loaded, and finally flashing (once every two seconds) when the system is loaded and running (e.g. the unit is ready).
- Firmware Update - blinks two times per second.
- Factory Reset via Reset Button - blinks three times per second when the reset button is pressed, and continues to blink three times per second during the 30 seconds the button needs to be held to initiate a factory reset. Once a factory reset is initiated the Status LED and the Warning LED both blink 3 times per second. The reset button should be released once factory reset is initiated. After the reset is complete, the device will reboot (see Unit Boot Process above).

Warning LED: the warning LED is normally off, and only blinks green in the following events:

- Firmware Update - blinks two times per second
- Secure Boot Failure - If the Secure Boot bootloader fails for any reason (including boot component verification), this LED will blink 2 quick blinks followed by a 1 second pause. It is recommended to boot the console manager with a console connection to view errors that are output during the boot process.
- Factory Reset via Reset Button - blinks three times per second after the reset button has been pressed for 30 seconds, to indicate that the factory reset process is initiated.

4: Quick Setup

This chapter provides the steps necessary to enable Ethernet connectivity to and management of the SLC 9000. The setup procedures assume you are starting with a factory default SLC unit.

If the Percepxion cloud-based management platform is used to onboard and manage devices, Percepxion can use zero touch provisioning (ZTP) to deploy an initial (or baseline) configuration to the SLC (see *8: Percepxion on page 149*).

Recommendations

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

- Complete the quick setup (see *Figure 4-2)* 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, any connected Ethernet interface - Eth1, Eth2, Eth3, and Eth4 - 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 by running the Lantronix Provisioning Manager application.*

IP Address

Your SLC 9000 advanced console server 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 and unique to your network. If a valid gateway address has not been assigned the IP address must be on the same subnet as workstations connecting to the SLC 9000 over the network.

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

Table 4-1 Methods of Assigning an IP Address

Method	Description
DHCP	A DHCP server automatically assigns the IP address and network settings. The SLC 9000 advanced console server 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. At this point, you can use SSH to connect to the SLC console manager or use the web interface.
BOOTP	Non-dynamic predecessor to DHCP.
Serial port login to command line interface	You assign an IP address and configure the SLC unit using a terminal or a PC running a terminal emulation program to the SLC serial console port connection.

Lantronix Provisioning Manager

You may use the Lantronix Provisioning Manager (LPM) application to locate a device and view its properties and details such as its IP address. Lantronix Provisioning Manager is a free utility program provided by Lantronix that discovers, configures, upgrades, and manages Lantronix devices. It can be downloaded from the Lantornix Provisioning Manager page on the Lantronix website.

Lantronix Provisioning Manager Online Help

For detailed instructions, see the Lantronix Provisioning Manager online help.

To install Lantronix Provisioning Manager:

Download the latest version of Lantronix Provisioning Manager from https://www.lantronix.com/products/lantronix-provisioning-manager/.

In most cases, you can simply extract the application from the archive and run the executable.

To access SLC 9000 using Lantronix Provisioning Manager:

Note: *For detailed instructions, see the Lantronix Provisioning Manager online help.*

1. Launch Lantronix Provisioning Manager.
2. If this is the first time you have launched Lantronix Provisioning Manager, you may need to proceed through an initial setup.
3. Locate the SLC in the device list. The device's firmware version, serial number, IP address, and MAC address will be shown. Additional information can be obtained by clicking the three dot menu and clicking Get Device Info.
4. In order to perform operations on the SLC such as upgrading the firmware, updating the configuration, or uploading to the file system, click the checkbox next to the device, click the menu button at the top and select an operation.

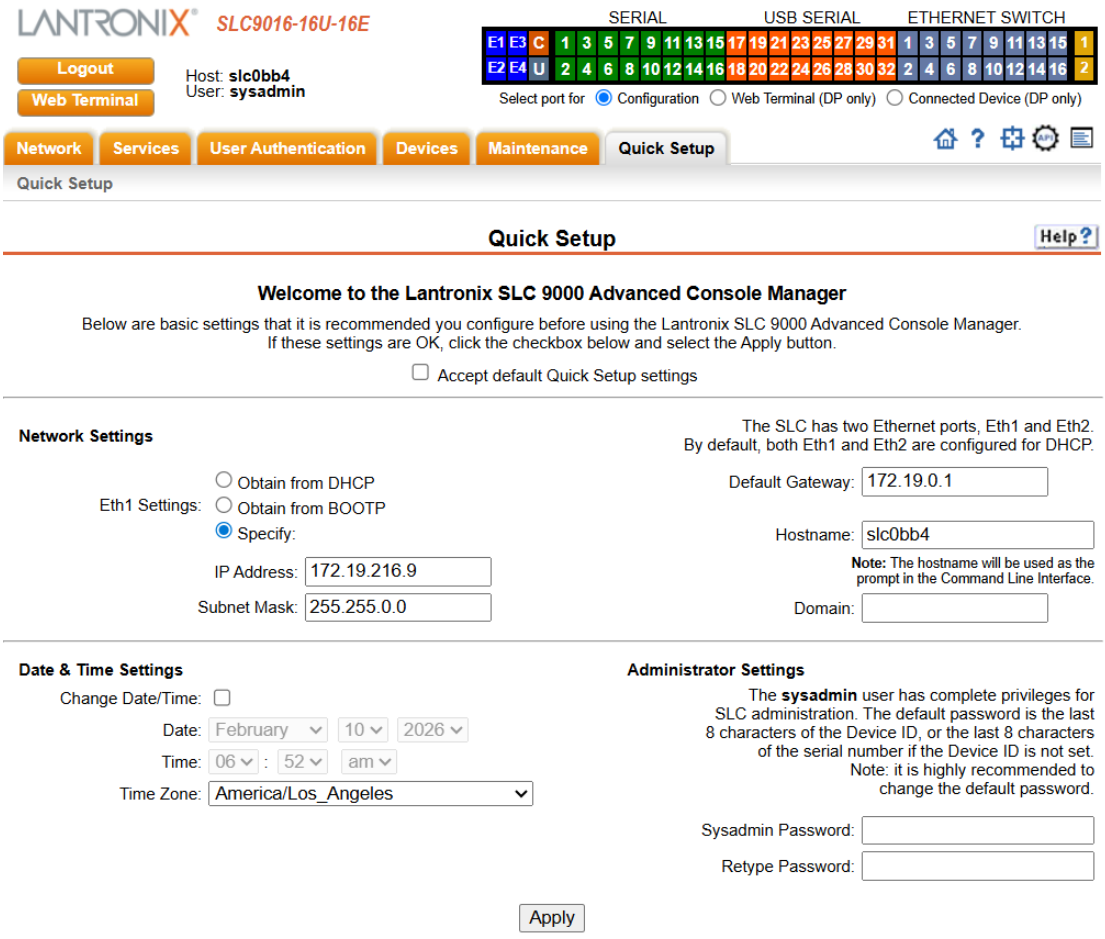
Method #1 Quick Setup on the Web Page

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 9000 advanced console server only. Otherwise, the SLC Home page displays.

To complete the Quick Setup page:

1. Open a web browser and in the URL field, type `https://` followed by the IP address of your SLC console manager.
2. Log in using `sysadmin` as the user name and the last 8 characters of the Device ID as the password. The first time you log in to the SLC unit, the *Quick Setup* page automatically displays.

Figure 4-2 Quick Setup



3. To accept the defaults, select the **Accept default Quick Setup settings** checkbox on 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 further.*

4. Enter the following settings:

Network Settings

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

Network Setting	Description
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.
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 octet. ***Note:*** *Currently, the SLC 9000 advanced console server 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 unit 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). ***Note:*** *The host name becomes the prompt in the command line interface.*
Domain	If desired, specify a domain name (for example, **support.lantronix.com**). The domain name is used for host name resolution within the SLC 9000 advanced console server. 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 unit attempts to resolve **abcd.mydomain.com** for the SMTP server.

Date & Time Settings

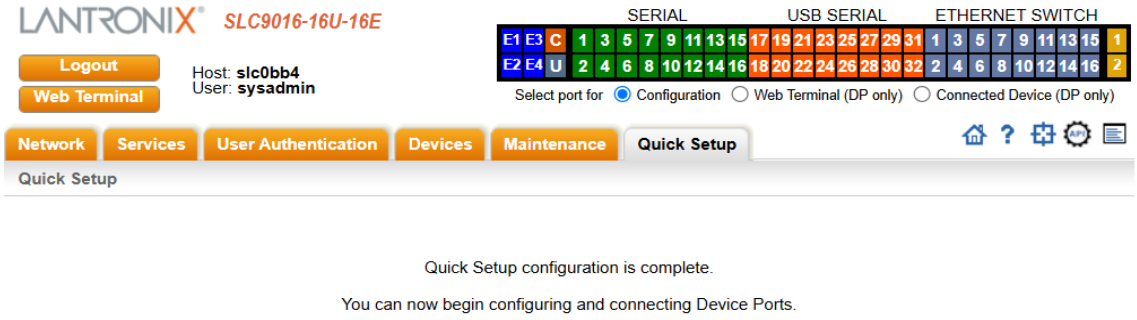
Date & Time Setting	Description
Change Date/Time	Select the checkbox to manually enter the date and time at the SLC unit's location.
Date	From the drop-down lists, select the current month, day, and year.
Time	From the drop-down lists, select the current hour and minute.
Time Zone	From the drop-down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

Administrator Settings

Administrator Setting	Description
Sysadmin Password	To change the password (e.g., from the default) enter a Sysadmin Password of up to 64 characters. Passwords must be at least eight characters long.
Retype Password	Re-enter the Sysadmin Password above in this field as a confirmation.

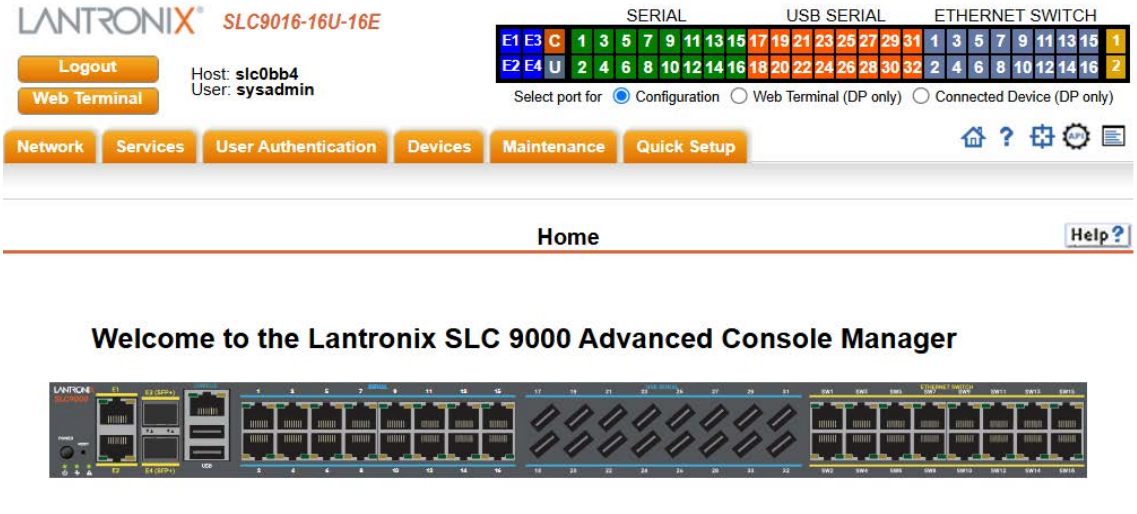
5. Click the **Apply** button to save your entries.

Figure 4-3 Quick Setup Completed in Web Manager



If Quick Setup has already been run the standard Home page will display.

Figure 4-4 Home



Method #2 Quick Setup on the Command Line Interface

If the SLC 9000 advanced console server 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 Terminals*.) If the unit has an IP address, you can use SSH or Telnet to connect to the SLC unit.

By default, Telnet is disabled and SSH is enabled. To enable Telnet, use the *Figure 7-1 Services > SSH/Telnet/Logging*.

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 client 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 the last 8 characters of the Device ID as the password and press **Enter**. The first time you log in, the Quick Setup script runs automatically. On subsequent logins, the command prompt displays.

Figure 4-5 Beginning of Quick Setup Script

```
Welcome to the Lantronix SLC9000 Advanced Console Server
Model Number: SLC9016-16U-16E
Percepxion: registered to cloud: percepxion.ai

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**.*

CLI Quick Setup Settings	Description
Config Eth1	Select one of the following: ◆ **(1) obtain IP Address from DHCP:** The unit will acquire the IP address, subnet mask, hostname, and gateway from the DHCP server. (The DHCP server may or may not provide the gateway and hostname, depending on its setup.) This is the default setting. ◆ **(2) obtain IP Address from BOOTP:** Permits a network node to request configuration information from a BOOTP "server" node. ◆ **(3) static IP Address:** Allows you to assign a static IP address manually. The IP address is generally provided by the system administrator.
IP Address (if specifying)	An IP address that is unique and valid on your network and in the same subnet as your PC. There is no default. If you selected **DHCP** or **BOOTP**, this prompt does not display. Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last octet. ***Note:*** *Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.*
Subnet Mask	The subnet mask specifies the network segment on which the SLC 9000 advanced console server resides. There is no default. If you selected DHCP or BOOTP, this prompt does not display.
Default Gateway	IP address of the router for this network. There is no default.

CLI Quick Setup Settings	Description
Hostname	The default host name is `slcXXXX`, where `XXXX` is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). ***Note:*** *The host name becomes the prompt in the command line interface.*
Domain	If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLC 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 9000 advanced console server attempts to resolve **abcd.mydomain.com** for the SMTP server.
Time Zone	If the time zone displayed is incorrect, enter the correct time zone and press **Enter**. If the entry is not a valid time zone, the system guides you through selecting a time zone. A list of valid regions and countries displays. At the prompts, enter the correct region and country.
Date/Time	If the date and time displayed are correct, type n and continue. If the date and time are incorrect, type y and enter the correct date and time in the formats shown at the prompts.
Sysadmin password	Enter a new sysadmin password.

After you complete the Quick Setup script, the changes take effect immediately.

Figure 4-6 Quick Setup Completed in CLI

```
Welcome to the Lantronix SLC9000 Advanced Console Server
Model Number: SLC9016-16U-16E
Percepxion: registered to cloud: percepxion.ai

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 SLC9016-16U-16E has four ethernet ports - Eth1, Eth2, Eth3 and Eth4.
By default, all 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: [3]

The SLC9032 can be configured to use a default gateway.
Enter gateway IP Address: [none]

____Hostname_____________________________________________________________
The current hostname is 'slc0bb4', and the current domain is
'<undefined>'.
The hostname will be shown in the CLI prompt.
Specify a hostname: [slc0bb4]
```

```
Specify a domain: [<undefined>]

____Time Zone_____________________________________________________________

The current time zone is 'GMT'.
Enter time zone: [GMT]

____Date/Time_____________________________________________________________
The current time is Fri May 22 05:01:34 2026
Change the current time? [n]

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

Quick Setup is now complete.

For a list of commands, type 'help'.
```

Next Step

After completing quick setup on the SLC 9000 advanced console server, 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: Networking*.
- To connect the SLC 9000 to Percepxion for cloud-based management, see *Chapter 8: Percepxion*.

5: Web and Command Line Interfaces

The SLC 9000 advanced console server offers a web interface (Web manager) and a command line interface (CLI) for configuring the SLC 9000 unit.

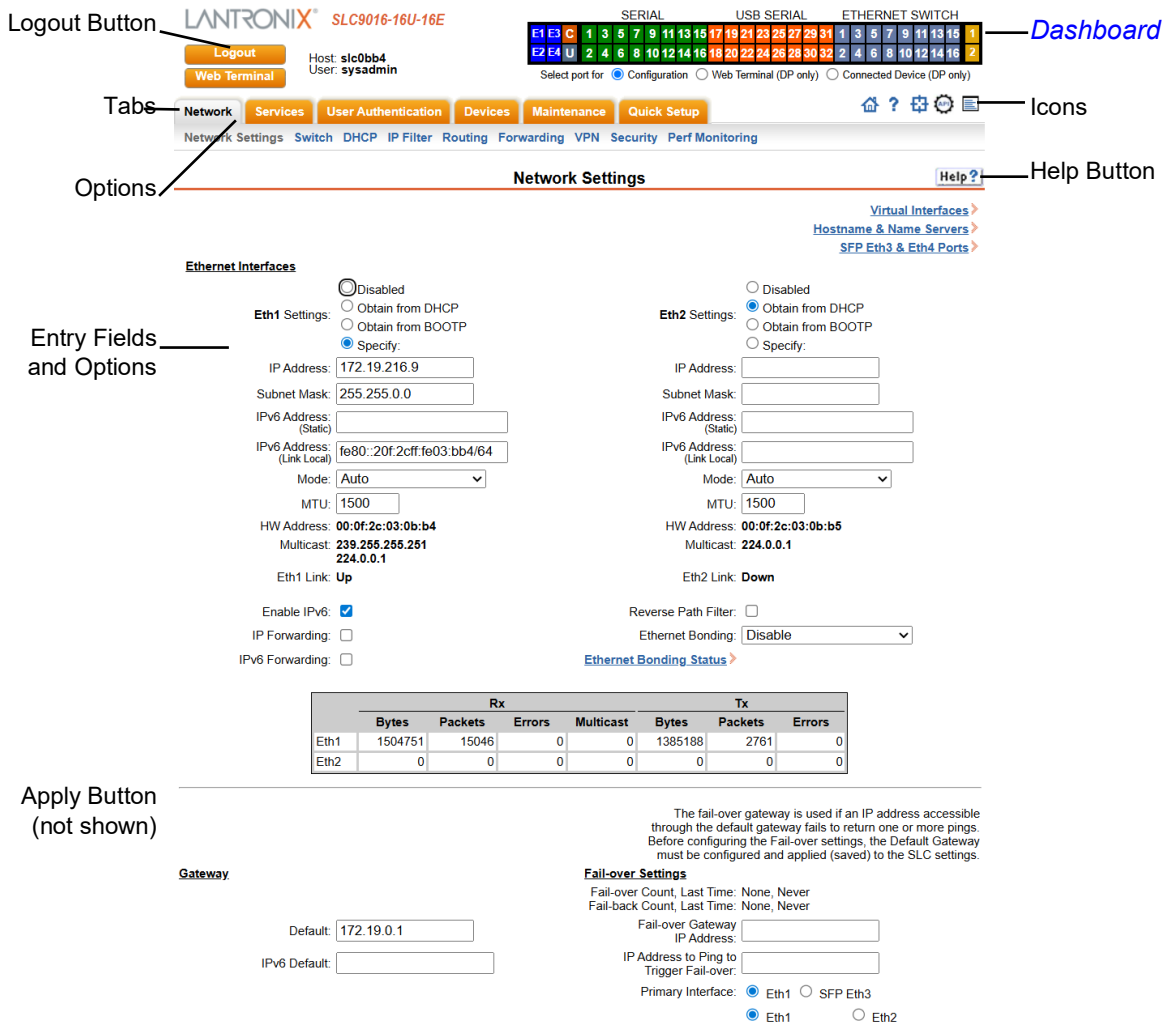
Note: *See Chapter 4: Quick Setup for instructions on configuring basic network settings using the Web manager or CLI quick setup.*

Web Manager

A Web Manager allows the system administrator and other authorized users to configure and manage the SLC 9000 advanced console server using most web browsers (Firefox, Chrome or Microsoft Edge with the latest browser updates). The SLC unit provides a secure, encrypted web interface over TLS.

The following figure shows a typical web page:

Figure 5-1 Web Page Layout



The web page has the following components:

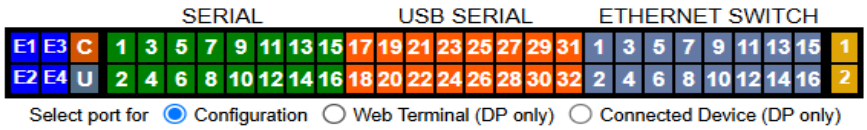
- **Tabs:** Groups of settings to configure.
- **Options:** Below each tab are options for specific types of settings.

Note: *Only those options for which the currently logged-in user has rights display.*

- **Dashboard**

The dashboard buttons allow you to view and configure SLC ports and interfaces. The appearance of the user interface dashboard will differ according to the type of installed modules in the SLC 9000 and active network interface or status.

Figure 5-2 Sample Dashboard



The dashboard buttons are defined below:

E1 E3 E2 E4	Network settings for the WAN Ethernet port (E1 and E2) or the SFP transceiver port (E3 and E4). See *Network Port Settings*.
C	Console port settings. See *Console Port*.
U1	USB device settings. See *Chapter 9: USB Port*.
1 2 3	Device port settings for RJ45 device ports (if installed). Only ports to which the currently logged in user has rights are enabled. See *Device Ports - Settings*
1 2 3	Device port settings for USB device ports (if installed). Only ports to which the currently logged in user has rights are enabled. See *Device Ports - Settings*
1 2 3	Device port settings for Ethernet switch ports ports (if installed). Only ports to which the currently logged in user has rights are enabled. See *Ethernet Switch*.
A B	Status of power supplies.

- **Dashboard Options:** Below the bar are options for use with the port buttons.
  - Select a port and the **Configuration** option takes you to the *Device Ports > Settings (1 of 2)* page.
  - Select a port and the **Web Terminal (DP only)** option displays the Web terminal window for the device port--if Web SSH is enabled, and if SSH is enabled for the device port.
  - Select a port and the **Connected Device (DP only)** button allows access to supported devices such as remote power managers (RPMs) 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 9000 advanced console server 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.

  API documentation.

  Status of the SLC 9000 advanced console server.
- **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 Manager. More than one user at a time can log in, but the same user cannot login more than once.

To log in to the SLC Web Manager:

1. Open a web browser.
2. In the URL field, type `https://` followed by the IP address of your SLC 9000 advanced console server.
3. To configure the SLC unit, log in using `sysadmin` as the user name and the last 8 characters of the Device ID as the password

   Note: *If the Device ID is not set, the default sysadmin password is the last 8 characters of the serial number.*

Note: *The system administrator may have changed the password using one of the Quick Setup methods in the previous chapter.*

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 Web Manager 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 Web Manager page. Online Help contents will appear in a new browser window.

Command Line Interface

A command line interface (CLI) is available for entering all the commands you can use with the SLC 9000 advanced console server. In this user guide, after each section of instructions for using the web interface, you will find the equivalent CLI commands. You can access the command line interface using Telnet, SSH, or a serial terminal connection.

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 9000 advanced console server 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 log in as the system administrator for setup and configuration, enter `sysadmin` as the user name and press **Enter**.
3. Enter the last 8 characters of the Device ID 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.*

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, or logout.

`<category>` is a group of related parameters whose settings you want to configure or view, such as ntp, deviceport, or network.

`<parameters>` is zero or more configurable parameters consisting of a name followed by the value to assign to the parameter.

For example, `set ldap server1 10.0.1.2` assigns the IP address 10.0.1.2 to the LDAP parameter `server1`.

With the exception of parameter values, any word may be shortened by entering only enough characters to make it unique. For exampe, the previous command can be shortened to: `se ld server1 10.0.1.2`

To view the parameters for <action> <category>, type 'help <action> <category>'.

Parameter Value Syntax:

- Values in all lowercase must be typed exactly as shown in the synopsis.
- Values which are mixed case can be set to any value that is appropriate.
- Values shown as '<aa|bb>' indicate that the parameter may be set to aa or bb.
- Values enclosed in square brackets '[]' are optional.
- Values which include spaces should be enclosed in single or double quotes.
- Values may be cleared (e.g., reset to '<none>') by entering '0.0.0.0' or
- '0:0:0:0:0:0:0:0' (for any IP address) or 'CLEAR' (for any non-IP address).

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 release notes for the current firmware release, type: `help release`
- For more information about a specific command, type help followed by the command. For example: `help set network` or `help admin firmware`

Tips

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

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

  to

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

- Use the Tab key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** either to complete the name if only one is possible, or to display the possible names if more than one is possible. Following a space after the preceding name, Tab displays all possible names.

- Should you make a mistake while typing, backspace by pressing the Backspace key and/or the Delete key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the left and right arrow keys to move within a command.
- Use the up and down arrows to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.
- To clear an IP address, type 0.0.0.0, or to clear a non-IP address value, type `CLEAR`.
- When the number of lines displayed by a command exceeds the size of the window (the default is 25), the command output is halted until 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 5-3 SCS Commands

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

To 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 9000 unit cannot detect the size of the terminal automatically.

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

To globally enable or disable the terminallines feature for all users. This command can only be run by the sysadmin user or a user who has full administrative rights.

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 15: User Authentication.*

Table 5-4 CLI Keyboard Shortcuts

Keyboard Shortcut	Description
Control + [a]	Move to the start of the line.
Control + [e]	Move to the end of the line.
Control + [b]	Move back to the start of the current word.
Control + [f]	Move forward to the end of the next word.
Control + [u]	Erase from cursor to the beginning of the line.
Control + [k]	Erase from cursor to the end of the line.

Show Commands Output Filtering

Reference: grep, with Posix Extended Regex functionality, see https://www.man7.org/linux/man-pages/man7/regex.7.html

```
show <category> <parameters> grepi|grepic|grepe|grepec <Token|RE:Regex
Token>
    grepi  - show output containing token (case sensitive)
    grepic - show output containing token (case insensitive)
    grepe  - show output not containing token (case sensitive)
    grepec - show output not containing token (case insensitive)
```

For example:

`show network all grepi Bytes` displays lines containing the string 'Bytes'

`show network all grepi RE:[0-9]` displays lines containing digits 0-9

`show network all grepi "RE:^Gateway "` displays lines starting with 'Gateway '

6: Networking

This chapter explains how to set networking settings for the SLC advanced console server using the web interface or the CLI.

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

Requirements

If you assign a different IP address from the current one, it must be within a valid range and unique to your network. If a valid gateway address has not been assigned the IP address must be on the same subnet as workstations connecting to the SLC 9000 over the network.

Network Port Settings

Network parameters determine how the SLC unit interacts with the attached network. Use this page to set the following basic configuration settings for the network ports (Ethernet and SFP+), configure advanced network settings, and configure a failover gateway and virtual interfaces.

The SLC supports the following types of network interfaces:

- RJ-45 ports, as part of the standard SLC RJ45 NIC board. In the web UI port banner bar, these are represented as E1 and E2. These ports can be configured for speeds of 10Mbit, 100 Mbit or 1000 Mbit, at full-duplex. The RJ45 Ethernet NIC LEDs display the following states:
  - **Green Light On:** indicates a link at 1000 BASE-T
  - **Green Light Off:** indicates a link at other speeds, or no link
  - **Yellow Light On:** indicates a link is established
  - **Yellow Light Blinking:** indicates link activity
- A variety of SFP modules, installed in the SLC SFP ports. In the web UI port banner bar, these are represented as **E3** and **E4**, in a variety of colors.
  - E3 Single mode 1G/10G SFP+ ports are shown in yellow.
  - E3 Multi mode 1G/10G SFP+ ports are shown in orange.
  - E3 RJ45 1G/10G SFP+ ports are shown in light blue.
  - E3 A port with no SFP module is shown in blue.
  - E3 A port with an unknown SFP module is shown in red.

  The SFP Ethernet NIC LEDs are located between the two SFP module slots; the LEDs for Ethernet 3 are on the left, and the LEDs for Ethernet 4 are on the right. They display the following states:
  - **Green Light On:** indicates a link is established
  - **Green Light Off:** indicates no link
  - **Yellow Light On:** indicates no link activity

- **Yellow Light Blinking:** indicates link activity

Lantronix supports and certifies a variety of SFP transceivers; if a SFP that has not been certified by Lantronix is used, the message Transceiver Not Recognized is displayed in the UI.

To enter settings for one or both network ports:

1. Click the **Network** tab and select the **Network Settings** option. The *Network > Network Settings (1 of 2)* and the *Network > Network Settings (2 of 2)* displays.

Figure 6-1 Network > Network Settings (1 of 2)

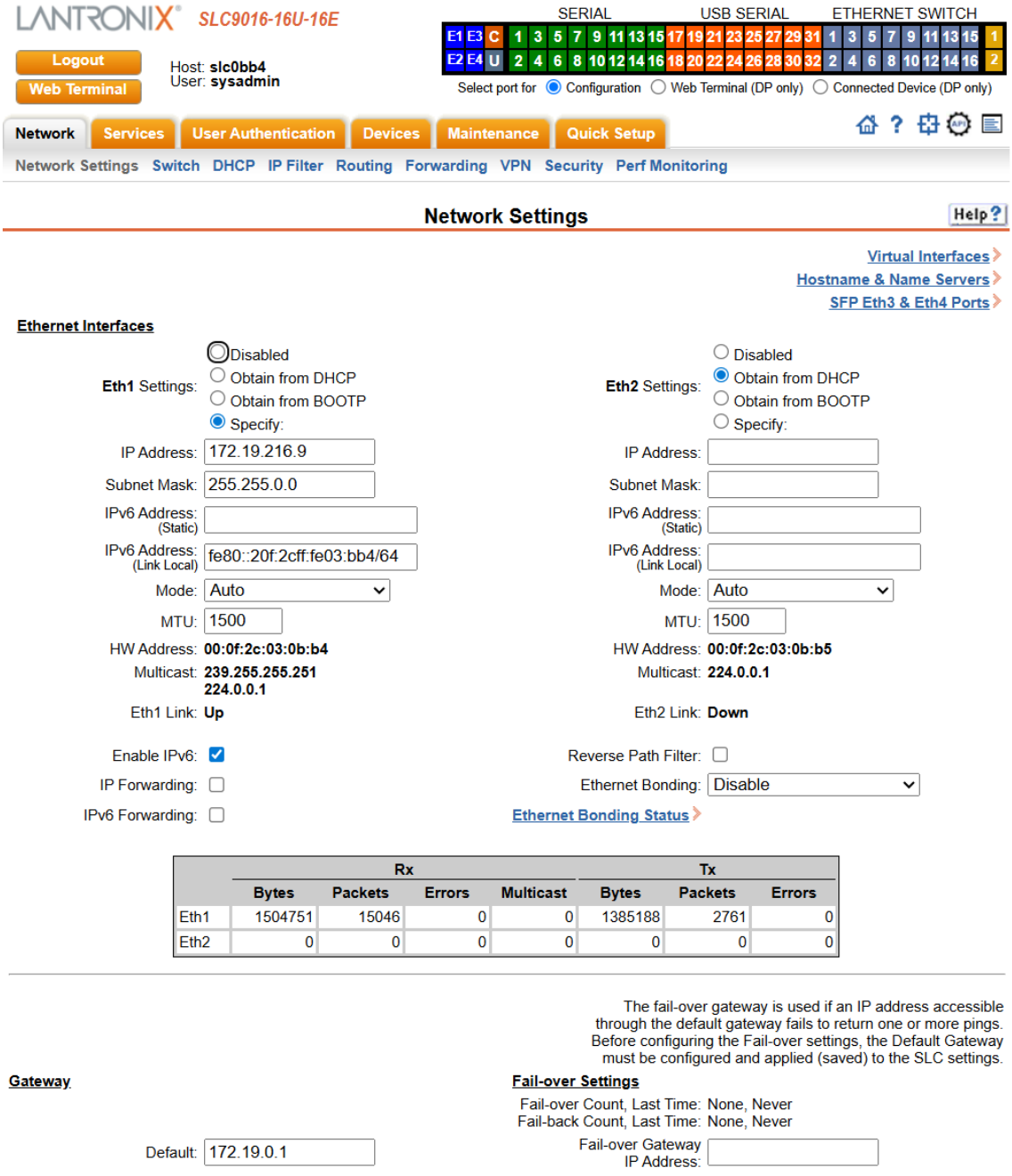
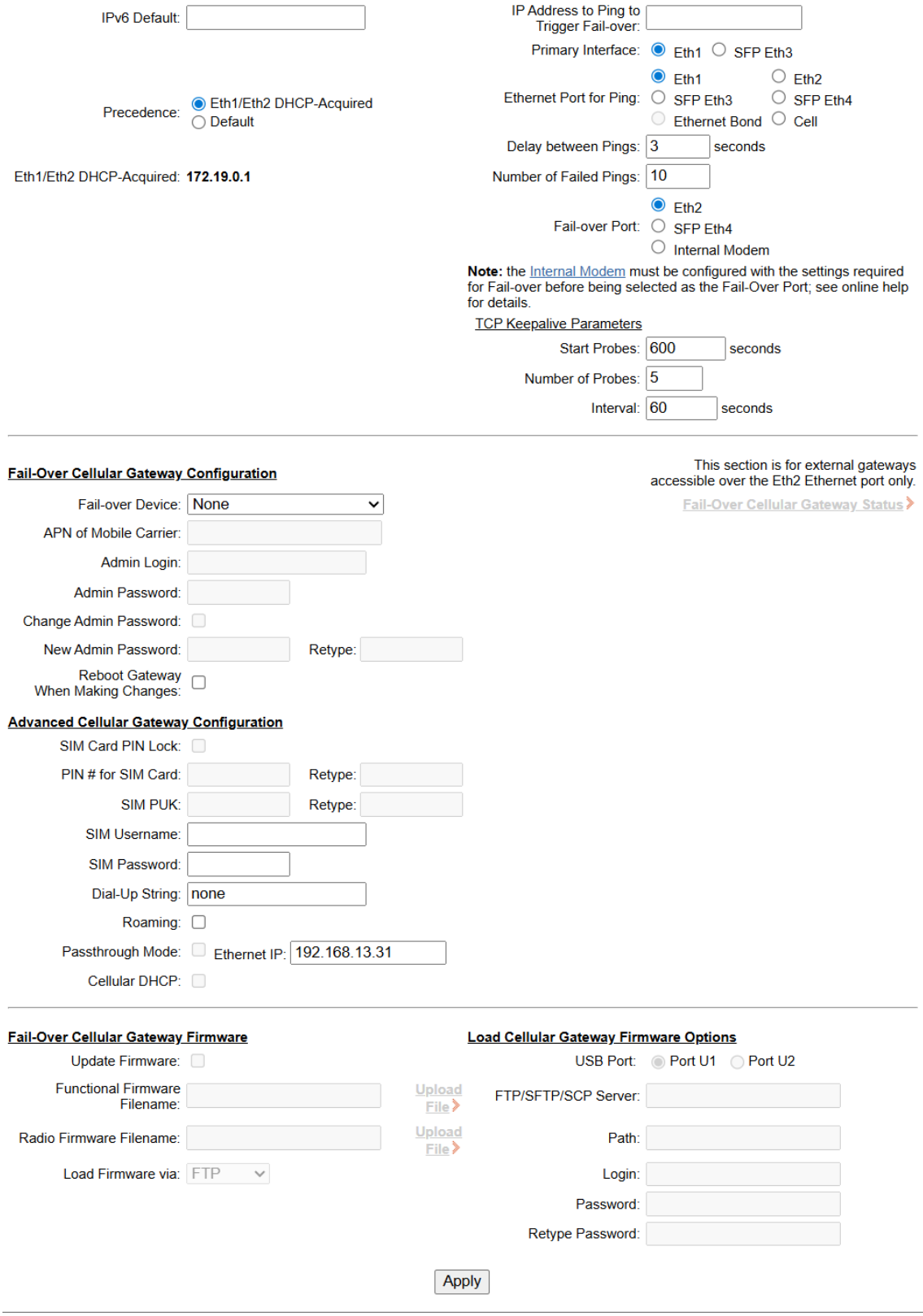


Figure 6-2 Network > Network Settings (2 of 2)



Enter the following information:

Ethernet Interfaces (Eth1 and Eth2)

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

Eth 1 Settings or **Eth 2 Settings**	◆ **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.) Acquires IP address, subnet mask, hostname, and gateway from the DHCP server. (The DHCP server may not provide the gateway and hostname, depending on its setup.) By default, both Eth3 and Eth4 are enabled, and send DHCP options requesting network configuration for option 1 (Subnet Mask), 3 (Router), 6 (Domain Name Server), 12 (Host Name), 15 (Domain Name), 28 (Broadcast Address), and (42) NTP Servers. If NTP servers are acquired, they will be used to update the time on the console manager if NTP is not enabled in the configuration (see *Date and Time* for more details). ***Note:*** *When attempting to acquire an IP address via DHCP, the console manager will send 5 DHCP discover packets with a 3 second delay between each packet. After a 10 second delay 5 more DHCP discover packets are sent; this is repeated until an IP address is acquired.* ◆ **Obtain from BOOTP:** Lets a network node request configuration information from a BOOTP "server" node. If you select this option, skip to Gateway. ◆ **Specify:** Lets you manually assign a static IP address, generally provided by the system administrator.
IP Address (if specifying)	◆ Enter an IP address that will be unique and valid on your network. There is no default. ◆ Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last segment octet. ***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 network segment on which the SLC unit resides. There is no default.
IPv6 Address (Static)	Address of the port in IPv6 format. ***Note:*** *The SLC 9000 advanced console server supports IPv6 connections for the following services: the web, SSH, Telnet, remote syslog, SNMP, NTP, LDAP, RADIUS, TACACS+, connections to device ports, and diagnostic ping.* 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`.
IPv6 Address (Global)	IPv6 address with global scope that is generated by address autoconfiguration. The address is generated from a combination of router advertisements and MAC address to create a unique IPv6 address. This field is read only. ***Note:*** *This field will not appear in the absence of an IPv6 global address.*
IPv6 Address (Link Local)	An IPv6 address that is intended only for communications within the segment of a local network. This field is read only.

Mode	Select the direction, duplex mode (full duplex or half-duplex), and speed (10, 100, or 1000 Mbit) 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.
MTU	Specifies the maximum transmission unit (**MTU**) or maximum packet size of packets at the IP layer (OSI layer 3) for the Ethernet port. When fragmenting a datagram, this is the largest number of bytes that can be used in a packet. The minimum MTU size is 108 bytes (to conform with RFC 2460) and the maximum size is 1500 bytes.
HW Address	Displays the hardware address of the Ethernet port.
Multicast	Displays the multicast address of the Ethernet port.
Enable IPv6	Select this box to enable the IPv6 protocol. If changed, the SLC unit will need to reboot. Enabled by default.
IP Forwarding	If enabled, IP forwarding enables IPv4 network traffic received on one interface (Eth1, Eth2, or an external/USB modem attached to the SLC unit 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 9000 advanced console server over a modem to access the network connected to Eth1 or Eth2.
IPv6 Forwarding	If enabled, IPv6 forwarding enables IPv6 network traffic received on one interface (Eth1, Eth2, or an external/USB modem attached to the SLC unit 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.
Ethernet Bonding	Ethernet 1 and Ethernet 2 can be bonded to support redundancy (Active Backup), aggregation (802.3ad), and load balancing. The Ethernet Bonding Status link displays detailed information about the bonding interface when bonding is enabled. Disabled by default. Note that if Ethernet Bonding is enabled, assigning individual IP Addresses to Device Ports is not supported. Note: if bonding is enabled, it is recommended that Eth1 and Eth2 be configured with the same subnet (different subnets may result in poor network performance).
Ethernet Bonding Status (Link)	Click the link to access Ethernet bonding status information. 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. Click Back to Network Settings link to return to the Network Settings page.
Reverse Path Filter	Select this option to allow the Reverse Path Filter mode, which is defined in RFC 3704. In this mode, each incoming packet is tested against the forwarding information base (FIB), and if the network interface is not the best reverse path, the packet check will fail and failed packets are discarded.

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

TCP Keepalive Parameters

Start Probes	Number of seconds the SLC unit 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 9000 advanced console server sends before closing a session. The default is 5.
Interval	The number of seconds the SLC unit waits between probes. The default is 60 seconds.

Gateway

Default	IP address of the IPv4 router for this network. If this has not been set manually, any gateway acquired by DHCP for Eth1 or Eth2 displays. All network traffic that matches the Eth1 IP address and subnet mask is sent out Eth1. All network traffic that matches the Eth2 IP address and subnet mask is sent out Eth 2. If you set a default gateway, any network traffic that does not match Eth1 or Eth2 is sent to the default gateway for routing. *If a fail-over gateway is configured, the default gateway must be configured for fail-over and fail-back (gateways acquired through DHCP can be changed or removed). Only Eth1 is supported as the primary interface in a Fail-over configuration.*
Eth1/Eth2 DHCP-Acquired (display only)	Gateway acquired by DHCP for Eth1 or Eth2. View only.
Precedence	Indicates which of the gateways take precedence (used as the default route). Available options are **Eth1/Eth2 DHCP-Acquired** and **Default**. The default is **Eth1/Eth2 DHCP-Acquired** gateway. If the Eth1/Eth2 DHCP Gateway is selected and both Eth1 and Eth2 are configured for DHCP, the SLC unit gives precedence to the gateway acquired via Eth1. If the Precedence gateway becomes unreachable, the console manager will not install one of the other gateways as the default gateway; this must be manually configured by the user.
IPv6 Default	Indicates the IP address of the IPv6 router for this network.

Fail-Over Settings

Fail-over Gateway IP Address	An alternate IP address of the router for your current network. **Fail-over Gateway IP Address** is used if an IP address usually accessible through the default gateway fails to return one or more pings. Fail-back occurs when the Ping device becomes reachable again, causing the primary default route to be restored. ***Note:*** *The fail-over gateway is not supported when DHCP is used on the primary interface because as a fail-back it needs a consistent IP address to update the routing table.* If a fail-over gateway is configured, the **Default Gateway** must be configured for fail-over and fail-back to work properly (gateways acquired via DHCP can change or be removed). Only Eth1 is supported as the primary interface in a Fail-over configuration. Fail-over statistics (count of fail-over and fail-back events, last time of fail-over, last time of fail-back) are displayed if a Fail-over Gateway is configured; the statistics are reset each time the fail-over settings are configured. ◆ When Eth2 is used as the **Fail-over Port** the **Fail-over Gateway IP Address** must be in the same subnet as the Eth2 network. This restriction is ignored if the failover device is Sierra ES450 and IP Passthrough Mode is enabled. ◆ When Internal modem is used as the **Fail-over Port**, the **Fail-over Gateway IP Address** should be set to the Remote IP address for the PPP connection. ◆ When cellular modem or WLAN is used as the Fail-over Port (EMG and SLC 9000 models only), the Fail-over Gateway IP Address should be set to the IP address of the cellular or WLAN interface. For information about specific requirements for configuring each type of port/ interface, see **Fail-over Port**. When a cellular modem is used as the **Fail-over Port** and it is configured for DHCP, whenever the IP address of the cellular modem changes, the IP address of the Fail-over Gateway will be automatically updated to be the same as the new cellular modem IP address.
IP Address to Ping to Trigger Fail-over	IP address to ping to determine whether to use the fail-over gateway.
Primary Interface	The SLC 9000 has both standard RJ45 Ethernet ports (Eth1 and Eth2) as well as SFP Ethernet ports (Eth3 and Eth4). For deployments that only use SFP ports, SFP Eth3 can be designated as the primary interface in a fail-over/fail-back configuration, with SFP Eth3 or SFP Eth4 selectable as the **Ethernet Port for Ping** and SFP Eth4 selectable as the **Fail-over Port**. If SFP Eth3 is selected as the Primary Interface, SFP Eth3 will be automatically selected as the **Ethernet Port for Ping** and SFP Eth4 will be automatically selected as the **Fail-over Port**.
Ethernet Port for Ping	Ethernet port to use for the ping. Ethernet Bond interface can be selected only when the Ethernet Bonding in in active-backup mode. SFP Eth3 and SFP Eth4 are only available on SLC 9000 models.
Delay between Pings	Number of seconds between pings
Number of Failed Pings	Number of pings that fail before the SLC 9000 advanced console server uses the fail-over gateway.

Fail-over Port	The network interface to use for fail-over. The Fail-over Gateway IP Address should either be accessible via this interface or assigned directly to this interface. Select **Eth2** (the default), **Cellular** if a Cellular modem module is installed, or **Internal Modem** if a Internal modem is installed. SFP Eth4 is only available on SLC 9000 models. When internal modem is selected, the internal modem should be configured as follows: ◆ State: Dial-on-Demand ◆ Mode: PPP ◆ PPP Mode: Local and Remote IPs ◆ Dial-out Number set to the appropriate analog phone number ◆ Remote/Dial-out Login and Password set to the appropriate authentication tokens. ◆ The Modem Timeout can be either disabled or enabled. When a fail-over happens, the console manager will automatically dial-out and establish a PPP connection over the phone line, and configure the default gateway so that traffic will be routed over the PPP connection. If the Modem Timeout is disabled, the PPP connection will remain up the entire time the network is in fail-over mode; at fail-back the PPP connection will be torn down and the dial-out will be terminated. If the Modem Timeout is enabled, the PPP connection remain up until no network traffic is received for the timeout specified; then the PPP connection will be torn down and the dial-out will be terminated (the PPP connection will automatically re-establish as needed during fail-back). ◆ When viewing fail-over status in the UIs, while the dial-out and PPP connection are being established, the UI will display fail-over in progress; once the PPP connection is established, the remote IP address of the connection will be displayed.

Fail-Over Cellular Gateway Configuration

Fail-over Device	***Note:*** *This section is for external gateways accessible over the Eth2 Ethernet port. For internal cellular modems, see Cellular Modem.* Select an integrated device to be used as the fail-over gateway. Currently the Lantronix PremierWave XC **HSPA**+ Cellular Gateway, Lantronix **G520** Series (G52x) Cellular Gateway, and the **Sierra** Wireless AirLink ES450 are supported. The HSPA+ gateway must be configured in gateway mode before it can be used as the fail-over gateway. It is recommended that the HSPA+ Cellular Connection Mode be set to **On Demand**, which will leave the link quiescent until an application attempts to make use of the cellular network connection. It is also recommended that the SNTP protocol be disabled, as On Demand mode uses the egress traffic as a trigger. The Lantronix G520 Series (G52x) gateway must be configured before it can be used as the fail-over gateway. The default **admin** user password must be changed to a new password, and the DHCP server must be disabled. For factory reset device, you need to first login as **root** and default password as **L@ntr0n1x**. Please note after factory reset, the G52x WebUI will show the default user as **admin**; you need to delete it and enter the username as **root**. Once you login as **root** with default password as **L@ntr0n1x**, you can change the password for **root** user and set a password for **admin** user. After you save and apply, the G52x WebUI will re-direct to login page where you can login as **admin** or **root**. The Sierra gateway must be properly provisioned before first use by initializing the APN of the installed SIM card. This is done by connecting the Sierra gateway to the second ethernet port of the SLC, and assigning a static IP address to the SLC port so that it is in the same subnet as the IP address of the Sierra gateway. Use the console CLI or web GUI to set the APN of the SIM card. After setting the APN, power cycle the Sierra gateway and allow it to reboot completely. The default IP Addresses are: ◆ Lantronix PW XC HSPA+: 192.168.0.1 ◆ Lantronix G52x Series: 192.168.1.1 ◆ Sierra Wireless ES450: 192.168.13.31 The failover feature requires that both Ethernet ports be configured with a static IP address. Using DHCP on one of the Ethernet ports may overwrite the default route, interfering with fail-over and fail-back. If the IP Passthrough Mode is enabled on the Sierra ES450 then the second ethernet port of the console server should be configured for DHCP and the Sierra ES450's DHCP server should be in "Auto" mode with starting and ending IP address of the IP pool set to "0.0.0.0". ***Note:*** *The commands sent to the fail-over device to retrieve status and update the configuration are shown in the syslog (messages may be displayed under Network syslog; at the Debug level). If there are errors retrieving status or updating the configuration, check messages in the Network syslog, the device administrator login/password, connectivity to the device and the firmware version of the fail-over device (the minimum required firmware version for HSPA+ is 8.1.0.0, Sierra Wireless ES450 is 4.9.2, and for Lantronix G52x Series (G52x) gateway is 2.1.0.0). For the HSPA+ gateway, if the firmware is updated and new items are added to the status output by the gateway, the new items will automatically be displayed on the SLC.*

Fail-over Device (continued)	When the SLC sends an updated configuration to the fail-over device, it is recommended to check the SLC syslog, even if the SLC indicates that the update was successful. Responses from the fail-over device indicating that the device needs to be rebooted for configuration changes to take affect may also be in the syslog. The configuration will be re-sent to the device if any of the fail-over device settings are changed, or the selected fail-over device is changed from None to one of the supported fail-over device types. When a fail-over or fail-back occurs, running applications such as VPN tunnel and Percepxion will be restarted.
APN of Mobile Carrier	For the HSPA+ Sierra and Lantronix G520 Series (G52x) gateways, configure the Access Point Name for the mobile carrier. May have up to 256 characters.
Admin Login and Password/Retype	For the selected **Fail-over Device**, the administrator login and password used to retrieve status from the device and send configuration updates to the device. The login may have up to 32 characters, and the password may have up to 64 characters. The **Admin Password** displays the current password masked. Default login credentials of the Lantronix PW HSPA+: Admin login name: admin Admin password: PASS Default login credentials of the Sierra Wireless ES450: Admin login name: user Admin password: 12345 Default login credentials of the Lantronix G520 Series (G52x): Admin login name: admin Admin password: No default password, use current G52x working password
Change Admin Password (check box)	Select this check box if you wish to update the admin password for the selected gateway **Fail-over Device**.
New Admin Password/Retype	For the selected **Fail-over Device**, the administrator password can be changed on the gateway. The password may have up to 64 characters. To change the Admin Password, click the Change Admin Password checkbox and enter the new password in the New Admin Password and Retype fields. Changing the HSPA+ Admin password will save the password on the SLC for status and configuration queries to the HSPA+ gateway. The password must match what is stored on the HSPA+ gateway. Changing the Sierra Admin password will save the password on the SLC for status and configuration queries to the Sierra gateway. The new password will also be configured on the Sierra gateway. The Sierra gateway login must be set as ‘user’. Changing the Lantronix G520 Series (G52x) Password will save the password on the console manager for status and configuration queries to the Lantronix G520 Series (G52x) gateway; the new password will also be configured on the Lantronix G520 Series (G52x) gateway. The Lantronix G520 Series (G52x) gateway login must be set as 'admin'.
Reboot Gateway When Making Changes	For the selected **Fail-over Device**, the administrator can reboot the gateway.
Fail-Over Cellular Gateway Status (link)	Clicking the link opens the Fail-Over Cellular Gateway status window, showing status and statistics about the fail-over gateway. Click Back to Network Settings to return to the Network Settings page.

Advanced Cellular Gateway Configuration

SIM Card PIN Lock (check box)	For the HSPA+, Sierra and Lantronix G520 Series (G52x) gateways, enable a lock so that the SIM card used by the gateway cannot be used by anyone who does not have the PIN.
Pin # for SIM Card/ Retype	For the HSPA+, Sierra and Lantronix G520 Series (G52x) gateways, the PIN number for the SIM card used by the gateway. May have up to 8 characters.
SIM PUK/Retype	For the HSPA+ and Lantronix G520 Series (G52x) gateways, the SIM Personal Unblocking Key. May have up to 16 characters. The Sierra gateway does not have this feature. HSPA+ does not store PUK in its configuration. It is required when incorrect PIN is entered for 3 times, otherwise HSPA+ will ignore PUK. SIM status in case of Lantronix G520 Series (G52x) gateway is not verified in SLC, SLC directly forwards the request to Lantronix G520 Series (G52x) gateway.
SIM Username	For the HSPA+ and Lantronix G520 Series (G52x) gateways, enter the username for dial up to the cellular carrier, if required. May have up to 64 characters. The Sierra gateway does not have this feature.
SIM Password	For the HSPA+ and Lantronix G520 Series (G52x) gateways, enter the password for dial up to the cellular carrier, if required. May have up to 64 characters. The Sierra gateway does not have this feature.
Dial-up String	For the HSPA+ and Lantronix G520 Series (G52x) gateways, enter the modem string used for making a connection to the carrier. May have up to 64 characters. The Sierra gateway does not have this feature.
Roaming	For the HSPA+ and Lantronix G520 Series (G52x) gateways, enable or disable network roaming. The Sierra gateway does not have this feature.
Passthrough Mode	For the Sierra ES450 gateway, select the IP **Passthrough Mode** check box to allow the Sierra ES450 gateway to pass its WAN IP address to the selected Ethernet interface of SLC. The Sierra ES450 gateway will get rebooted on enabling or disabling this option. The IP Passthrough Mode is also supported in Failover/Failback scenario for a consistent IP and Gateway (requires static IP from the network provider). The Fail-over feature does not handle changes in the Fail-over Gateway IP address for IP Passthrough configurations. If there is a communication failure with the Sierra ES450 on setting or unsetting Passthrough related parameters (such as Passthrough Mode, Cellular DHCP or Ethernet IP) with Eth2 set to DHCP, to workaround this issue: first retry the configuration with a static IP setting for Eth2 and then subsequently change the Eth2 mode to DHCP. The Lantronix G520 Series (G52x) gateway does not support this feature.
Ethernet IP	Ethernet IP address of the Sierra ES450 gateway. This is used in conjunction with **Passthrough Mode** to remotely configure the Sierra ES450 options. If IP passthrough mode is disabled then this IP address will be ignored and IP address of the alternate gateway field will be used to configure Sierra ES450. ***Note:*** *We recommend you wait till Sierra ES450 completes the rebooting process before you configure any other network parameter, or else, an error appears indicating that Sierra ES450 could not respond to the request.* The Lantronix G520 Series (G52x) gateway does not support this feature.

Cellular DHCP	For the Sierra ES450 gateway, use this option in conjunction with Passthrough Mode to enable or disable the DHCP server. The Sierra ES450 gateway will get rebooted whenever you enable or disable this option. ***Note:*** *We recommend you wait till Sierra ES450 completes the rebooting process before you configure any other network parameter, or else, an error appears indicating that Sierra ES450 could not respond to the request.* The Lantronix G520 Series (G52x) gateway does not support this feature.

Fail-Over Cellular Gateway Firmware

Note: *The HSPA+ or **Sierra** fail-over device must be selected in order for you to be able to update the firmware.*

Update Firmware (check box)	Select this option to update firmware on the HSPA+ gateway, Sierra gateway or on Lantronix G520 Series (G52x) gateway. The **Functional Firmware file** and the **Radio Firmware file** (required for the Sierra gateway only) will be transferred to the SLC using the method selected by the **Load Firmware via** option. Once the file(s) have been transferred to the SLC, the SLC will initiate the firmware update on the gateway. The Lantronix G520 Series (G52x) gateway firmware upgrade may take 3 to 6 minutes.
Functional Firmware Filename	Enter the name of the firmware filename exactly as it is represented.
Radio Firmware Filename	Enter the name of the radio firmware filename exactly as it is represented.
Load Firmware via	Select the method to load the firmware from the options in the drop-down menu. Options are: FTP, TFTP, SCP, USB, and HTTPS. FTP is the default. ◆ If you select HTTPS, the Upload File link becomes active. Select the link to open a popup window that allows you to browse to a firmware update file to upload. ◆ If you select NFS, the mount directory must be specified. ***Note:*** *Connections available depend on the model of the SLC unit.*

Load Cellular Gateway Firmware Options

USB Port	Select the USB port. The firmware files must be stored in the top level directory of the USB flash drive.
FTP/SFTP/SCP Server	Enter the IP address or host name of the server used for obtaining the firmware files. May have up to 64 alphanumeric characters; may include hyphens and underscore characters.
Path	Enter the path on the server for obtaining firmware update files.
Login	Enter the user login for the FTP/SFTP/SCP server to verify access. May be blank.
Password/ Retype Password	Enter the FTP/SFTP/SCP user password. Retype the password in the **Retype Password** field.

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

Ethernet Counters

The *Network > Network Settings (2 of 2)* page displays statistics for each of the SLC 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

Go to *Network Commands* to view CLI commands which correspond to the web page entries described above.

SFP Port Settings

This page describes configuring SFP+ ports on the SLC 9000.

The SLC 9000 supports a variety of SFP+ modules in the Eth3 port or the Eth4 port. In the web UI port banner bar, these are represented as **E3** and **E4**, in a variety of colors.

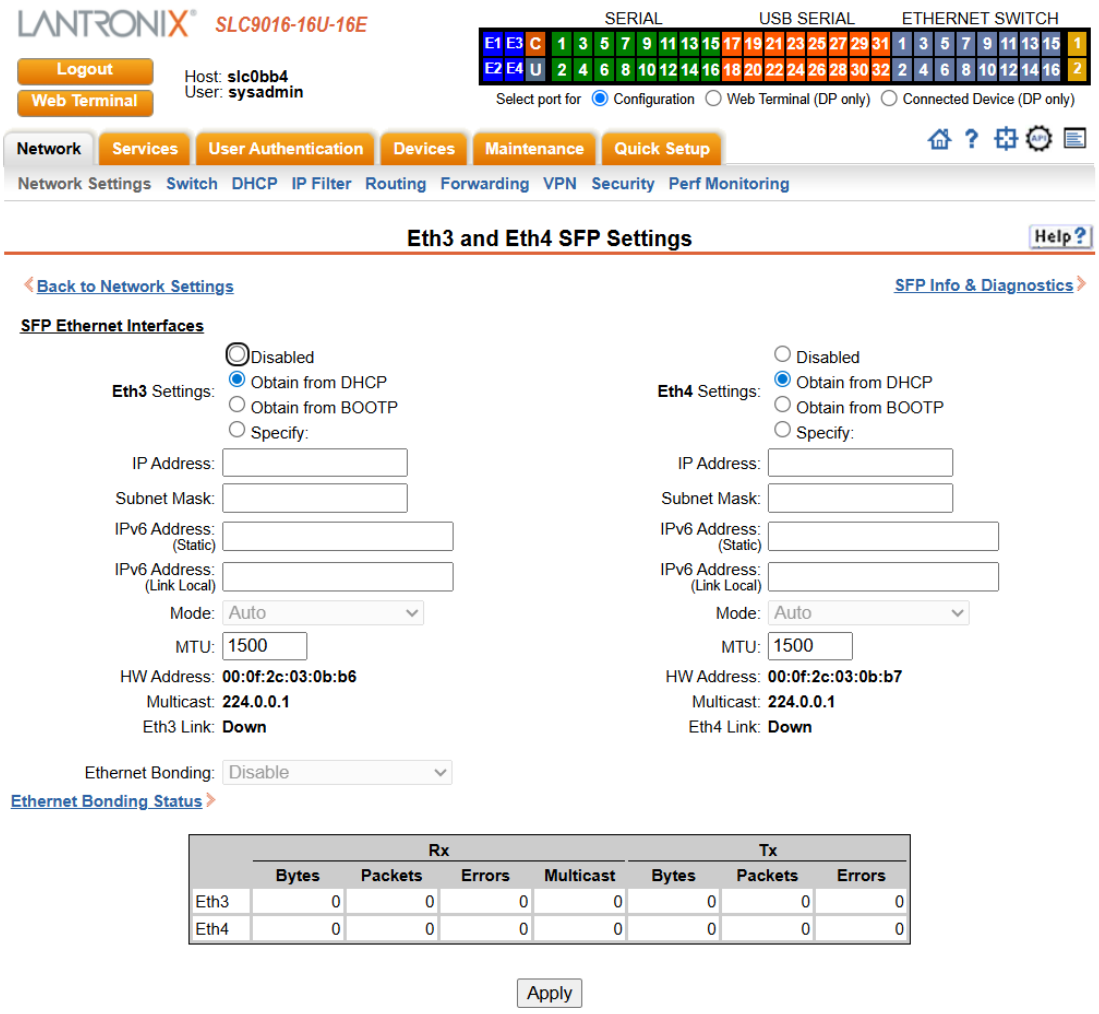
- E3 Single mode 1G/10G SFP+ ports are shown in yellow.
- E3 Multi mode 1G/10G SFP+ ports are shown in orange.
- E3 RJ45 1G/10G SFP+ ports are shown in light blue.
- E3 A port with no SFP module is shown in blue.
- E3 A port with an unknown SFP module is shown in red.

The SFP Ethernet NIC LEDs are located between the two SFP module slots; the LEDs for Ethernet 3 are on the left, and the LEDs for Ethernet 4 are on the right. They display the following states:

- **Green Light On:** indicates a link is established
- **Green Light Off:** indicates no link
- **Yellow Light On:** indicates no link activity
- **Yellow Light Blinking:** indicates link activity

To complete the Eth3 and Eth4 SFP Settings page:

1. On the **Network Settings** page, click the **SFP Eth3 & Eth4 Ports** link. The following page appears:



2. Enter the following information for one or both network ports in the following sections:

Ethernet Interfaces

SFP Ethernet Settings	**Disabled**: If selected, disables the network port. Defaults are Eth3 and Eth4 enabled. **Obtain from DHCP**: Acquires IP address, subnet mask, hostname, and gateway from the DHCP server. (The DHCP server may not provide the gateway and hostname, depending on its setup.) By default, both Eth3 and Eth4 are enabled, and send DHCP options requesting network configuration for option 1 (Subnet Mask), 3 (Router), 6 (Domain Name Server), 12 (Host Name), 15 (Domain Name), 28 (Broadcast Address), and (42) NTP Servers. If NTP servers are acquired, they will be used to update the time on the console manager if NTP is not enabled in the configuration (see *Date and Time* for more details). ***Note:*** *When attempting to acquire an IP address via DHCP, the console manager will send 5 DHCP discover packets with a 3 second delay between each packet. After a 10 second delay 5 more DHCP discover packets are sent; this is repeated until an IP address is acquired.* **Obtain from BOOTP**: Lets a network node request configuration information from a BOOTP "server" node. **Specify**: Lets you manually assign a static IP address, generally provided by the system administrator.
IP Address (if specifying)	An IP address that will be unique and valid on your network. There is no default. ***Note:*** *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.*
Subnet Mask	The network segment on which the console manager resides. There is no default.
IPv6 Address	Address of the Ethernet port in IPv6 format. ***Note:*** *The console manager supports IPv6 connections for a limited set of services: the web, ssh, and Telnet.* IPv6 addresses are written as 8 sets of 4-digit hexadecimal numbers separated by colons. There are several rules for modifying the address. For example, 1234:0BCD:1D67:0000:0000:8375:BADD:0057 may be shortened to 1234:BCD:1D67::8375:BADD:57.
IPv6 Address (Link Local)	The IPv6 address that is intended only for communications within the segment of a local network.
Mode	For SFP modules, the mode cannot be changed and is fixed at Auto.
MTU	Specifies the Maximum Transmission Unit (or Maximum Packet Size) of packets at the IP layer (OSI layer 3) for the Ethernet port. When fragmenting a datagram, this is the largest number of bytes that can be used in a packet. The minimum MTU size is 108 bytes (to conform with RFC 2460) and the maximum size is 1500 bytes. When Bonding is enabled, the bonding interface will use the MTU configured for Ethernet 1.
HW Address	Displays the hardware address of the Ethernet port.
Multicast	Displays the multicast address of the Ethernet port.
Eth1/Eth2 Link	Displays the Ethernet interface link status.

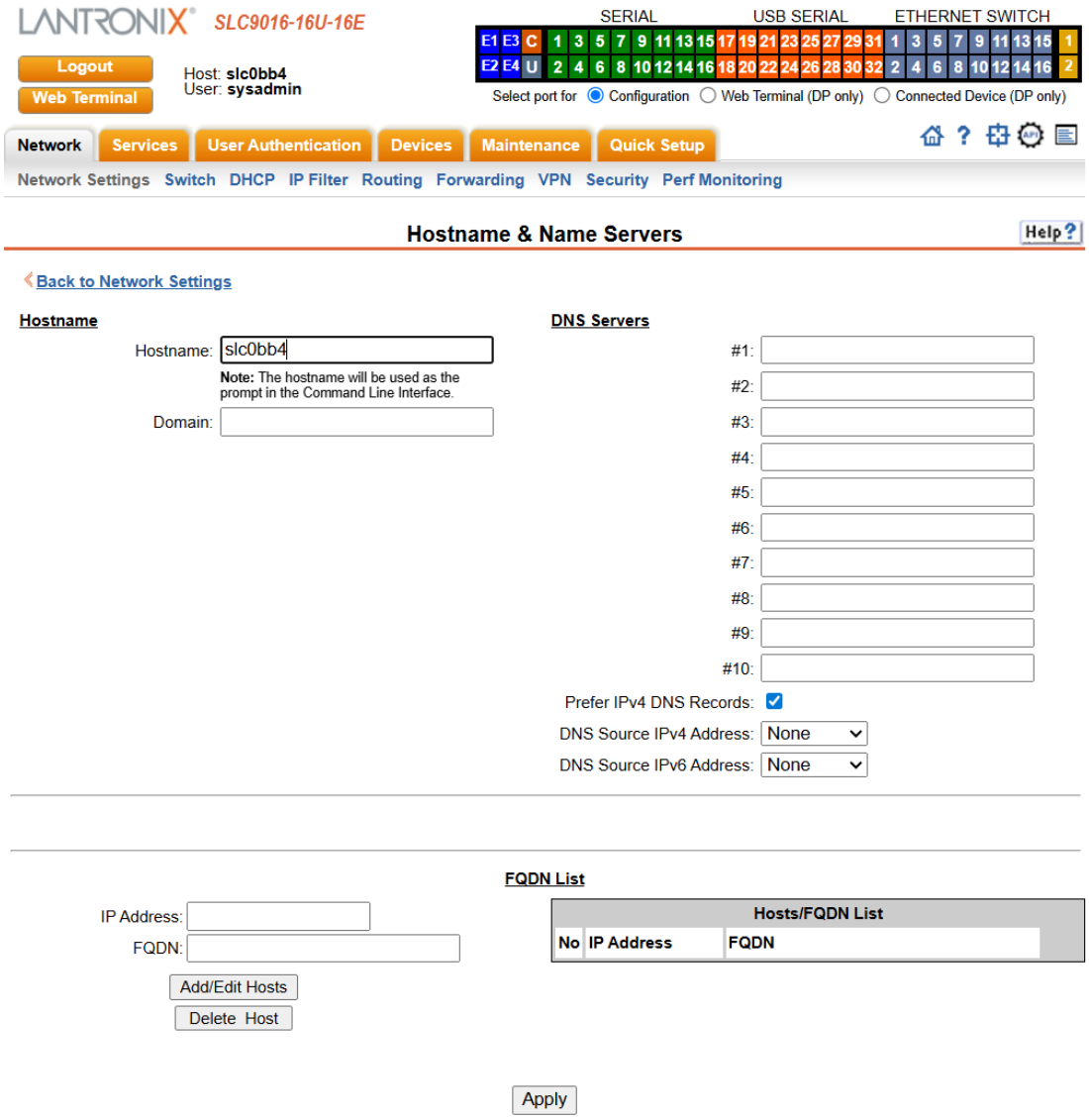
Ethernet Bonding	Ethernet 3 and Ethernet 4 can be bonded to support redundancy (Active Backup), aggregation (802.3ad), and load balancing. The Ethernet Bonding Status link displays detailed information about the bonding interface when bonding is enabled. Disabled by default. Note that if Ethernet Bonding is enabled, assigning individual IP Addresses to Device Ports is not supported. Note: if bonding is enabled, it is recommended that Eth3 and Eth4 be configured with the same subnet (different subnets may result in poor network performance). ***Note:*** *Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.*

To save your entries, click the **Apply** button. Apply makes changes effective immediately.

Hostname and Name Servers

To configure the hostname and name servers:

1. On the **Network Settings** page, click the **Hostname & Name Servers** link. The following page appears:



2. Enter the following information:

Hostname & Name Servers

Hostname	The default host name is `slcXXXX`, where `XXXX` is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). The host name becomes the prompt in the command line interface.
Domain	If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the SLC 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 9000 advanced console server attempts to resolve **abcd.mydomain.com** for the SMTP server.

DNS Servers #1 - #10	Configure up to three name servers with an IPv4 or IPv6 address. #1 is required if you choose to configure DNS (Domain Name Server) servers. The SLC will attempt to contact each DNS server in the order that they are given. If a DNS server cannot be reached, the next DNS server will be tried. If a DNS server is reachable, but does not resolve a hostname, no other attempts will be made to resolve the hostname using the remaining DNS servers. The first three DNS servers acquired via DHCP through Eth1 and/or Eth2 display automatically.
DHCP-Acquired DNS Servers (view only)	Displays the IP address of DNS servers acquired via DHCP over Eth1, Eth2, VPN
Prefer IPv4 DNS Records	If enabled, IPv4 DNS records will be preferred when DNS hostname lookups are performed. Otherwise IPv6 records will be preferred (when IPv6 is enabled). Enabled by default.
DNS Source IPv4 Address	The DNS Source IPv4 Address can be used to configure which interface (and source IPv4 address) is used for sending DNS packets. By default, the source address for sending DNS traffic is not specified, and the source address of a DNS packet is selected according to the routing table. **DNS Source IPv4 Address** can be used to select the IPv4 address of Eth1, Eth2, VEth1 or VEth2 as the source IPv4 address for packets sent to all DNS servers defined with an IPv4 address. Before selecting an interface, make sure the interface is enabled and has a valid IPv4 address.
DNS Source IPv6 Address	The DNS Source IPv6 Address can be used to configure which interface (and source IPv6 address) is used for sending DNS packets. By default, the source address for sending DNS traffic is not specified, and the source address of a DNS packet is selected according to the routing table. **DNS Source IPv6 Address** can be used to select the IPv6 address of Eth1, Eth2, VEth1 or VEth2 as the source IPv6 address for packets sent to all DNS servers defined with an IPv6 address. Before selecting an interface, make sure the interface is enabled and has a valid IPv6 address.
DNS Query	

3. Click **Apply**.

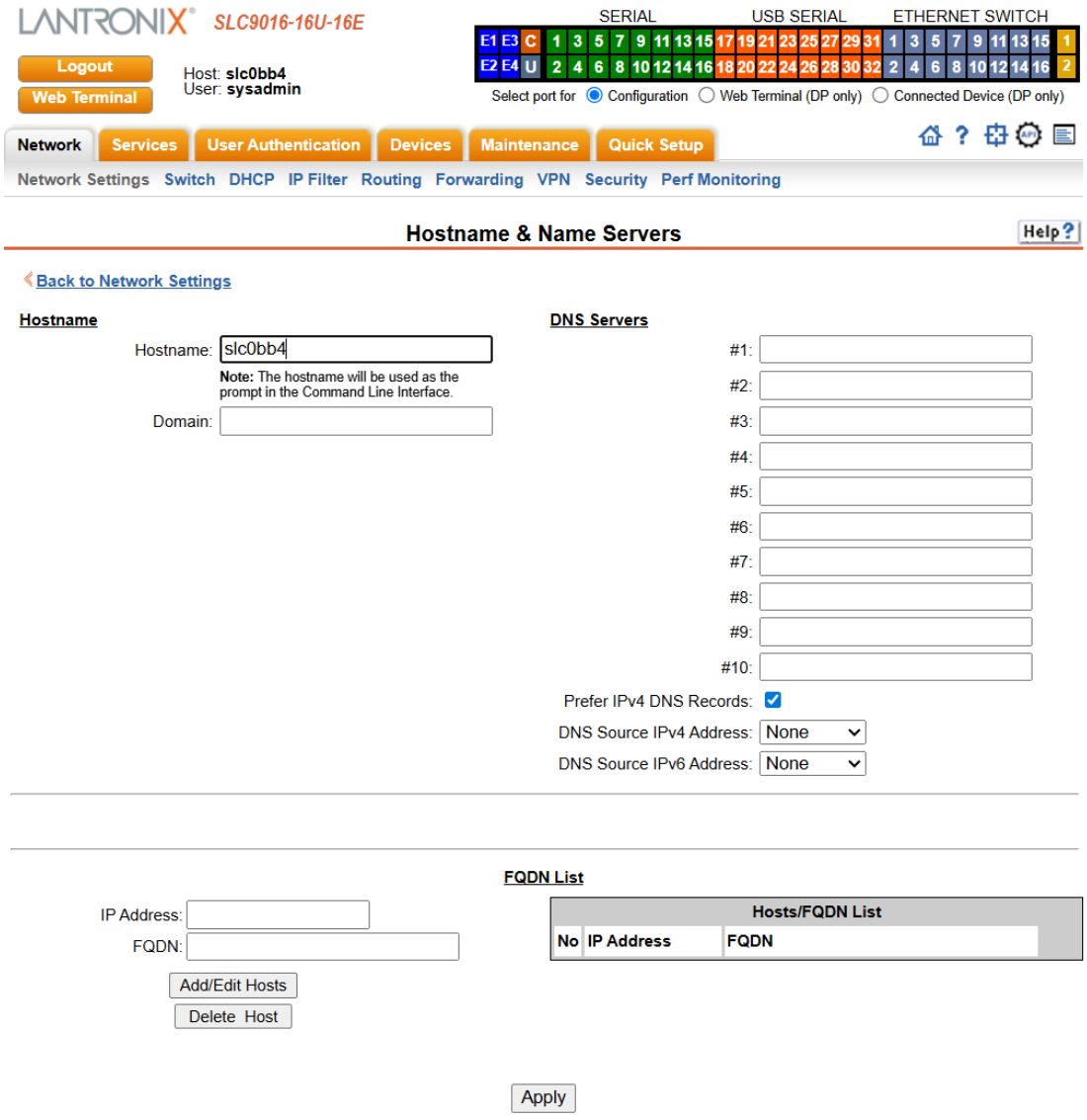
FQDN List

Use the FQDN List to add static hostname entries to the local hosts table so that the SLC 9000 can resolve hostnames that are not resolved via DNS. This feature is useful for referring to OOB-managed devices by hostname in environments without full DNS coverage.

To add/edit/delete hosts:

1. On the **Network Settings** page, click the **Hostname & Name Servers** link. The following page appears:

Figure 6-3 Hostname and Name Serverst



2. At the FQDN List section, enter the following information:
   - To add a Host, enter the **IP address**, **FQDN**, and click **Add/Edit Hosts**. The IP address and hostname displays in the Hosts/FQDN List. You may add up to 15 hosts.

- To edit a Host entry, select the radio button next to the host in the Hosts/FQDN List, change the IP address, FQDN fields as desired, and click **Add/Edit Hosts**.
- To delete a Host, select the radio button next to the host in the Hosts/FQDN List and click **Delete Host**.

3. Click **Apply**.

Virtual Interfaces

The console manager supports two Ethernet virtual interfaces (VEth1 and VEth2). These interfaces act similar to a real physical interface (with a user-assigned IPv4 address and netmask, and optionally an IPv6 address). VEth1 and VEth2 are reachable via the physical Eth1 or Eth2 interface. The interfaces are "virtual" in that they exist in software only. Virtual interfaces can serve as a "device" IPv4 or IPv6 address, which in a network topology can be different than the Eth1 or Eth2 IPv4 or IPv6 address.

Use virtual interfaces when you need the SLC 9000 to appear at a different IP address for management traffic, separate from its physical Ethernet addresses.

In addition to acting as an independent "device" IP address, virtual interfaces can be selected as the interface to bind with, or virtual interface IPv4 addresses can be selected as the source IP address for outgoing connections or protocols (not supported for virtual interface IPv6 addresses):

SSH out connections: CLI SSH out connections using the `connect direct ssh` command can select which interface to use with the **iface** parameter.

NTP packets: by default, no interface is defined for NTP traffic and all available network addresses are available for processing NTP packets. The Source IPv4 Address parameter can be used to select only one interface for processing NTP packets and for all NTP servers defined with an IPv4 address or a name which resolves to an IPv6 address. See *Date and Time* for more details.

SNMP outbound traffic (traps): by default, no source IP address is defined for SNMP traffic; the console manager will use the IP address of the interface through which the SNMP trap packet is sent (based on the routing table). The **Traps Source IPv4 Address** parameter can be used to configure the interface (and which source IPv4 address) is used for sending SNMP traps to NMS servers defined with an IPv4 address or a name which resolves to an IPv4 address. The **Traps Source IPv6 Address** parameter can be used to configure the interface (and which source IPv6 address) is used for sending SNMP traps to NMS servers defined with an IPv6 address or a name which resolves to an IPv6 address. See *SNMP* for more information.

DNS packets: by default, no source interface or IP address is defined for DNS traffic; the console manager will use the IP address of the interface through which the DNS UDP packet is sent (based on the routing table). The **DNS Source IPv4 Address** parameter can be used to set the source IPv4 address of all DNS packets sent to DNS servers defined with an IPv4 address. The **DNS Source IPv6 Address** parameter can be used to set the source IPv6 address of all DNS packets sent to DNS servers defined with an IPv6 address. See *Network Port Settings* for more details.

TACACS+ Authentication packets: by default, no source interface or IP address is defined for TACACS+ traffic; the console manager will use the IP address of the interface through which the TACACS+ TCP packet is sent (based on the routing table). The **Source IPv4 Address** parameter can be used to set the source IPv4 address of packets sent to all TACACS+ servers defined with an IPv4 address or a name which resolves to an IPv4 address. The **Source IPv6 Address** parameter can be used to set the source IPv6 address of packets sent to all TACACS+ servers

defined with an IPv6 address or a name which resolves to an IPv6 address. See *TACACS+* for more details.

It is highly recommended that an IP address / subnet for VEth1 and VEth2 be different than the IP address / subnet for Eth1 and Eth2. Configuring VEth1 or VEth2 with the same IP address / subnet as Eth1 or Eth2 may cause the console manager to become unreachable.

To utilize a virtual interface on the console manager, other devices on the network may need to create routing rules, such as a static route, so that network traffic can be routed to the virtual interface via one of the SLC 9000's network attached physical interfaces, such as Eth1, Eth2, or Modem PPP network interfaces. For example, in this configuration on the console manager:

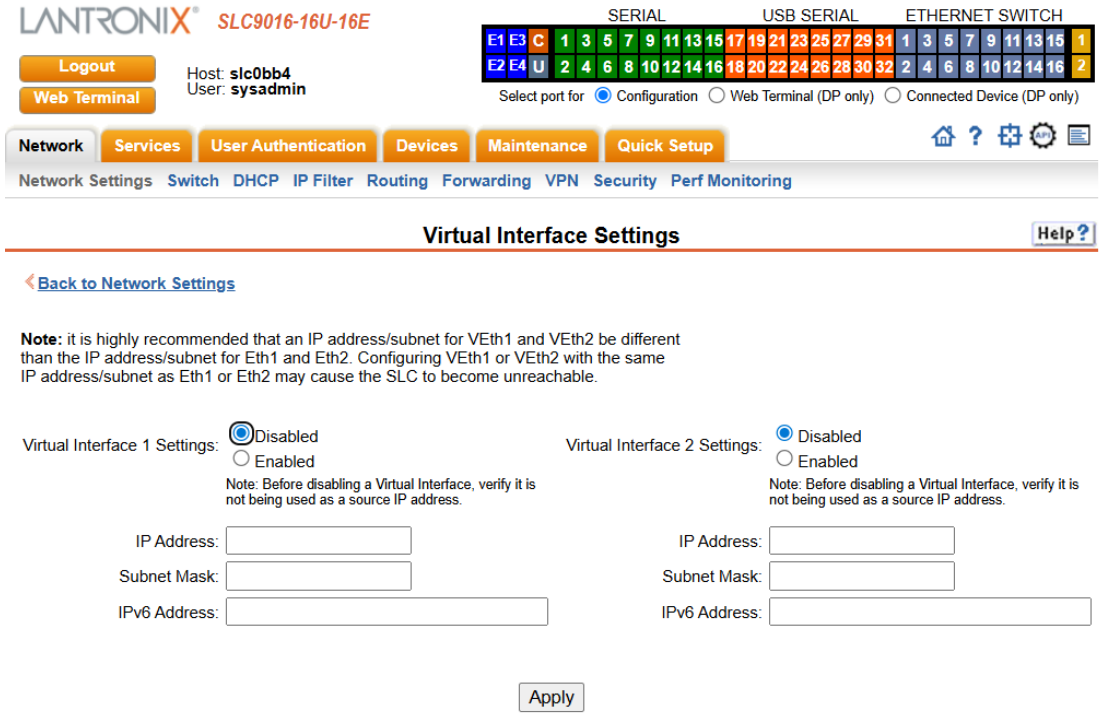
```
Eth1    : 192.168.84.100/24
Gateway : 192.168.84.1
VEth1   : 192.168.44.100/24
```

Another device on the 192.168.84.0/24 network (for example 192.168.84.2) would need to add a static route so that traffic between 192.168.84.2 and 192.168.44.100 can be routed. For example, for Linux devices, this command would be issued on 192.168.84.2:

```
ip route add 192.168.44.100/32 via 192.168.84.100
```

To configure a virtual interface:

1. On the Network Settings page, click the Virtual Interfaces link to display the Virtual Interface Settings configuration page.



2. Enter the following information for one or both virtual interface ports:

Virtual Interface 1/ Virtual Interface 2 Settings	◆ Disabled: If selected, disables the virtual interface. Defaults are VEth1 and VEth2 disabled. ◆ Enabled: Allows the user to manually assign a static IP address and netmask to the virtual interface, and bring the interface up.

IP Address	An IPv4 address that will be unique and valid on your network. There is no default. ***Note:*** ~~***Note:***~~ *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.*
Subnet Mask	The network segment for the IP address. There is no default.
IPv6 Address	Address of the Virtual Interface in IPv6 format. IPv6 addresses are written as 8 sets of 4-digit hexadecimal numbers separated by colons. For example, 1234:0BCD:1D67:0000:0000:8375:BADD:0057 may be shortened to 1234:BCD:1D67::8375:BADD:57. The IPv6 address will require a /bit mask prefix at the end of the address, 1234:0BCD:1D67:0000:0000:8375:BADD:0057/64

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

Ethernet Switch

The SLC 9000 supports an integrated managed Ethernet Switch that can be used to connect network devices to the console manager. This switch can be used as a management LAN to provide secure access to these network devices. DHCP services are available to provide IP addresses and other network information to devices connected to the switch.

SLC 9000 models support expanded switch capabilities:

- **Access or Trunk Ports**: access ports can be assigned to only a single VLAN, and trunk ports can be assigned to multiple VLANs
- **VLANs**: configure up to 10 VLANs on up to 32 switch ports, and a port can be a member of up to 5 VLANs
- **Port Egress Policy**: determines if a VLAN tag is added (tagged) or removed (untagged) when traffic leaves the port

On the SLC 9000 with two 16 port Ethernet Switch modules, for best performance, it is recommended that devices that require high bandwidth communication with other devices on the switch be connected on the same Ethernet Switch module.

The default IP address and subnet mask on the Ethernet Switch is 192.168.10.1 / 255.255.255.0. The IP address and subnet mask on the Ethernet switch can be changed via the DHCP settings.

The Ethernet Switch port LEDs display the following states:

- **Green Light On**: indicates a link at 1000 BASE-T
- **Green Light Off**: indicates a link at other speeds, or no link
- **Yellow/Orange Light On**: indicates a link is established
- **Yellow/Orange Light Blinking**: indicates link activity

On console server models with a managed Ethernet Switch installed, the user can:

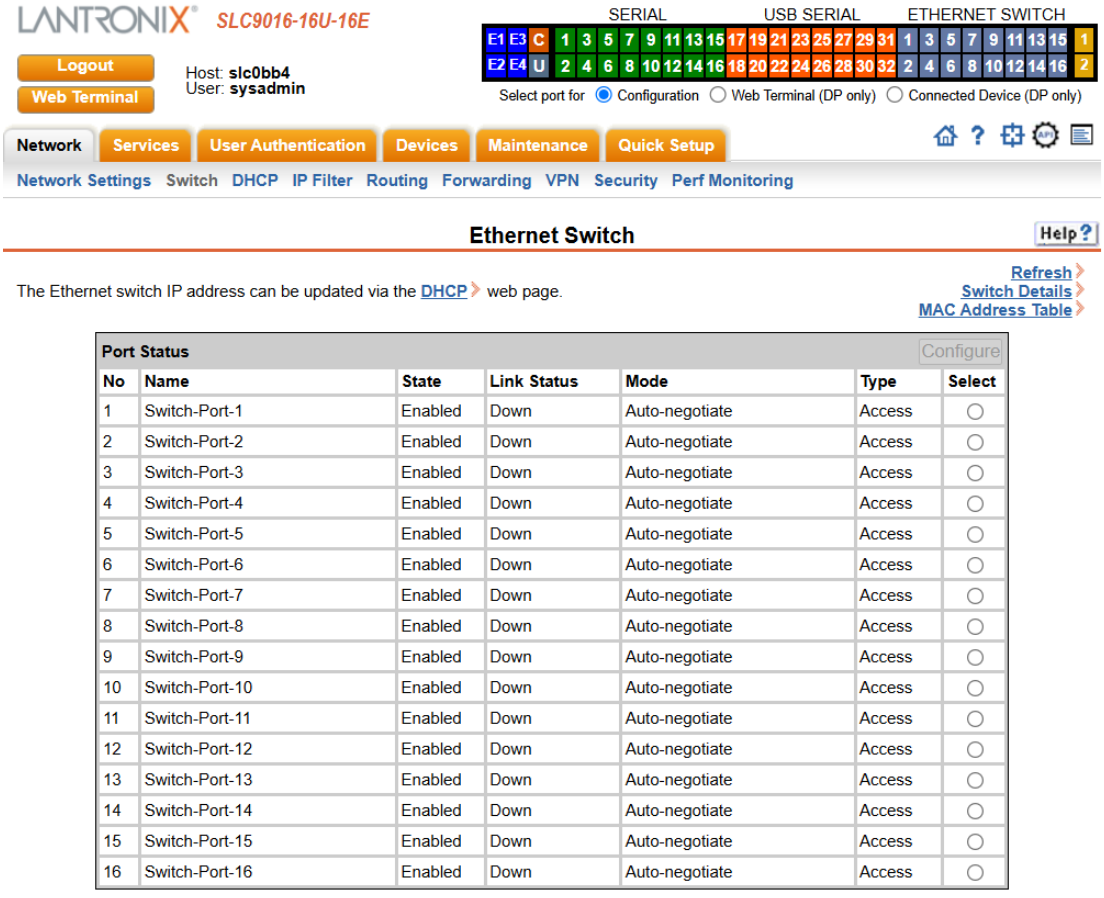
- **Configure Ports and View Status**: configure the speed and duplex on each port, and see the link status

- **View Port Statistics:** view frame statistics (errors, unicast, broadcast, etc) and frame details (undersize, collisions, etc)
- **View MAC address table**: view static and dynamic MAC address table entries

To configure a switch port:

1. Click the **Network** tab and select the **Switch** option. The Network > Ethernet Switch page displays.

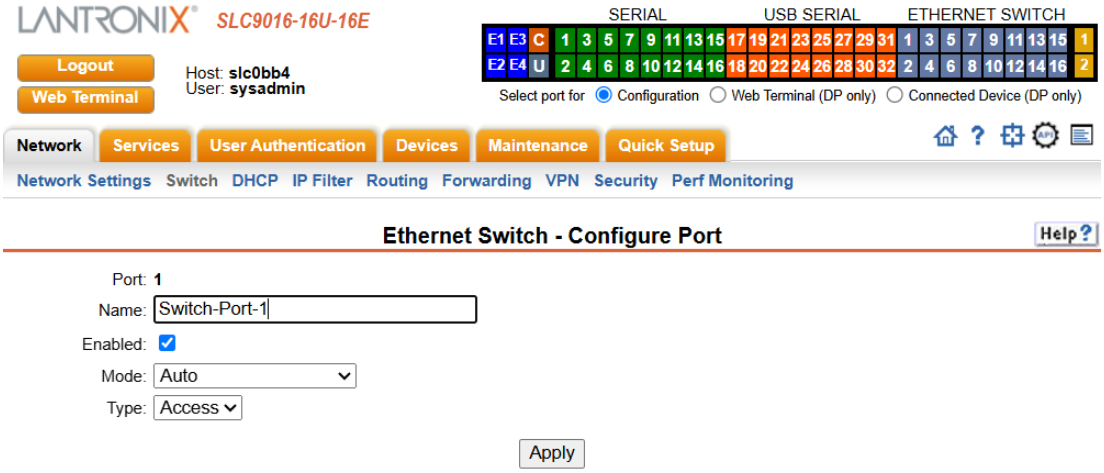
Figure 6-4 Network > Ethernet Switch



No	Name	State	Link Status	Mode	Type	Select
1	Switch-Port-1	Enabled	Down	Auto-negotiate	Access	
2	Switch-Port-2	Enabled	Down	Auto-negotiate	Access	
3	Switch-Port-3	Enabled	Down	Auto-negotiate	Access	
4	Switch-Port-4	Enabled	Down	Auto-negotiate	Access	
5	Switch-Port-5	Enabled	Down	Auto-negotiate	Access	
6	Switch-Port-6	Enabled	Down	Auto-negotiate	Access	
7	Switch-Port-7	Enabled	Down	Auto-negotiate	Access	
8	Switch-Port-8	Enabled	Down	Auto-negotiate	Access	
9	Switch-Port-9	Enabled	Down	Auto-negotiate	Access	
10	Switch-Port-10	Enabled	Down	Auto-negotiate	Access	
11	Switch-Port-11	Enabled	Down	Auto-negotiate	Access	
12	Switch-Port-12	Enabled	Down	Auto-negotiate	Access	
13	Switch-Port-13	Enabled	Down	Auto-negotiate	Access	
14	Switch-Port-14	Enabled	Down	Auto-negotiate	Access	
15	Switch-Port-15	Enabled	Down	Auto-negotiate	Access	
16	Switch-Port-16	Enabled	Down	Auto-negotiate	Access	

2. Select a port in the **Ethernet Switch Port status** table, and select **Configure**. The **Ethernet**

Switch - Configure Port page will be displayed.



3. Complete the following:

Name	User definable name for the port. The name can be up to 30 characters long and contain letters, numbers, underscore, hyphen and period.
Enabled	Select this box to enable the port and allow devices to connect to it. Enabled by default.
Mode	Select the direction (Full-Duplex or Half-Duplex) and speed (10, 100, or 1000 Mbit) 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.
Type	Select the port type - Access (assigned to a single VLAN only) or Trunk (can be assigned to multiple VLANs). The default is Access.

4. Click **Apply** to save the port settings.

Port Statistics

Rx - Good	The sum of lengths of good frames received, e.g., the sum of lengths of Rx - Unicast, Rx - Broadcast, Rx - Multicast and Rx - Pause.
Rx - Errors	The sum of lengths of bad frames received, e.g., the sum of lengths of Rx - Undersize, Rx - Fragments, Rx - Oversize, Rx - Jabber, Rx - RxErr and Rx - FCSErr.
Rx - Unicast	The number of good frames received that have a Unicast destination MAC address.
Rx - Broadcast	The number of good frames received that have a Broadcast destination MAC address.
Rx - Multicast	The number of good frames received that have a Multicast destination MAC address. This does not include frames counted in Rx - Pause nor does it include frames counted in Rx - Broadcast.
Rx - Pause	The number of good frames received that have a Pause destination MAC address. This includes Priority Flow Control (PFC) Pause frames.
Tx - Good	The sum of lengths of all Ethernet frames sent.

Tx - Unicast	The number of frames sent that have a Unicast destination MAC address.
Tx - Broadcast	The number of frames sent that have a Broadcast destination MAC address.
Tx - Multicast	The number of frames sent that have a Multicast destination MAC address. This does not include frames counted in Tx - Pause nor does it include frames counted in Tx - Broadcast.
Tx - Pause	The number of Flow Control frames sent. This includes Pause and Priority Flow Control (PFC) Pause frames.
Tx - Pause	The number of good frames received that have a Pause destination MAC address. This includes Priority Flow Control (PFC) Pause frames.
Rx - Undersize	Total frames received with a length of less than 64 octets but with a valid FCS.
Rx - Fragments	Total frames received with a length of less than 64 octets and an invalid FCS.
Rx - Oversize	Total frames received with a length of more than MaxSize octets but with a valid FCS.
Rx - Jabber	Total frames received with a length of more than MaxSize Octets but with an invalid FCS.
Rx - RxErr	Total frames received with an RxErr signal from the PHY. This includes 10 GE MAC Termination Errors.
Rx - FCSErr	Total frames received with a CRC error not counted in Rx - Fragments, Rx - Jabber or Rx - RxErr.
Tx - Deferred	The total number of successfully transmitted frames that experienced no collisions but are delayed because the medium was busy during the first attempt. This counter is applicable in half-duplex only.
Tx - Collisions	The number of collision events seen by the MAC not including those counted in Single, Multiple, Excessive, or Late. This counter is applicable in half-duplex only.
Tx - Single Collision	The total number of successfully transmitted frames that experienced exactly one collision. This counter is applicable in half-duplex only.
Tx - Multiple Collisions	The total number of successfully transmitted frames that experienced more than one collision. This counter is applicable in half-duplex only.
Tx - Excessive Collisions	The number frames dropped in the transmit MAC because the frame experienced 16 consecutive collisions. This counter is applicable in half-duplex only.
Tx - Late	The number of times a collision is detected later than 512 bits-times into the transmission of a frame. This counter is applicable in half-duplex only.
Tx - FCSErr	The number of frames transmitted with an invalid FCS. Whenever a frame is modified during transmission (e.g., to add or remove a tag) the frame's original FCS is inspected before a new FCS is added to a modified frame. If the original FCS is invalid, the new FCS is made invalid too and this counter is incremented. This can occur because frames with a bad FCS are allowed into the switch.
All - 64 Octets	Total frames received and/or transmitted with a length of exactly 64 octets, including those with errors.
All - 65-127 Octets	Total frames received and/or transmitted with a length of between 65 and 127 octets inclusive, including those with errors.

All - 128-255 Octets	Total frames received and/or transmitted with a length of between 128 and 255 octets inclusive, including those with errors.
All - 256-511 Octets	Total frames received and/or transmitted with a length of between 256 and 511 octets inclusive, including those with errors.
All - 512-1023 Octets	Total frames received and/or transmitted with a length of between 512 and 1023 octets inclusive, including those with errors.
All - 1024-Max Octets	Total frames received and/or transmitted with a length of between 1024 and MaxSize octets inclusive, including those with errors. MaxSize (the jumbo frame size) is 10240 bytes.

Switch Commands

Go to *Switch Commands* to view CLI commands which correspond to the web page entries described above.

DHCP

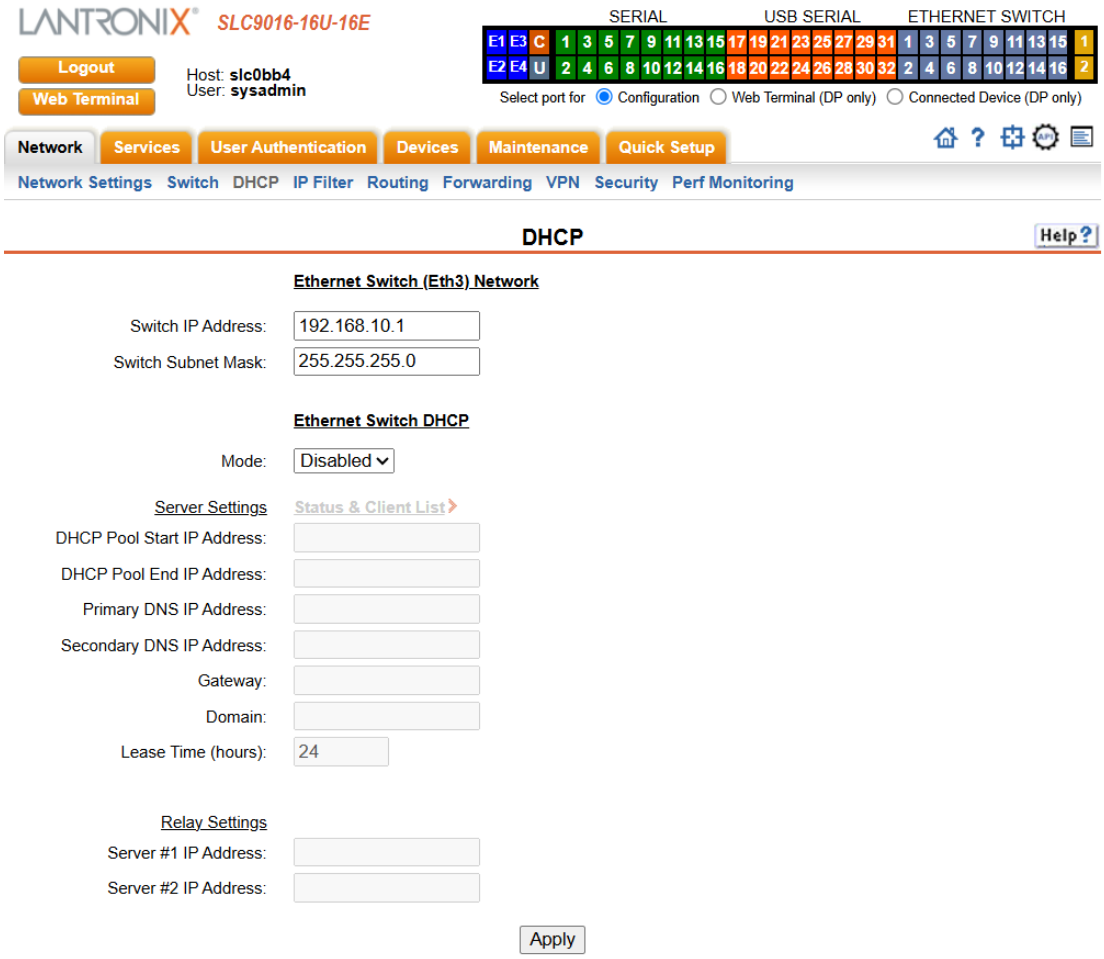
On models with an Ethernet Switch installed, the console manager can provide DHCP services to clients connected to the Ethernet Switch. By default DHCP is disabled. Two DHCP modes are supported:

- **DHCP Server:** provides IP addresses and other networking parameters to devices connected to the Ethernet Switch that are running DHCP clients. The server can provide IP address, subnet mask, primary DNS IP address, secondary DNS IP address, gateway and domain. Lease times are given in hours, up to a maximum of 14 days.
- **DHCP Relay:** forwards DHCP packets between devices connected to the Ethernet Switch and DHCP servers that are accessible via one of the other interfaces (Eth1, Eth2, cellular, or WiFi). This allows hosts connected to the Ethernet Switch to acquire IP addresses from a DHCP server already in service and reachable on the network. Because DHCP is a broadcast-based protocol, by default its packets do not pass from devices connected to the Ethernet Switch to other subnets. A DHCP relay agent receives any DHCP broadcasts on the Ethernet Switch and forwards them via unicast to DHCP servers on a different subnet. Since the DHCP servers are located on a different subnet they may need routes back to the Ethernet Switch that is requesting DHCP addresses on behalf of its connected clients. DHCP Relay can be configured to use one or two DHCP servers.

To configure DHCP:

1. Click the **Network** tab and select the **DHCP** option. The Network > DHCP page displays.

Figure 6-5 Network > DHCP



2. Complete the following:

Switch IP Address	The internal IP address assigned to the Ethernet Switch.
Switch Subnet Mask	The internal subnet mask assigned to the Ethernet Switch.
Mode	Select the type of DHCP service for devices connected to the Ethernet Switch: Server to run a DHCP server that provides IP addresses to clients, or Relay to relay DHCP requests between devices and a DHCP server on the network.

DHCP Server Settings

Note: *Changing any DHCP server option will clear all DHCP client leases from the table maintained by the console manager.*

DHCP Pool Start IP Address / DHCP Pool End IP Address	The beginning IP address and ending IP address for the pool of IP addresses that are distributed to DHCP clients on the Ethernet Switch. The pool IP addresses should be in the same subnet as the Ethernet Switch IP address / subnet mask.
Primary / Secondary DNS IP Address	An optional primary and secondary DNS IP address that may be provided to DHCP clients on the Ethernet Switch.

Gateway	An optional gateway (default router) IP address that may be provided to DHCP clients on the Ethernet Switch.
Domain	An optional domain that may be provided to DHCP clients on the Ethernet Switch. Maximum length is 64 characters.
Lease Time	The lease duration that will be provided in a DHCP Lease Offer to a DHCP client. The default is 24 hours. Lease times in the range of 1 hour to 336 hours (14 days) may be specified.

DHCP Relay Settings

Note: *IP Forwarding must be enabled if a DHCP client uses unicast (instead of broadcast) to communicate with a DHCP server.*

Server #1 IP Address	The IP address of the first DHCP server to send DHCP requests to, when DHCP Relay mode is enabled.
Server #2 IP Address	The IP address of the second DHCP server to send DHCP requests to, when DHCP Relay mode is enabled. If a second DHCP server is specified, DHCP requests will be sent to both Server #1 and Server #2 at the same time.

3. Click **Apply** to save the DHCP settings.
4. When DHCP server mode is enabled, click **Status & Client List** to see status and the current list of DHCP clients and their lease times.

DHCP Commands

Go to *DHCP Commands* to view CLI commands which correspond to the web page entries described above.

IP Filter

IP filters (also called a rule set) act as a firewall to allow or deny an individual MAC address or 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 access to your SLC unit.***

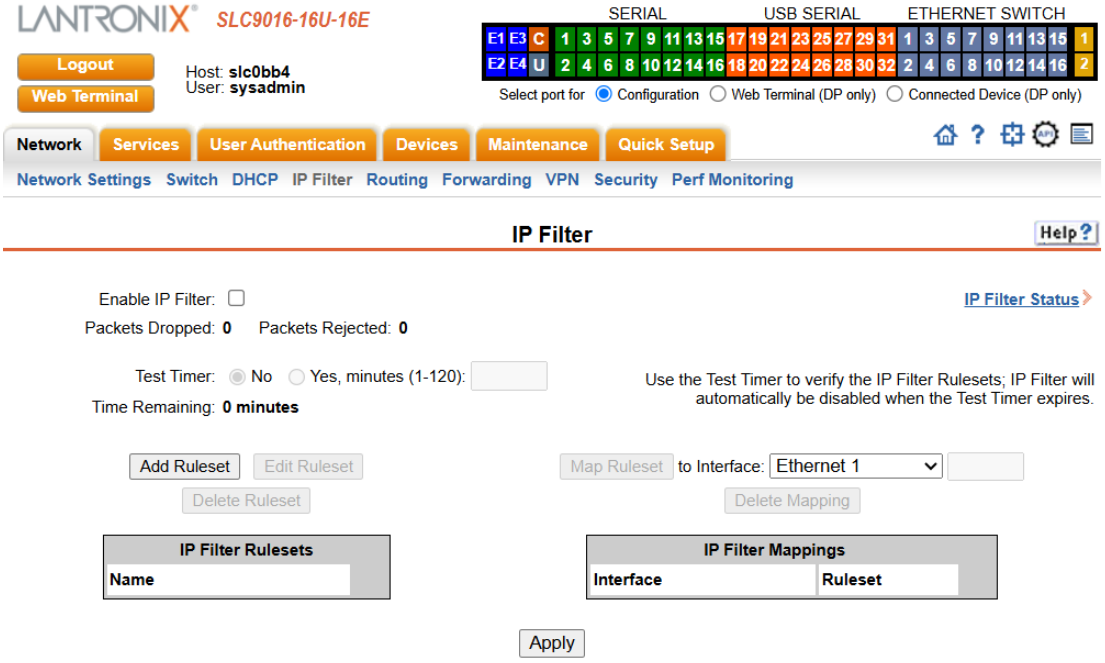
Viewing IP Filters

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:

Figure 6-6 Network > IP Filter



Mapping Rulesets

The administrator can assign an IP Filter Rule Set to a network interface (Ethernet interface), a modem connected to a device port, or a USB modem or an internal modem (if installed).

To map a ruleset to a network interface:

1. Click the **Network** tab and select the **IP Filter** option. The *Network > IP Filter* page displays.
2. Select the IP filter rule set to be mapped.
3. From the **Interface** drop-down list, select the desired network interface and click the **Map Ruleset** button. The Interface and rule set display in the IP Filter Mappings table.

To delete a mapping:

1. Click the **Network** tab and select the **IP Filter** option. The *Network > IP Filter* page displays.
2. Select the mapping from the list and click the **Delete Mappings** button. The mapping no longer displays.
3. Click the **Apply** button.

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:

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

Configuring IP Filters

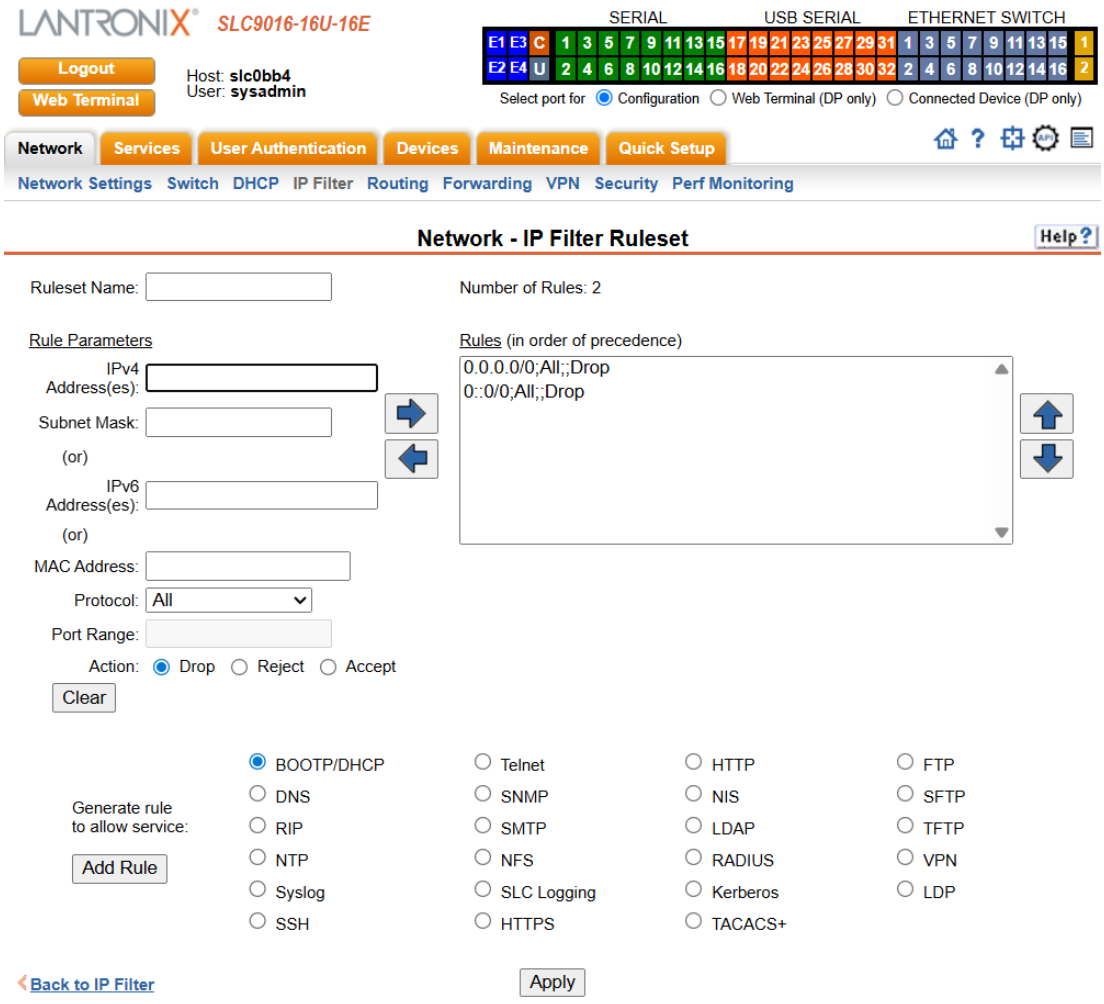
The administrator can add, edit, delete, and map IP filters.

Note: *A configured filter has no effect until it is mapped to a network interface.*
See “Mapping Rulesets” on page 79.

To add an IP filter:

1. On the *Network > IP Filter* page, click the **Add Ruleset** button. The following page displays:

Figure 6-7 Network > IP Filter Ruleset (Adding/Editing Rulesets)



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

IPv4 Address(es)	Specify a single IP address to act as a filter (this will also require a Subnet Mask) 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 or 172.19.220.60-172.19.220.68.
Subnet Mask	Specify a subnet mask to act as a filter. Example: 255.255.0.0

IPv6 Address(es)	Specify a single IPv6 address with a subnet mask (prefix) to act as a filter, or specify a range of IPv6 addresses if the range cannot be defined by an IPv6 address and subnet mask (prefix). Example: 1234:0BCD:1D67:0000:0000:8375:BADD:0057/64.
MAC Address	Specify a single MAC address to act as a filter. Example: 10:7d:1a:33:5c:e1
Protocol	From the drop-down list, select the type of protocol through which the filter will operate. The default setting is **All**.
Port Range	Enter a range of destination TCP or UDP port numbers to be tested. An entry is required for TCP, TCP New, TCP Established, and UDP, and is not allowed for other protocols. Separate multiple ports with commas. Separate ranges of ports by colons. Examples: ◆ 22 – filter on port 22 only ◆ 23,64,80 – filter on ports 23, 64 and 80 ◆ 23:64,80,143:150 – filter on ports 23 through 64, port 80 and ports 143 through 150
Action	Select whether to **Drop**, **Reject**, or **Allow** communications for the specified IP address, subnet mask, protocol, and port range. Drop ignores the packet with no notification. Reject ignores the packet and sends back an error message. Allow permits the packet through the filter.
Clear	Click the **Clear** button to clear any Rule Parameter information set above.
Generate rule to allow service	You may wish to “punch holes” in your filter set for a particular protocol or service. For instance, if you have configured your NIS server and wish to create an opening in your filter set, select the NIS option and click the **Add Rule** button. This entry adds a new rule to your filter set using the NIS -configured IP address. Other services and protocols added automatically generate the necessary rule to allow their use.

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 256 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, select the IP filter ruleset to be edited and click the **Edit Ruleset** button to return to the *Network > IP Filter Ruleset (Adding/Editing Rulesets)* page (see *Figure 6-7*).

Deleting an IP Filter

To delete an IP filter rule set:

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

IP Filter Commands

Go to *IP Filter Commands* to view CLI commands which correspond to the web page entries described above.

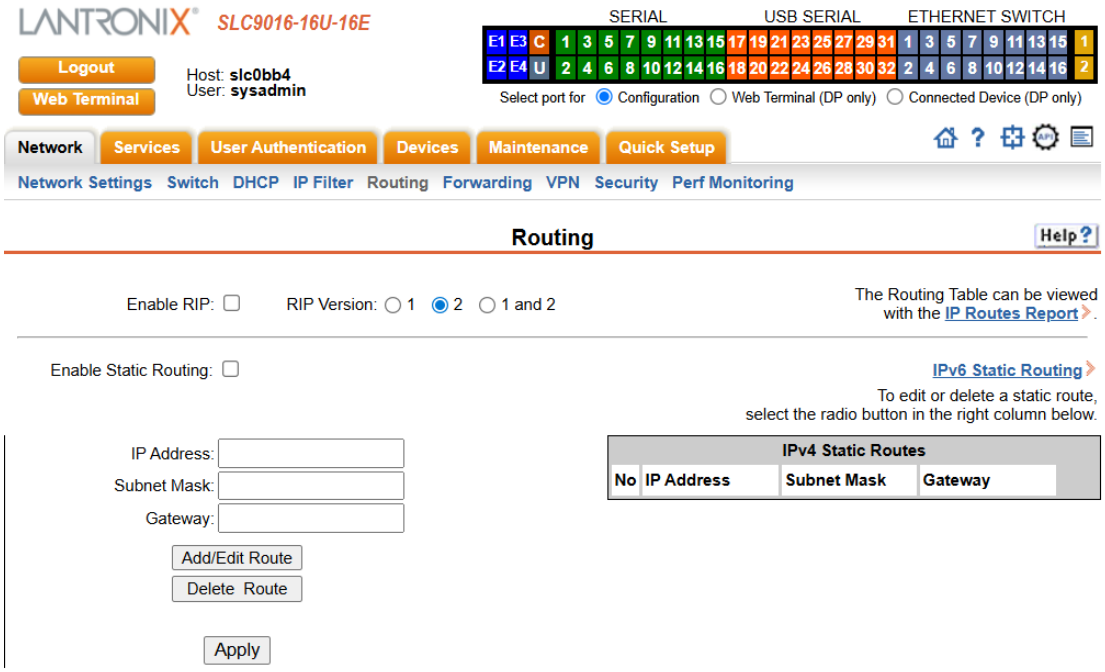
Routing

The SLC 9000 advanced console server allows you to define static IPv4 and IPv6 routes and, for networks using Routing Information Protocol (RIP)-capable routes, to enable the RIP protocol to configure the routes dynamically. Up to 64 IPv4 static routes and 64 IPv6 static routes can be configured.

To configure routing (RIP and IPv4 static routes):

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

Figure 6-8 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 and IPv4 Static Routes

Enable Static Routing	Select to manually configure IPv4 or IPv6 static routes. The system administrator usually provides the routes. Disabled by default.
IP Address/Subnet Mask/Gateway	Used to manually configure a single IPv4 static route. ◆ 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 IPv4 Static Routes table. ◆ 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.

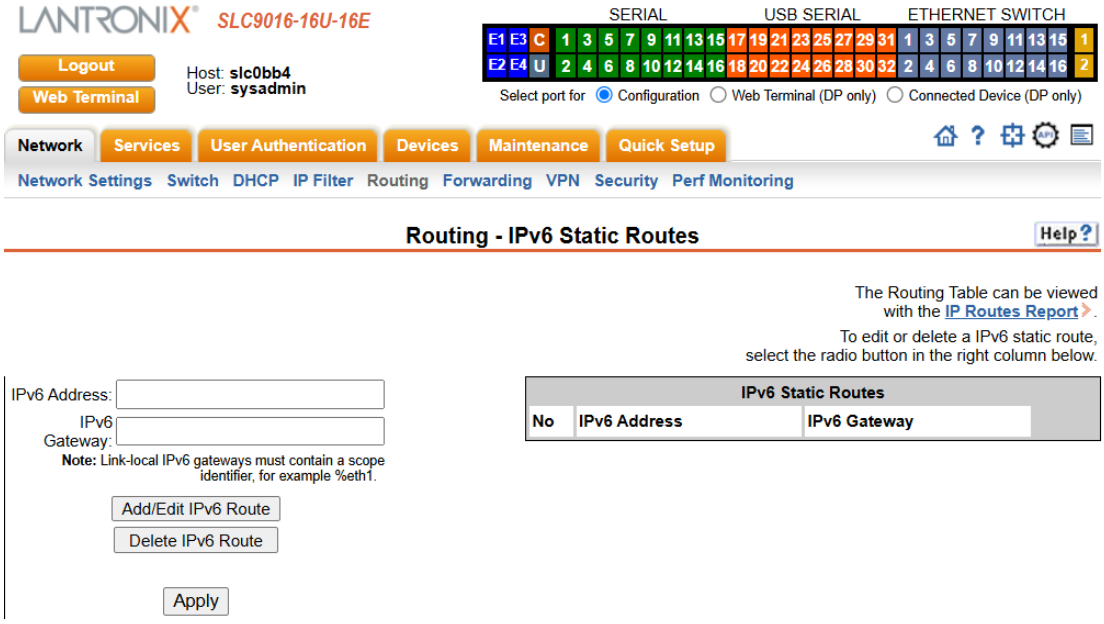
3. Click the **Apply** button.

Note: *To display the routing table, status or specific report, see the section,* *Status/Reports on page 333*.

IPv6 Static Routing

To configure routing (IPv6 static routes):

1. Click the **Network** tab and select the **Routing** option.
2. Click the IPv6 Static Routing link to navigate to the Routing - IPv6 Static Routes page.



3. Enter the following information:

IPv6 Address / IPv6 Gateway	Used to manually configure a single IPv4 static route. ◆ To add a static route, enter the **IPv6 Address** (including prefix/mask bits), and **IPv6 Gateway** for the route and click the **Add/Edit IPv6 Route** button. IPv6 addresses are written as 8 sets of 4-digit hexadecimal numbers separated by colons, followed by a forward slash and mask bits, for example 1234:0BCD:1D67:0000:0000:8375:BADD:0057/64. After adding the route it will be displayed in the IPv6 Static Routes table. Note: link-local gateways must be appended with a scope identifier, for example **%eth1** or **%eth2**. ◆ To edit a static route, select the radio button to the right of the route, change the IPv6 Address and prefix/mask bits, and IPv6 Gateway fields as desired, and click the **Add/Edit IPv6 Route** button. ◆ To delete a static route, select the radio button to the right of the route and click the **Delete IPv6 Route** button.

4. Click the **Apply** button.
5. Navigate back to the Routing page.

Enable Static Routing	On the Routing page, select this option to manually configure **IPv4** or **IPv6** static routes. The system administrator usually provides the routes. The default is disabled.

6. Click **Apply**.

Routing Commands

Go to *Routing Commands* to view CLI commands which correspond to the web page entries described above.

Forwarding

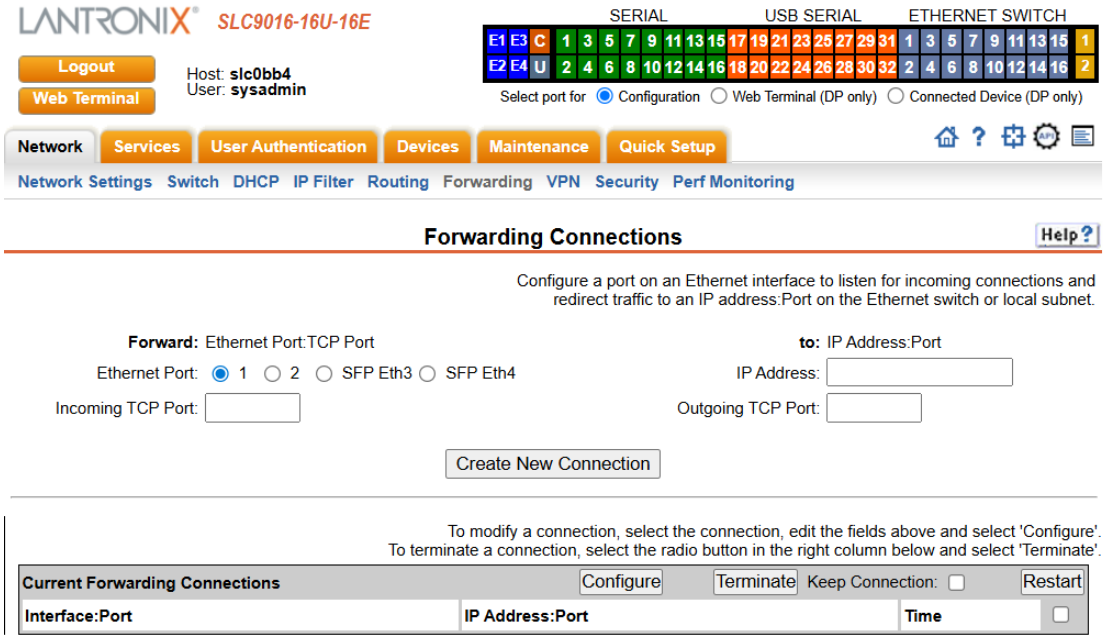
Port Forwarding can be used to configure a port on the Eth1, Eth2, SFP Eth3 or SFP Eth4 Ethernet interface to listen for incoming TCP connections, and redirect traffic to an IP address:TCP Port on the Ethernet Switch or the local subnet. This allows network traffic on one interface to be securely routed to another network (including devices connected directly to the Ethernet Switch). For example, a port forwarding connection can be configured to route traffic between a browser and a unique TCP Port on Eth1 to port 443 of a device connected to the Ethernet Switch. This direct port to port forwarding does not support applications requiring dynamic port redirection.

Note: *Note: when the web server is enabled, it listens on port 443 for all interfaces (Eth1, Eth2, Eth3, Eth4, WLAN, Cellular, PPP - this list depends on the components installed) for incoming connections. It listens on interfaces even if they are disabled in the Web Server settings (the connection to a disabled interface is blocked and logged by the web server). In order to use port 443 for the incoming TCP port the web server must be disabled.*

To create a new forwarding connection:

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

Figure 6-9 Network > Forwarding Connections



2. Complete the following:

Ethernet Port	Select 1 to create a listening connection on Eth 1 or select 2 to create a listening connection on Eth 2.
Incoming TCP Port	Enter a unique (currently unused) TCP Port to listen on. The Diagnostics Netstat tool can be used to view all in-use TCP ports.
IP Address	The IP address to route the traffic to.

Outgoing TCP Port	The TCP port to route the traffic to. This should be a TCP port that is open and listening on the device.

3. To create a new connection, click **Create New Connection**. Return to the Forwarding page, the new connection will be shown in the **Current Forwarding Connections** table at the bottom.

   Note: *In the CLI "show connections" output, an extra SSH In connection to the console manager will be shown for each forwarding connection - this is the SSH tunnel for the port forwarding connection.*

4. To edit an existing connection, click the checkbox in the right column in the **Current Forwarding Connections** table. This will fill in the text fields at the top with the current settings. Change the settings as needed and then click **Configure**. This will tear down the current connection and restart it with the new settings. After returning to the **Forwarding** page, the updated connection will be shown in the **Current Forwarding Connections** table at the bottom. The connection will persist across reboots until it is terminated.

5. To terminate an existing connection, click the checkbox in the right column in the **Current Forwarding Connections** table. Select the **Keep Connection** checkbox to suspend the connection (it can be restarted later using the Restart button). Click **Terminate**. This will tear down and remove the connection.

Forwarding Connections Commands

Go to *Connection Commands* to view CLI commands which correspond to the web page entries described above.

VPN Settings

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

The SLC provides a strongSwan-based VPN implementation (version 5.6.3). The SLC UI provides access to a subset of the strongSwan configuration options, and also allows upload of a custom ipsec.conf file, which gives an administrator access to most strongSwan configuration options. For more information on strongSwan, see https://www.strongswan.org and the strongSwan FAQ. A list of Internet Key Exchange IKEv1 and IKEv2 cipher suites is available on the strongSwan Wiki. NAT Traversal is handled automatically without any special configuration. VPN related routes are installed in a separate table and can be viewed in the detailed VPN status or in the IP Routes table.

When a tunnel is up, the amount of data passed through the tunnel can be viewed in the status with the bytes_i (bytes input) and bytes_o (bytes output) counters. An example of the VPN status is below (the status will vary depending on the authentication, subnets and algorithms used). For example, the status displays the IP addresses on either side of the tunnel (192.168.1.103 and 220.41.123.45), the type of authentication (pre-shared key authentication), the algorithms in use

(IKEv1 Aggressive and 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024), when the tunnel will be rekeyed/SA Lifetime (rekeying in 7 hours), the bytes in and out (131 bytes_i (1 pkt, 93s ago), 72 bytes_o (1 pkt, 94s ago)), a dynamic address assigned to the console manager side of the tunnel (child: dynamic and 172.28.28.188), and the subnets on both sides of the tunnel (172.28.28.188/32 === 10.3.0.0/24 10.81.101.0/24 10.81.102.0/24 10.81.103.0/24).

```
Connections:
   MyVPNConn:  192.168.1.103...220.41.123.45  IKEv1 Aggressive,
dpddelay=30s
   MyVPNConn:   local:  [vpnid] uses pre-shared key authentication
   MyVPNConn:   local:  [vpnid] uses XAuth authentication: any with XAuth
identity 'gfountain'
   MyVPNConn:   remote: [220.41.123.45] uses pre-shared key
authentication
   MyVPNConn:   child:  dynamic === 0.0.0.0/0 TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
   MyVPNConn[1]: ESTABLISHED 26 minutes ago,
192.168.1.103[vpnid]...220.41.123.45[220.41.123.45]
   MyVPNConn[1]: IKEv1 SPIs: 62c06b5b5fc3c5de_i* 74300552060118f6_r,
pre-shared key+XAuth reauthentication in 2 hours
   MyVPNConn[1]: IKE proposal: 3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/
MODP_1024
   MyVPNConn{1}:  INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c6b71deb_i
95f877ec_o
   MyVPNConn{1}:  3DES_CBC/HMAC_MD5_96/MODP_1024, 131 bytes_i (1 pkt, 93s
ago), 72 bytes_o (1 pkt, 94s ago), rekeying in 7 hours
   MyVPNConn{1}:   172.28.28.188/32 === 10.3.0.0/24 10.81.101.0/24
10.81.102.0/24 10.81.103.0/24
```

The SLC loads a subset of the available strongSwan plugins. If an option is given in a custom ipsec.config file that requires a plugin that is not loaded by the SLC, this may cause an error during tunnel negotiation. The loaded plugins can be viewed in the VPN Status when the VPN tunnel is enabled.

Sample ipsec.conf Files are provided for a variety of tunnel configurations and peers. The strongSwan Wiki also provides a variety of usable examples and sample configurations, in addition to interoperability recommendations.

Depending on the VPN configuration, it may be necessary to enable IP Forwarding (see *Network Port Settings*) or to add static routes; in some cases traffic may not be passed through the tunnel without enabling IP Forwarding or static routes (see *Routing*). Refer to the VPN routing table that is displayed with the VPN status.

A watchdog program is automatically run when the VPN tunnel is enabled. This program will detect if the VPN tunnel goes down (for reasons other than the user disabling the tunnel). The watchdog program will:

- Generate a syslog message when the tunnel goes up or down
- If traps are enabled, send a slcEventVPNTunnel SNMP trap when the tunnel goes up or down
- If an email address is configured in the VPN configuration, send an email when the tunnel goes up or down
- If enabled, automatically restart the VPN tunnel

When using VPN with Network Fail-over, the Local IP Address should not be configured for the VPN tunnel. This will allow strongSwan to automatically determine the IP address on the local

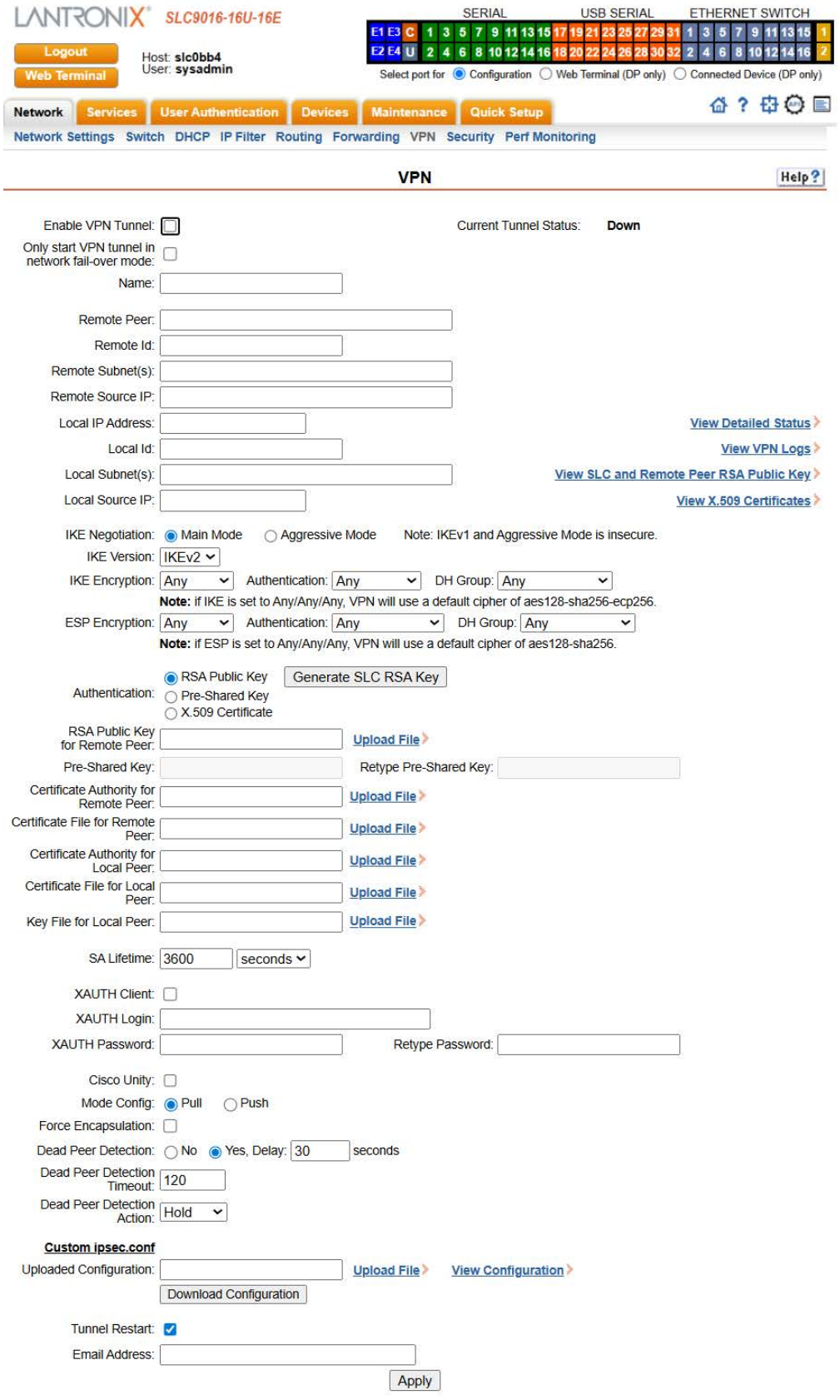
(console manager) side of the tunnel based on the network configuration during both fail-over and fail-back.

VPN tunnels over an console manager Ethernet interfaces that is configured with an MTU less than 256 may experience issues (traffic loss, etc).

To set up a VPN connection:

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

Figure 6-10 Network > VPN



2. Enter the following:

Enable VPN Tunnel	Select to create a tunnel. Disabling this option will terminate any currently running tunnel. ***Note:*** *The VPN peer that sends the first packet in tunnel bringup is the initiator or client; the VPN peer that listens for and responds to the first packet is the responder or server. In general, the responder / server side should be started before the initiator / client side. If it is desired to have the console manager VPN tunnel automatically reconnect when the remote peer disconnects and then reconnects, the console manager side of the tunnel should be started first so that it will act as a responder or server. If the console manager side of the tunnel is started after the remote peer, the console manager will act as a initiator / client, and may not automatically reconnect when the remote peer disconnects and is brought back up.*
Only start VPN tunnel in network fail-over mode	Select to start the VPN tunnel only in network fail-over mode. When this option is selected, the VPN tunnel will not start if the network fail-over parameters are not configured, and the network is not in fail-over mode. Whenever there is a network fail-over, the VPN tunnel will automatically start, and when network fail-back happens, the VPN tunnel will automatically go down. If this feature is enabled but the network fail-over parameters are not configured, this setting will be ignored and the VPN tunnel will be started normally and run continuously. By default, this option is disabled.
Name	The name assigned to the tunnel. Required to create a tunnel.
Remote Peer	The IP address or FQDN of the remote host's public network interface. The special value of **any** can be entered to signify an address to be filled in by automatic keying during negotiation. The console manager will act as a responder/server.
Remote Id	How the remote host should be identified for authentication. The Id is used to select the proper credentials for communicating with the remote host.
Remote Hop/Router	If the remote host is behind a gateway, this specifies the IP address of the gateway's public network interface. **This option is deprecated and is no longer supported.**
Remote Subnet(s)	One or more allowed subnets behind the remote host, expressed in CIDR notation (IP address/mask bits). If multiple subnets are specified, the subnets should be separated by a comma. Up to 10 local subnets supported. Configured subnets of the peers may differ, the protocol narrows it to the greatest common subnet. In IKEv1, this may lead to problems with other implementations. Make sure to configure identical subnets in such configurations. If the remote subnet is not defined, it will be assumed that the remote end of the connection goes to the remote peer only.
Remote Source IP	The internal source IP to use in a tunnel(Virtual IP). Currently the accepted values are **config**, **CIDR Notation**, I**P Address Range** or **poolname**. If the value is config on the responder side, the initiator must propose an address which is then echoed back. The supported address pools are expressed as CIDR notation and IP Address range as - or the use of an external IP address pool using poolname is the name of the IP address pool used for the lookup.

Local IP Address	The IP address of the SLC (local) side of the tunnel, specifically the public-network interface. If no IP address is given, the value **%any** will be used in ipsec.conf (this is the default), signifying an address to be filled in (by automatic keying) during negotiation. If the SLC initiates the connection setup the routing table will be queried to determine the correct local IP address. In case the SLC is responding to a connection setup then any IP address that is assigned to a local interface will be accepted.
Local Id	How the SLC unit should be identified for authentication. The Id is used by the remote host to select the proper credentials for communicating with the SLC unit.
Local Hop/Router	If the SLC unit is behind a gateway, this specifies the IP address of the gateway's public network interface. **This option is deprecated and is no longer supported.**
Local Subnet(s)	One or more subnets behind the SLC unit, expressed in CIDR notation (IP address/mask bits). If multiple subnets are specified, the subnets should be separated by a comma. Up to 10 local subnets supported. Configured subnets of the peers may differ, the protocol narrows it to the greatest common subnet. In IKEv1, this may lead to problems with other implementations. Make sure to configure identical subnets in such configurations. If the local subnet is not defined, it will be assumed that the local end of the connection goes to the console manager only.
Local Source IP	The internal source IP to use in a tunnel (Virtual IP). Currently the accepted values are **config4**, **config6** or **Valid IP Address**. With config4 and config6 an address of the given address family will be requested explicitly. If an IP address is configured, it will be requested from the responder, which is free to respond with a different address.
IKE Negotiation	The Internet Key Exchange (IKE) protocol is used to exchange security options between two hosts who want to communicate via IPSec. The first phase of the protocol authenticates the two hosts to each other and establishes the Internet Security Association Key Management Protocol Security Association (ISAKMP SA). The second phase of the protocol establishes the cryptographic parameters for protecting the data passed through the tunnel, which is the IPSec Security Association (IPSec SA). The IPSec SA can periodically be renegotiated to ensure security. The IKE protocol can use one of two modes: **Main Mode**, which provides identity protection and takes longer, or **Aggressive Mode**, which provides no identity protection but is quicker. With Aggressive Mode, there is no negotiation of which cryptographic parameters will be used; each side must give the correct cryptographic parameters in the initial package of the exchange, otherwise the exchange will fail. If Aggressive Mode is used, the **IKE Encryption**, **IKE Authentication**, and **IKE DH Group** must be specified.
IKE Version	IKE Version settings to be used. Currently the accepted values are IKEv1, IKEv2 and Any. Default is IKEv2. Any uses IKEv2 when initiating but will accept any protocol version while responding. It is recommended that any IKE Encryption or ESP Encryption parameters that are selected be supported by the IKE Version that is used. Refer to the list of IKEv1 and IKEv2 cipher suites for more information.

IKE Encryption	The type of encryption, **3DES**, **AES**, **AES192** or **AES256**, used for IKE negotiation. Any can be selected if the two sides can negotiate which type of encryption to use. ***Note:*** *If IKE Encryption, Authentication and DH Group are set to* ***Any****, default cipher suite(s) will be used. If the console manager acts as an initiator, the tunnel will use a default IKE cipher of aes128-sha256-ecp256 (for IKEv1). For IKEv2 or when the console manager is the responder in tunnel initiation, it will propose a set of cipher suites and will accept the first supported proposal received from the peer.*
IKE Authentication	The type of authentication, **SHA2_256**, **SHA2_384**, **SHA2_512**, **SHA1,** or **MD5**, used for IKE negotiation. **Any** can be selected if the two sides can negotiate which type of authentication to use.
IKE DH Group	The Diffie-Hellman Group, 2 (modp1024), 5 (modp1536), 14 (modp2048), 15 (modp3072), 16 (modp4096), 17 (modp6144), 18 (modp8192) or 19 (ecp256) can be used for IKE negotiation. Any can be selected if the two sides can negotiate which Diffie-Hellman Group to use.

ESP Encryption	The type of encryption, **3DES** , **AES**, **AES192** or **AES256**, used for encrypting the data sent through the tunnel. **Any** can be selected if the two sides can negotiate which type of encryption to use.
	Note: *If ESP Encryption, Authentication and DH Group are set to* ***Any****, default cipher suite(s) will be used. If the console manager acts as an initiator, the tunnel will use a default ESP cipher of aes128-sha256 (for IKEv1). For IKEv2 or when the console manager is the responder in tunnel initiation, it will propose a set of cipher suites and will accept the first supported proposal received from the peer. The proposal sent from the remote peer and the proposal used by the console manager can be viewed in the VPN logs. If there is no match between the two sets of proposals, the tunnel will fail with the message* `no matching proposal found, sending NO_PROPOSAL_CHOSEN`*. If a matching proposal is found, tunnel negotiation will proceed. Below is an example of no matching proposal in the log messages:*
	`charon: 04[CFG] received proposals: ESP:AES_CBC_128/HMAC_SHA2_256_128/ECP_256/ NO_EXT_SEQ`
	`charon: 04[CFG] configured proposals: ESP:AES_CBC_128/AES_CBC_192/ AES_CBC_256/ HMAC_SHA2_256_128/ HMAC_SHA2_384_192/ HMAC_SHA2_512_256/ HMAC_SHA1_96/AES_XCBC_96/ NO_EXT_SE`
	`charon: 04[IKE] no matching proposal found, sending NO_PROPOSAL_CHOSEN`

ESP Authentication	The type of authentication, **SHA2_256**, **SHA2_384**, **SHA2_512**, **SHA2_256_96**, **SHA1,** or **MD5**, used for authenticating data sent through the tunnel. **Any** can be selected if the two sides can negotiate which type of authentication to use.

ESP DH Group	The Diffie-Hellman Group, 2 (modp1024), 5 (modp1536), 14 (modp2048), 15 (modp3072), 16 (modp4096), 17 (modp6144), 18 (modp8192) or 19 (ecp256) can be used for the key exchange for data sent through the tunnel. **Any** can be selected if the two sides can negotiate which Diffie-Hellman Group to use. ***Note:*** *PFS is automatically enabled by configuring ESP Encryption to use a DH Group (ESP Encryption without a DH Group will disable PFS); see Perfect Forward Secrecy below.*
Authentication	The type of authentication used by the host on each side of the VPN tunnel to verify the identity of the other host. ◆ For **RSA Public Key**, each host generates a RSA public-private key pair, and shares its public key with the remote host. The RSA Public Key for the SLC unit (which has 4096 bits) can be viewed at either the web or CLI. ◆ For **Pre-Shared Key**, each host enters the same passphrase to be used for authentication. ◆ For **X.509 Certificate**, each host is configured with a Certificate Authority certificate along with a X.509 certificate with a corresponding private key, and shares the X.509 certificate with the remote host. The following error message appears whenever the X.509 certificate expires: “Expired” Before using RSA Public Key authentication, select **Generate SLC RSA Key** to generate the SLC’s RSA public/private key pair. This RSA key can be regenerated at any time. ***Note:*** *strongSwan does not support IKEv1 aggressive mode with Pre-Shared Key authorization without XAUTH enabled. If a tunnel is initiated with this configuration the log message* `Aggressive Mode PSK disabled for security reasons` *will be displayed, and a tunnel will not be initiated. It is possible to override this behavior, but it is not recommended.*

RSA Public Key for Remote Peer	If **RSA Public Key** is selected for authentication, the remote peer's public key can be uploaded or deleted. If a public key has been uploaded this field will display key installed. The peer RSA public key must be in Privacy Enhanced Mail (PEM) format, e.g.:
	`-----BEGIN PUBLIC KEY-----`
	`(certificate in base64 encoding)`
	`-----END PUBLIC KEY-----`

Pre-Shared Key	If **Pre-Shared Key** is selected for authentication, enter the key.
Retype Pre-Shared Key	If **Pre-Shared Key** is selected for authentication, re-enter the key.

Certificate Authority for Remote Peer
Certificate File for Remote Peer
	A certificate can be uploaded to the SLC unit for peer authentication. The certificate for the remote peer is used to authenticate the SLC to the remote peer, and at a minimum contains the public certificate file of the remote peer. The certificate may also contain a Certificate Authority file; if the Certificate Authority file is omitted, the SLC may display "issuer cacert not found" and "X.509 certificate rejected" messages, but still authenticate. The Certificate Authority file and public certificate File must be in PEM format, e.g.:
	`-----BEGIN CERTIFICATE-----`
	`(certificate in base64 encoding)`
	`-----END CERTIFICATE-----`

Certificate Authority for Local Peer
Certificate File for Local Peer
Key File for Local Peer
	A certificate can be uploaded to the SLC unit for peer authentication. The certificate for the local peer is used to authenticate any remote peer to the SLC, and contains a Certificate Authority file, a public certificate file, and a private key file. The public certificate file can be shared with any remote peer for authentication. The Certificate Authority and public certificate file must be in PEM format, e.g.:
	`-----BEGIN CERTIFICATE-----`
	`(certificate in base64 encoding)`
	`-----END CERTIFICATE-----`
	
	The key file must be in RSA private key file (PKCS#1) format, eg:
	`-----BEGIN RSA PRIVATE KEY-----`
	`(private key in base64 encoding)`
	`-----END RSA PRIVATE KEY-----`

Perfect Forward Secrecy (PFS)	When a new IPSec SA is negotiated after the IPSec SA lifetime expires, a new Diffie-Hellman key exchange can be performed to generate a new session key to be used to encrypt the data being sent through the tunnel. If this is enabled, it provides greater security, since the old session keys are destroyed. **This option is deprecated and is no longer supported.** With strongSwan, PFS is automatically enabled by configuring ESP Encryption to use a DH Group (ESP Encryption without a DH Group will disable PFS). Using PFS introduces no significant performance overhead, unless rekeying is done more than 80 IPsec SAs per second.

SA Lifetime	How long a particular instance of a connection should last, from successful negotiation to expiry, in seconds. Normally, the connection is renegotiated (via the keying channel) before it expires.
	The formula for how frequently rekeying (renegotiation) is done is:
	`rekeytime = lifetime - (margintime + random(0, margintime * rekeyfuzz))`
	where the default **margintime** is 9m (or 540 seconds) and the default **rekeyfuzz** is 100%. For example, if the SA Lifetime is set to 3600 seconds (1 hour), how often the tunnel is rekeyed is calculated as:
	`rekeytime minimum = 1h - (9m + 9m) = 42m rekeytime maximum = 1h - (9m + 0m) = 51m`
	So the rekeying time will vary between 42 minutes and 51 minutes.
	It is recommended that the SA Lifetime be set greater than 540 seconds; any values less than 540 seconds may require adjustments to the margintime and rekeyfuzz values (which can be set with a custom ipsec.conf file). Some peer devices (Cisco, etc) may require that the SA Lifetime be set to a minimum of 3600 seconds in order for the VPN tunnel to come up and rekeying to function properly.
	
	For more information see the strongSwan Expiry documentation.

Mode Configuration Client	If this is enabled, the SLC unit can receive network configuration from the remote host. This allows the remote host to assign an IP address/netmask to the SLC side of the VPN tunnel. **This option is deprecated and is no longer supported.**

XAUTH Client	If this is enabled, the SLC unit will send authentication credentials to the remote host if they are requested. XAUTH, or Extended Authentication, can be used as an additional security measure on top of the Pre-Shared Key or RSA Public Key. This is typically used with Cisco peers, where the Cisco peer is acting as an XAUTH server.
XAUTH Login (Client)	If **XAUTH Client** is enabled, this is the login used for authentication.
XAUTH Password/Retype Password	If **XAUTH Client** is enabled, this is the password used for authentication.
Remote Peer Type	Defines the type of the remote peer, either IETF (non-Cisco) or Cisco. When set to Cisco, support for Cisco IPsec gateway redirection and Cisco obtained DNS and domainname are enabled. **This option is deprecated and is no longer supported.**
Cisco Unity	If enabled, sends the Cisco Unity vendor ID payload (IKEv1 only), indicating that the SLC is acting as a Cisco Unity compliant peer. This indicates to the remote peer that **Mode Config** is supported (an IKE configuration method that is widely adopted, documented here).
Mode Config	In remote access scenarios, it is highly desirable to be able to push configuration information such as the private IP address, a DNS server's IP address, and so forth, to the client. This option defines which mode is used: **pull** where the config is pulled from the peer (the default), or **push** where the config is pushed to the peer. Push mode is not supported with IKEv2.
Force Encapsulation	In some cases, for example when ESP packets are filtered or when a broken IPsec peer does not properly recognise NAT, it can be useful to force RFC-3948 encapsulation.
Dead Peer Detection	Sets the delay (in seconds) between Dead Peer Detection (RFC 3706) keepalives (R_U_THERE, R_U_THERE_ACK) that are sent for the tunnel (default 30 seconds). Dead Peer Detection can also be disabled.
Dead Peer Detection Timeout	Sets the length of time (in seconds) the SLC will idle without hearing either an R_U_THERE poll from the peer, or an R_U_THERE_ACK reply. The default is 120 seconds. After this period has elapsed with no response and no traffic, the SLC will declare the peer dead, remove the Security Association (SA), and perform the action defined by **Dead Peer Detection Action**.
Dead Peer Detection Action	When a Dead Peer Detection enabled peer is declared dead, the action that should be taken. **Hold** (the default) means the tunnel will be put into a hold status. **Clear** means the Security Association (SA) will be cleared. **Restart** means the SA will immediately be renegotiated.

Custom ipsec.conf Configuration	A custom ipsec.conf file can be uploaded to the SLC. This file can include any of the strongSwan options which are not configurable from the UIs. The ipsec.conf file should include one `conn <Tunnel Name>` section which defines the tunnel parameters. An ipsec.conf file containing more than one `conn` section will be rejected for upload. When a custom ipsec.conf file has been uploaded to the console manager, any VPN options configured via the UIs (with the exception of authentication tokens, see below) are ignored, and the UIs will not display the options given in the custom ipsec.conf file. A description of the format of the ipsec.conf file as well as all strongSwan options is available here. The SLC uses strongSwan version 5.6.3, so not all options listed in the strongSwan ipsec.conf documentation will be supported by the SLC. Any authentication tokens (pre-shared keys, RSA keys, X.509 certificates) required by the custom ipsec.conf must be configured through the SLC UIs, and must be configured or installed before a tunnel is brought up with an uploaded ipsec.conf file. When a tunnel is started with a custom ipsec.conf file, the authentication tokens required for the `authby` parameter are verified to exist before the tunnel is started. For example, if `authby=rsasig`, the SLC will verify that the SLC RSA public/private key has been generated and that the peer RSA public key has been uploaded. To upload a custom ipsec.conf file, select the **Upload File** link next to the Uploaded Configuration field. To delete an uploaded custom ipsec.conf file, select the **Delete Configuration File** checkbox next to the Uploaded Configuration field. To view an uploaded custom ipsec.conf file, select the **View Configuration** link next to the Uploaded Configuration field. If a file has been uploaded it will be displayed; otherwise the auto-generated file will be displayed if it exists. The file is auto-generated when a tunnel is enabled (if a custom file has not been uploaded). To download the current in-use ipsec.conf file (either the ipsec.conf file automatically generated by the SLC or an uploaded custom ipsec.conf file), select the **Download Configuration** button. Downloading the ipsec.conf file automatically generated by the SLC is a good starting point for adding extra VPN options; the tunnel must be enabled in order for the SLC to auto-generate an ipsec.conf file that can be downloaded.
Tunnel Restart	If enabled, the watchdog program will automatically restart the VPN tunnel when the tunnel goes down. Initially, when the tunnel goes down, it will be restarted immediately. However, after the first restart, if the tunnel still fails to come up, the watchdog program will try to restart the tunnel periodically every X seconds, where X is the Dead Peer Detection Timeout plus 60 seconds, until the tunnel comes back up.
Email Address	Email address to receive email alerts when the tunnel goes up or down.

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

More Actions on the VPN page:

- To see details of the VPN tunnel connection, including the cryptographic algorithms used, select the **View Detailed Status** link.
- To see the last 200 lines of the logs associated with the VPN tunnel, select the **View VPN Logs** link.

- To see the RSA public key for the SLC unit (required for configuring the remote host if RSA Public Keys are being used), and the RSA public key for the remote peer, select the **View console manager and Remote Peer RSA Public Key** link.
- To see the X.509 Certificates for the local peer and the remote peer, select the **View X.509 Certificates** link.

Sample ipsec.conf Files

Sample ipsec.conf files are provided for a variety of tunnel setups and peers. In all examples, any left options are for the console manager/local side of the tunnel, and any right options are for the remote side of the tunnel.

- Cisco Pre-Shared Key / XAUTH / MODECFG / IKEv1
- Cisco ASA5525x Pre-Shared Key / IKEv1
- Cisco ASA5525x Pre-Shared Key / IKEv2
- Cisco ISR 2921 Pre-Shared Key / XAUTH / IKEv2

Cisco Pre-Shared Key / XAUTH / MODECFG / IKEv1

This configuration is an example of a remote access connection to a Cisco VPN server / responder that uses XAUTH and MODECFG to authenticate and push dynamic IP addresses and DNS servers to a VPN client. The use of aggressive mode requires that **ike** and **esp** algorithms be specified and exactly match what the Cisco server is expecting.

Console manager configuration

The pre-shared key and the XAUTH password need to be configured via the console manager UI.

```
conn Cisco
  keyexchange=ikev1
  ike=3des-md5-modp1024!
  esp=3des-md5-modp1024!
  aggressive=yes
  lifetime=28800s
  forceencaps=no
  authby=xauthpsk
  left=10.0.1.55
  leftsourceip=%config4
  leftid=@vpnid
  xauth=client
  xauth_identity=username
  modeconfig=pull
  right=220.41.123.45
  rightsubnet=0.0.0.0/0
  dpddelay=30
  dpdtimeout=120
  dpdaction=hold
  auto=start
  type=tunnel
```

Cisco ASA5525x Pre-Shared Key / IKEv1

This configuration is an example of a remote access connection to a Cisco ASA5525 VPN server / responder.

Console manager configuration

The pre-shared key needs to be configured via the console manager UI.

```
conn ASA5525
  keyexchange=ikev1
  ike=aes-sha1-modp1536!
  esp=aes-sha1-modp1536!
  aggressive=yes
  lifetime=86400s
  forceencaps=no
  authby=secret
  left=%any
  leftsubnet=192.168.0.0/24
  modeconfig=pull
  right=192.168.1.130
  rightsubnet=192.168.3.0/24
  dpddelay=10
  dpdtimeout=5
  dpdaction=restart
  auto=start
  type=tunnel
```

Cisco configuration

Note: *Main or aggressive mode is determined by the SLC side of the tunnel, and does not require any change in the Cisco configuration:*

```
interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address 192.168.1.130 255.255.255.0

interface GigabitEthernet0/3
  nameif inside security-level 100
  ip address 192.168.3.130 255.255.255.0

object-group network local-network
  network-object 192.168.3.0 255.255.255.0
object-group network remote-network
  network-object 192.168.0.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network

route outside 192.168.0.0 255.255.255.0 192.168.1.204 1
route inside 192.168.3.250 255.255.255.255 192.168.3.250 1

crypto ipsec ikev1 transform-set ipsecvpn esp-aes esp-sha-hmac
```

```
crypto ipsec security-association pmtu-aging infinite

crypto map site2site 10
  match address asa-router-vpn
  set pfs group5
  set peer 192.168.1.204
  set ikev1 transform-set ipsecvpn
crypto map site2site interface outside

crypto ikev1 enable outside
crypto ikev1 policy 10
  authentication pre-share encryption aes
  hash sha
  group 5
  lifetime 86400

tunnel-group 192.168.1.204 type ipsec-l2l
tunnel-group 192.168.1.204 ipsec-attributes
 ikev1 pre-shared-key *****
```

Cisco ASA5525x Pre-Shared Key / IKEv2

This configuration is an example of a remote access connection to a Cisco ASA5525 VPN server / responder. The aggressive setting can be either **yes** or **no**; the Cisco ASA will honor the peer configuration.

Console manager configuration

The pre-shared key needs to be configured via the console manager UI.

```
conn ASA5525
  keyexchange=ikev2
  ike=3des-sha2_256-modp1536!
  esp=3des-sha2_256-modp1536!
  aggressive=no
  lifetime=86400s
  forceencaps=no
  authby=secret
  left=%any
  leftsubnet=192.168.0.0/24
  modeconfig=pull
  right=192.168.1.130
  rightsubnet=192.168.3.0/24
  dpddelay=0
  dpdtimeout=5
  dpdaction=restart
  auto=start
  type=tunnel
```

Cisco configuration

```
interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address 192.168.1.130 255.255.255.0

interface GigabitEthernet0/3
  nameif inside security-level 100
  ip address 192.168.3.130 255.255.255.0

object-group network local-network
  network-object 192.168.3.0 255.255.255.0
  network-object 192.168.3.250 255.255.255.255 ikev2 local-
authentication pre-shared-key
object-group network remote-network
  network-object 192.168.0.0 255.255.255.0
  network-object 192.168.0.222 255.255.255.255

access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
access-list ASA-SLC-ACCESS extended permit ip object-group local-network
object-group remote-network

route outside 192.168.0.0 255.255.255.0 192.168.1.204 1
route inside 192.168.3.250 255.255.255.255 192.168.3.250 1

crypto ipsec ikev2 ipsec-proposal IPSECv2
  protocol esp encryption 3des
  protocol esp integrity sha-256
crypto ipsec security-association pmtu-aging infinite

crypto map CM 20
  match address ASA-SLC-ACCESS
  set pfs group5
  set peer 192.168.1.204
  set ikev2 ipsec-proposal IPSECv2
crypto map CM interface outside

crypto ikev2 policy 20
  encryption 3des integrity sha256
  group 5
  prf sha256
  lifetime seconds 86400
crypto ikev2 enable outside

tunnel-group 192.168.1.204 type ipsec-l2l
tunnel-group 192.168.1.204 ipsec-attributes
  ikev2 remote-authentication pre-shared-key *****
  ikev2 local-authentication pre-shared-key *****
```

Cisco ISR 2921 Pre-Shared Key / XAUTH / IKEv2

This configuration is an example of a remote access connection to a Cisco ISR2921 VPN server / responder.

Console manager configuration

The pre-shared key needs to be configured via the console manager UI.

```
conn ISR2921
  keyexchange=ikev2
  ike=aes-sha2_384-modp1536!
  esp=3des-sha2_384-!
  aggressive=no
  lifetime=86400s
  forceencaps=no
  authby=secret
  left=%any
  leftsubnet=192.168.0.0/24
  modeconfig=pull
  right=192.168.1.102
  rightsubnet=192.168.2.0/24
  dpddelay=0
  dpdtimeout=120
  dpdaction=restart
  auto=start
  type=tunnel
```

Cisco configuration

```
crypto ikev2 proposal PROP
  encryption aes-cbc-128
  integrity sha256
  group 2
crypto ikev2 policy ikev2policy
  proposal PROP
crypto ikev2 keyring KEYRING
  peer ALL
  address 0.0.0.0 0.0.0.0
  pre-shared-key local cisco123
  pre-shared-key remote cisco123

crypto ikev2 profile IKEv2_Profile
  match identity remote address 192.168.1.100 255.255.255.0
  identity local address 192.168.1.102
  authentication remote pre-share
  authentication local pre-share
  keyring local KEYRING

crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
```

```
crypto isakmp policy 5
  encr 3des
  authentication pre-share
  group 5

crypto isakmp policy 10
  lifetime 120
crypto isakmp key cisco123 address 192.168.1.100

crypto ipsec transform-set ISR esp-3des esp-sha384-hmac
  mode tunnel

crypto map CM 10 ipsec-isakmp
  set peer 192.168.1.100
  set transform-set ISR
  set ikev2-profile IKEv2_Profile
  match address VPN-TRAFFIC

crypto map IPSEC-SITE-TO-SITE 10 ipsec-isakmp
  set peer 192.168.1.100
  set transform-set ISR
  set pfs group2
  match address VPN-TRAFFIC
```

VPN Commands

Go to *VPN Commands* to view CLI commands which correspond to the web page entries described above.

Security

The console manager supports a security mode that is FIPS-like but not FIPS certified. FIPS (Federal Information Processing Standard) 140-2 is a security standard developed by the United States federal government that defines rules, regulations and standards for the use of encryption and cryptographic services. The National Institute of Standards and Technology (NIST) maintains the documents related to FIPS at: http://csrc.nist.gov/publications/PubsFIPS.html. The FIPS 140-2 standard is available at: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

FIPS 140-2 defines four security levels, Level 1 through Level 4. The console manager can be placed into a FIPS mode which behaves the same as the SLC 8000 FIPS mode, but is not FIPS certified. FIPS 140-2 compliance requires a defined cryptographic boundary around the cryptographic module on a device. In FIPS mode, the console manager allows only FIPS-approved cryptographic algorithms to be used, and weak algorithms (such as MD5 and DES) are disabled.

To enable FIPS mode, the Network -> Security -> FIPS Mode flag needs to be enabled and the console manager rebooted. Each time a FIPS application is started, it will perform a power up self test to verify the integrity of the console manager's cryptographic module. If there are any issues with the integrity of the cryptographic module, the application will terminate and an error will be logged in the system log.

When the console manager is running in FIPS mode, the services listed below will be supported:

TLS/SSL (Web Server, WebSSH): the TLS ciphers for incoming TLS/SSL connections will be configured to a FIPS-approved set when booting into FIPS mode. SSL/secure certificates imported for use with the web server must use a RSA public key with 2048, 3072 or 4096 bits with the SHA2 hashing algorithm.

LDAP: SSL/secure certificates imported for use with LDAP authentication must use a RSA public key with 2048, 3072 or 4096 bits with the SHA2 hashing algorithm. Encryption with StartTLS or SSL encryption over port 636 (the default) or another port is required. If the console manager is booted in FIPS mode with insecure LDAP settings, LDAP will automatically be disabled.

SSH (connections in and out of the console manager, including WebSSH): DSA keys cannot be used, and SSH algorithms for incoming SSH connections will be configured to a FIPS-approved set when booting into FIPS mode. SSH Keys imported for use with SSH authentication (e.g. public key cryptography or asymmetric cryptography) must use a RSA public key of 2048, 3072 or 4096 bits, with the SHA2 hashing algorithm. SSH Keys exported by the console manager use a RSA public key of 2048, 3072 or 4096 bits, with the SHA2 (SHA256) hashing algorithm. Insecure SSH Keys will be automatically removed when booting into FIPS mode. SSH authentication will be enabled on all device ports.

SNMP: only SNMPv3 can be used, and insecure algorithms (DES, MD5, SHA1) cannot be used. The Security setting must be set to Auth/Encrypt (No Auth and No Encrypt cannot be used). If the console manager is booted in FIPS mode with insecure SNMP settings, SNMP will automatically be disabled.

VPN: insecure algorithms (MD5, SHA1, DH Group 2, DH Group 5) cannot be used. If the console manager is booted in FIPS mode with insecure VPN settings, the VPN tunnel will automatically be disabled.

WiFi: the access point cannot use security of None (WPA or WPA2 is required). The WLAN client cannot use a security suite of None or WEP (WPA-WPA2 mixed mode is required). WLAN profiles are required to use an encryption algorithm of CCMP. If the console manager is booted in FIPS mode with insecure access point settings or WLAN profile settings, the access point or WLAN profile will be disabled.

Percepxion: supported in FIPS mode. No additional configuration required; the Percepxion client automatically uses FIPS-approved TLS ciphers when FIPS mode is enabled.

When the console manager is running in FIPS mode, the following services will not be supported: RADIUS, TACACS+, Telnet, FTP, PPP, Email (SMTP), TCP, UDP, and unencrypted LDAP. If any of these protocols/functions are enabled prior to enabling FIPS mode, they will be automatically disabled.

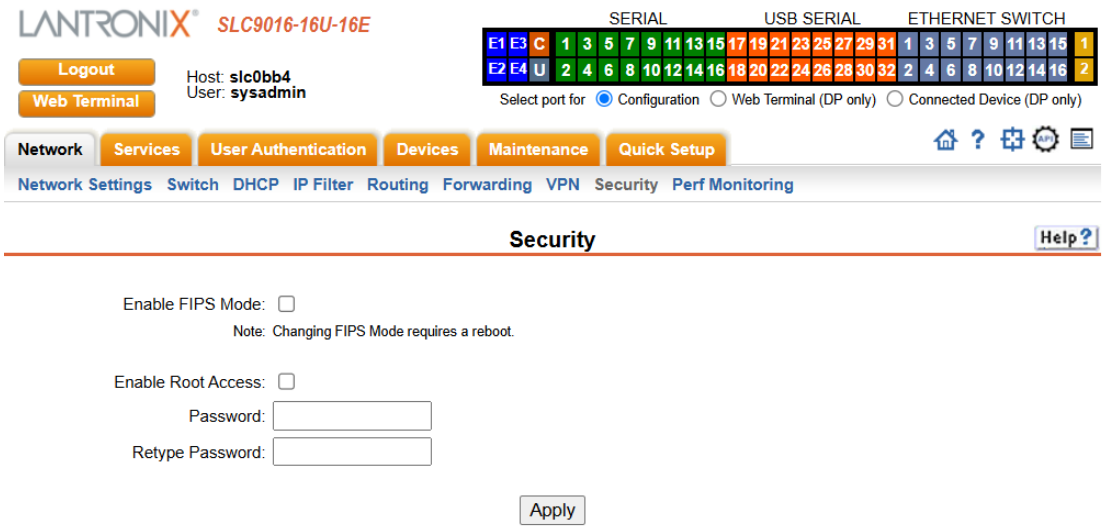
The following table shows the algorithms allowed in FIPS mode and how they are used:

Algorithm	Usage	Key Sizes
AES (CBC, CCM, CFB, CTR, ECB, GCM, OFB, XTS)	Symmetric encryption & decryption	128/192/256 bit key lengths
AES CMAC	Generate & verify data integrity with CMAC	128/192/256 bit key lengths
TDES / 3-Key (CBC, CFB, ECB, OFB)	Symmetric encryption & decryption	112/168 bits key length
TDES / 3-Key CMAC	Message Digests	112/168 bits key length
SHA2	Keyed Hash & Message Digests	224/256/384/512 bits key lengths

Algorithm	Usage	Key Sizes
RSA	Digital Signature and Asymmetric Key Generation	2048 bit key length and longer, with SHA2 with 256-bit to 512-bit key lengths
Diffie-Hellman (DH)	Key Agreement / Exchange	2048 bit key lengths and longer
Elliptic Curve Cryptography (ECC)	Key Agreement / Exchange	All NIST defined B, K and P curves except sizes 163 and 192
Elliptic Curve Diffie-Hellman (ECDH); key agreement algorithm that is a variant of Diffie-Hellman using ECC	Key Agreement / Exchange	224-521 bits
Elliptic Curve Digital Signature Algorithm (ECDSA); digital signature algorithm that is a variant of DSA using ECC	Digital Signature Key Generation	224-521 bits
Hash DRBG	Random number generator	V (440/888 bits) and C (440/888) bits
HMAC DRBG	Random number generator	V (160/224/256/384/512 bits) and Key (160/224/256/384/512 bits)
CTR DRBG (AES)	Random number generator	V (128 bits) and Key (AES 128/192/256 bits)

To enable FIPS:

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



1. Check the **Enable FIPS Mode** check box.
2. Click **Apply**. The console manager will need to be rebooted to initiate FIPS mode. Once the console manager is running in FIPS mode, the Security page will display all processes that are running in FIPS mode.

To disable FIPS:

1. Uncheck the **Enable FIPS Mode** check box.

2. Click **Apply**. The console manager will need to be rebooted for this change to take effect.

Performance Monitoring

The SLC supports Performance Monitoring probes for analyzing network performance. Probes for DNS Lookup, HTTP Get, ICMP Echo, TCP Connect, UDP Jitter and UDP Jitter VoIP are supported. Up to 15 different probes can be configured. Each probe will run a series of operations, each of which sends a series of packets to a destination host. The SLC will measure how long it took to receive a response, and record the results. For each operation, the user can view the results for each packet (round trip times), or the accumulated statistics for all packets - minimum, average and maximum latency, and for jitter probes, minimum, average, maximum and standard deviation of the jitter delay. Dropped packets and other error conditions are recorded for each operation. This capability allows an administrator to analyze network efficiency across the network.

An operation consists of sending a specified number of packets to a destination host and optional port, with a specified amount of time between each packet. All results for each operation are stored in one data file, and the results can be viewed later. Accumulated statistics can also be pulled from the SLC via SNMP Gets.

Repository and Operations Kept: The SLC can be configured to store probe results on the local SLC storage, or an external USB thumb drive. The number of operations that can be stored per probe on the local SLC storage is 50 operations; for external USB thumb drive, 200 operations can be stored per probe.

Responders: The SLC can act as a responder for probes that require a responder to answer packets that are sent from the SLC (UDP jitter, UDP jitter VoIP, UDP Echo and TCP Connect). The SLC UDP jitter responder can support packet responses for up to 15 UDP jitter or UDP jitter VoIP probes. The UDP Echo and TCP Connect can support packets responses for one UDP Echo or TCP Connect probe.

Jitter Probes and Clock Skew: For jitter probes, it is important to have both the sender and responder synchronized to a reliable NTP server. Significant clock skew can greatly affect jitter results, as timestamps are recorded in the sender probe and the responder, and these timestamps are used to measure one-way latency for the packets. At the start of each jitter operation, the clock skew between the sender and the responder will be output to the system log.

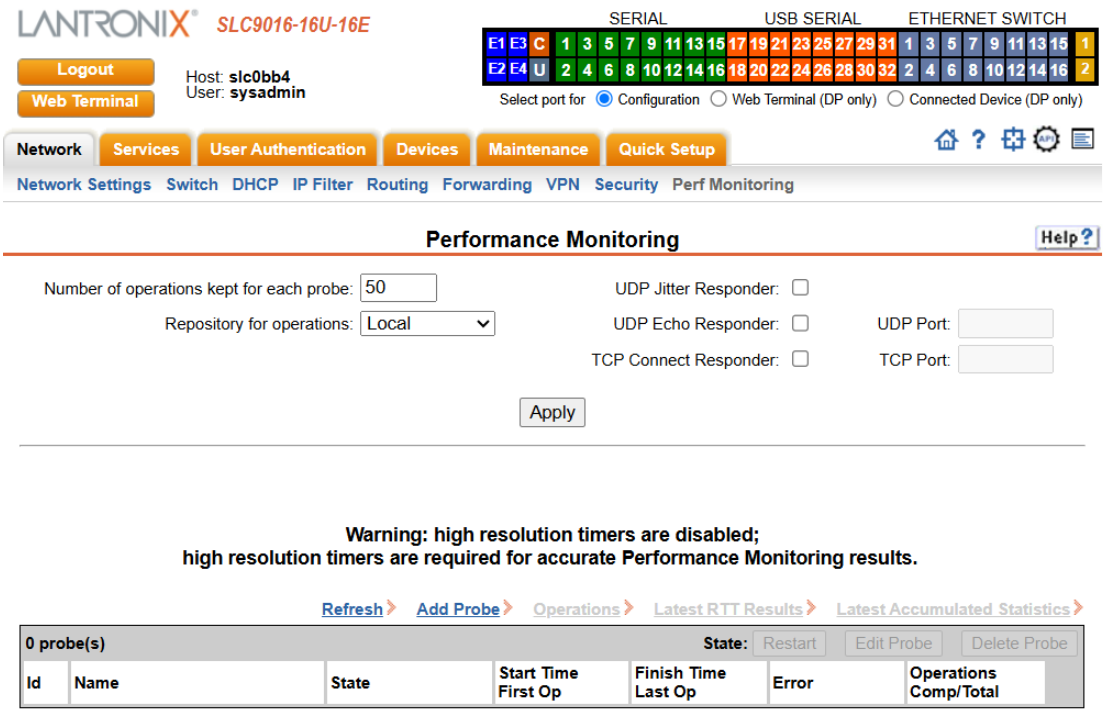
Compatibility with Cisco Responders: The SLC Performance Monitor sender is compatible with Cisco IP SLA responders (IOS versions 12.2 and 15.0) for jitter probes. The SLC uses a simplified version of the IP SLA v2 (Engine II) protocol to communicate with the Cisco IP SLA responders. This compatibility gives the administrator a large number of devices with which to measure network performance.

High Resolution Timers: Performance Monitoring requires that high resolution timers be enabled in order to generate accurate results down to the microsecond. The high resolution timers are disabled by default, and can be enabled on the *Maintenance > Firmware & Configurations* web page. A reboot is required if the setting is changed. Enabling high resolution timers may affect SLC performance.

To manage or view status for a Performance Monitoring probe:

1. Click the **Network** tab and select the **Perf Monitoring** option. The following page displays.

Figure 6-11 Network > Perf Monitoring



2. In the upper section of the page, modify the global Performance Monitoring settings:

Number of operations kept for each probe	Specifies the number of operation set files to keep for each probe. The limit for Local storage is 50 sets. The limit for external (USB) is 200 sets. While a probe is running, the operation set files will be automatically culled to remove the oldest operation set files.
Repository for operations	The repository where the operation set files will be kept - **Local** storage, a USB thumb drive inserted in the upper **USB Port U1** or lower **USB Port U2.** The data is stored in individual directories under a directory called "perfmon". Once probes have been run and operation set files have been generated, changing the repository will cause all of the existing files to be moved from the old repository directory to the new repository directory. It is recommended that the repository only be changed when probes are not actively running. If external storage is used for the repository, it is recommended that the external storage device not be removed from the SLC while probes are actively running.
UDP Jitter Responder	Starts the UDP Jitter responder to reply to UDP jitter or UDP jitter VoIP packets. The responder will listen on UDP port 1967 for control messages requesting to start individual responders on a specific UDP port. The SLC UDP jitter responder can support up to 15 UDP jitter senders.
UDP Echo Responder	Starts the UDP Echo responder on the port configured in **UDP Port** to reply to UDP echo packets. The SLC UDP Echo responder supports one UDP echo sender. When the UDP Echo responder is enabled, the SLC will verify that the responder UDP port is not being used by any other SLC processes, including port 1967 which is reserved for the UDP Jitter responder.

TCP Connect Responder	Starts the TCP Connect responder on the port configured in **TCP Port** to reply to TCP connect requests. The SLC TCP Connect responder supports one TCP connect sender. When the TCP Connect responder is enabled, the SLC will verify that the responder TCP port is not being used by any other SLC processes.

3. Click the **Apply** button.
4. In the lower section of the page, select a probe by clicking the radio button to the far right in the probe's row. The options that are available for that probe will be ungreyed. Select one of the following options:

Refresh	Refreshes the information on the Performance Monitoring page.
Add Probe	Displays the *Performance Monitoring - Add/Edit Probe* web page to add a new probe.
Operations	Displays a list of completed operations for the selected probe and allows the user to view either raw packet results or accumulated statistics for any operation.
Latest Results	Displays the latest raw packet results for the selected probe.
Latest Accumulated	Displays the latest accumulated statistics for the selected probe.
State: Restart	Allows the state of a probe to be controlled: the user can Restart a completed or running probe. When a probe is added, it will automatically start running, depending on how the probe start time is configured. Once a probe has run all of its configured operations, it will be in the "Complete" state. If the SLC is rebooted, all probes will automatically be restarted.
Edit Probe	Displays the *Performance Monitoring - Add/Edit Probe* web page to edit the currently selected probe.
Delete	Deletes the selected probe, after a confirmation.

The table at the bottom of the page lists information about completed and running probes.

Id	Unique identifier for the probe.
Name	Name assigned to the probe.
State	The current state of the probe: Complete if all operations have been run, or Running if there are still operations that need to be run.
Start Time First Op	The date and time that the first operation started.
Finish Time Last Op	The date time that the most recently completed operation finished.
Error	Any errors reported by the probe: ◆ NMT: the current repository is an external source, but the USB thumb drive is not mounted ◆ NDR: the repository directory for the probe does not exist ◆ OPF: failed to open an operation data file ◆ SCT: error initializing a socket ◆ CFG: error retrieving probe configuration ◆ EXP: probe start time has expired
Operations Comp/ Total	The number of operations that have been completed and the total number of operations that will be run.

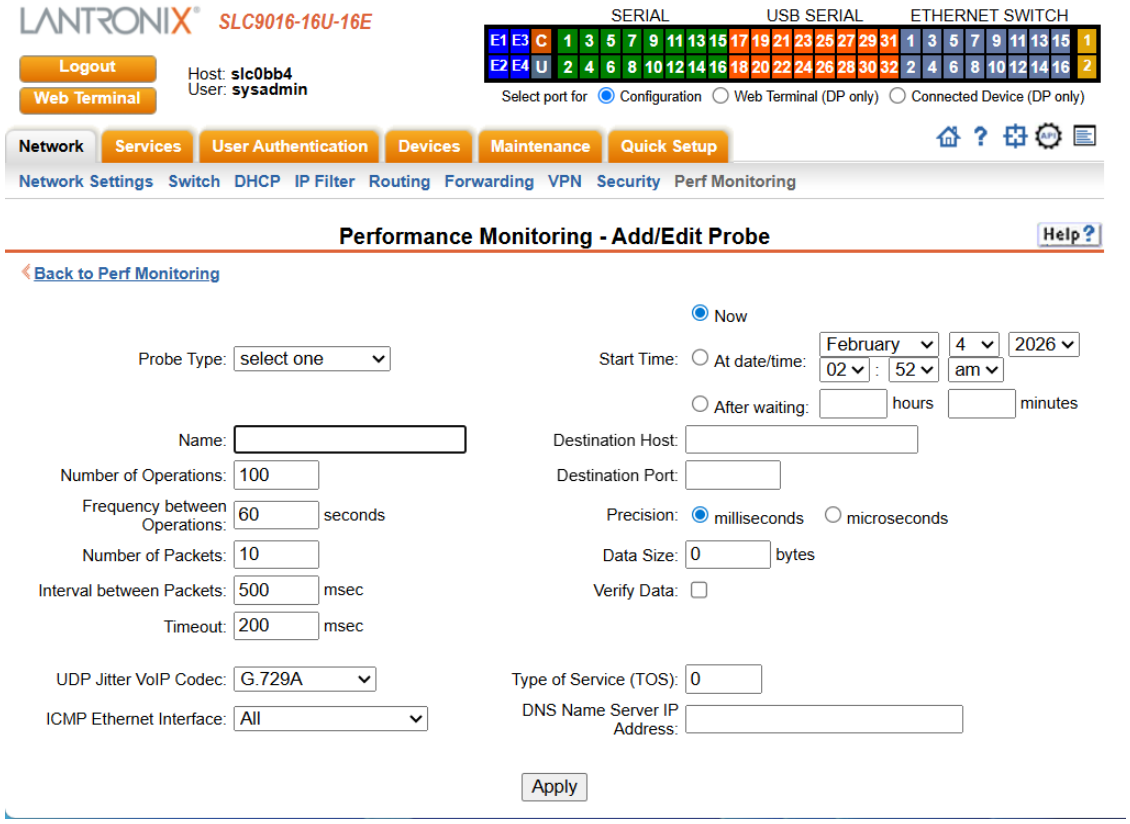
Performance Monitoring - Add/Edit Probe

The *Performance Monitoring - Add/Edit Probe* web page allows a user to add a new Performance Monitoring probe or edit an existing Performance Monitoring probe.

To add a new probe or edit an existing probe:

1. Click the **Network** tab and select the Perf Monitoring option. The *Network > Perf Monitoring* page displays.
2. To add a new probe, in the lower section of the page, select the **Add Probe** link. To edit an existing probe, select a probe by clicking the radio button to the right in the probe's row, then select the **Edit Probe** button. In both cases, the following page displays.

Figure 6-12 Performance Monitoring - Add/Edit Probe



3. Modify the probe settings:

Probe Type	Select from one of the available probe types: ◆ **DNS Lookup -** Performs a DNS lookup on the hostname specified in the Destination Host using the Name Server. By default port 53 is always used as the Destination Port. ◆ **HTTP Get -** Performs an HTTP Get to the home (root) of the web server at the Destination Host and Destination Port. ◆ **ICMP Echo -** Sends ICMP Echo (ping) packets to the Destination Host. ◆ **TCP Connect -** Performs a TCP Connection to the Destination Host and Destination Port. ◆ **UDP Echo -** Sends UDP Echo packets to the Destination Host and Destination Port. ◆ **UDP Jitter -** Sends UDP jitter packets using a simplified version of the Cisco IP SLA v2 (Engine II) protocol to the Destination Host and Destination Port. ◆ **UDP Jitter VoIP -** Sends UDP jitter packets configured to simulate Voice over IP network traffic (VoIP) using a simplified version of the Cisco IP SLA v2 (Engine II) protocol to the Destination Host and Destination Port.
Name	Probe name, up to 40 characters long. Valid characters are letters, numbers, dashes (-), periods and underscores (_).
Number of Operations	Number of operations to perform for the probe. Probes can for a specific number of operations. The valid range is 1 - 1000, and the default is 100.
Frequency between Operations	Time between probe operations, in seconds. The valid range is 5 - 3600 seconds, and the default is 60 seconds.
Number of Packets	Number of packets to send for each probe. For DNS Lookup probes, this is the number of lookups to perform. For HTTP Get probes, this is the number of HTTP Gets to perform. For TCP Connect probes, this is the number of TCP connections to perform. The valid range is 1 - 1000 for the Local repository and 1 - 2000 for a USB repository. The default is 10 packets.
Interval between Packets	Interval between packets in milliseconds. The valid range is 10 - 5000 milliseconds, and the default is 500 milliseconds. For HTTP Get, DNS Lookup and TCP Connect probes, the timeout must be less than the interval due to a new socket being created and destroyed for each packet.
Start Time	Time to start the probe: **Now** starts the probe immediately; **At date/time** will start the probe at the specified date and time in the future; **After waiting** will start the probe after waiting a period of time that is less than 24 hours. When the SLC is rebooted, the probe will start according to the **Start Time** settings: (a) immediately if it set to **Now**, (b) at a date and time in the future if it is set to **At date/time** and the date and time is in the future, (c) after waiting a period of time if it is set to **After waiting**.
Destination Host	The hostname or IP address to send packets to. For DNS Lookup probes this is the hostname to lookup.
Destination Port	The TCP or UDP port to send packets to. For ICMP probes, the port setting is not used. For DNS Lookup probes, the destination port is always port 53. Port 1967 is reserved for the UDP jitter responder. The valid range is 1 - 65535.
Precision	The precision to view results in - milliseconds (the default) or microseconds. Jitter results are always displayed in milliseconds.

Data Size	The size in bytes to use for the payload portion of the packet - this size is in addition to the IPv4 header and the TCP, UDP or ICMP header. Any additional space in the packet that is not used by the protocol will be padded with random data that can be used for data verification (see below). This parameter is only supported for ICMP Echo, TCP Connect, UDP Echo, UDP Jitter, and UDP Jitter VoIP probes. The maximum payload for any probe is 1460 bytes. The minimum payload size for probes is: UDP Jitter VoIP G.729a codec probes - 32 bytes; all other UDP Jitter probes - 64 bytes; ICMP Echo probes - 18 bytes; TCP Connect probes - 1 bytes; UDP Echo probes - 4 bytes. If no data size is specified (e.g., it is set to zero), a default payload size will be used for the probes as follows: ◆ **ICMP Echo** - 56 bytes ◆ **UDP Jitter VoIP G.729A** - 32 bytes ◆ **UDP Jitter (all others)** - 64 bytes ◆ **TCP Connect and UDP Echo** - 256 bytes
Verify Data	If enabled, indicates that the SLC should verify if there is data corruption in the reply packets. This parameter is only supported for ICMP Echo, UDP Echo, UDP Jitter, and UDP Jitter VoIP probes.
Timeout	How long the SLC will wait for a packet to arrive, in milliseconds. If the packet arrives after the timeout it will be considered a Late Arrival error (see *Table 6-13 Error Conditions*). The valid range is 10 - 1000, and the default is 200 msec.
UDP Jitter VoIP Codec	For UDP Jitter VoIP probes, the codec to simulate. The following codecs are available: ◆ **G.729A -** 32 byte packets sent 20 msec apart, 1000 packets per operation, 60 seconds between operations ◆ **G.711 A-law -** 172 byte packets sent 20 msec apart, 1000 packets per operation, 60 seconds between operations ◆ **G.711 mu-law -** 172 byte packets sent 20 msec apart, 1000 packets per operation, 60 seconds between operations The default values for the VoIP probes can be overridden to use different packet sizes, intervals, etc.
ICMP Ethernet Interface	For ICMP Echo probes, which Ethernet interface can be used for the probe: both interfaces, Ethernet Port 1, Ethernet Port 2, SFP Ethernet Port 3, or SFP Ethernet Port 4.
TOS (Type of Service)	Sets the IPv4 Type of Service field in the IPv4 header. This is available for UDP Jitter and UDP Jitter VoIP probes only. The range is 0 - 255, and the default value is 0.
DNS Name Server IP Address	For DNS Lookup probes, the IP address of the DNS name server to use for lookups.

4. Click the **Apply** button.

Performance Monitoring - Results

The Performance Monitoring - Operations page displays all of the operations that have been saved for a selected probe. The probe ID and name are shown at the top of the web page. From this page, the user may select any operation to view its round trip time (RTT) results, or the accumulated statistics for all round trip times in an operation.

An operation consists of sending a specified number of packets to a destination host and optional port, with a specified amount of time between each packet. All results for each operation are stored in one data file.

Round Trip Times

The results for each packet in an operation can be displayed with the **RTT Results** link. Each packet will be displayed with the packet start time and any error that resulted from sending the packet. For non-jitter probes, the total round trip time is displayed in either milliseconds or microseconds, depending on the probe's precision setting:

```
Probe 6/icmp-probe, operation icmp_260627_235709.dat:
Pkt  Time                    RT Time        Result
  1  26-06-27 23:57:09.171       0.419 ms  OK
  2  26-06-27 23:57:09.211       0.378 ms  OK
  3  26-06-27 23:57:09.251       0.366 ms  OK
  4  26-06-27 23:57:09.291       0.354 ms  OK
  5  26-06-27 23:57:09.332       0.448 ms  OK
  6  26-06-27 23:57:09.372       0.382 ms  OK
  7  26-06-27 23:57:09.412       0.308 ms  OK
  8  26-06-27 23:57:09.452       0.334 ms  OK
  9  26-06-27 23:57:09.492       0.365 ms  OK
 10  26-06-27 23:57:09.532       0.361 ms  OK
```

For jitter probes, the source to destination and destination times are displayed in the probe's configured precision:

```
Probe 7/udp-jitter-probe, operation udpjitter_260628_002049.dat:
Pkt  Time                    Src To Dst Time  Dst To Src Time  Result
 1  26-06-28 00:20:49.621      31029 usec       44191 usec  OK
 2  26-06-28 00:20:49.717      35409 usec       44170 usec  OK
 3  26-06-28 00:20:49.808      35558 usec       34120 usec  OK
 4  26-06-28 00:20:49.898      25500 usec       34175 usec  OK
 5  26-06-28 00:20:49.988      35210 usec       34196 usec  OK
 6  26-06-28 00:20:50.079      25517 usec       34177 usec  OK
 7  26-06-28 00:20:50.169      35210 usec       54166 usec  Late Arrival
 8  26-06-28 00:20:50.259      25549 usec       34170 usec  OK
 9  26-06-28 00:20:50.350      25313 usec       34255 usec  OK
10  26-06-28 00:20:50.440      24848 usec       34351 usec  OK
```

Accumulated Statistics

A summary of all round trip time and any error conditions is displayed. The display will vary for non-jitter and jitter results. For example, non-jitter accumulated results will show:

```
Probe 6/icmp-probe, operation icmp_260627_235709.dat:
Operation Type:
    ICMP Echo to 10.0.1.162, Ethernet Port: both
    30 packets sent 40 ms apart, timeout 1000 ms
Operation Start Time: 26-06-27 23:57:09.171
Last Packet RTT: 0.340 msec
Round Trip Time Results:
    Number of RTT: 30
    RTT Min/Avg/Max: 0.306/0.362/0.448 msec
Number of Successes: 30
Number of Errors: 0
    Lost Packet: 0 (0%)
    Out of Sequence: 0
    Late Arrival: 0
    Miscellaneous Error: 0
```

For jitter probes, positive (increasing latency) and negative (decreasing latency) statistics are shown, as well as the number of positive or negative jitter samples in each direction, and the sum and (and sum squared) of the positive or negative jitter times. These numbers give a summary of how much variation there was in latency times and if the variation was small or large.

```
Probe 7/udp-jitter-probe, operation udpjitter_260628_002049.dat:
Operation Type:
    UDP Jitter to 10.0.1.93:50505
    50 packets sent 60 ms apart, timeout 1000 msec
Operation Start Time: 26-06-28 00:20:49.071
Last Packet RTT: 69.334 msec
Round Trip Time Results:
    Number of RTT: 50
    RTT Min/Avg/Max: 57.327/63.863/89.376 msec
One-way Latency Results:
    Number of samples: 50
    Source to Destination Min/Avg/Max: 23.174/27.467/45.206 msec
    Destination to Source Min/Avg/Max: 34.068/36.396/54.166 msec
Jitter, Source to Destination:
    Number of Samples: 49
    Positive and Negative Min/Avg/Max: 1/4/20 msec
    Positive Min/Avg/Max: 1/7/20 msec
    Positive Number Of/Sum of All/Sum of All Squared: 13/100/1090 msec
    Negative Min/Avg/Max: 1/5/20 msec
    Negative Number Of/Sum of All/Sum of All Squared: 17/96/1018 msec
Jitter, Destination to Source:
    Number of Samples: 49
    Positive and Negative Min/Avg/Max: 10/3/20 msec
    Positive Min/Avg/Max: 10/12/20 msec
    Positive Number Of/Sum of All/Sum of All Squared: 7/90/1300 msec
    Negative Min/Avg/Max: 10/12/20 msec
    Negative Number Of/Sum of All/Sum of All Squared: 8/100/1400 msec
Number of Successes: 49
Number of Errors: 1
    Lost Packet: 0 (0%)
    Out of Sequence: 0
    Late Arrival: 1
    Miscellaneous Error: 0
```

Table 6-13 Error Conditions

The following error conditions are detected by the probes. Except where noted, the RTT results for a packet with errors will not be counted in the accumulated statistics.

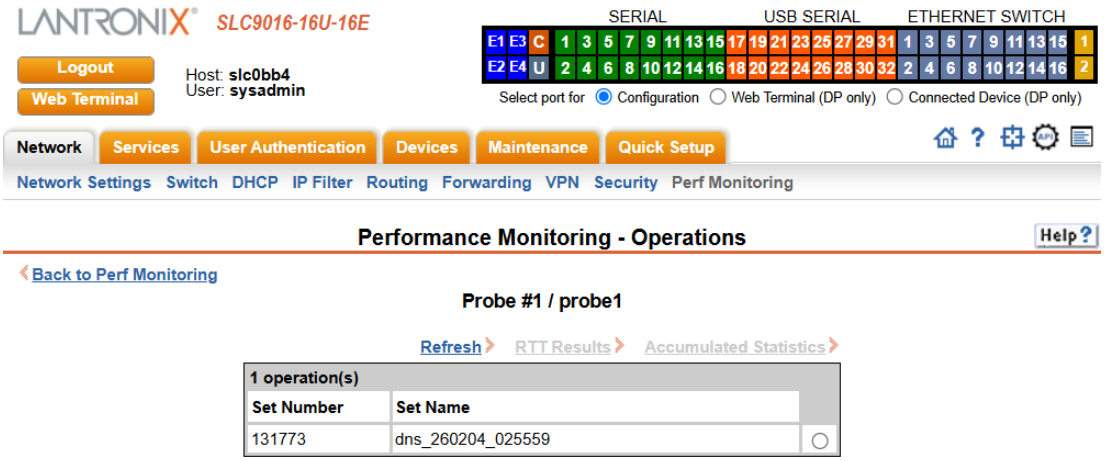
Error Condition	Description
Timeout	A response was never received for the packet. These packets are listed as Lost Packets under the accumulated statistics.
Late Arrival	A response was received for a packet, but the response was received after the timeout configured for the probe. The SLC will wait at most 2 times the probe's timeout for late arrival packets. The RTT results will be included in the accumulated statistics.

Error Condition	Description
Not Connected	A packet could not be sent because the connection to the destination host could not be established, or because the attempt to send the packet failed.
Sequence Error	A packet response was received with an unexpected sequence number. Possible reasons are: a duplicate packet was received, a response was received after it timed out, a corrupted packet was received and was not detected.
Verify Data Error	A response was received for a packet with payload data that does not match the expected data.
DNS Server Timeout	A DNS lookup could not be completed because the SLC could not connect to the DNS name server.
DNS Lookup Error	A DNS lookup failed - the requested hostname could not be resolved. This is not considered a protocol error, but rather an expected result, depending on the hostname being resolved. The RTT results will be included in the accumulated statistics.
TCP Connect Timeout	A TCP connect could not be completed because a connection to the TCP server could not be established.
HTTP Transaction Timeout	An HTTP Get that failed because no response was received from the HTTP server before the timeout expired.
HTTP Error	An HTTP Get succeeded, but the HTTP content (base page) that was downloaded had errors: missing "HTTP/" header string, missing "Connection: close" string, or response has an HTTP error code (the code was not 200/OK). This is not considered a protocol error. The RTT results will be included in the accumulated statistics.
Generic Error	Any error that does fall into any of the above error conditions.

To view results for a Performance Monitoring probe:

1. Click the **Network** tab and select the **Perf Monitoring** option. The *Network > Perf Monitoring* page displays.
2. Select a probe from the table in the lower part of the page and select the **Operations** link. The **Performance Monitoring - Operations** page displays.

Figure 6-14 Performance Monitoring - Operations



3. A table will list all available operations for the selected probe, with the most recent operation listed first. The table may be empty if no operations have been run for the probe or the operations for the probe have been deleted. Select an operation by clicking the radio button to the far right in the operation's row. The options that are available for that operation will be ungreyed. Select one of the following options:

Refresh	Refreshes the information on the Performance Monitoring - Operations page.
RTT Results	Displays the round trip time (RTT) results for the selected operation in a separate window. The results show: ◆ the time that the packet was sent, ◆ the total round trip time for non-jitter probes or the source to destination time and destination to source time for jitter probes, and ◆ the status for the packet - OK/successful or an error condition. For more information, see *Round Trip Times* or *Error Conditions*).
Accumulated Results	Displays the accumulated statistics for the selected operation in a separate window. The results show parameters used for the selected operation, and the minimum, average and maximum round trip times for all probes. For jitter probes, the results show minimum, average and maximum one way latency times, as well as jitter results for source to destination and destination to source. For a probes, a summary of lost packets and error conditions is displayed.

Performance Monitoring Commands

Go to *Performance Monitoring Commands* to view CLI commands which correspond to the web page entries described above.

7: Services

System Logging and Other Services

Use the **Services** tab 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 advanced console server 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 console manager and device ports. See the MIB definition file for details.*

- View the status of the Secure Lantronix network - for example, Lantronix out-of-band devices reachable on the local subnet.
- Set the date and time.
- Configure NFS mounts.
- Configure the web server.
- Configure the SMTP (Email) server and security when sending emails. Emails are sent in plain text.

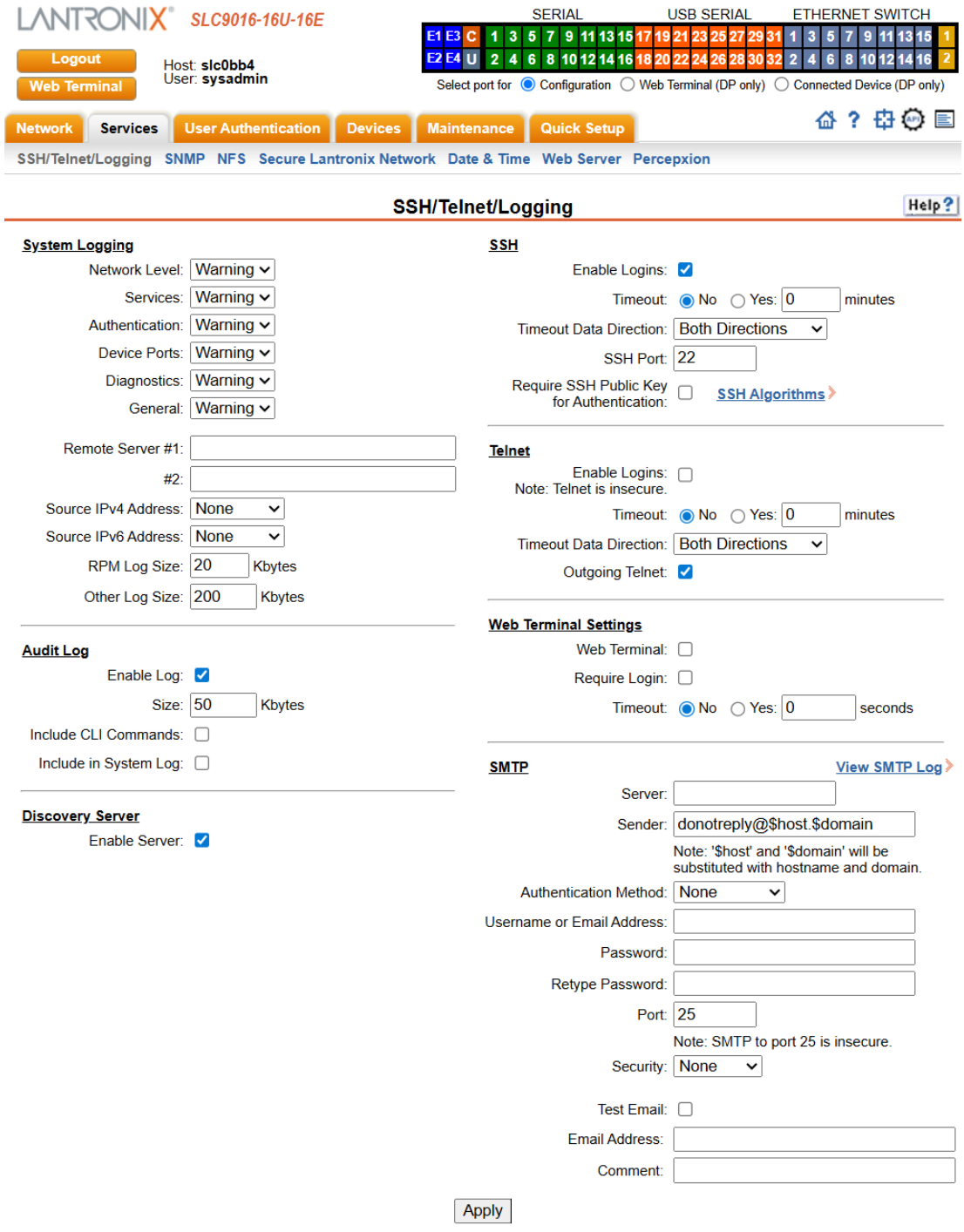
  Note: *Some email applications (such as Outlook) may strip line feed or carriage returns from emails, causing lines to run together; when this happens there may be a link included with the email that can be used to restore the deleted characters. Alternatively, it may be possible to disable the* ***Remove extra breaks in plain text messages*** *behavior in some applications.*

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

Note: *Firmware version 9.0.0.0 and prior versions use syslog format defined by RFC3164. Firmware versions 9.1.0.0 and later use syslog format defined by RFC5424. RFC5424 provides a more precise timestamp as well as other enhancements to the syslog format.*

Alert Levels	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.
Network Level	Messages concerning the network activity, for example about Ethernet and routing.
Services	Messages concerning services such as SNMP and SMTP.
Authentication	Messages concerning user authentication.
Device Ports	Messages concerning device ports and connections.
Diagnostics	Messages concerning system status and problems.
General	Any message not in the categories above.
Remote Servers (#1 and #2)	The IPv4 or IPv6 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 **Other Log Size** (see below). 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. ***Note:*** *If the SLC is unable resolve the Remote Server hostnames or contact the Remote Servers to send syslog messages, the syslog messages that cannot be sent to a Remote Server may appear on the SLC console port.*
Source IPv4	The Source IPv4 Address can be used to configure which interface (and source IPv4 address) is used for sending syslog messages. By default, the source IP address for sending syslog messages is not specified, and the source IPv4 address is selected according to the routing table. **Source IPv4 Address** can be used to select the IP address of Eth1, Eth2, VEth1 or VEth2 (the default is none) as the source IPv4 address. Before selecting an interface, make sure the interface is enabled and has a valid IPv4 address.
Source IPv6	The Source IPv6 Address can be used to configure which interface (and source IPv6 address) is used for sending syslog messages. By default, the source IP address for sending syslog messages is not specified, and the source IPv6 address is selected according to the routing table. **Source IPv6 Address** can be used to select the IP address of Eth1, Eth2, VEth1 or VEth2 (the default is none) as the source IPv6 address. Before selecting an interface, make sure the interface is enabled and has a valid IPv6 address.
RPM Log Size	The maximum size in Kbytes that RPM (Remote Power Manager) logs can grow to before they are pruned. When the file is pruned, it will be pruned to 50% of the RPM Log Size.
Other Log Size	The maximum size in Kbytes that all logs other than the RPM logs can grow to before they are pruned. When the file is pruned, it will be pruned to 50% of the Other Log Size.

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 171)* 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.
Timeout Data Direction	If idle connection timeouts are enabled, this setting indicates the direction of data used to determine if the connection has timed out. Select the type of data direction: ◆ Both Directions ◆ Incoming Network ◆ Outgoing Network
SSH Port	Allows you to change the SSH login port to a different value in the range of 1 - 65535. The default is 22. Use of ports other than 22 that are less than 1025 is not recommended.
Require SSH Public Key for Authentication	If enabled, the remote user needs a public key in addition to a password to login to the console manager. This setting is disabled by default.

Telnet

Enable Logins	Enables or disables Telnet logins to the SLC unit 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 (1 of 2) (on page 172)* 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.
Timeout Data Direction	If idle connection timeouts are enabled, this setting indicates the direction of data used to determine if the connection has timed out. Select the type of data direction: ◆ Both Directions ◆ Incoming Network ◆ Outgoing Network
Escape Sequence	A single character or a two-character sequence that causes the SLC unit to terminate a Telnet client. Currently the Escape Sequence is only used for Web Telnet sessions. The default value is **Esc+T** (escape key, then uppercase "T" performed quickly but not simultaneously). You would specify this value as **\x1bT**, which is hexadecimal **(\x)** character 27 **(1B)** followed by a **T**. A control character can be specified with the hexadecimal number for the control character; for example, **Control-E** can be specified as \x05. Note that some browsers do not report key press events if Control is pressed for non-alphanumeric keys, so it is recommended to only use letters with Control character sequences.
Outgoing Telnet	Enables or disables the ability to create Telnet out connections.

Audit Log

Enable Log	Select to save a history of all configuration changes in a circular log. Disabled by default. The audit log is saved through SLC 9000 advanced console server 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. If an SMTP server is not specified, the SLC module will attempt to look up the MX record for the domain in the destination email addresses of outgoing emails.
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.
Authentication Method	Enables or disables SMTP authentication. Supported authentication methods are **Automatic**, **Plain**, **CRAM-MD5**, and **Login**. If Automatic is selected, SLC will choose the best secure method that the SMTP server supports. This option is disabled by default. ***Note:*** *The Plain and Login methods send authentication data in cleartext over the network.*
Username or Email Address	User name for SMTP authentication. Up to 128 characters are accepted; forward slash (/), backward slash (\), single quote (') and double quote (") characters are not allowed.
Password/Retype Password	Password for SMTP authentication. Up to 128 characters are accepted; forward slash (/), backward slash (\), single quote (') and double quote (") characters are not allowed.
Port	The TCP port that the SMTP server listens on. Before the introduction of secure email (with StartTLS or TLS), port 25 was the standard port for SMTP. However, with the rise of spam, fewer email services use port 25 and now use port 465 for **TLS** and port 587 for **StartTLS**.The default port is 25.
Security	Enables TLS encrypted connections to the SMTP server. Select **StartTLS** to initiate a connection in unencrypted mode but switch to TLS if it can negotiate with the server, and select **TLS** to use only use encrypted connection mode with the server. This option is disabled by default.
Test Email	Select the check box to send a test email.
Email Address	Email address to send the test email.
Comment	Allows you to provide a comment, if desired.
View SMTP Log	Allows you to view SMTP logs.

Web SSH/Web Telnet Settings

Terminal Buffer Size	Number of lines in the Web SSH or Web Telnet terminal window that are available for scrolling back through output. ***Note:***

Discovery Server

Enable Server	This protocol is used when the network is searched for Lantronix devices - see Secure Lantronix Network. Enable this if you use the Secure Lantronix Network browser feature to discover devices on the local subnet. Disable in environments where broadcasting device presence is a security concern.

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

SSH/Telnet/Logging Commands

Go to *Services Commands* to view CLI commands which correspond to the web page entries described above.

SNMP

Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks. The SLC unit 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 unit and device ports. See the MIB definition file for details. The SLC MIB definition file and the top level MIB file for all Lantronix products is accessible from the SNMP web page.

SLC supports SNMP v1, v2c and v3. It also supports SNMP v3 over TLS via TCP. For information, see *Version 3 TLS (over TCP)*.

Note: *TLS via UDP is not supported.*

To configure SNMP:

1. Click the **Services** tab and select the **SNMP** option. The following page displays:

Figure 7-2 Services > SNMP (1 of 2)

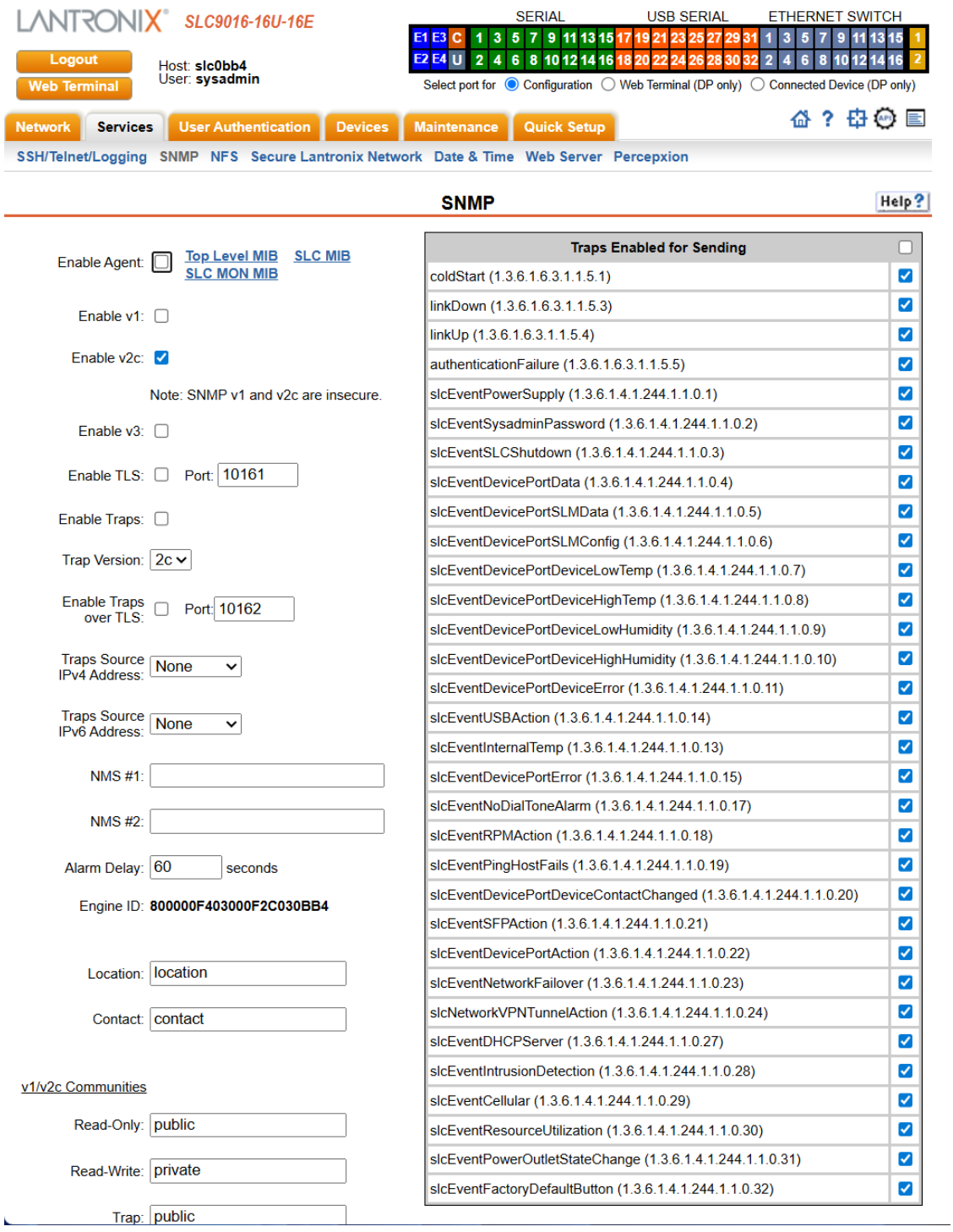
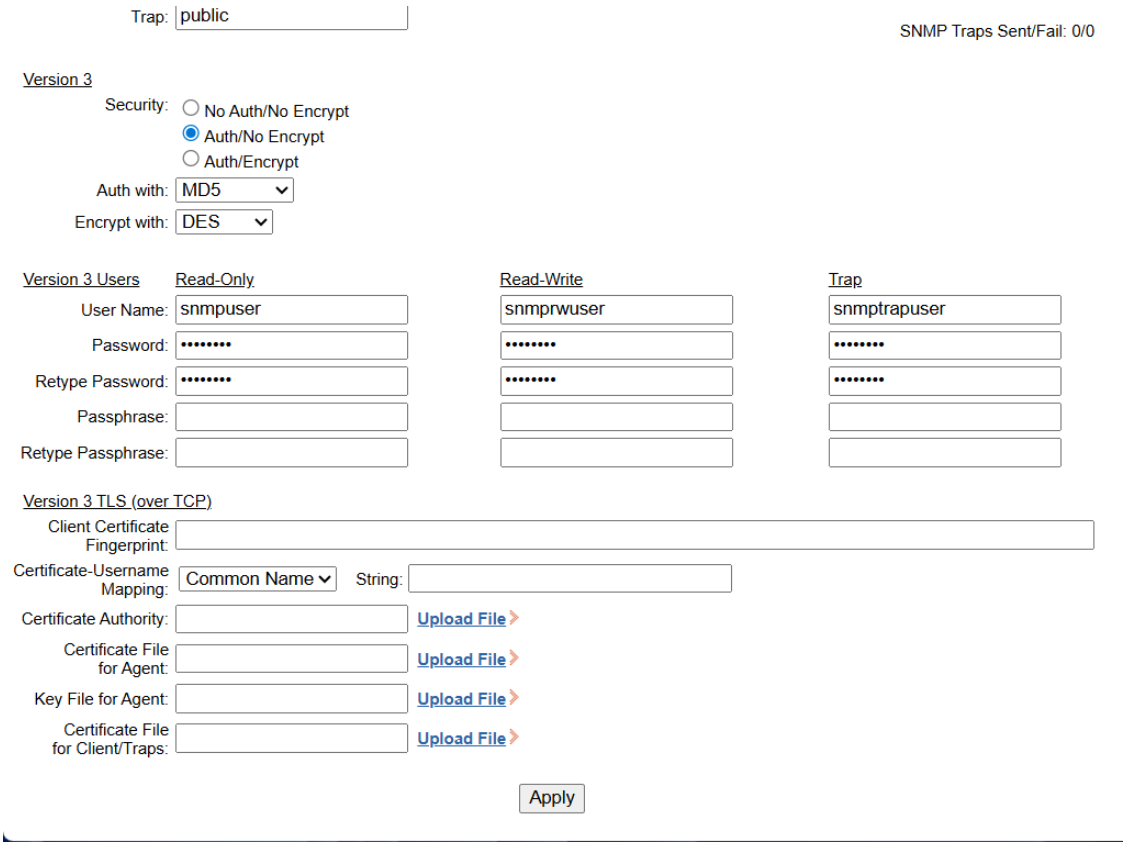


Figure 7-3 Services > SNMP (2 of 2)



2. Enter the following:

Enable Agent	Enables or disables the Simple Network Management Protocol (SNMP) agent, which allows read-only access to the system. Disabled by default.
Top Level MIB (link)	Click the link to access the top level MIB file for all Lantronix products.
SLC MIB (link)	Click the link to access the SLC MIB definition file for SLC 9000 advanced console servers.
SLC MON MIB (link)	Click the link to access the SLC monitor MIB definition file for SLC 9000 advanced console servers.
Enable v1	If selected, SNMP version 1 is enabled, and the default is disabled. SNMP version 1 uses the **Read-Only** and **Read-Write** Communities for authentication.
Enable v2c	If selected, SNMP version 2c, is enabled, and the default options are enabled. SNMP version 2c uses the **Read-Only** and **Read-Write** Communities for authentication
Enable v3	If selected, SNMP version 3 is enabled, and the default is disabled. SNMP version 3 uses configurable security parameters, and **Read-Only**, **Read-Write** and **Trap** Communities for authentication.
Enable TLS	If selected, SNMP version 3 over TLS (which uses X.509 certificates for authentication) is enabled, and the default is disabled. You must enable SNMP v3 to enable TLS.
Port	Indicates the port number that the TLS agent listens to. The port number of the traps sent over TLS will be the next port number. For example, if the **Enable TLS** port is 10161, the **Enable Traps over TLS** port number will be 10162.

Enable Traps	Traps are notifications of certain critical events. Disabled by default. This feature is applicable when SNMP is enabled. Traps that the SLC unit sends include: ◆ coldStart (generic trap 0, OID 1.3.6.1.6.3.1.1.5.1) ◆ linkDown (generic trap 2, OID 1.3.6.1.6.3.1.1.5.3) ◆ linkUp (generic trap 3, OID 1.3.6.1.6.3.1.1.5.4 ◆ authenticationFailure (generic trap 4, OID 1.3.6.1.6.3.1.1.5.5) ◆ slcEventPowerSupply (1.3.6.1.4.1.244.1.1.0.1) ◆ slcEventSysadminPassword (1.3.6.1.4.1.244.1.1.0.2) ◆ slcEventSLCShutdown (1.3.6.1.4.1.244.1.1.0.3) ◆ slcEventDevicePortData (1.3.6.1.4.1.244.1.1.0.4) ◆ slcEventDevicePortSLMData (1.3.6.1.4.1.244.1.1.0.5) ◆ slcEventDevicePortSLMConfig (1.3.6.1.4.1.244.1.1.0.6) ◆ slcEventDevicePortDeviceLowTemp (1.3.6.1.4.1.244.1.1.0.7) ◆ slcEventDevicePortDeviceHighTemp (1.3.6.1.4.1.244.1.1.0.8) ◆ slcEventDevicePortDeviceLowHumidity (1.3.6.1.4.1.244.1.1.0.9) ◆ slcEventDevicePortDeviceHighHumidity (1.3.6.1.4.1.244.1.1.0.10) ◆ slcEventDevicePortDeviceError (1.3.6.1.4.1.244.1.1.0.11) ◆ slcEventUSBAction (1.3.6.1.4.1.244.1.1.0.14) ◆ slcEventInternalTemp (1.3.6.1.4.1.244.1.1.0.13) ◆ slcEventDevicePortError (1.3.6.1.4.1.244.1.1.0.15) ◆ slcEventNoDialToneAlarm (1.3.6.1.4.1.244.1.1.0.17) ◆ slcEventRPMAction (1.3.6.1.4.1.244.1.1.0.18) ◆ slcEventPingHostFails (1.3.6.1.4.1.244.1.1.0.19) ◆ slcEventDevicePortDeviceContactChanged (1.3.6.1.4.1.244.1.1.0.20) ◆ slcEventSFPAction (1.3.6.1.4.1.244.1.1.0.21) ◆ slcEventDevicePortAction (1.3.6.1.4.1.244.1.1.0.22) ◆ slcEventNetworkFailover (1.3.6.1.4.1.244.1.1.0.23) ◆ slcNetworkVPNTunnelAction (1.3.6.1.4.1.244.1.1.0.24) ◆ slcEventWireless (1.3.6.1.4.1.244.1.1.0.26) ◆ slcEventDHCPServer (1.3.6.1.4.1.244.1.1.0.27) ◆ slcEventIntrusionDetection (1.3.6.1.4.1.244.1.1.0.28) ◆ slcEventCellular (1.3.6.1.4.1.244.1.1.0.29) ◆ slcEventResourceUtilization (1.3.6.1.4.1.244.1.1.0.30) ◆ slcEventPowerOutletStateChange (1.3.6.1.4.1.244.1.1.0.31) ◆ slcEventFactoryDefaultButton (1.3.6.1.4.1.244.1.1.0.32) The SLC unit sends the traps to the host identified in the **NMS #1** and **NMS #2** field using the selected **Trap Version**. If **Enable Traps over TLS** is selected, traps will be sent over TLS for v3 traps. For information on these traps, view the SLC enterprise MIB, which is available on the SNMP web page. ***Note:*** *When the DSR signal drops on a device port, indicating that the attached cable has been disconnected or the attached device has been powered off, the SLC will log the event in the Device Ports system log and send a slcEventDevicePortAction SNMP trap. The log message and SNMP trap only occur if there is an active (connect direct or network connection) to the device port.*
Trap Version	When traps are sent, which SNMP version to use when sending the trap: v1, v2c or v3. The default is v2c.
Enable Traps over TLS	If selected, the support for outgoing traps and incoming traps using SNMP version 3 over TLS (which uses X.509 certificates for authentication) is enabled, and the default is disabled. You must select **Enable TLS** to enable traps over TLS, and set the **Trap Version** to v3.
Port	Indicates the port number of the traps sent over TLS. It is the port number preceding the **Enable TLS** port number. For example, if the **Enable TLS** port is 10161, the **Enable Traps over TLS** port number will be 10162.

Traps Source IPv4 Address	The Traps Source IPv4 Address can be used to configure the interface (and which source IPv4 address) is used for sending SNMP traps. By default, the source address for sending SNMP traps is not specified, and the source address of an SNMP trap packet is selected according to the routing table. **Traps Source IPv4 Address** can be used to select the IPv4 address of Eth1, Eth2, VEth1 or VEth2 as the source IPv4 address for packets sent to all NMS servers defined with an IPv4 address or a name which resolves to an IPv4 address. Before selecting an interface, make sure the interface is enabled and has a valid IPv4 address. ***Note:*** *the source IPv4 address for packets sent by the agent in response to SNMP GET packets will be the destination IP address of the packet that initiated the SNMP GET.*
Traps Source IPv6 Address	The Traps Source IPv6 Address can be used to configure the interface (and which source IPv6 address) is used for sending SNMP traps. By default, the source address for sending SNMP traps is not specified, and the source address of an SNMP trap packet is selected according to the routing table. **Traps Source IPv6 Address** can be used to select the IPv6 address of Eth1, Eth2, VEth1 or VEth2 as the source IPv6 address for packets sent to all NMS servers defined with an IPv6 address or a name which resolves to an IPv6 address. Before selecting an interface, make sure the interface is enabled and has a valid IPv6 address. ***Note:*** *the source IPv6 address for packets sent by the agent in response to SNMP GET packets will be the destination IP address of the packet that initiated the SNMP GET.*
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 9000 advanced console server and receive traps from the SLC unit. Enter the IPv4 or IPv6 address of the NMS server. At least NMS #1 is required if you selected **Enable Traps**.
Alarm Delay	Number of seconds delay between outgoing SNMP traps.
Engine ID	The unique SNMP engine identifier for the SLC. This identifier may be required by the NMS in order to received v3 traps.
Location	Physical location of the SLC 9000 advanced console server (optional). Useful for managing the SLC unit using SNMP. Up to 20 characters.
Contact	Description of the person responsible for maintaining the SLC 9000 advanced console server, for example, a name (optional). Up to 20 characters.

v1/v2c Communities

Read-Only	A string that SNMP agent provides. The Read-Only Community is used for SNMP v1 and v2c. The default is **public**.
Read-Write	A string that acts like a password for an SNMP manager to access the read-only data from the SLC unit SNMP, 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 Read-Write Community is used for SNMP v1 and v2c. 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**.

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 Encrypt** or **Auth/Encrypt**, the authentication method: ◆ **MD5:** Message-Digest algorithm 5 (default) ◆ **SHA:** Secure Hash Algorithm ◆ **SHA2:** Secure Hash Algorithm 2: SHA2_224, SHA2_256, SHA2_384, and SHA2_512
Encrypt with	Encryption standard to use: ◆ **DES:** Data Encryption Standard (default) ◆ **AES:** Advanced Encryption Standard ◆ **AES192:** Advanced Encryption Standard with 192-bit length ◆ **AES256:** Advanced Encryption Standard with 256-bit length

V3 User Read-Only

User Name	SNMP v3 is secure and requires user-based authorization to access SLC MIB objects. Enter a user ID. The default is **snmpuser**. Up to 20 characters.
Password/Retype Password	Password for a user with read-only authority to use to access SNMP v3. The default is **SNMPPASS**. Up to 20 characters.
Passphrase/ Retype Passphrase	Passphrase associated with the password for a user with read-only authority. Up to 20 characters. If this is not specified it will default to the v3 Read-Only Password.

V3 User Read-Write

User Name	SNMP v3 is secure and requires user-based authorization to access SLC MIB objects. Enter a user ID for users with read-write authority. The default is **snmprwuser**. Up to 20 characters.
Password/ Retype Password	Password for the user with read-write authority to use to access SNMP v3. The default is **SNMPRWPASS**. Up to 20 characters.
Passphrase/ Retype Passphrase	Passphrase associated with the password for a user with read-write authority. Up to 20 characters. If this is not specified it will default to the v3 Read-Write Password.

V3 User Trap

User Name	SNMP v3 is secure and requires user-based authorization to access SLC unit MIB objects. Enter a user ID for users with authority to send traps. The default is **snmptrapuser**. Up to 20 characters.
Password/ Retype Password	Password for the user with authority to send v3 traps. The default is **SNMPTRAPPASS**. Up to 20 characters.
Passphrase/ Retype Passphrase	Passphrase associated with the password for a user with authority to send v3 traps. Up to 20 characters. If this is not specified it will default to the v3 Trap Password.

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

Version 3 TLS (over TCP)

SNMP v3 over TLS requires three X.509 certificate files for authenticating the SLC SNMP agent with a client or tool that queries the agent for information. SNMP v3 also requires two X.509 certificate files for authenticating the SLC client application that issues traps with the NMS application that receives traps. The certificates required for the modes are:

- **For authenticating an SLC agent with a client or tool that queries the agent:** the certificate authority (or root) file, certificate file, and private key file are required.
- **For authenticating an SLC client application that issues traps with the NMS application that receives the traps:** certificate authority (or root) file and client (or trap) certificate file are required.

If the SLC is used in both the modes, the agent certificate file and client (or trap) certificate file must share the same the certificate authority (or root) file. All certificate files should be in PEM format, e.g.:

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

Certificate fingerprints may be required by applications interfacing the SNMP applications of SLC when TLS is used. SLC will display the SHA1 and SHA256 fingerprint of the certificate authority and certificate files when they are uploaded into SLC. The fingerprint of the client certificate must also be configured when authenticating the SLC agent with a client or tool that queries the agent.

For information about generating a certificate authority (or root) file, agent (or server) certificate and key, and client certificate and key with OpenSSL, see *Creating a Certificate*. We recommend that you set the message digest used when creating the certificates to SHA1 or SHA256, depending on the level of security required. To set the message digest used by OpenSSL, in step (1b) of the instructions referenced above, change default in the line below in openssl.cnf to either SHA1 or SHA256.

```
default_md = default # use public key default MD
```

To configure TLS v3 (over TCP):

1. Click **Services** tab and select **SNMP**. The **SNMP** page appears.
2. In the **Version 3 TLS (over TCP)** section, enter the following:

Client Certificate Fingerprint	Enter the SHA1 or SHA256 fingerprint of the certificate used by the client or tool that queries the SLC agent. For example, a SHA256 fingerprint is a string of 59 characters: `D9:E5:DD:11:58:D2:DF:E0:D9:99:AE:A3:DB:57:24:21:A7:0A:20:5A`

Certificate-Username Mapping / String	SLC requires a mapping from a field in the certificate used by the client or tool that queries the console manager agent to an SNMP v3 user name used internally by the console manager. This provides an extra layer of security to verify the client's identity. The console manager will extract the designated field from the certificate and match it with what is specified in **String**. Select among the following fields in the client certificate: ◆ **User Name:** The SNMP v3 user name. It does not need to be a field in the certificate. ◆ **E-mail Address:** The email address mentioned in the `subjectAltName` field of the certificate. ◆ **FQDN:** The DNS name mentioned in the `subjectAltName` field of the certificate. For example, abc.lantronix.com. ◆ **IP Address:** The IP address mentioned in the `subjectAltName` field of the certificate. For example, 10.0.1.150. ◆ **Common Name:** The common name mentioned in the certificate. For example, "SLC" or "John Smith". By default, this option is selected. ◆ **Any:** Indicates that any of the `subjectAltName` fields in the certificate can be used. For example, if the common name in the certificate is "John Smith", select **Common Name** for **Certificate-Username Mapping.** and then enter John Smith in the String field.
Certificate Authority	Indicates the Certificate Authority used by the agent certificate and the client/traps certificate. ***Note:*** *The certificate authority, agent certificate and client/traps certificate can be viewed by clicking the **View** link to the associated the filename. It will also display the SHA1 and SHA256 fingerprint of the certificate. All certificate files can be deleted by clicking the **Delete Certificate Files** check box.*
Certificate File for Agent	The certificate file for the SLC agent.
Key File for Agent	The private key file for the SLC agent.
Certificate File for Client/Traps	The certificate file for the SLC agent that issues traps.

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

Services Commands

Go to *Services Commands* to view CLI commands which correspond to the web page entries described above.

NFS

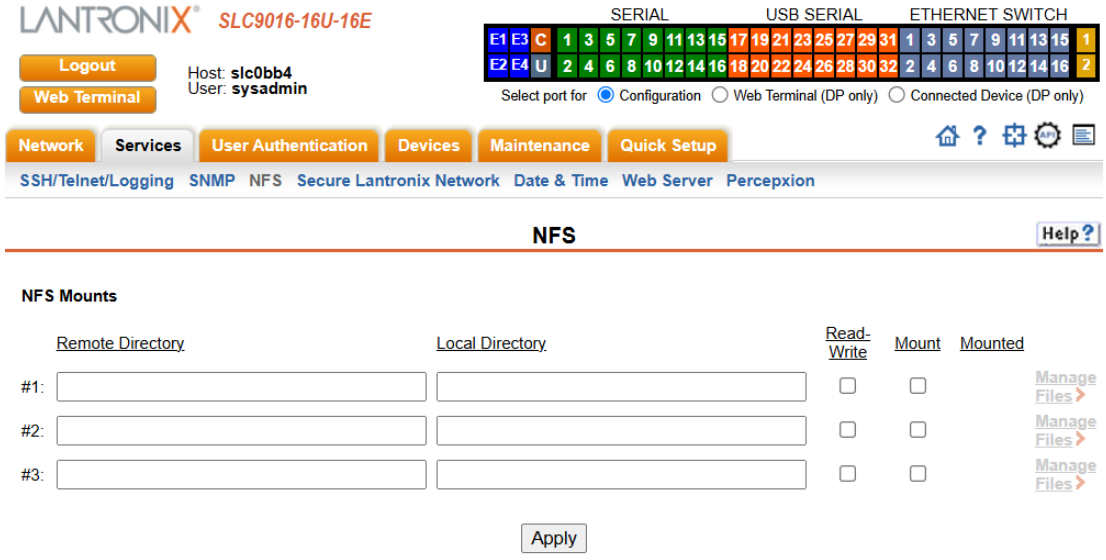
Use the NFS page if you want to save configuration and logging data onto a remote NFS server.

Mounting an NFS shared directory on a remote network server onto a local SLC directory enables the SLC ~~advanced console manager~~advanced console server 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.

To configure NFS:

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

Figure 7-4 Services > NFS



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 9000 advanced console server on which to mount the remote directory. The SLC unit creates the local directory automatically.
Read-Write	If enabled, indicates that the SLC 9000 advanced console server 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. Disabled by default.
Mounted	Indicates if the SLC was able to successfully mount the NFS share directory.

3. To save, click the **Apply** button.
4. Click the Firmware & Configurations link to access the *Firmware & Configurations (on page 310)* to save SLC configuration, as desired.

NFS Commands

Go to *NFS Commands* to view CLI commands which correspond to the web page entries described above.

Secure Lantronix Network

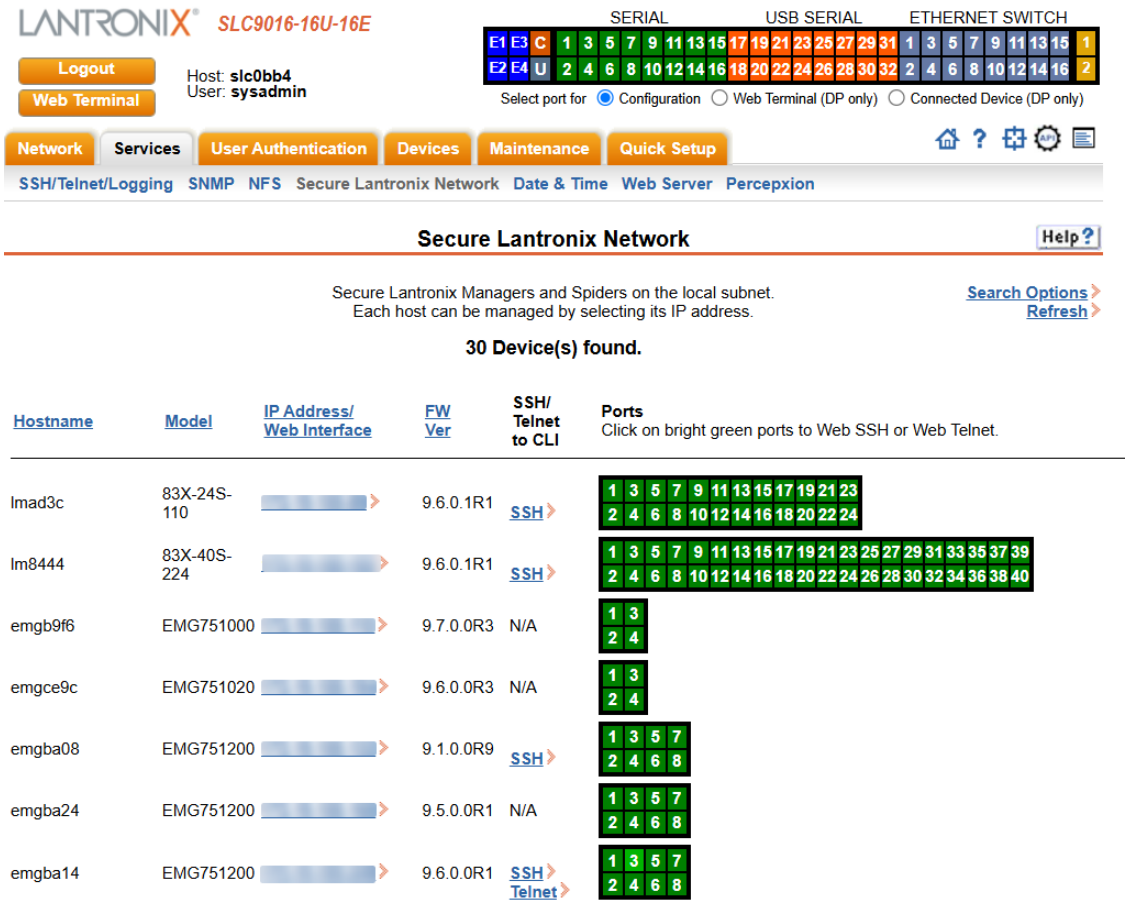
Use the **Secure Lantronix Network** option to view and manage SLC and SLB console managers, SLC 9000 advanced console servers, and Lantronix Spider® devices on the local subnet.

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

To access SLC and SLB console managers, and Lantronix Spider devices on the local network:

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

Figure 7-5 Services > Secure Lantronix Network



2. Access your device or device port through any of the methods below.

To directly access the web interface for a secure Lantronix device:

1. Make sure Web Telnet and Web SSH is enabled for the specific device or device port.
2. Click the IP address of a specific secure Lantronix device to open a new browser page with the web interface for the selected secure Lantronix device.

3. Log in as usual.

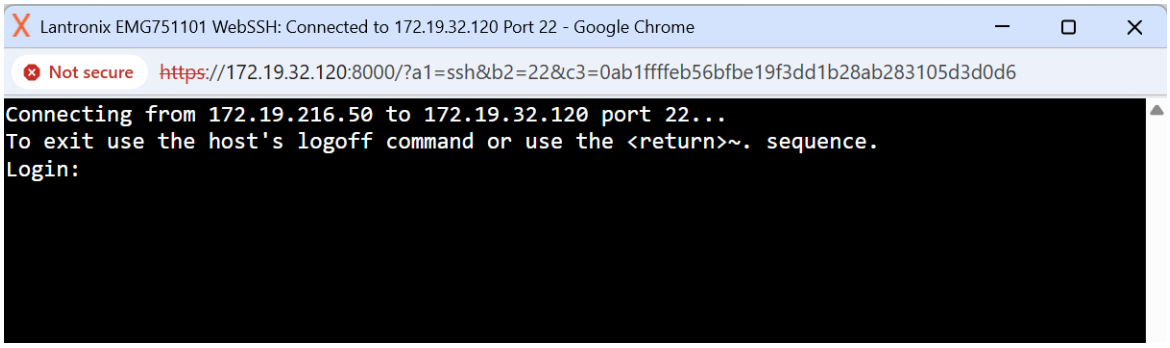
Figure 7-6 IP Address Login Page



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.
2. Click your mouse into the CLI login interface that appears and login. The CLI interface will indicate when your connection is established.

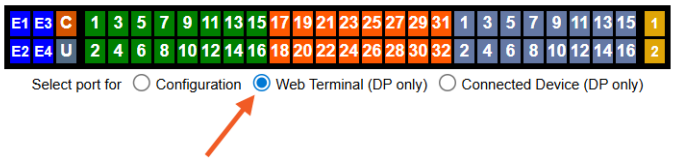
Figure 7-7 SSH or Telnet CLI Session



To directly access a specific port on a particular device:

1. You have two options:
   - **Dashboard**
     Make sure the **Web Terminal (DP only)** radio button directly beneath the Dashboard is selected and click the desired port number. The Dashboard is located on the upper right corner of each Web Manager page (see *Web Page Layout on page 44*.) An SSH popup window appears.

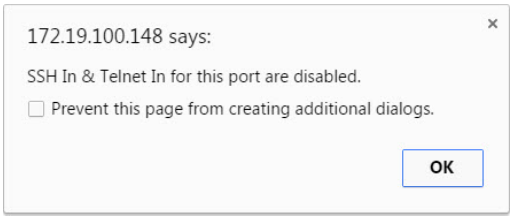
Note: *WebTelnet is not available from the Dashboard. See* ***Dashboard on page 45*** *as the dashboard may vary in appearance.*



- **Secure Lantronix Network Page**
  Click the **Services** tab, then click the **Secure Lantronix Network** link (see *Figure 7-5*.) Select the port you want to configure. Enabled port numbers are in bright green boxes and will allow you to select either a **Web Terminal** or a **WebTelnet** session. If enabled, an SSH or Telnet popup window appears depending on what is clicked.

  Note: *Port numbers that are disabled are in dark green boxes; clicking a disabled port number generates a popup window indicating the port is disabled (see Figure 7-8 below.)*

Figure 7-8 Disabled Port Number Popup Window

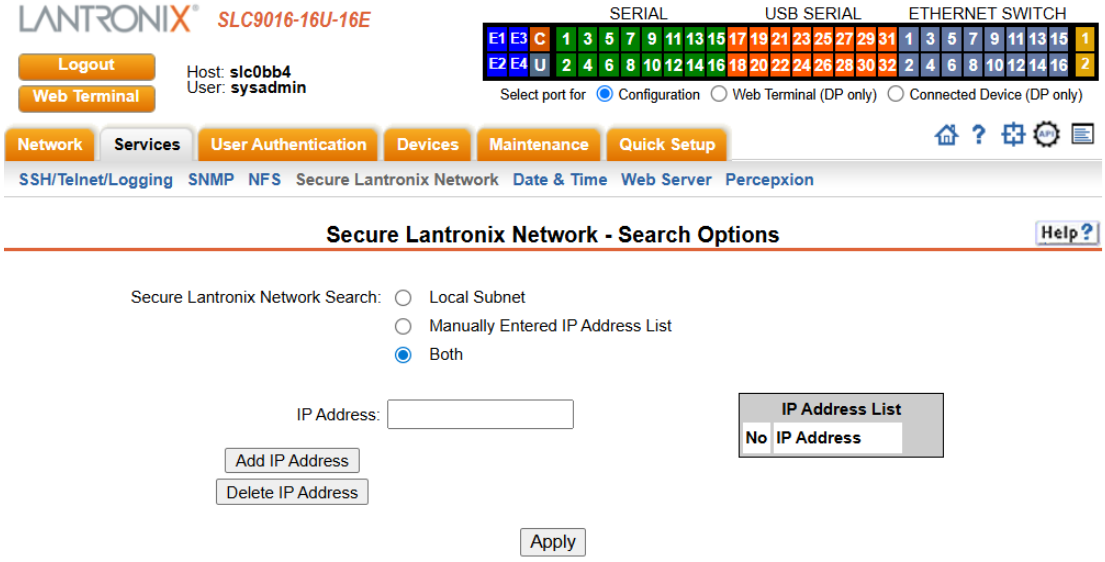


2. Click your mouse into the CLI login interface that appears (see *Figure 7-7*) and login. The CLI interface will indicate when your connection is established.

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:

Figure 7-9 Services > Secure Lantronix Network > Search Options



2. Enter the following:

Secure Lantronix Network Search	Select the type of search you want to conduct. ◆ **Local Subnet** performs a broadcast to detect secure Lantronix devices on the local subnet. ◆ **Manually Entered IP Address List** provides a list of IP addresses that may not respond to a broadcast because of how the network is configured. ◆ **Both** is the default selection.
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.

Web SSH/Telnet Copy and Paste

There are security issues with letting a web page access the system clipboard, which is the main clipboard on a system that is shared between all applications. Because of this, browsers limit access to the system clipboard. The Web SSH and Web Telnet windows provide copy and paste functionality via a right-click menu: the Copy option will copy what is highlighted in the Web SSH or Web Telnet window into an internal (non-system) clipboard, and the contents can be pasted into the Web SSH or Web Telnet window with the Paste.

Support for copying and pasting content between the system clipboard and the Web SSH or Web Telnet window will vary from browser to browser. With the exception of Internet Explorer, most browsers will not allow highlighted content from the Web SSH or Web Telnet window to be copied

to the system clipboard (Internet Explorer will display a prompt confirming the copy). Likewise, most browsers will not allow content from the system clipboard to be directly pasted into the Web SSH or Web Telnet window with the standard Control-V paste key sequence. With some browsers, the user will be able to use the Paste from browser option in the right-click menu to paste content from the system clipboard into a text field in a popup, and after hitting Enter, the content will be sent to the Web SSH or Web Telnet window. Paste from Browser only handles a single line, and will strip out LF/CR.

Secure Lantronix Network Commands

Go to *SLC Network Commands* to view CLI commands which correspond to the web page entries described above.

Date and Time

Use the Date & Time Settings page to specify the local date, time, and time zone at the SLC location, or enable the SLC unit to use NTP to synchronize with other NTP devices on your network. Note that changing the date/time and/or timezone, or enabling NTP may affect the user's ability to login to the web; if this happens, use the CLI **admin web restart** command to restart the web server.

NTP servers acquired via DHCP: Any Ethernet interfaces that are configured to use DHCP will request NTP servers (option 42) from a DHCP server. If NTP servers are received via DHCP, and NTP is not enabled in the console manager configuration, the DHCP NTP servers will be used to synchronize the time on the console manager; NTP will be auto-enabled to use these servers. The DHCP NTP servers will be displayed in the CLI and web page if they are in use. Only one Ethernet interface will be used as the source for NTP servers (the first interface that provides the NTP servers); NTP servers received subsequently on other Ethernet interfaces will be ignored.

When the console manager first boots, and after a factory default reset, it checks the date and time to verify that it is after the manufacturing date code on the unit; if it is found to be prior to the manufacturing date code, the console manager will attempt to synchronize the time to well known time servers so that there are no issues with TLS negotiations at boot.

The CLI 'show ntp' command and Date and Time web page will display the current NTP status if NTP is enabled. The currently selected peer is marked with a "*", while additional peers designated acceptable for synchronization, but not currently selected, are marked with a "+". Peers marked * and + are included in the weighted average computation to set the local clock; the data produced by peers marked with other symbols are discarded. The columns displayed are:

- **remote**: Hostname or IP address of the configured upstream NTP server.
- **refid**: Identification of the time stream to which the NTP server is synchronized. If a refid of ".INIT." is displayed, the console manager has not received a response from the configured NTP server; this could be due to several reasons including (1) the NTP server is unreachable (2) the NTP server is down (3) IP filters rulesets are blocking NTP traffic.
- **st**: Stratum is a value representing the hierarchy of the upstream NTP servers. Higher values indicate NTP servers further away from the root time source. Values are relative, and can be set manually by an NTP server.
- **t**: Type of packet exchange used for NTP communication (usually "u" for unicast UDP (other values are m = multicast, b = broadcast, l = local, - = don't know).
- **when**: Quantity of seconds which have elapsed since the last attempted poll of the configured upstream NTP server.

- **poll**: Interval in seconds which the console manager polls the configured NTP server.
- **reach**: n 8-bit shift register in octal (base 8), with each bit representing success (1) or failure (0) in contacting the configured NTP server. A value of 377 is 11111111 (base 2), which indicates that every query was successful during the last 8 poll intervals. This can be used to check whether the connection to the remote host is consistent or there are any intermittent losses which could potentially cause the system clock on your host to become unsynchronized. In the event when >= 8 polls have been made to the ntp server and reach is not 377, this could indicate that your server is not consistently reachable.
- **delay**: Round trip delay (in milliseconds) for communication between the configured NTP server and the console manager.
- **offset**: The offset (in milliseconds) between the time on the configured NTP server and the console manager. A value closer to 0 is ideal.
- **jitter**: The observed timing jitter or variation between clock pulses of time with the configured NTP server. A value closer to 0 is ideal.

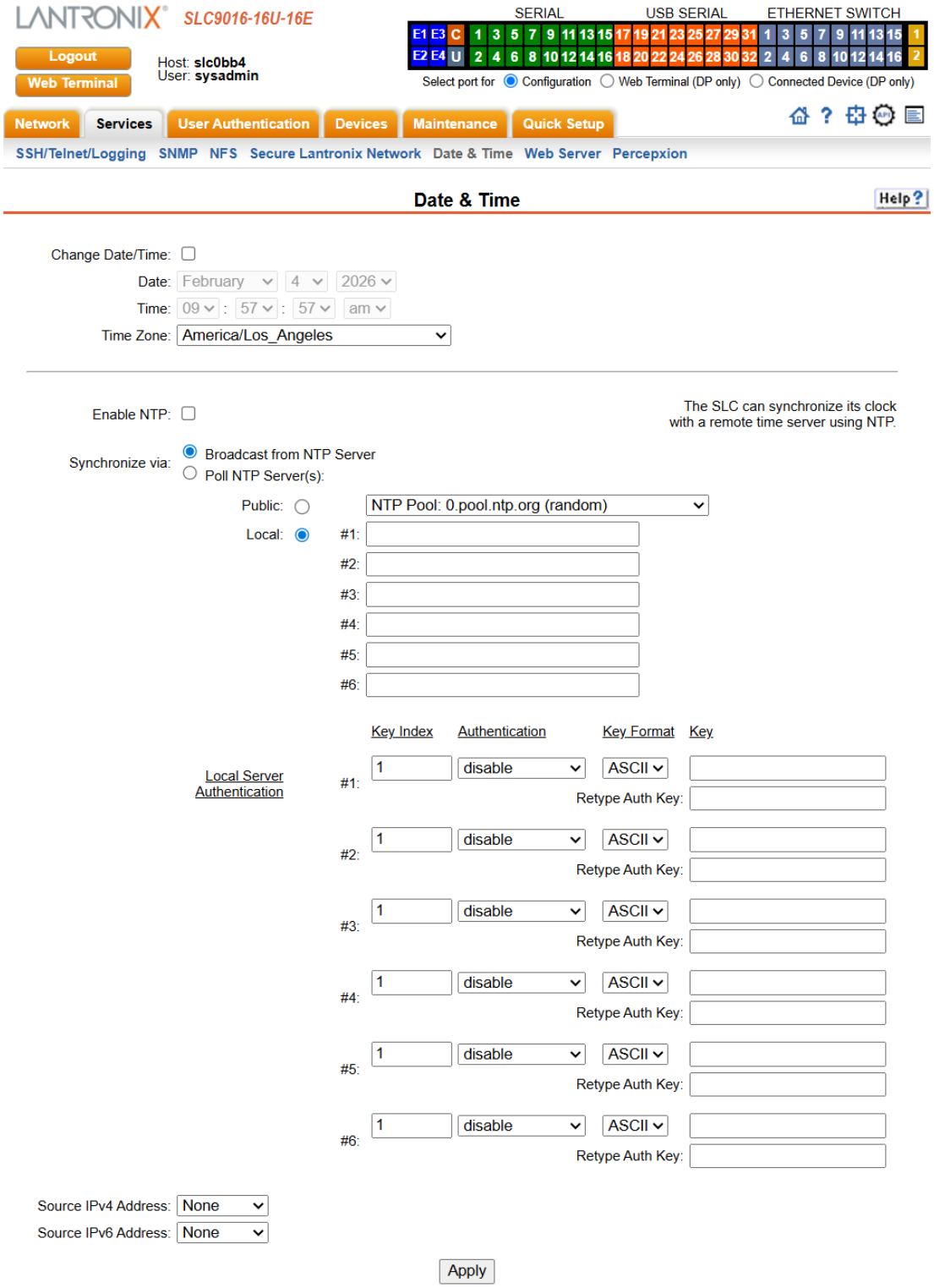
The NTP uses the intersection algorithm, a modified version of Marzullo's algorithm, to select accurate time servers and is designed to mitigate the effects of variable network latency.

When NTP is initially enabled, it can take some time (possibly as long as 20 minutes) for the console manager clock to be synchronized with an NTP source. NTP first establishes that a time server is trusted, and then begins exchanging packets to synchronize the time. See this explanation for how time is synchronized.

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 7-10 Services > Date & Time



2. Enter the following:

Change Date/Time	Select the checkbox to manually enter the date and time at the SLC location.
Date	From the drop-down lists, select the current month, day, and year.
Time	From the drop-down lists, select the current hour and minute.
Time Zone	From the drop-down list, select the appropriate time zone. For information on each timezone, see http://en.wikipedia.org/wiki/List_of_tz_database_time_zones

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

To enable NTP synchronization:

1. Enter the following:

Enable NTP	Select the checkbox to enable NTP synchronization. NTP is disabled by default.
Current NTP status	Displays the current NTP status if NTP is enabled above.
Synchronize via	Select one of the following: ◆ **Broadcast from NTP Server:** Enables the SLC unit to accept time information periodically transmitted by the NTP server. This is the default if you enable NTP. ◆ **Poll NTP Server:** Enables the SLC 9000 advanced console server to query the NTP Server for the correct time. If you select this option, complete one of the following: ➢ ***Local:*** Select this option if the NTP servers are on a local network, and enter the IPv4 or IPv6 address of the NTP server. This is the default, and it is highly recommended. ➢ ***Public:*** Select this option if you want to use a public NTP server, and select the address of the NTP server from the drop-down list. This is not recommended because of the high load on many public NTP servers. All servers in the drop-down list are stratum-2 servers. (See www.ntp.org for more information.) Each public NTP server has its own usage rules --please refer to the appropriate web site before using one. Our listing them here is to provide easy configuration but does not indicate any permission for use.
Local Server Authentication	Any of the local servers can be configured to use NTP Authentication to verify that the local server is known and trusted. The NTP packets are authenticated with symmetric key authentication. The server should be configured with the same shared **Key Index** (or ID) and **Key** that is configured on the console manager. For each local server that uses NTP Authentication, configure the following: **Key Index**: This may also be called a Key ID. NTP servers and clients must use the same Key and Key Index to authenticate NTP packets. During the synchronization of time, the client requests the Key Index from the server and the server sends a response; if the Key Index is different, time will not be synchronized. The valid range is 1-65535 and the default Key Index is 1. **Authentication**: Select a message digest to enable authentication, or select **disable** for no NTP Authentication. The available message digest algorithms are **AES128CMAC**, **RIPEMD160**, **SHA1** and **MD5**. **Key Format**: Select the format that the shared key will be entered in: **ASCII** or **HEX**. **Key:/Retype Auth Key**: Enter the shared key in either ASCII (up to 20 characters) or hexadecimal (up to 40 characters). The minimum key length for both ASCII and HEX is 8 characters.

Source IPv4 Address	The Source IPv4 Address can be used to configure which interface (and source IPv4 address) is used for receiving and sending NTP packets. By default, no interface is defined for NTP traffic and all available network addresses are available for processing NTP packets. The **Source IPv4 Address** parameter can be used to select only one interface for processing NTP packets for all NTP servers defined with an IPv4 address or a name which resolves to an IPv4 address. Select Eth1, Eth2, VEth1 or VEth2 (the default is none). Before selecting an interface, make sure the interface is enabled and has a valid IPv4 address.
Source IPv6 Address	The Source IPv6 Address can be used to configure which interface (and source IPv6 address) is used for receiving and sending NTP packets. By default, no interface is defined for NTP traffic and all available network addresses are available for processing NTP packets. The **Source IPv6 Address** parameter can be used to select only one interface for processing NTP packets for all NTP servers defined with an IPv6 address or a name which resolves to an IPv6 address. Select Eth1, Eth2, VEth1 or VEth2 (the default is none). Before selecting an interface, make sure the interface is enabled and has a valid IPv6 address.

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

Date and Time Commands

Go to *Date and Time Commands* to view CLI commands which correspond to the web page entries described above.

Web Server

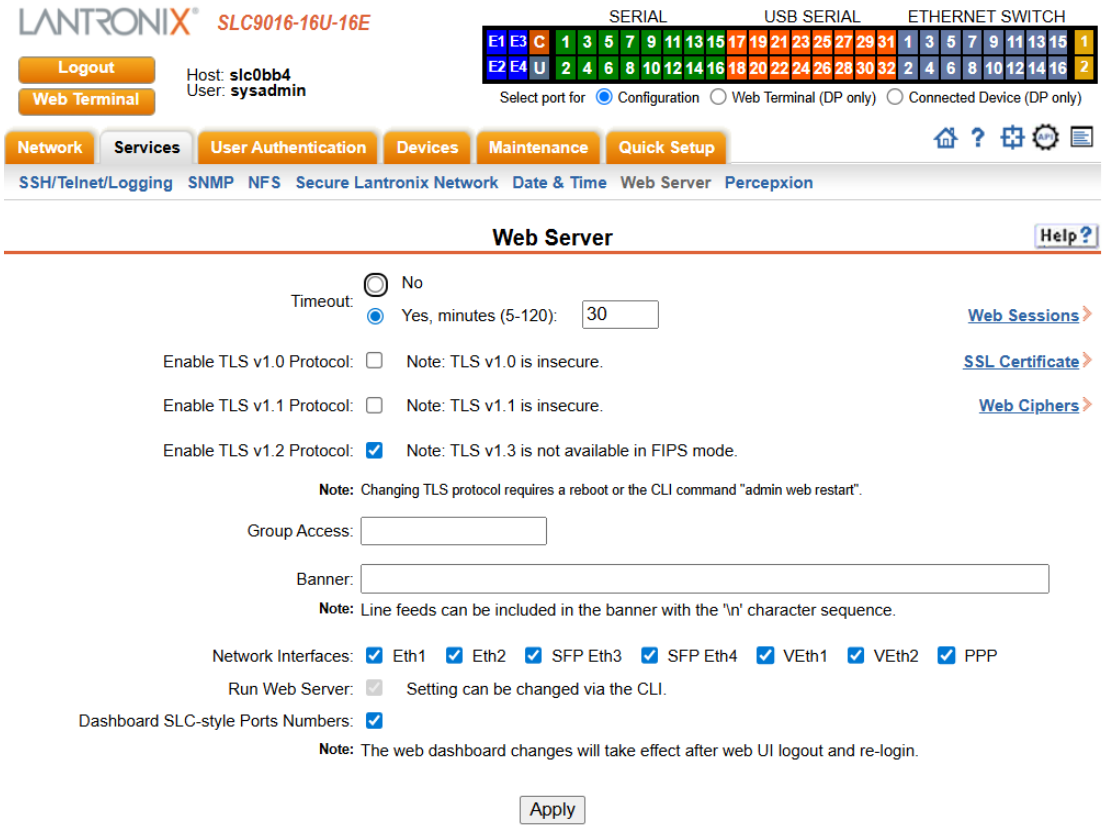
The Web Server supports all versions of the TLS protocol (TLSv1.0, TLSv1.1, TLSv1.2 and TLSv1.3), but due to security concerns, does not support any versions of the SSL protocol. TLSv1.0, TLSv1.1, TLSv1.2, can be disabled. In addition to providing user access to the web interface, the web server also provides a REST API interface. The Web Server page allows the system administrator to:

- Configure attributes of the web server, including supported TLS versions.
- View and terminate current web sessions (see *Web Server - Web Sessions*).
- Import a site-specific SSL certificate (see *Web Server - SSL Certificate*).
- View and configure the active cipher list for the current web server (see *Web Server - Ciphers*).

To configure the Web Server:

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

Figure 7-11 Services > Web Server



2. Enter the following fields:

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. *If a session times out, refresh the browser page and enter your user ID and password top open a new web session.* ***Note:*** *If you close the browser without logging off the SLC unit first, you will have to wait for the timeout time to expire. You can also end a web session by using the admin web terminate command at the CLI or by asking your system administrator to terminate your active web session.* ◆ To view or terminate current web sessions, click the Web Sessions link. See *Web Server - Web Sessions*. ◆ To view, import, or reset the SSL Certificate, click the SSL Certificate link. See *Web Server - SSL Certificate*.
API Timeout	Number of minutes (5-60) after which the console manager API session times out. The default is **30**. ***Note:*** *The API session is automatically closed when the configured timeout time expires, even if the session is actively in use. For inactive API sessions, the console manager monitors session activity every 5 minutes and terminates any session that exceeds the configured timeout time.*
Enable TLS v1.0 Protocol	The web supports the TLS v1.0 protocol. Use this check box to enable or disable the TLS v1.1 protocol. You must reboot or restart the web server with the CLI command "admin web restart" for the change to take effect.
Enable TLS v1.1 Protocol	The web supports the TLS v1.1 protocol. Use this check box to enable or disable the TLS v1.1 protocol. You must reboot or restart the web server with the CLI command "admin web restart" for the change to take effect.
Enable TLS v1.2 Protocol	By default, the web supports the TLS v1.2 protocol. Clear this check box to disable the TLS v1.2 protocol. You must reboot or restart the web server with the CLI command "admin web restart" for the change to take effect.
Group Access	Specify one or more groups to allow access to the Web Manager user interface. 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. 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	Enter to replace default text displayed on the Web Manager home page after the user logs in. May contain up to 1024 characters. Blank by default. 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.
Run Web Server	If enabled, the web server will run and listen on TCP port 443. By default, the web server is enabled. This setting is read only in the web UI but can be configured in the CLI.

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

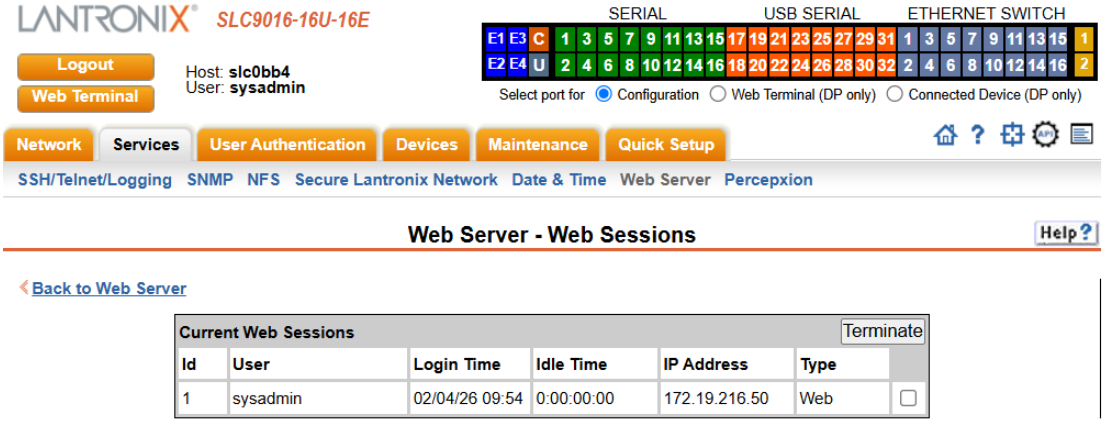
Web Server - Web Sessions

The *Services > Web Server* page enables you to view and terminate current web sessions and REST API 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:

Figure 7-12 Web Sessions



2. To terminate, click the check box in the row of the session you want to terminate and click the **Terminate** button.
3. To return to the *Services > Web Server* page, click the **Back to Web Server** link.

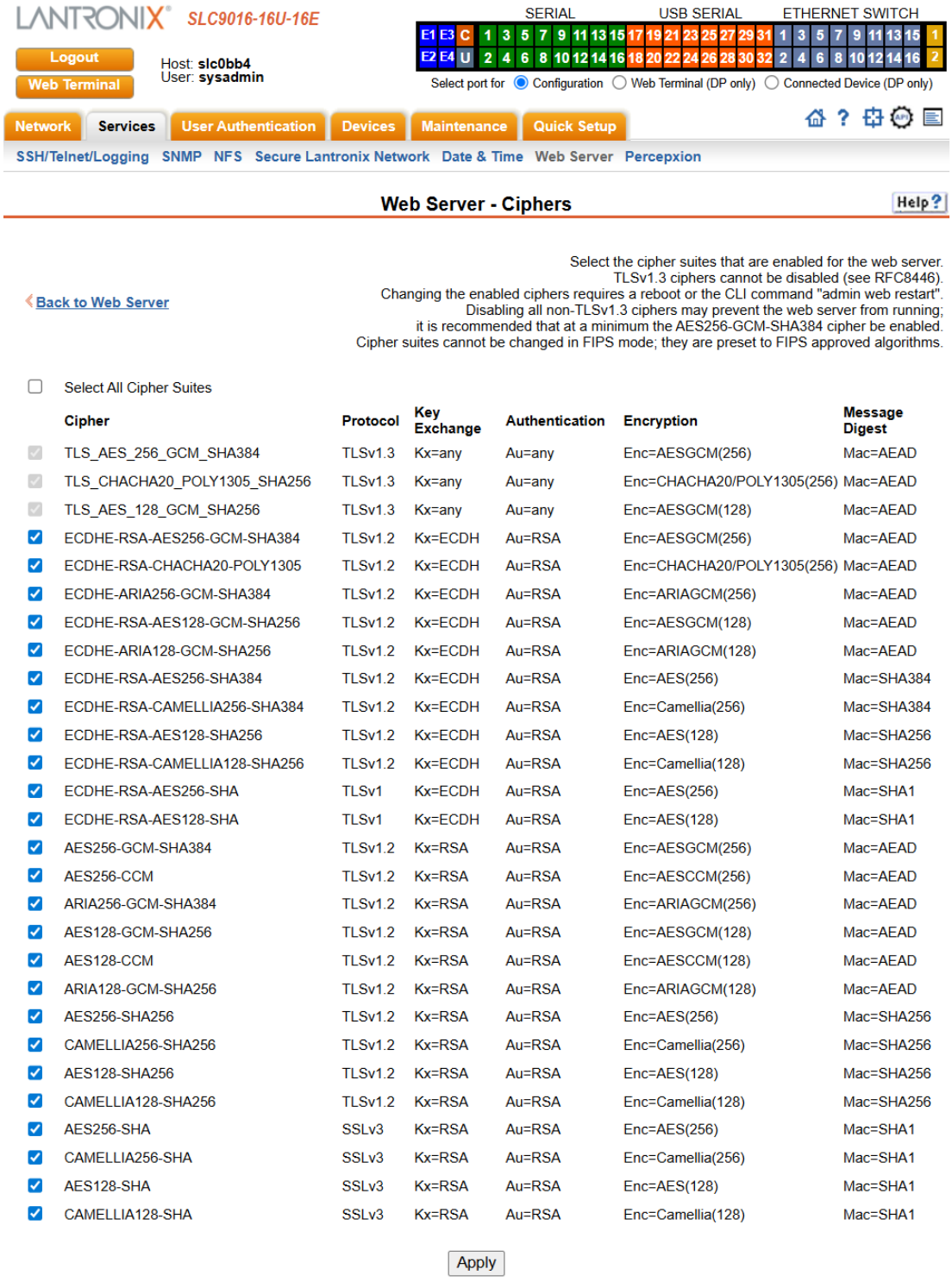
Web Server - SSL Certificate

The Web Server - SSL Certificate 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 or generate a custom self-signed SSL certificate. The custom self-signed SSL certificates generated by the SLC use the SHA256 hash algorithm.

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.

Figure 7-13 Web Server - 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**, **SFTP**, or **HTTPS**). The default is **HTTPS**.
Root Filename	Filename of the imported root or intermediate Certificate Authority (optional). If HTTPS is selected as the method for import, the Upload File link will be selectable to upload a certificate file. The certificate file should be in PEM format: -----BEGIN CERTIFICATE----- (root file in base64 encoding) -----END CERTIFICATE-----
Certificate Filename	Filename of the imported certificate. If HTTPS is selected as the method for import, the Upload File link will be selectable to upload a certificate file. The certificate file should be in PEM format: -----BEGIN CERTIFICATE----- (certificate in base64 encoding) -----END CERTIFICATE-----
Key Filename	Filename of the imported private key for the certificate. If HTTPS is selected as the method for import, the Upload File link will be selectable to upload a key file. The key file should be in PEM format: -----BEGIN RSA PRIVATE KEY----- (private key in base64 encoding) -----END RSA PRIVATE KEY-----
Passphrase / Retype Passphrase	Enter the passphrase associated with the SSL certificate if the private key is encrypted.
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.
Generate custom self-signed SSL Certificate	To generate your own custom self-signed certificate with attributes specific to your site, select the checkbox. The SHA256 hashing algorithm will be used to generate the certificate. Unselected by default.
Number of Bits	The number of bits to use when generating the certificate: 2048, 3072 or 4096.
Number of Days	The number of days that the certificate can be used before it expires, up to 7500 days.
Country Name	The two letter country code for the custom certificate, e.g. "US" or "FR".
State or Province Name	The state or province for the custom certificate, e.g. "California". Must be at least 2 characters long.
Locality Name	The locality or city for the custom certificate, e.g. "Los Angeles". Must be at least 2 characters long.
Organization Name	The organization or company name for the custom certificate, e.g. "Lantronix". Must be at least 2 characters long.
Organization Unit Name	The unit name for the custom certificate, e.g. "Engineering" or "Sales". Must be at least 2 characters long.
Hostname or Common Name	The hostname or other name associated with the SLC the certificate is generated on, e.g., "slc100.engineering.lantronix.com". Must be at least 2 characters long.
Email Address	An optional email address to associate with the custom certificate.

Optional Challenge Password & Retype Password	An optional password use to encrypt the custom certificate.

3. Click the **Apply** button.

Note: *You must restart the web server or reboot the SLC advanced console server for the update to take effect.*

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

Web Server - Ciphers

The Web Server - Ciphers List displays a list of the available TLS ciphers suites for the web server, which ones are currently enabled and allows the user to select ciphers to enable or disable. Disabling ciphers may prevent some web clients from connecting to the console manager. In FIPS mode, the web ciphers cannot be changed; the ciphers are pre-configured to a set of FIPS approved ciphers.

The TLSv1.3 ciphers supported by the web server are TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, and TLS_AES_128_GCM_SHA256. All TLSv1.3 ciphers are required to be enabled to be compliant with the TLSv1.3 protocol (see RFC8446 for more information).

The TLSv1.0 protocol use SSLv3 ciphers, so the list of cipher suites that can be configured will include SSLv3 ciphers.

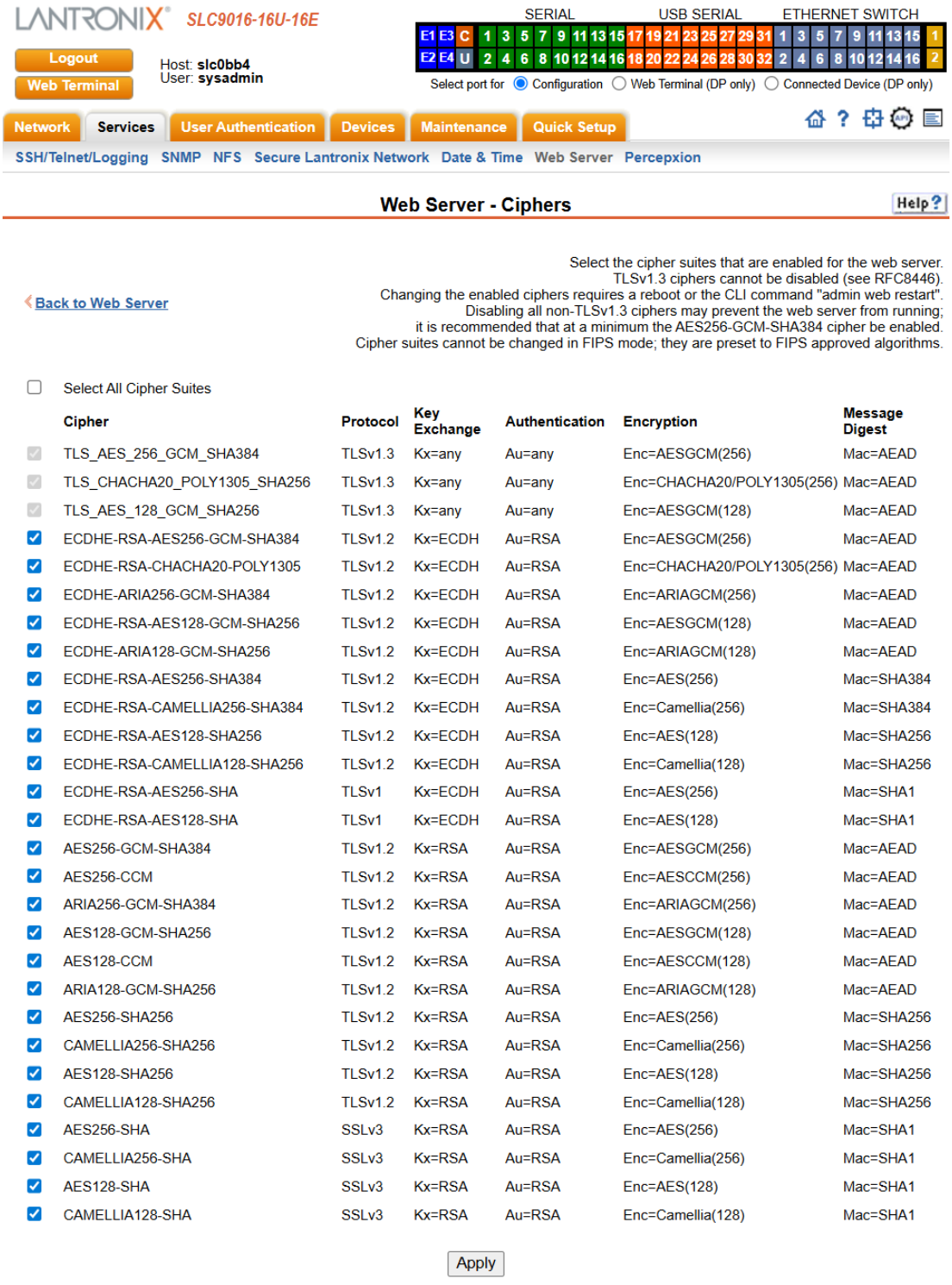
The columns in the Web Ciphers table are as follows:

- **Cipher** - Name of the cipher suite.
- **Protocol** - The minimum protocol version that the cipher suite supports, such as TLSv1.2. Note that this is not always the same as the protocol version in which the cipher suite was first defined because some cipher suites are backwards compatible with earlier protocol versions.
- **Key Exchange** - Key exchange method such as RSA, ECDHE, etc.
- **Authentication** - Authentication method such as RSA, etc.
- **Encryption** - Symmetric encryption method, with number of secret bits, such as AESGCM(128)
- **Message Digest** - Message digest, such as SHA256

To view and configure the web ciphers for the web server:

1. On the **Services** tab, click the **Web Server** page, and click the **Web Ciphers** link. The **Web Server - Ciphers List** page appears. See *Figure 7-14*.
2. Select the cipher suites that are enabled for the web server.
3. Click **Apply**.

Figure 7-14 Web Server - Ciphers List



Admin Web Commands

Go to *Administrative Commands* ('admin web') to view CLI commands which correspond to the web page entries described above.

REST API

The REST API provides an interface to retrieve console manager configuration and status. Users must authenticate to the API before accessing information via the API. Authentication uses the same authentication methods that are enabled for the console manager (see Authentication Methods). A maximum of 20 simultaneous API sessions is supported.

Below is an example API session. Note: URLs and data sent in a payload may need to be encoded if it contains special characters; see this link for more information. The v1 API is documented below; the documentation for the v2 API can be found by clicking the API Documentation link on the Web Server page or the API icon in the web UI dashboard.

Authentication to the REST API returns a token used for the remainder of the API session:

```
$ curl -k -d '{ "login": "sysadmin", "password": "PASS" }' -X POST -H
"Content-Type: application/json" https://slc.mydomain.com/api/v1/login
{
"token_id": "20642a56-99d5-4cd3-874a-7565ef5d3a37",
"group": "Administrators",
"authenticated": "Local Users",
"link": "https://slc.mydomain.com/api/v1/login/token/20642a56-99d5-4cd3-
874a-7565ef5d3a37",
"expiration": "00:30:00"
}
```

Discovering the APIs that are available:

```
$ curl -k --header "X-auth-token: 20642a56-99d5-4cd3-874a-7565ef5d3a37"
https://slc.mydomain.com/api/v1
console manager /api/v1 URIs:
/login
/version
/status
```

Full documentation is available in the web Services->Web Server online help

Retrieving version information:

```
$ curl -k --header "X-auth-token: 20642a56-99d5-4cd3-874a-7565ef5d3a37"
https://slc.mydomain.com/api/v1/version
{
"model": "SLC8040",
"num_ports": 40,
"power_supply": "AC, 1 power supply",
"num_front_usb_ports": 2,
"internal_modem": "Not Installed",
"serial_num": "0080A396431D",
"firmware_version": "7.6.0.0R4",
"firmware_updated": "Thu Apr 26 16:08:29 2018",
"current_bank": 1,
"bootloader_version": "2.0.0.0R8",
"os_version": "IT Management Gateway OS 7.0",
"memory_size": "512 MB",
"flash_size": "512 MB",
```

```
"eth1_macaddr": "00:80:a3:96:43:1d",
"eth2_macaddr": "00:80:a3:96:43:1e",
"nic_board_type": "N/A",
"nic_board_version": "N/A",
"eth1_nic_sfp": "N/A",
"eth2_nic_sfp": "N/A",
"main_board_version": "080-542-R/330-298-R (Rev 2)",
"io_module_types": "RJ45-08, USB-16, USB-16",
"io_module_versions": "08SPB, 16UBA, 16UBA",
"site_tag": "San Jose SLC9000"
}
```


Terminating the API session:

```
$ curl -k -X DELETE --header "X-auth-token: 20642a56-99d5-4cd3-874a-
7565ef5d3a37" https://slc.mydomain.com/api/v1/login/token/20642a56-99d5-
4cd3-874a-7565ef5d3a37
```

8: Percepxion

Percepxion™ is the cloud management platform for the SLC 9000. When your device is connected to Percepxion, you can:

- Access the console ports of any connected device from anywhere, without a VPN
- Monitor fleet health, port connection status, and system telemetry across all your SLC 9000 units
- Push firmware updates and configuration changes to individual devices or the entire fleet
- Set up automated configuration deployment so new devices self-configure when they come online
- Run CLI commands across multiple devices from a single interface

Percepxion is available as a cloud service or an on-premise deployment option is also available for air-gapped or compliance-restricted environments.

If you are deploying multiple SLC 9000 units to remote sites, See *Zero-Touch Deployment via Percepxion* later in this section before configuring individual devices.

Before You Begin

Before configuring the Percepxion client on the SLC 9000, confirm the following:

1. You have an active Percepxion account.
2. The SLC 9000 can reach the internet on TCP port 443 via any Ethernet interface.

Connect the SLC 9000 Unit to Percepxion

1. Log into the SLC 9000 web manager. Click the **Services** tab, then select **Percepxion**.
2. In Device Attributes, confirm that Device ID is populated (32 alphanumeric characters).
3. If this field is blank, stop here. Contact Lantronix Technical Support to provision a Device ID.
4. Confirm that **Registration Host** is set to api.percepxion.ai (cloud) or your on-premise server hostname (on-premise installations).

   The Registration Port defaults to 443. Leave this at the default unless your Percepxion administrator has specified a different port.
5. Confirm that Percepxion Client is set to **Enabled**.
6. Click **Apply**.
7. Watch the **Status of Client** field. Within 30–60 seconds, it should progress through:
   - **Registered**, the device successfully authenticated with the Registration Host.
   - **Telemetry Handshake**, the device established the telemetry connection.
   - **Messaging connected**, the device is receiving commands and publishing status.
8. Log into the Percepxion portal at percepxion.ai and confirm the device appears in your device list.

If **Status of Client** is unable to register or shows other errors: Check that TCP 443 is open from the SLC 9000 to the internet. Run `diag lookup api.percepxion.ai` from the CLI to verify the name can be resolved. Run `show px connecttest` to observe if there are any connection

errors. If registration fails, the client retries every 30 seconds to 16 minutes automatically, check the General log (Services > SSH/Telnet/Logging) for error messages.

Percepxion Client Settings

Percepxion Client	Enables or disables the Percepxion client. Enabled by default. When enabled, the client registers with the Registration Host at startup. Disabling may take up to 30 seconds to take effect.
Interval between Status Updates	How often the device sends status to Percepxion. Default: 2 minutes. Range: 1–60 minutes.
Interval between FW and Config Checks	How often the device checks for firmware and configuration updates from Percepxion. Default: 24 hours. Range: 1–72 hours.
Firmware Updates via Percepxion	When enabled, Percepxion can push firmware updates to this device. The update is applied to the inactive boot bank (the device retains the previous firmware for rollback). Enabled by default.
Configuration Updates via Percepxion	When enabled, Percepxion can push configuration updates to this device. ***Warning:*** ***WARNING: When a configuration update is found, it is applied and the device reboots immediately. If this device is in production, coordinate with your Percepxion administrator before enabling, and ensure that any scheduled configuration pushes are timed to maintenance windows. Enabled by default.***
Reboot after Firmware Update	When enabled, the device reboots automatically after a successful firmware update from Percepxion. Disabled by default.
Allow Remote Connections	When enabled, Percepxion users can open CLI and device port sessions directly from the Percepxion portal. Enabled by default.
Audit Log Messages	When enabled, audit log entries from this device are pushed to Percepxion for central viewing. Enabled by default.
Connect to	Cloud or On-Premise. Cloud connects to Percepxion's hosted service. On-Premise connects to a self-hosted Percepxion server. Cloud is selected by default.

Device Attributes

Device Name	The name this device displays as in the Percepxion portal. Default is "SLC" plus the last 4 characters of the Eth1 MAC address. ***Note:*** *"Device Name" is a unique configurable field that is different than the SLC hostname.*
Device Description	Optional longer description shown in the Percepxion portal.
Device ID	The unique 32-character identifier for this device. Read-only. If blank, contact Lantronix Technical Support.
Configuration Version	(read-only) Percepxion users can assign a user defined configuration version to a configuration that is pushed to a console manager. The configuration version can consist of digits and periods, starting and ending with a digit, up to 32 characters.

Remote Access Idle Timeout

Remote Access CLI Timeout	Remote Access CLI Connection will be idle timed out after a specified number of seconds as defined in the Seconds field to the right. Enter a value from 1 to 1800 seconds. The default is 600 seconds.

Remote Access Device Port Timeout	Remote Access Device Port Connection will be idle timed out after a specified number of seconds as defined in the Seconds field to the right. Enter a value from 1 to 1800 seconds. The default is 600 seconds.

Registration Host Settings

Registration Host	The Percepxion server the device registers with. For Percepxion Cloud, use api.percepxion.ai. For on-premise, enter the hostname your Percepxion administrator provides.
Registration Port	TCP port for registration. Default: 443.
Use HTTPS for registration	Should always be enabled. Enabled by default.
Validate certificates with HTTPS	Enable if your organization requires certificate validation for Percepxion connections. If enabled and no certificate authority file has been uploaded, the client may fail to connect.
Messaging Services	If enabled, messaging services are used for status updates and commands. Enabled by default.

Proxy Server Settings

If your network requires a proxy to reach the internet, configure the proxy here before enabling the Percepxion client.

Use Proxy	Enable to route Percepxion traffic through a proxy server. The Percepxion client must be disabled before changing proxy settings.
Proxy Type	HTTP or SOCKS5.
Proxy Host	FQDN or IP address of the proxy server.
Proxy Port	Port the proxy listens on. Default: 8080.
Proxy User Name / Password	Credentials for proxy authentication, if required.

How Percepxion Connects (Connection Sequence)

When the Percepxion client starts, at device boot, or when you enable it, it follows this sequence. Each stage is visible in the **Status of Client** field.

For more detailed information about the registration process and Percepxion client behavior, see the SLC 9000 online help.

1. **Registration**: The client contacts the Registration Host using the Device ID. If registration fails, it retries every 30 seconds to 16 minutes until successful. Registration may fail if the Device ID is invalid, or if the Registration Host is unreachable.
2. **Telemetry**: After registration, the client connects to the Telemetry Host (provided during registration) and performs a handshake. The device then publishes statistics at the interval you configure in the Percepxion web UI.
3. **Messages and Status Updates**: The client connects to the Messaging Host to receive commands and publish status updates at the configured interval.
4. **Firmware and Configuration Updates**: At the configured check interval, the client checks for firmware and configuration updates. Firmware is applied to the inactive boot bank. Configuration updates are applied immediately and trigger an immediate reboot after being applied.

5. **Web Terminal Connections**: Percepxion users can open secure CLI and device port sessions from the portal. Sessions are shown in the Connections list in the SLC web UI and CLI.
6. **Performance Monitoring Probes and Custom Scripts**: Percepxion can deploy probes and scripts to this device for performance monitoring and automation.
7. **CLI Commands**: Percepxion can issue CLI commands to this device. Commands requiring interactive input, abbreviated commands, and multiple CLI commands sent together are not supported.

Zero-Touch Deployment via Percepxion

For fleet deployments, deploying 10 or more SLC 9000 units to remote sites, Percepxion supports a bulk pre-registration workflow. Devices shipped to remote sites call home automatically when powered on, join your Percepxion project, and receive their configuration without any on-site intervention.

What you need:

- A Percepxion account with your project already set up
- The Serial Number and Device ID for each device you are deploying (printed on device labels; also available from your Lantronix order documentation)
- A configuration template saved in Percepxion (Operations > Configuration > Basic > Templates)
- Login to Percepxion to view the Percepxion help, accessible with the ? Icon.

Step 1: Bulk import devices into Percepxion

1. Create a CSV file. The file must be formatted exactly as follows:

   serial_num,device_id,device_name,device_description,tag

2. Add one row per device. Example:

   serial_num,device_id,device_name,device_description,tag
   A1B2C3D4,AABBCCDDEEFF00112233445566778899,Chicago-SLC-01,Chicago datacenter,datacenter:chicago

3. In the Percepxion portal, navigate to Explore > + Devices > Lantronix Device.
4. Select **Multiple Devices**, click **Upload Device List**, and select your CSV file.
5. If you want devices automatically assigned to a specific tenant, enable **Auto Assign Devices** and select the target organization.
6. Click **Import**.

Once the devices are imported they will appear in your device list when they come online.

Step 2: Set up a configuration template

1. Configure one SLC 9000 exactly as you want all deployed devices configured.
2. In the Percepxion portal, navigate to Operations > Configuration > Basic. Refer to the Percepxion help for Configuration and Templates, and follow the instructions on how to create a Template that can be applied to multiple devices.
3. Click the Templates tab, then click + Template.

4. Select your configured device as the source and save the template with a descriptive name.

Step 3: Create a Smart Group for new devices

Smart Groups automatically collect devices that match rules you define. Use a Smart Group to target newly registered devices.

1. Navigate to Explore > Smart Groups and click + Smart Group.
2. Define a rule using the model name (e.g., model:SLC 9000) or a device tag you applied during the CSV import (e.g., tag.datacenter:chicago).
3. Save the Smart Group.

Step 4: Create a configuration update job

1. Navigate to Operations > Configuration > Basic and click **+ Update**.
2. Select your configuration template.
3. Assign the update to the Smart Group you created.
4. Check **Enable Update when created**.
5. Click **Save**.

When a new device registers with Percepxion, it is automatically added to matching Smart Groups. The enabled configuration update job pushes the template to the device at its next content check interval. The device applies the configuration and reboots if required.

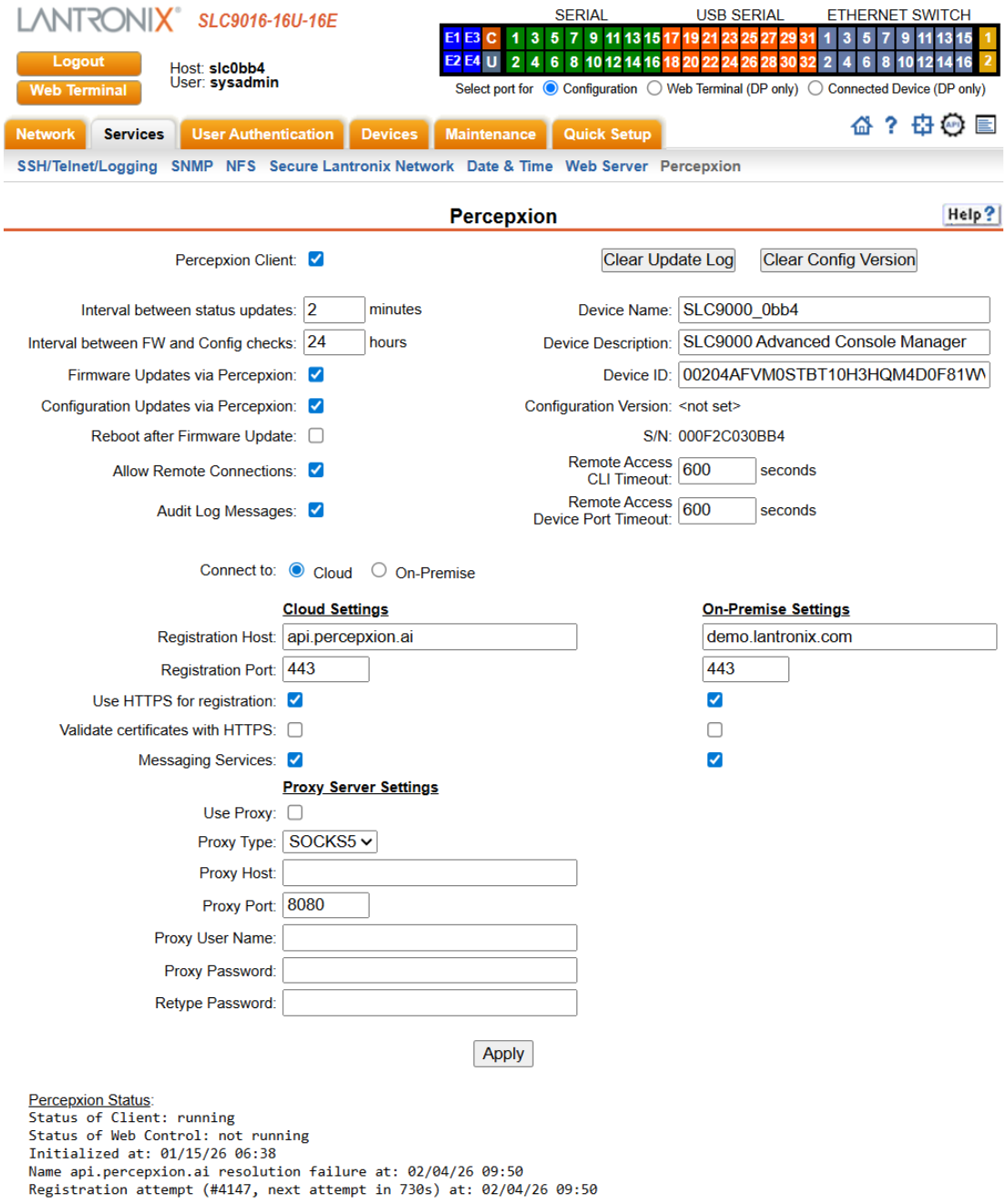
Step 5: Ship devices to the remote site

Devices require no additional configuration before shipping. When a device is powered on with internet access, it calls home to api.percepxion.ai using its Device ID, joins your project, receives its configuration, and is ready for use, no on-site visit required.

To configure Percepxion settings:

1. Click the **Services** tab and select the **Percepxion** option. The following page displays.

Figure 8-1 Services > Percepxion



2. Configure settings as required.
3. To save, click **Apply**.

Percepxion Commands

Go to *Percepxion Commands* to view CLI commands which correspond to the web page entries described above.

9: USB Port

This chapter describes how to configure storage (thumb drive), USB modems, and USB serial devices. A thumb drive is useful for firmware updates, saving and restoring configurations and for device port logging. See *Firmware & Configurations (on page 310)*.

The console manager supports a variety of thumb drives, and modems.

This chapter describes the Web Manager pages and available CLI commands that configure the SLC USB ports. This chapter contains the following sections:

- *USB Storage*
- *USB Modem Settings*
- *USB Serial Settings*

USB Storage

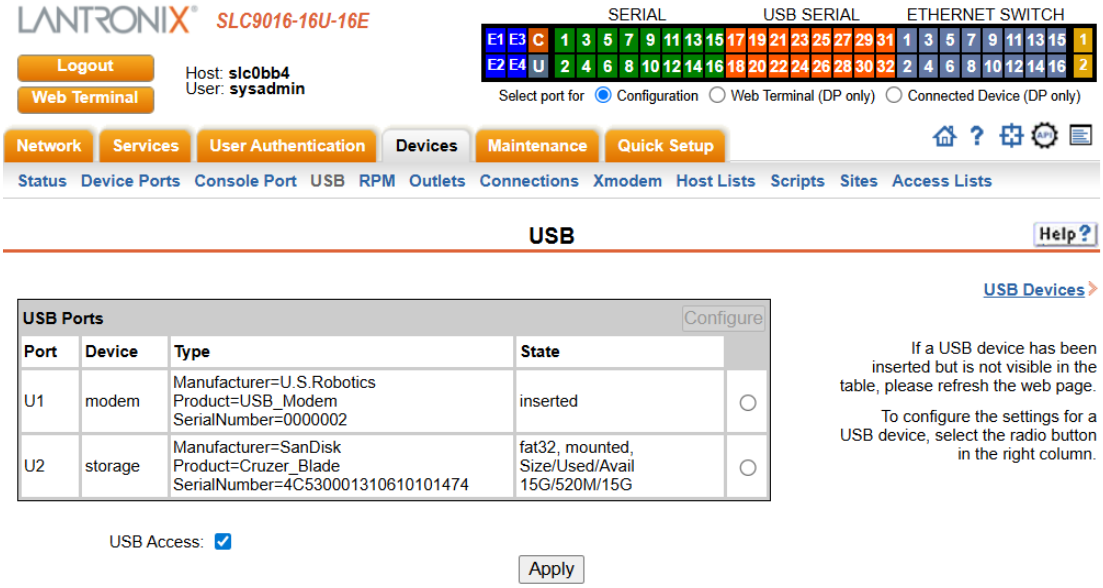
The *Devices > USB* page has a checkbox for USB access. This checkbox is a security feature to ensure that access to any USB deviceis disabled if the box is unchecked. If unchecked, the SLC unit ignores any device plugged into the port.

To set up USB storage in the SLC 9000 advanced console server:

1. Insert any of the supported storage devices into the USB port on the front of the SLC unit. You can do this before or after powering up the SLC 9000 advanced console server. If the first partition on the storage device is formatted with a file system supported by the SLC unit (ext2, FAT16 and FAT32), the card mounts automatically.
2. Log into the SLC unit and click **Devices**.
3. Click **USB**. *Figure 9-1* shows the page that displays. Your storage device should display in the appropriate row of the USB ports table if you have inserted it. If it does not display and you have inserted it, refresh the web page.
4. View the USB information and options available on the page:

Port (view only)	Port on the SLC unit where the USB device is inserted.
Device (view only)	Type of USB device (modem or storage).
Type (view only)	Information read from USB device.
State (view only)	Indicates if the device is mounted, and if mounted, how much space is available.
USB Access (check box)	Check to enable **USB Access**. Uncheck to disable USB access.

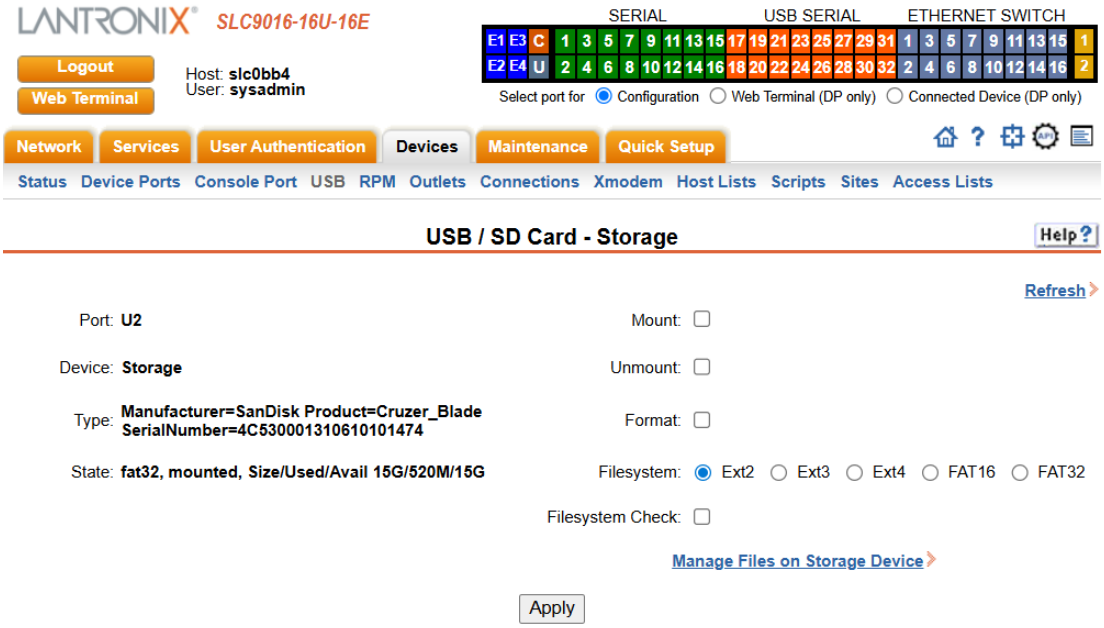
Figure 9-1 Devices > USB



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

1. Click the radio button (on the far right) of a USB device storage port.
2. Click **Configure**.
   - *Figure 9-2* shows the page that displays if a USB storage device is inserted.

Figure 9-2 Devices > USB > USB - Storage



3. Enter the following fields.

Mount	Select the checkbox to mount the first partition of the storage device on the SLC unit (if not currently mounted). Once mounted, a USB thumb drive is used for firmware updates, device port logging and saving/ restoring configurations.
Unmount	To eject the USB thumb drive from the SLC unit , first unmount the thumb drive. Select the checkbox to unmount it. ***Warning:*** ***If you eject a thumb drive from the SLC unit without unmounting it, subsequent mounts of a USB thumb drive may fail, and you will need to reboot the device to restore thumb drive 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 **ext3**, **ext4**, **ext2**, **FAT16** or **FAT32**, the filesystems the console manager 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**.
5. Click the **Manage Files on Storage Device** link to view and manage files on the selected USB thumb drive. See the next section for more information.

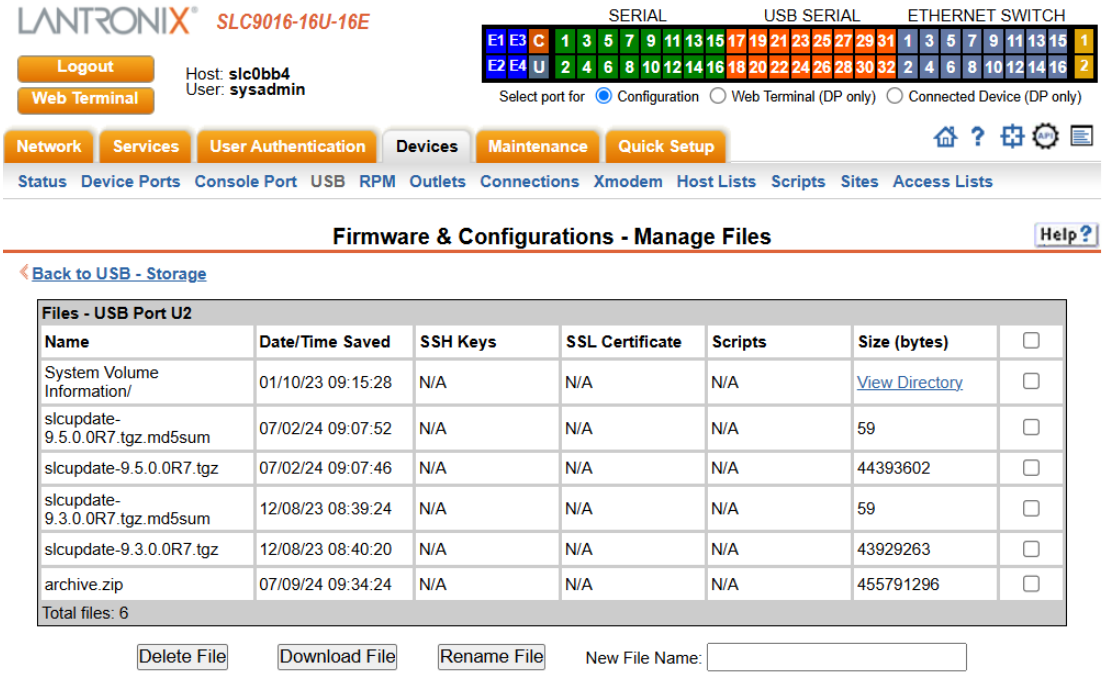
Manage Files on Storage Device

Files on the storage device may then be deleted, downloaded or renamed.

To manage files, perform the following steps.

1. Click the **Manage Files on the Storage Device** link on the *Devices > USB > USB - Storage* page.

Figure 9-3 Firmware and Configurations - Manage Files



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**.

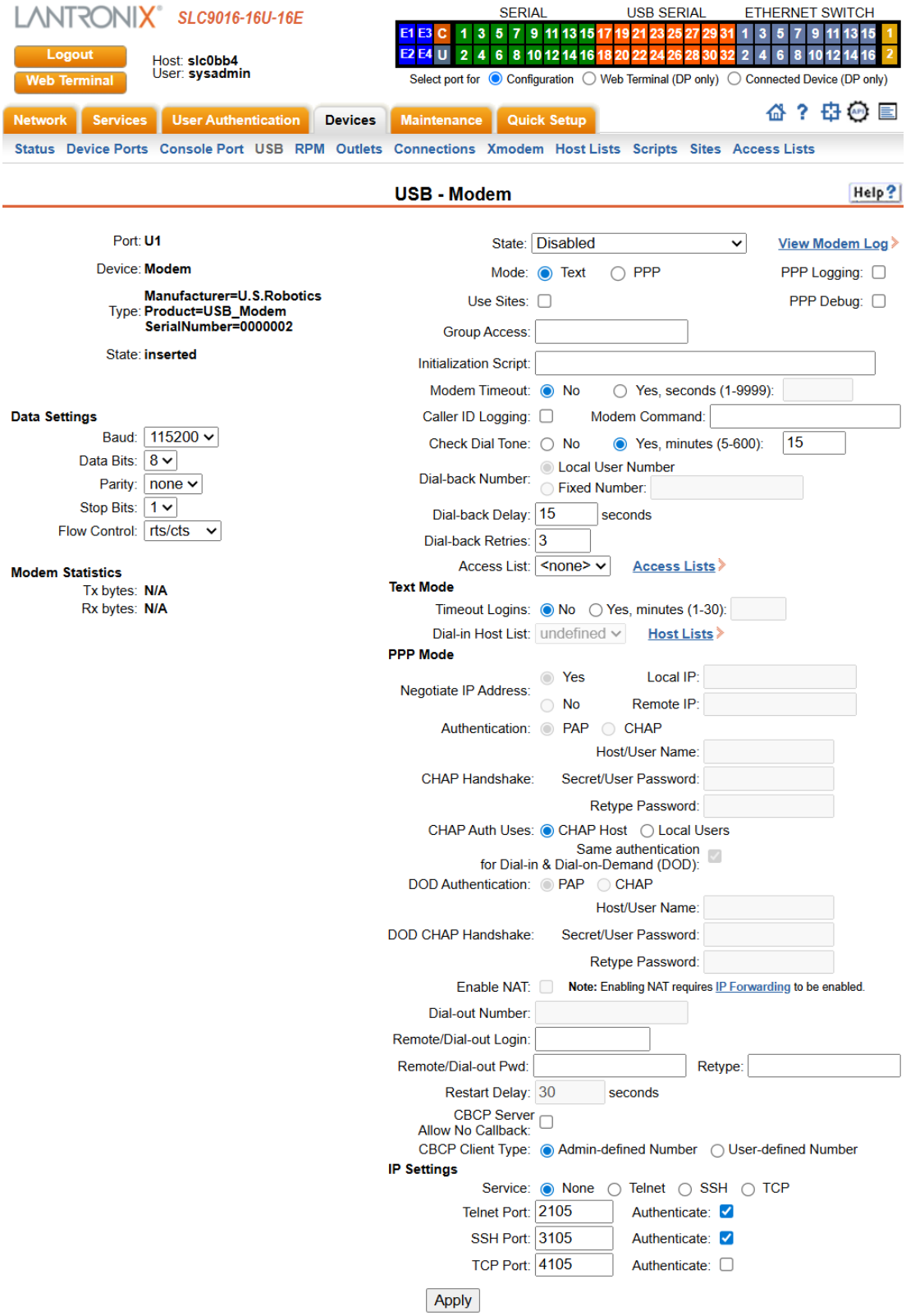
USB Modem Settings

Use a USB modem to provide out-of-band management access when the primary network is unavailable.

To enter USB modem settings for a USB:

1. Insert any of the supported USB modem devices into the USB port on the front of the SLC unit. You can do this before or after powering up the console manager.
2. Log into the SLC unit and click **Devices**.
3. Click **USB**. *Figure 9-1* shows the page that displays. Your USB device should display in the appropriate row of the USB ports table if you have inserted it. If it does not display and you have inserted it, refresh the web page.
4. Click the radio button (on the far right) for Port U1 or U2.
5. Click **Configure**. *Figure 9-4* shows the page that displays if a USB modem is inserted in Port U1, or Port U2, if that port is selected.

Figure 9-4 Devices > USB > USB - Modem



6. 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. ***Note:*** *Cypress ACM-based USB to serial chip set does not support 230400 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**.

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, dial-on-demand, dial-in/host list, or dial in, dial-on-demand, CBCP Server, and CBCP Client. Disabled by default. See *Modem Dialing States (on page 234)* for more information.
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 9000 advanced console server connects to an external network), dial-in mode (e.g., the external computer connects to the network that the SLC unit 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 9000 advanced console server. 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 unit may properly control the modem.*
Modem Timeout	Timeout for all modem connections. Select **Yes** (default) for the SLC 9000 advanced console server 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.
Check Dial Tone	If enabled, the SLC will periodically check the modem for a dial tone while waiting for a dial in (e.g., if the Modem State is set to Dial-in, or if the Modem State is set to Dial-back and the SLC unit is in the Dial-in portion of the sequence). The SLC unit can issue a trap or an event can be setup to notify the user if no dial tone is detected. Enabled by default (every 15 minutes).
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 9000 advanced console server 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 171)* 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	Specify the number of times to retry dialing back.
Access List	For the dial-in state, a modem access list (or white list) that defines which phone numbers will be granted access to the console manager. See *Access Lists on page 232* for more information.

Text Mode

Text mode passes raw serial data. PPP mode establishes a network-layer connection.

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 unit successfully connects to one. To establish and configure host lists, click the **Host Lists** link. *Host Lists (on page 197)*

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 unit 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** and **Chap Local** 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 access the network connected to Eth1 and/or Eth2. ***Note:*** *IP forwarding must be enabled on the Network > Network Settings (2 of 2) page for NAT to work. See 6: Networking on page 51.*
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 device when it dials in. 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.
Remote/Dial-out Pwd	Password for authentication when dialing out to a remote system, or if a remote system requests authentication from the SLC 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.
Restart Delay	The number of seconds after the timeout and before the SLC 9000 advanced console server 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.

IP Settings

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

7. Click **Apply**.

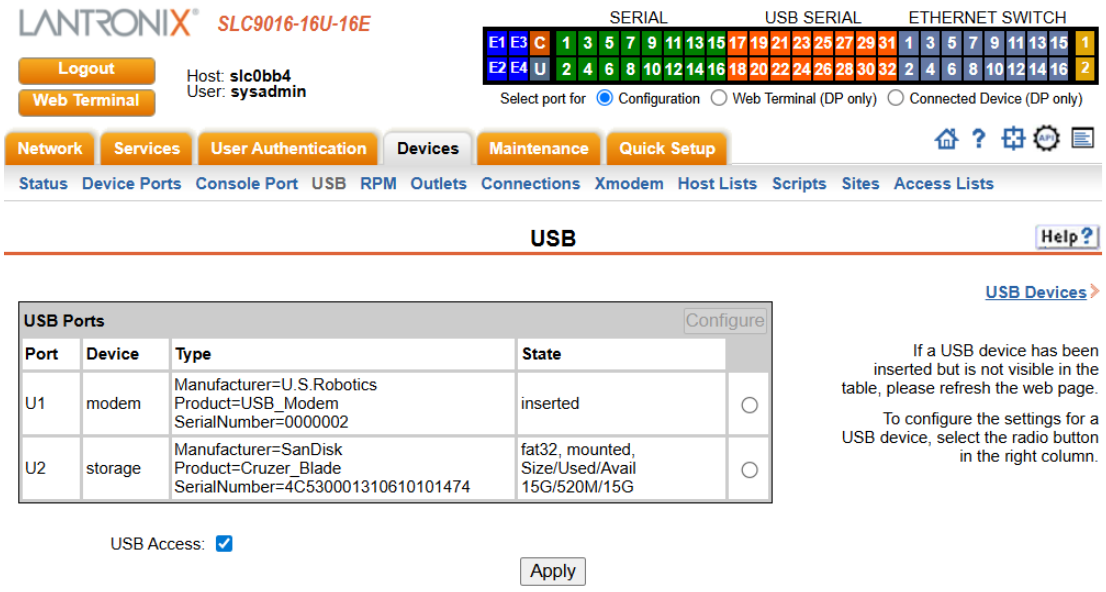
USB Serial Settings

The console manager supports connecting USB serial devices to the front USB ports. A user can interact with the device by logging into the CLI and performing a **connect direct** to the USB port, or by establishing a SSH, Telnet or TCP connection to the USB port. A maximum of 3 concurrent sessions to the port are allowed.

To enter serial settings for a USB:

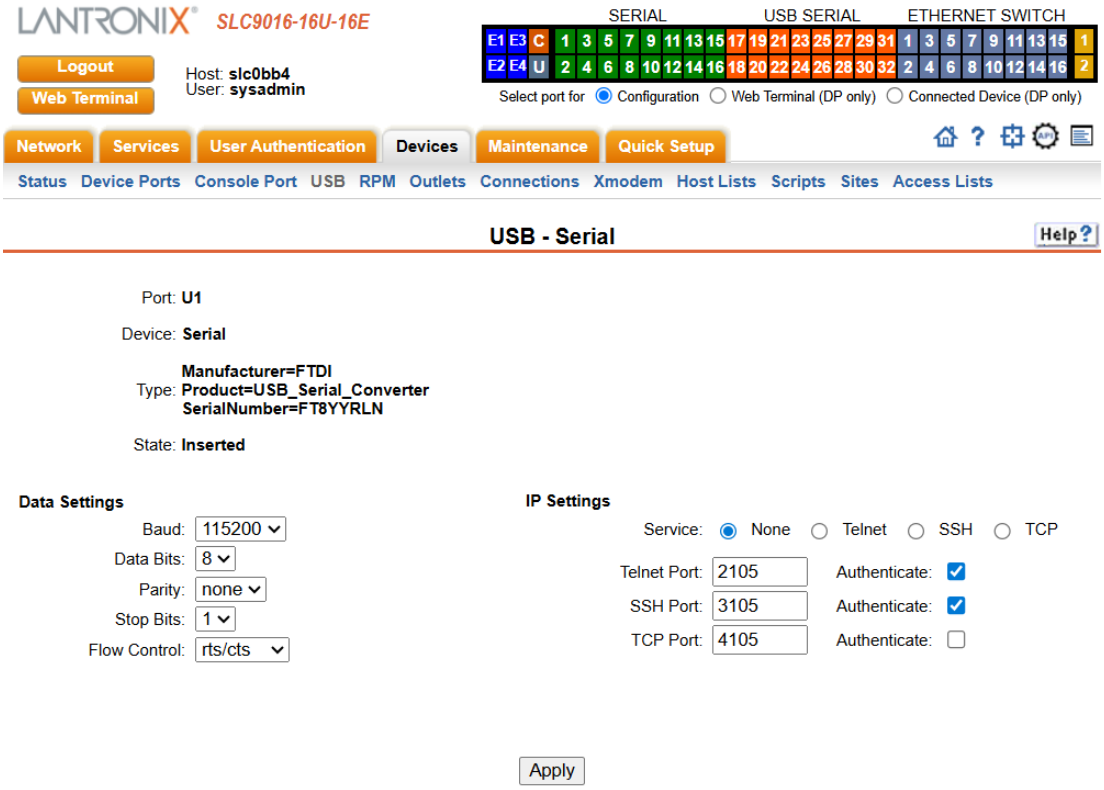
1. Insert any of the supported USB serial devices into the USB port on the front of the SLC unit. You can do this before or after powering up the console manager.
2. Log into the SLC unit and click **Devices**.
3. Click **USB**. *Figure 9-5* shows the page that displays. Your USB device should display in the appropriate row of the USB ports table if you have inserted it. If it does not display and you have inserted it, refresh the web page.

Figure 9-5 Devices > USB - Serial Port



4. Click the radio button (on the far right) for Port U1 or U2.
5. Click **Configure**. *Figure 9-6* shows the page that displays if a USB modem is inserted in Port U1, or if Port U2 is selected.

Figure 9-6 Devices > USB > USB - Serial



6. Complete or view the following sections:

Data Settings

Baud	The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so this is the default. Check the equipment settings and documentation for the proper baud rate.
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.
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.
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.
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.

IP Settings

Service	The available connection services for this USB Port (Telnet, SSH, or TCP). Only one can be active at a time. The default is None.
Telnet Port	Telnet Port Telnet session port number to use if you selected Telnet. Defaults: ◆ USB Port U1: **2049** ◆ USB Port U2: **2050** ◆ Range: **1025-65535**
SSH Port	The SSH session port number to use if you selected SSH. Defaults: ◆ USB Port U1: **3049** ◆ USB Port U2: **3050** ◆ Range: **1025-65535**
TCP Port	The TCP (raw) session port number to use if you selected TCP. Defaults: ◆ USB Port U1: **4049** ◆ USB Port U2: **4050** ◆ Range: **1025-65535**
Authenticate	If selected, the console manager requires user authentication before granting access to the port. Authenticate is selected by default for Telnet Port and SSH Port, but not for TCP Port.

7. To save settings for just this port, click **Apply**.

USB Commands

Go to *USB Access Commands*, *USB Device Commands*, *USB Storage Commands*, *USB Modem Commands*, and *USB Serial Commands* to view CLI commands which correspond to the web page entries described above.

10: Device Ports

This chapter describes how to configure and use an SLC advanced console server port connected to an external device, such as a server or a modem. The subsequent chapter, *Chapter 14: Connections* describes how to use the *Devices > Connections* 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 the IP address. For Telnet and SSH, use the default TCP port number (23 and 22, respectively) to connect to the device port. For raw TCP, use the TCP port number defined for TCP In to the device port according to the *Device Ports - Settings* section.
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/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).

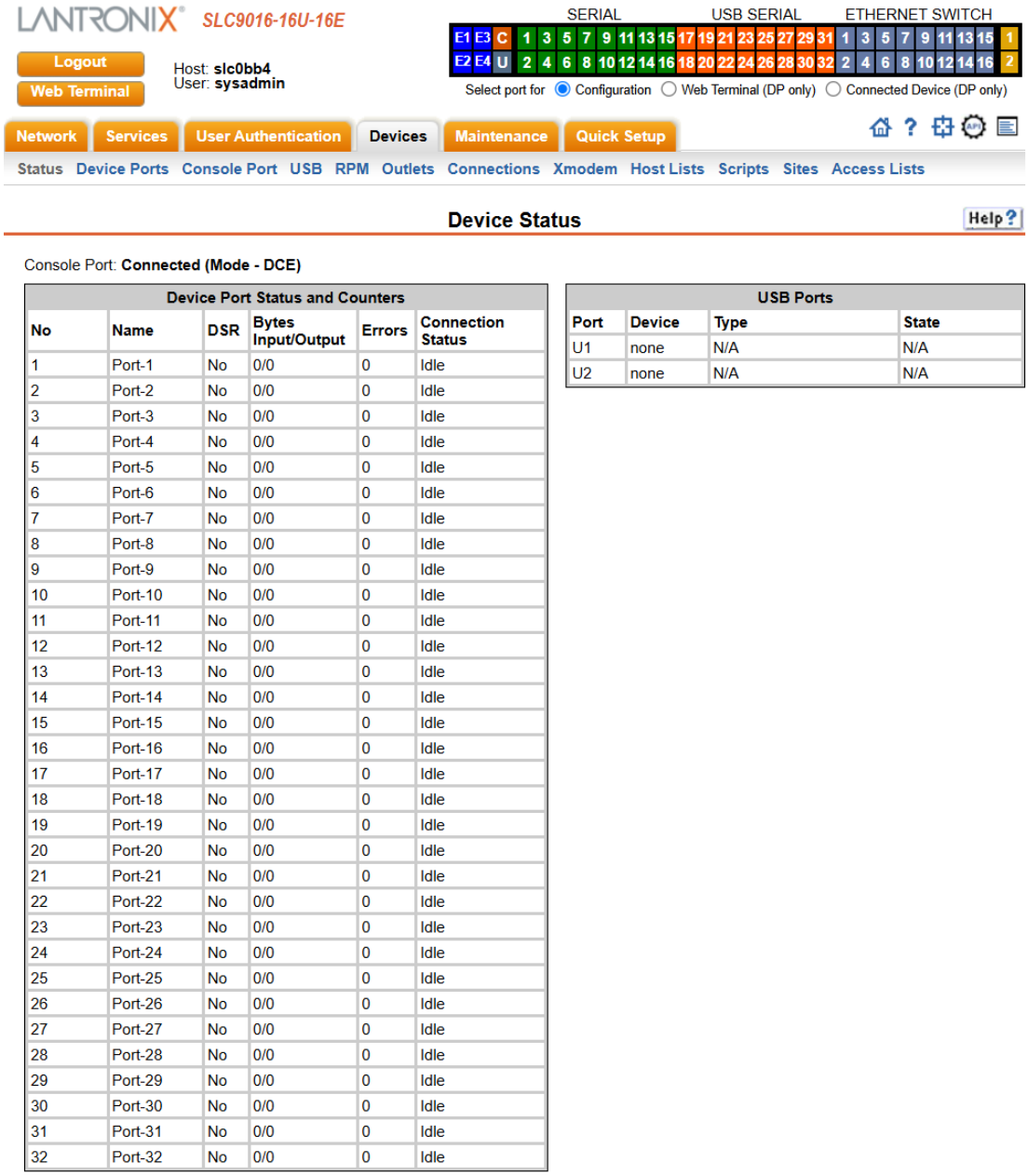
The administrator and users with local user rights may assign individual port permissions to local users. The administrator and users with remote authentication rights assign port access to users authenticated by NIS, RADIUS, LDAP, and TACACS+.

Device Status

The *Devices > Device Status* page displays the status of the SLC ports and USB ports.

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

Figure 10-1 Devices > Device Status

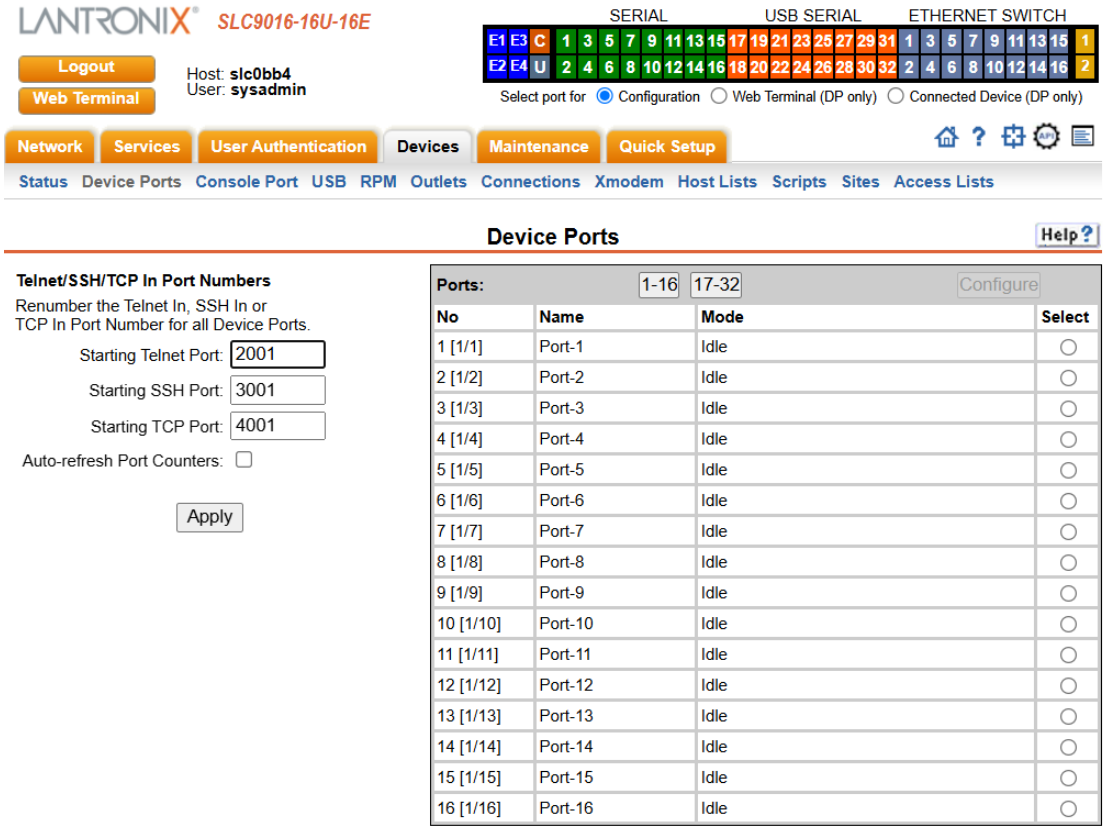


Device Ports

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 10-2 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 171).*
	An external modem is connected to the port. The user may dial into or out of the port.
	Telnet in or SSH in is enabled for the device port. The device port is either waiting for a Telnet or SSH login or has received a Telnet or SSH login (a user has logged in).

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

1. Enter the following:

Telnet/SSH/TCP in Port Numbers

Starting Telnet Port	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, port 1 will be 2001 and subsequent 2000 ports are automatically assigned numbers 2001, 2002, and so on.
Starting SSH Port	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, port 1 will be 3001 and subsequent 3000 ports are automatically assigned numbers 3001, 3002, and so on.
Starting TCP Port	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, port 1 will be 4001 and subsequent 4000 ports are automatically assigned numbers 4001, 4002, 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 send print jobs to the printer over the network. ***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).*
Auto-refresh Port Counters	Select to enable auto-refresh of the Device Port Status and Counters (bytes input, bytes output) on the Device Port Settings page. Disabled by default.

Caution: ***Ports 1-1024 are RFC-assigned and may conflict with services running on the SLC 9000 advanced console server. Avoid this range.***

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 (1 of 2)* 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 171)*.

Device Port Global Commands

Go to *Device Port Commands* to view CLI commands which correspond to the web page entries described above.

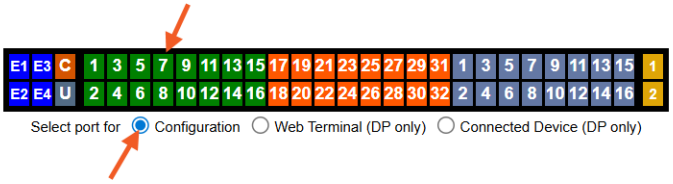
Device Ports - Settings

On the *Device Ports > Settings (1 of 2)* page, configure IP and data (serial) settings for individual ports, and if the port connects to an external modem, modem settings as well.

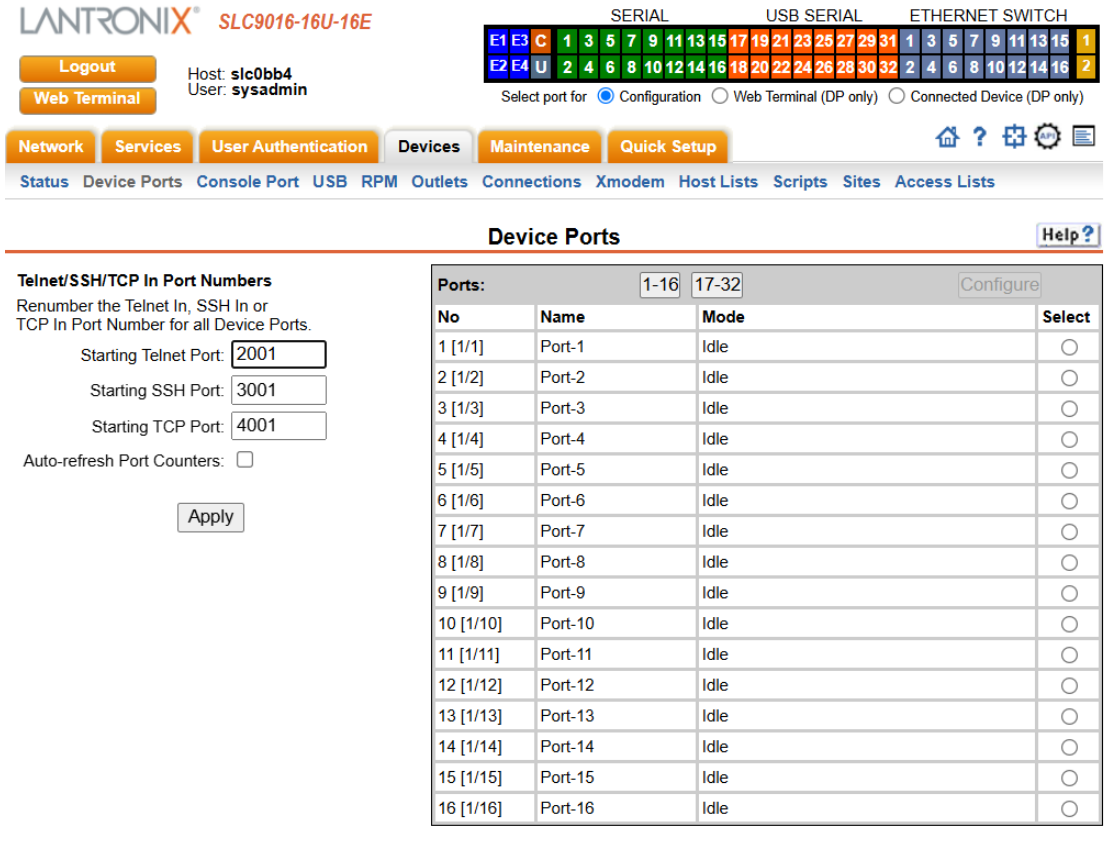
To open the Device Ports - Settings page:

1. You have two options:

   - **Dashboard**
     Make sure the **Configuration** radio button directly beneath the *Dashboard* is selected and click the desired port number in the *Dashboard*.



   - **Device Ports Page**
     Click the Devices tab, then click the Device Ports link. Select the port you want to configure and then click the Configure button. Higher numbered ports can be displayed using the "1-16", "17-32" and "33-48" buttons at the top of the Device Port list.



The following page displays:

Figure 10-3 Device Ports > Settings (1 of 2)

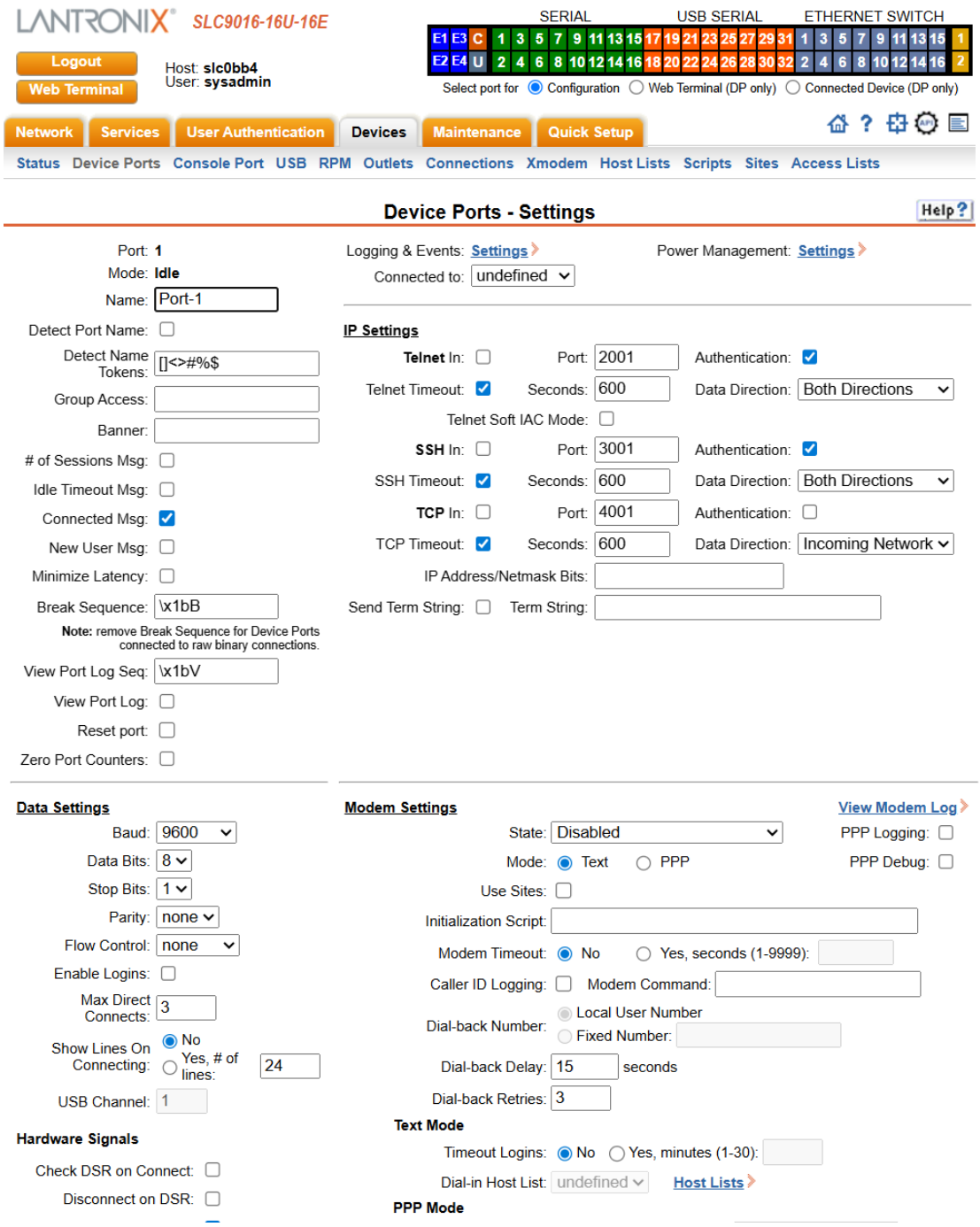
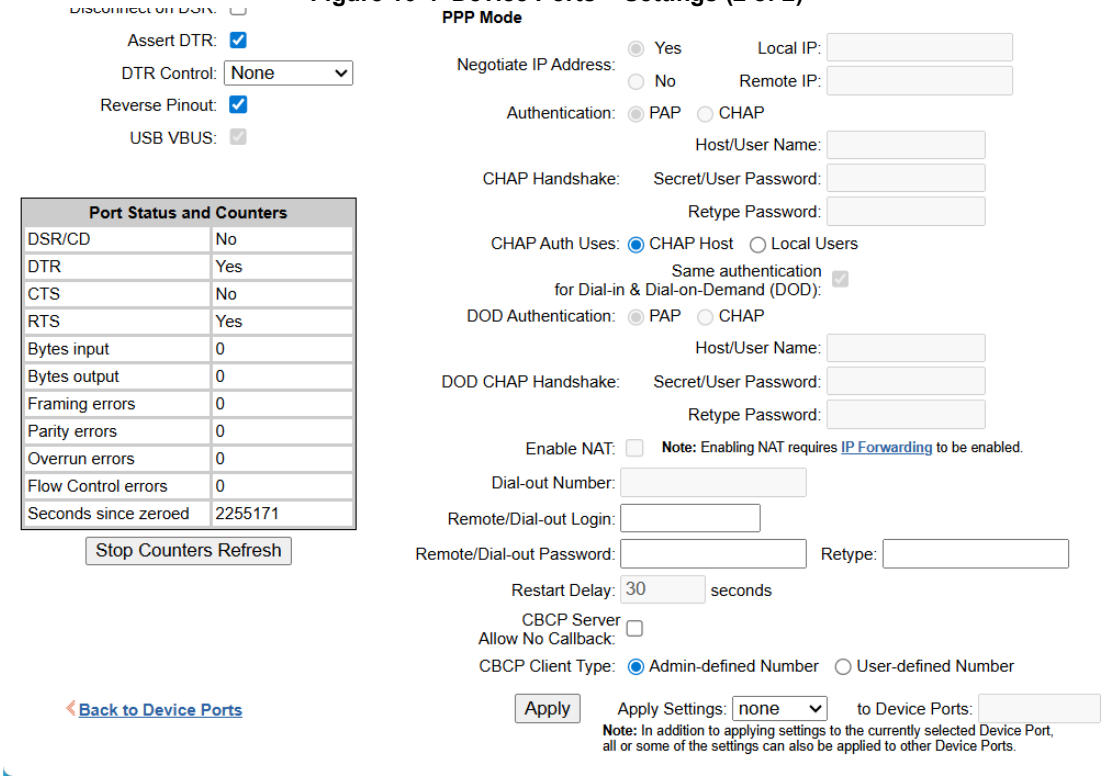


Figure 10-4 Device Ports > Settings (2 of 2)



2. Enter the following:

Device Port Settings

Port	Displays number of port; displays automatically.
Mode	The status of the port; displays automatically.
USB Device	This field is only displayed for USB ports. If a USB device is connected to the device port, this displays the USB version, speed, and a short type description for the USB device. The SLC supports up to 48 USB type A (Host) devices at data rates of HS (480 Mbit/s), FS (12 Mbit/s) or LS (1.5 Mbit/s). Each port has VBUS 5V support of up to 100mA (but not too exceed 600mA total per 16-port USB I/O module). Drawing more than 150 mA on a USB device port will shut down the VBUS 5V. USB ports are designed for data traffic only, and are not designed for charging or powering devices. Overcurrent conditions may disrupt operations.
Name	The name of the port. Valid characters are letters, numbers, dashes (-), periods, and underscores (_).
Detect Port Name	If enabled, the SLC will attempt to detect the hostname of the device connected to the device port, and set the device port name to the detected hostname. Many devices use their hostname or another identifier as the device prompt, and the SLC can extract this name from the prompt using the **Detect Name Tokens**. If the device port name is set to the default value, when a user interacts with a device connected to a device port, the SLC will look for the device prompt and set the device port name. The device prompt must be output at least 3 times in a single session for the prompt to be detected and the name extracted from the prompt. Any characters that are not part of the allowed characters for the device port **Name** will be removed. If the device name is automatically detected, the name will be logged in the Device Ports log.

Detect Name Tokens	If **Detect Port Name** is enabled, the SLC will attempt to extract a hostname or other identifier from the device prompt, to use as the device port name. The SLC will extract any name between either the start of a line sent from the device up until one of the tokens, or any part of a prompt that does not include the tokens, as the device port name. For example, if the device prompt is set to [slc431d]>, and the Detect Name Tokens include "[" and "]", the SLC will extract the identifier **slc431d** and set it as the device port name. If the device prompt is set to myrouter>, and the Detect Name Tokens include ">", the SLC will extract the identifier myrouter and set it as the device port name.
Group Access	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 "group=group1,group2;" or "group1,group2,group3".
Banner	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.
# of Sessions Msg	If enabled, a message will be displayed to a user when connecting to a device port that indicates how many users are currently connected to the device port. Disabled by default.
Idle Timeout Msg	If enabled, a message will be displayed to a user when their connection to a device port will be terminated soon due to the connection being idle. Disabled by default. ***Note:*** *When the Idle Timeout Msg is enabled, the terminal application timeout values for Telnet, SSH and TCP should be set to a value greater than 15 seconds.*
Connected Msg	If enabled, a message will be displayed to a user when they initially connect to a device port. Enabled by default.
New User Msg	If enabled, a message will be displayed to all the users connected to the device port when a new user connects to the same device port. Disabled by default.
Minimize Latency	Minimize device port latency by reducing read delays. This may improve communication efficiency in scenarios where a series of short messages are exchanged, but may increase CPU utilization and decrease throughput in cases where large messages are transmitted. Disabled by default.
Break Sequence	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**. See *Key Sequences on page 238* for notes on key sequence precedence and behavior.
View Port Log Seq	The key sequence used to view the Port Log while in Connect Direct mode. Non-printing characters can be specified by giving their hexidecimal code (see **Break Sequence** above). The default is **Esc+V** (\x1bV). See *Key Sequences on page 238* for notes on key sequence precedence and behavior.
View Port Log	Select to allow the user to enter the View Port Log Sequence to view the Port Log during Connect Direct mode. The default is disabled.

Zero Port Counters	Resets all of the numerical values in the Port Counters table at the bottom of the page to zero (0).
Logging & Events	Click the **Settings** link to configure file logging (see *Device Ports - Logging and Events on page 188*), email logging, local logging, and USB logging.
Power Management	Click the **Settings** link to configure power supplies for the device connected to this device port on the *Device Ports - Power Management* page.
Connected to	The type of device connected to the device port. Currently, the SLC unit supports Remote Power Managers (PDUs and UPSes) from 140+ vendors, as well as Sensorsoft devices. If the connected device is an RPM, the user can assign an RPM to the device port by either select an existing RPM (via the **Select** dropdown) or clicking the **Add RPM** link to configure a new RPM for the SLC. If an RPM is already assigned to the device port, the user can click on the **Selected RPM** link to view status and configuration for the RPM. If the connected device is a Sensorsoft device, the user can click on **Device Commands** to manage the Sensorsoft device. If the type of device connected to the device port is not listed, select **Undefined**. ***Note:*** *Sensorsoft temperature/humidity devices are supported with USB-to-serial adapters (ftdi/pl2303/cp210x) but are not supported for use with USB-to-Serial CDC_ACM devices.*

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. The value must be unique on the SLC 9000; for example, you cannot have two or more ports numbered 10001.
Authentication	If selected, the SLC unit requires user authentication before granting access to the port. **Authenticate** is selected by default for **Telnet** in and **SSH in**, but not for **TCP in**.
Telnet/SSH/TCP Timeout	Select the checkbox to cause an idle Telnet, SSH or TCP connection to disconnect after a specified number of seconds as defined in the Seconds field to the right.
Seconds	Enter a value from 1 to 3600 seconds if selecting the Telnet, SSH or TCP Timeout checkbox to the left. The default is 600 seconds. ***Note:*** *When the Idle Timeout Msg is enabled, the terminal application timeout values for Telnet, SSH and TCP should be set to a value greater than 15 seconds.*
Data Direction	If a Telnet, SSH or TCP connection has the idle **Timeout** enabled, this setting indicates the direction of data use to determine if the connection has timed out: incoming network data, outgoing network data, or data from both directions. The default is **Both Directions** for **Telnet** and **SSH**, and **Incoming Network** data for **TCP**.
Telnet Soft IAC Mode	When Telnet Soft IAC mode is enabled, the Telnet server will not block waiting for the initial Telnet protocol IAC option responses. An abbreviated list of IAC options will be sent to the client, including a request for client side Echoing. Disabled by default.

IP Address/Netmask Bits	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. ***Note:*** *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.*
Send Term String/Term String	If **Send Term String** is enabled and a **Term String** is defined, when a network connection to a device port is terminated, the termination string is sent to the device connected to the device port. The string should be defined so that it sends the appropriate command(s) to the device to terminate any active user sessions, e.g. "logout" or "exit". The string may contain multiple commands separated by a newline ("\n") character. This is a security mechanism used to close sessions that are inadvertently left open by users.

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.*

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. The baud rate can also be set from the Power Management and Baud Rate menu. See the Device Ports - Power Management page.
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.
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**.
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**.
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**.
Enable Logins	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.
Max Direct Connects	Enter the maximum number (1-15) of simultaneous connections for the device port. The default is 1.

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 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. For example, if the SLC user issues the `ls` command to display a directory on a Linux server, then exits the connection, the results of the `ls` will be stored in the buffer. When the SLC user then 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.
USB Channel	Applies to USB device ports only. When a dual channel USB device is connected to the device port, this allows the user to select which of the channels is the active channel used for all connections. Only one channel can be active at any time. Enter the number **1** or **2**. The default is **1**.

Hardware Signal Triggers

Note: *When the DSR signal drops on a device port, indicating that the attached cable has been disconnected or the attached device has been powered off, the SLC will log the event in the Device Ports system log and send a slcEventDevicePortAction SNMP trap. The log message and SNMP trap only occur if there is an active (connect direct or network connection) to the device port.*

Check DSR on Connect	If this setting is enabled, the device port only establishes a connection if DSR (Data Set Ready) is in an asserted state. DSR should already be in an asserted state, not 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. ***Note:*** *Applies to serial RJ45 device ports only.*
Disconnect on DSR	If a connection to a device port is currently in session, and the DSR signal transitions to a de-asserted state, the connection disconnects immediately. Disabled is the default unless dial-in, dial-out, or dial-back is enabled for the device port. ***Note:*** *Applies to serial RJ45 device ports only.*
Assert DTR	By default, DTR (Data Terminal Ready) is asserted on a device port nearly all of the time (except momentarily when a port is opened for operations). Unchecking this option will deassert DTR, simulating a cable disconnection for the device that is connected to a device port. ***Note:*** *Applies to serial RJ45 device ports only.*

DTR Control	The type of DTR control feature. The options include: **None**, **Toggle DTR**, or **Auto Enable DTR**: **None:** No option selected. **Toggle DTR:** If enabled, when a user disconnects from a device port, DTR will be toggled. DTR will be de-asserted, and after a 2-second delay, will be re-asserted. This feature can be used when a serial connection requires DSR to be active for the attached device to connect. In this case, toggling DTR will end any active connection on the device. **Auto Enable DTR:** If enabled, DTR will be de-asserted and will remain de-asserted until the first connection (Connect Direct, Telnet, SSH, TCP In or Percepxion Web Terminal Session) is established to the device port. At this time, DTR will be asserted. DTR will remain asserted as long as any connection exists to the device port. Once the last connection is terminated, DTR will be deasserted. The Assert DTR setting is ignored if DTR Control is set to Auto Enable. ***Note:*** *Applies to serial RJ45 device ports only.*
Reverse Pinout	If enabled, swaps the positions of the serial lines, such that the direction of data or the signal is reversed. For instance, TX is swapped with RX. Enabling Reverse Pinout facilitates connections to Cisco and Sun style RS-45 console ports using a straight through Ethernet patch cable, without the need for a rolled cable or adapter. Enabled by default. ***Note:*** *Applies to serial RJ45 device ports only. All Lantronix serial adapters are intended to be used with Reverse Pinout disabled. If you are replacing an original SLC unit with an SLC 9000 advanced console server, disable the reverse pinout so you can use the original cables and adapters.*
USB VBUS	For USB Device Ports only. If enabled, the USB VBUS signal provides power to the USB device attached to a device port. Disabling VBUS will power down the device as long as it is bus-powered instead of self-powered. The VBUS 5V signal is up to 100 mA per port, but not to exceed 600mA total per USB I/O Module. Drawing more than 150 mA on a USB port will shut down the VBUS 5V. ***Caution:*** ***USB ports are designed for data traffic only. They are not designed for charging or powering devices. Over-current conditions on VBUS 5V may disrupt operations.***

Modem Settings (Device Ports)

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

State	Used if an external modem is attached to the device port. If enabling, set the modem to dial-out, dial-in, dial-back, dial-on-demand, dial-in/host list, dial-back & dial-on-demand, dial in & dial-on-demand, CBCP Server, and CBCP Client. Disabled by default. See *Modem Dialing States (on page 234)* for more information.
Mode	The format in which the data flows back and forth: ◆ **Text:** In this mode, the SLC 9000 advanced console server 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 9000 advanced console server 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 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 9000 advanced console server 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`*. Serial modems may need to include &B1 in the modem initialization string to set the DTE rate to a fixed baud rate.*
Modem Timeout	Timeout for all modem connections. Select **Yes** (default) for the SLC unit 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 device to log caller IDs on incoming calls. Disabled by default. ***Note:*** *For the Caller ID* `AT` *command, refer to the modem user guide.*
Modem Command	Modem `AT` command used to initiate caller ID logging by the modem. ***Note:*** *For the* `AT` *command, refer to the modem user guide.*
Dial-Back Number	Users with dial-back access can dial into the SLC device and enter their login and password. Once the SLC 9000 advanced console server 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 171)* 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 unit will retry the dial-out portion of the dialing sequence if the first attempt to dial-out fails.

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 9000 advanced console server successfully connects to one. To establish and configure host lists, click the **Host Lists** link. *See "Host Lists" on page 197.*

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 advanced console server 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 9000 advanced console server access the network connected to Eth1 and/or Eth2. ***Note:*** *IP forwarding must be enabled on the Network > Network Settings (2 of 2) page for NAT to work. See Chapter 6: Networking .*
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 dialing out to a remote system. May have up to 32 characters.
Remote/Dial-out Password	Password for dialing out to a remote system. 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 unit 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.

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.*

Port Status and Counters

Port Counters describe the status of signals and interfaces. SLC advanced console server 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.

Table 10-5 Port Status and Counters

Port Status and Counters	
DSR/CD	No
DTR	Yes
CTS	No
RTS	Yes
Bytes input	0
Bytes output	0
Framing errors	0
Parity errors	0
Overrun errors	0
Flow Control errors	0
Seconds since zeroed	106734

Note: *Status and statistics shown on the web interface represent a snapshot in time. To see the most recent data, reload the web page, or enable Auto-refresh Port Counters on the Device Ports web page which will refresh the data every 10 seconds. The Stop Counters Refresh button can be used to temporarily disable the counters auto-refresh so that the page can be viewed/ scrolled or values updated (auto-refresh resumes when the page is reloaded). Auto-refresh of Port Status or Counters in the CLI can be implemented with a simple script:*

```
[slc]> set script import batch via copypaste name dpCounterAutoRefresh
Please paste script; enter '.' (period) on a blank line to terminate
entry:
set cnt 5
while { $cnt >= 1 } {
    show portcounters deviceport 3
    sleep 5
    set cnt [expr $cnt - 1]
}
.
Batch script 'dpCounterAutoRefresh' imported.
[slc]> set script runcli dpCounterAutoRefresh
```

Device Ports - Power Management

In the Device Ports - Power Management page, configure power supplies that provide power to the device or server connected to the device port. Up to 4 power supplies can be configured, by selecting an RPM, an outlet on the RPM, and defining a unique name for the RPM/outlet pair. The RPM outlet pair can also be controlled (power cycled, turned on, turned off).

This page also allows the user to define the Power Management Sequence, which, when entered while the user is connected to a device port via the connect direct command, will display the Power Management and Baud Rate menu:

```
------------------------------------------
Power Management and Baud Rate Menu
------------------------------------------
RPM/outlet>>> trippOUT4        sentry3OUT15
A. Status     E. Turn On       H. Turn On
B. Help       F. Turn Off      I. Turn Off
C. Set Baud   G. Power Cycle    J. Power Cycle
D. Quit
```

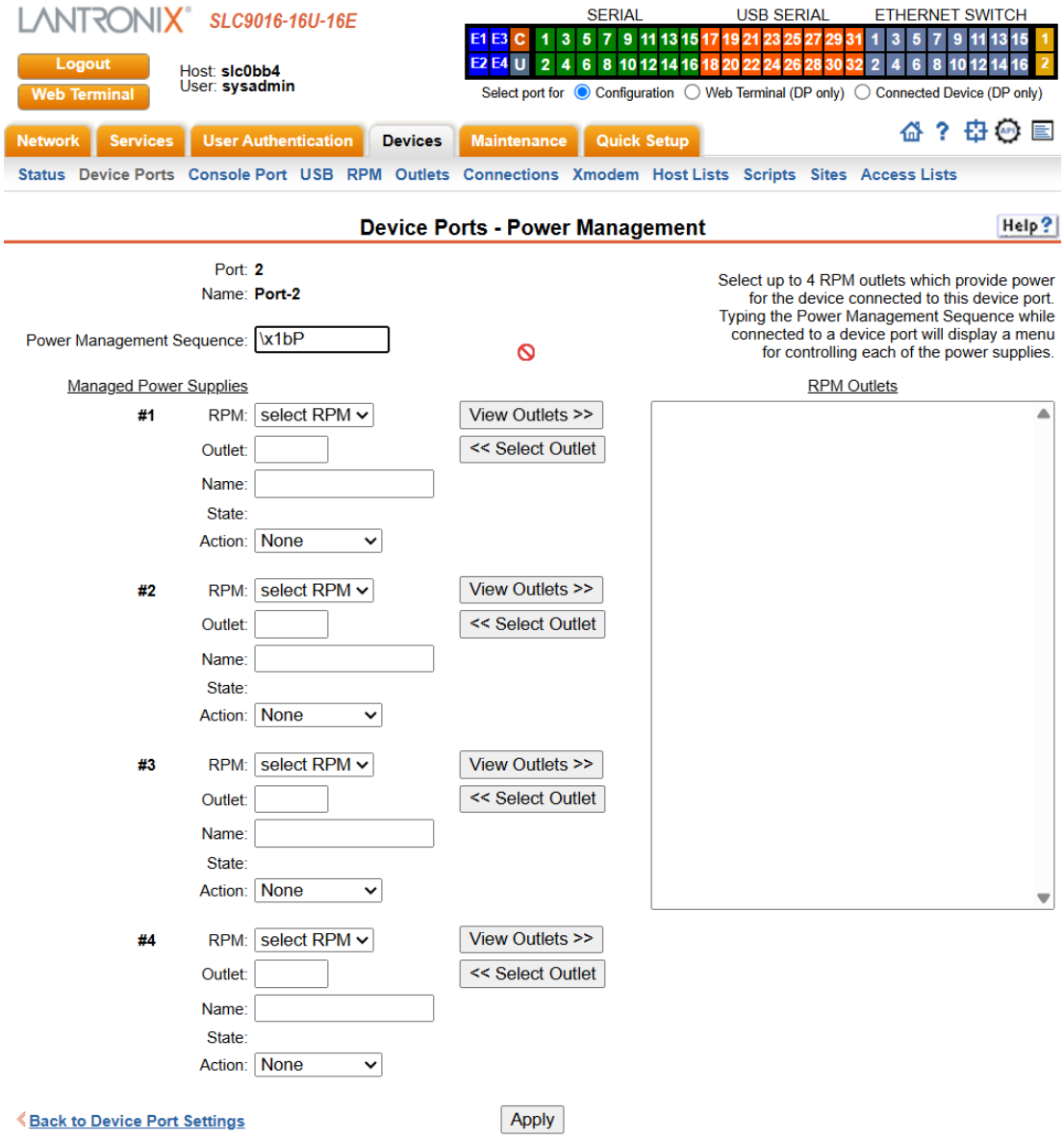
This menu allows the administrator to query status and control any of the power supplies that provide power to the device connected to the device port and change the Baud Rate of the device port.

Note: *The Baud Rate can be configured while connected to a device port by entering the* ***Power Management Sequence.*** *This will display the* ***Power Management and Baud Rate*** *menu, which provides an option to set the Baud Rate.*

To configure power management settings for a device port:

1. Connect to a specific port on the **Devices > Device Ports** page according to instructions in *To open the Device Ports - Settings page: (on page 171)*.
2. Click the **Settings** link beside **Power Management** to access the *Device Ports - Power Management* page.

Figure 10-6 Device Ports - Power Management



3. Enter the following:

Power Management Sequence	A series of one to ten characters that will display the Power Management menu when connected to the device port. The default value is **Esc+P** (escape key, then uppercase "P"). This value is specified as `\x1bP`, which is hexidecimal (`\x`) character 27 (`1B`) followed by a `P`. See *Key Sequences on page 238* for notes on key sequence precedence and behavior.
RPM	For each managed power supply, select a RPM, most likely a PDU, which has outlets that can be individually controlled, and which provides power to the device connected to the device port.

Outlet	For each managed power supply, enter the outlet on the selected RPM. As an aid to selecting the outlet, click the **View Outlets** button, then select an outlet from the list and click the **Select Outlet** button. The managed power supply outlet number will be filled in, as well as the managed power supply outlet name if a name is listed for the outlet and one has not already been defined for the managed power supply. A unique name for the managed power supply name is required; this is what will be displayed on the Power Management menu.
Name	For each managed power supply, enter the name on the selected RPM. As an aid to selecting the name, click the **View Outlets** button, then select an outlet from the list and click the **Select Outlet** button. The managed power supply outlet number will be filled in, as well as the managed power supply outlet name if a name is listed for the outlet and one has not already been defined for the managed power supply. A unique name for the managed power supply name is required; this is what will be displayed on the Power Management menu.
State	Displays the current state of the outlet when the Device Ports - Power Management web page is loaded: **on**, **off** or **unknown** if the RPM does not provide status for individual outlets or the SLC was unable to obtain the status of the outlet.
Action	The action to take on the outlet: **Cycle Power**, **On** or **Off**.

4. To save, click **Apply**.

Device Ports - RPMs - Add Device

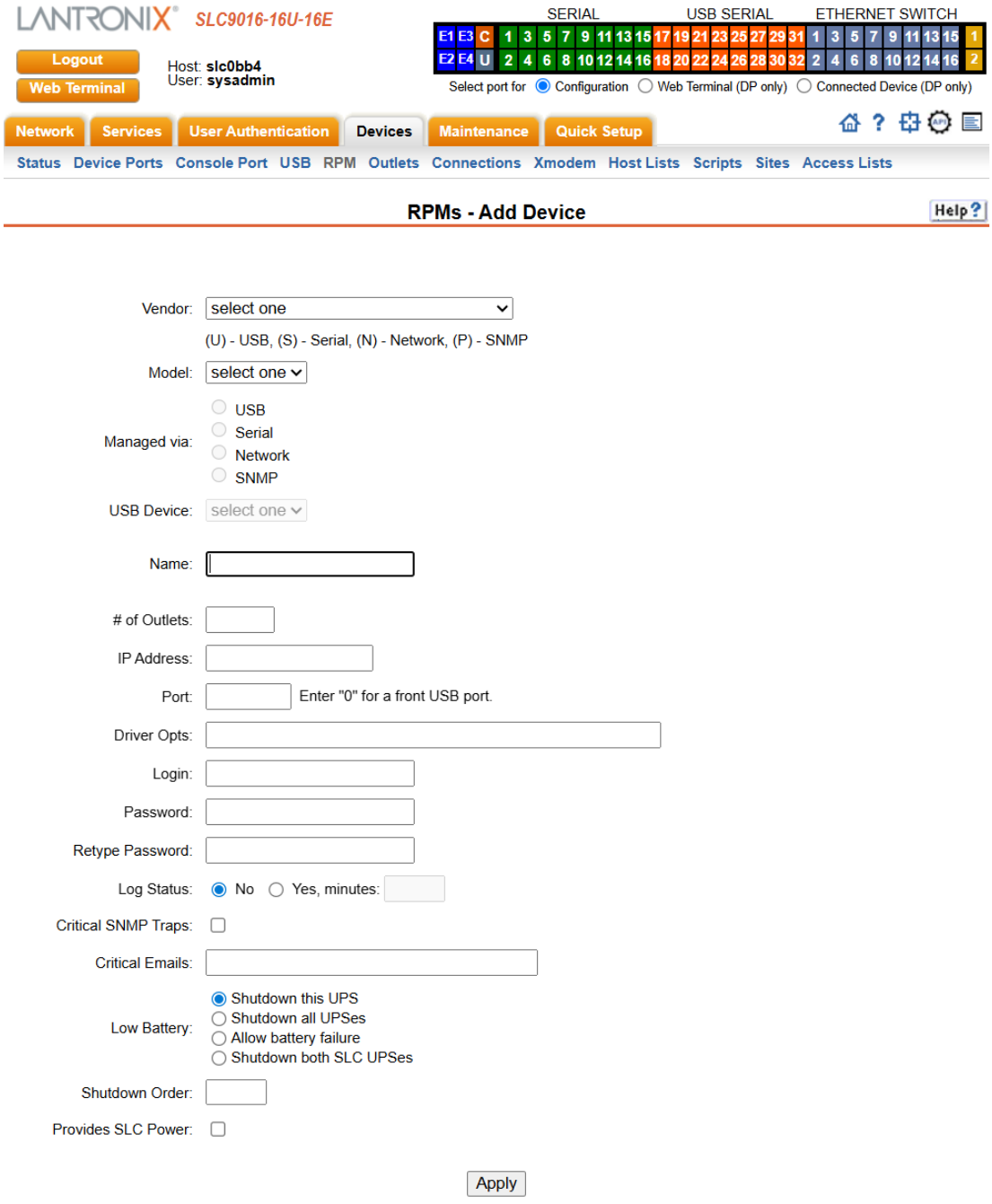
On the *Devices > Device Ports* page, access the *Device Ports > RPMs - Add Device* page to configure a new managed remote power manager (RPM) for the SLC configuration.

To add a new managed RPM :

1. Connect to a specific port on the **Devices > Device Ports** page according to instructions in *To open the Device Ports - Settings page: (on page 171)*.
2. In the **Connected to** drop-down menu above the IP Settings section of the *Device Ports > Settings (1 of 2)* page, select **RPM**.
3. Click the **Add RPM** link. The *Device Ports > RPMs - Add Device* page displays.

   Note: *The Device Ports > RPMs - Add Device page can also be accessed via the Devices > RPMs page.*
4. Update the configuration settings on this page according to directions in *RPMs - Add Device (on page 254)*.

Figure 10-7 Device Ports > RPMs - Add Device



Device Port - Sensorsoft Device

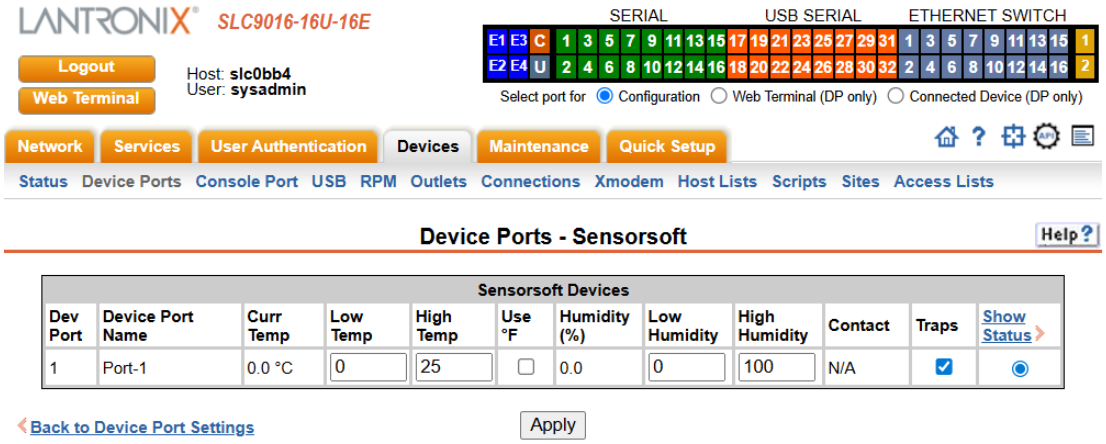
Devices made by Sensorsoft are used to monitor environmental conditions. Sensorsoft devices are third-party temperature, humidity, and flood sensors that connect via serial.

1. In the **Connected to** drop-down menu above the IP Settings section of the *Device Ports > Settings (1 of 2)* page, select **Sensorsoft**.

Note: *Sensorsoft temperature/humidity devices are supported with USB-to-serial adapters (ftdi/pl2303/cp210x) but not supported for use with USB-to-Serial CDC_ACM devices.*

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

Figure 10-8 Devices > Device Ports > Sensorsoft



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.
Curr 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 9000 advanced console server 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.
Low Humidity	Enter the relative humidity permitted on the device the sensor is monitoring below which the sensor sends a trap to the SLC advanced console server.
High Humidity	Enter the highest relative acceptable humidity permitted on the device above which the sensor sends a trap to the SLC unit.
Contact	Displays the current contact closure status of the sensor, if supported by the connected Sensorsoft device. If the Sensorsoft device does not report a contact status, N/A will be displayed. If Traps are enabled for the Sensorsoft device, an `slcEventDevicePortDeviceContactChanged` trap will be sent when the contact state changes from Open to Closed and from Closed to Open.

Traps	Select to indicate whether the SLC 9000 unit should send a trap or configured Event Alert when the sensor detects an out-of-range configured threshold.

4. Click the **Apply** button.
5. To view the status detected by the Sensorsoft, click the **Show Status** link in the far right column of the table.

Device Port Commands

Go to *Device Port Commands* to view CLI commands which correspond to the web page entries described above.

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>
```

Notes: *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.*

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, or TACACS+ user, or any local user who does not have an escape sequence defined, the default escape sequence is Esc+A.*

When connecting to a USB device port, buffered data collected while there was no active connection to the device port may be displayed initially. This is due to clearing internal buffers in preparation for the new connection to the device port.

Device Ports - Logging and Events

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 captures console output from connected devices. Use it to audit activity, debug device behavior, or maintain a permanent record of serial console sessions. Port logging is disabled by default. You can enable more than one type of logging (local, NFS file, token and data detection, 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 & Events* 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 9000 advanced console server 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 Logging

Data can be logged to a USB flash drive that is loaded into the USB ports. Data logged locally to the SLC advanced console server 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
```

Token/Data Detection

The system administrator can configure the device log to detect when a user-defined string or number of characters is received from the device, and automatically perform one or more actions: send a message to the system log, send an SNMP trap, send an email alert, send a string to the device, or control one of the power supplies associated with the device.

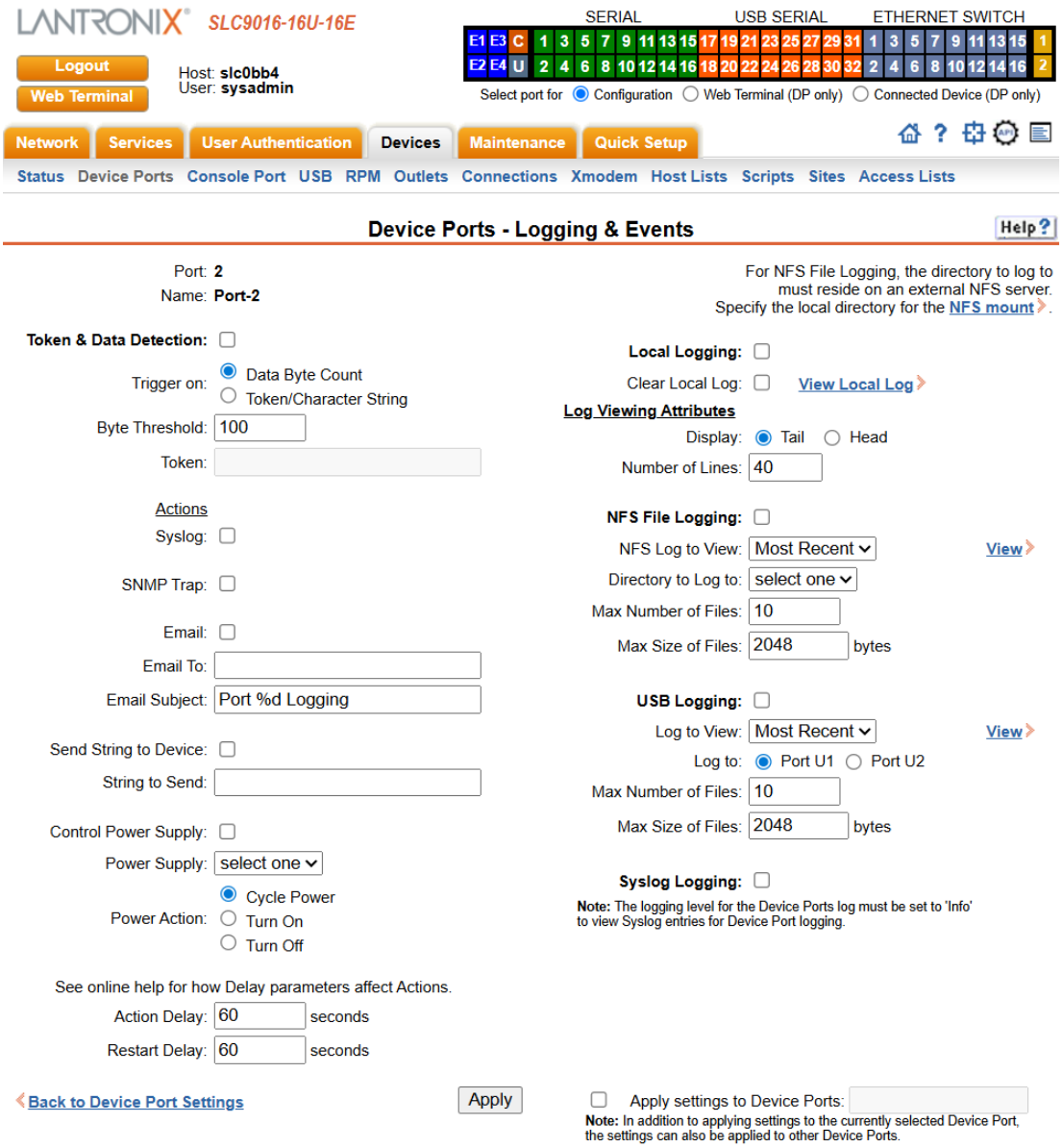
Syslog Logging

Data can be logged to the system log. If this feature is enabled, the data will appear in the Device Ports log, under the Info level. The log level for the Device Ports log must be set to Info for the data to be saved to the system log. See *Device Ports - Logging and Events (on page 188)*.

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:

Figure 10-9 Devices > Device Ports - Logging & Events



2. Enter the following:

Token & Data Detection

Token & Data Detection	Select to enable token and data detection on the selected device port, with a set of actions that can be enabled if a data trigger occurs. The default is disabled.
Trigger on	Select the method of triggering an action: ◆ **Data Byte Count:** A specific number of bytes of data. This is the default. ◆ **Token/Character String:** A specific pattern of characters, which you can define by a regular expression. ***Note:*** *Token/Character 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 will receive before the SLC unit will capture log data and initiate the selected actions. 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 unit receives a small number of bytes, it perceives that your device needs some attention. A threshold set to 30 characters means that as soon as the unit receives 30 bytes of data, it performs the actions that are selected for this port.
Token	The specific pattern of characters the SLC unit must recognize before initiating the actions configured for this port. The maximum is 100 characters. You may use a regular expression to define the pattern. For example, the regular expression "abc[def]g" recognizes the strings abcdg, abceg, abcfg. The SLC console manager supports GNU regular expressions; for more information, see: ◆ http://www.gnu.org/software/libc/manual/html_node/Regular-Expressions.html ◆ http://www.delorie.com/gnu/docs/regex/regex.html
Actions	Select one or more actions to perform if there is a data trigger: ◆ **Syslog:** A message is logged to the system log indicating what the data trigger was along with the initial portion of the data received. ◆ **SNMP Trap:** A slcEventDevicePortData trap will be sent to the NMS configured in the SNMP settings. ◆ **Email:** An email alert will be sent to the address configured for the device port. ◆ **Send String to Device:** A string will be sent to the device connected to the device port. ◆ **Control Power Supply:** The state of one or more of the device port power supplies can be changed.
Email to	The email address of the message recipient(s) for an email alert. To enter more than one email address, separate the addresses with a single space. You can enter a total of 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). ***Note:*** *The character sequence %d anywhere in the email subject is automatically replaced with the device port number.*
Send String to Device	If selected, the string provided in the field below will be sent to the device connected to the device port.
String to Send	The string to send to the device connected to the device port. The string supports the following special characters: newline (`"\n"`), double quote (`"\""`), single quote (`"\'"`), and escape (`"\x1b"`). You can enter a total of 128 characters.
Power Supply	The power supply that provides power to the device connected to the device port which to control. Select either all power supplies or an individual power supply.
Power Action	The action to perform on the selected power supply or power supplies - **Cycle Power**, **Turn On** or **Turn Off**.
Action Delay	A time limit of how long, in seconds, the device port will capture data after the data trigger is detected and before closing the log file (with a fixed internal buffer maximum capacity of 1500 bytes) and performing the selected actions. The default is 60 seconds.
Restart Delay	The number of seconds for the period of time, after performing the selected action, during which the device port will ignore additional characters received. The data will simply be ignored and not trigger additional actions until this time elapses. The default is **60** seconds.

Local Logging

Local Logging	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.
Clear Local Log	Select the checkbox to clear the local log.
View Local Log	Click this link to see the local log in text format.

Log Viewing Attributes

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

NFS File Logging

NFS File Logging	Select the checkbox to log all data sent to the device port to one or more files on an external NFS server. Disabled by default.
NFS Log to View	Available log files in the selected NFS Directory to view.
Directory to Log to	The path of the directory where the log files will be stored. ***Note:*** *This directory must be a directory exported from an NFS server mounted on the SLC 9000 advanced console server 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 unit begins generating a new file.

USB Logging

USB Logging	Select to enable USB logging. A USB thumb drive must be loaded into one of the ports of the SLC and properly mounted. Disabled by default.
Log to View	Available log files in the selected USB slot to view.
Log To	Select the USB port 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 9000 advanced console server 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.*

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

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

Logging Commands

Go to *Logging Commands* to view CLI commands which correspond to the web page entries described above.

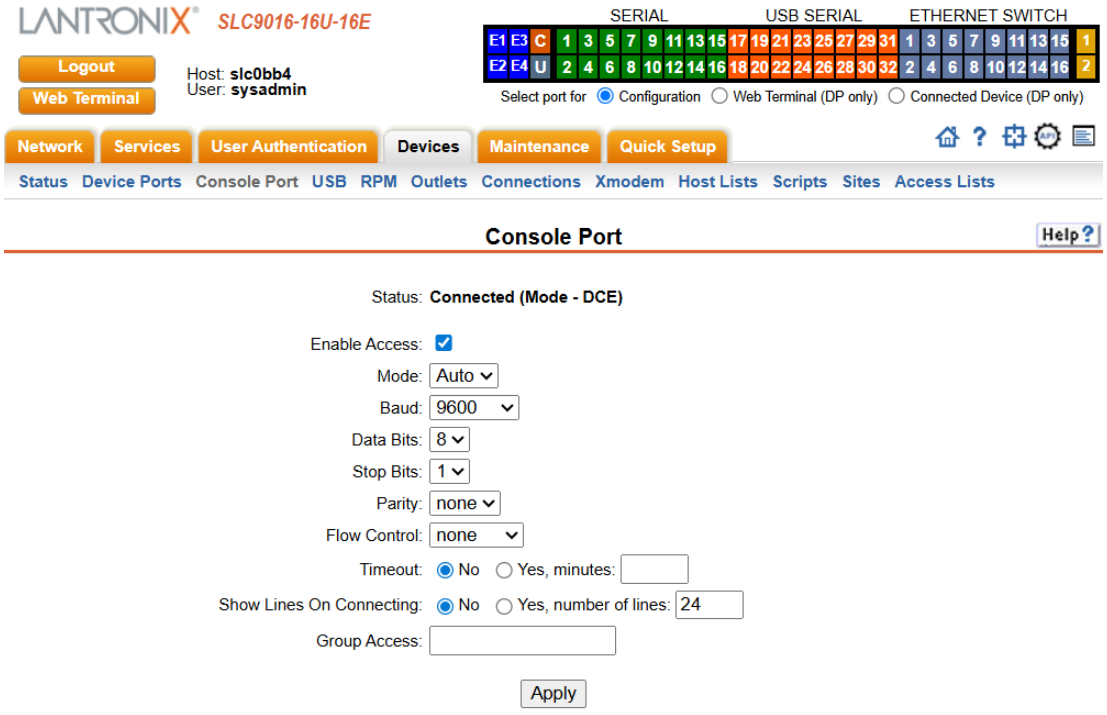
Console Port

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:

Figure 10-10 Devices > Console Port



2. Change the following as desired:

Enable Access	Enables or disables the console port access.
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 console port defaults to this value.

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.
Stop Bits	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**.
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**.
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**.
Timeout	The number of minutes (1-30) after which an idle session on the console is automatically logged out. Disabled by default.
Show Lines on Connecting	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.
Group Access	If undefined, any group can access the console 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 console 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 9000 advanced console server. 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".

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

Console Port Commands

Go to *Console Port Commands* to view CLI commands which correspond to the web page entries described above.

Xmodem

The SLC supports using the Xmodem, Ymodem, or Zmodem protocols to send and receive files across serial ports. An Xmodem repository on the SLC holds files that can be sent or have been received. In order to use one of the protocols, the device port that will be used must not be currently in use for any other purpose.

An example of sending a file with Zmodem to device port 3 using the CLI:

```
[slc431d]> set xmodem send 3 file update.bin protocol zmodem xfer binary
Starting Zmodem send of 117K file update.bin...
Sending: update.bin
Bytes Sent: 117988 BPS:919

Transfer complete
```

An example of receiving the same file with Zmodem from device port 4 using the CLI:

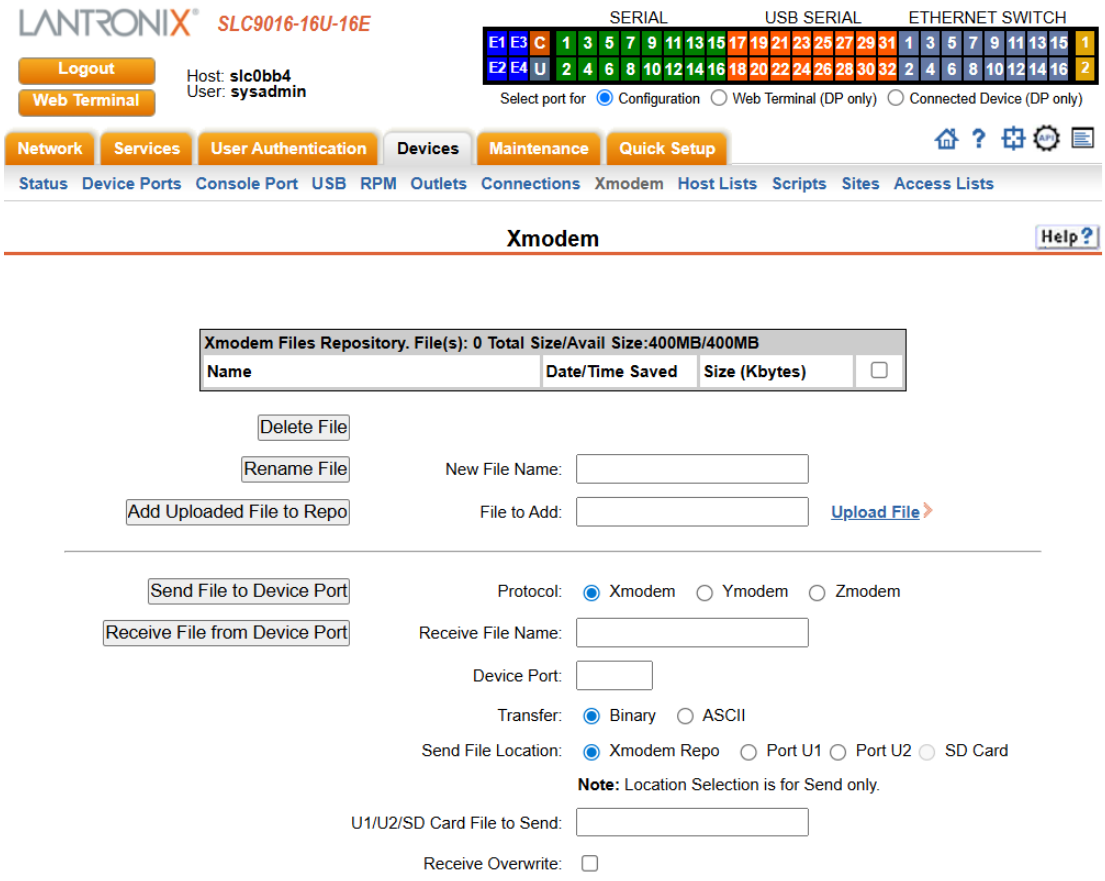
```
[slc431d]> se xmodem receive 4 protocol zmodem xfer binary
Starting Zmodem receive of file specified by protocol...
Receiving: update.bin.0
Bytes received: 117988/ 117988 BPS:937
```

```
Transfer complete
```

Note: *When performing critical operations (such as firmware update over a serial connection) with Xmodem, Ymodem or Zmodem, it is recommended to use the CLI to send and receive files instead of the web interface, as web browsers may be subject to timeouts which can interrupt the operation. It is also recommended that any timeouts that may affect the CLI session be disabled so that the operation is not interrupted.*

To manage the Xmodem repository, send files or receive files:

1. Click the **Devices** tab and select the **Xmodem** option. The Xmodem page displays:



2. To upload a file to the repository, click the **Upload File** link and upload a file in the window that is displayed. Upload file size should not exceed 20 MB. The maximum length for the upload file name is 40 characters. The file name should not contain the following characters: forward slash '/', backslash '\', colon ':', asterisk '*', question mark '?', double quotation mark ("), less than symbol '<', greater than symbol '>', or the vertical bar symbol '|'. After upload is complete, the filename will appear in the **File to Add** field. Click the **Add Uploaded File to Repo** button to add the file to the repository. The maximum repository size is 25 MB.

3. To rename a file, select the box to the right of the file in the **Xmodem Files Repository** list, enter the new file name in the **New File Name** field, and click the **Rename File** button.
4. To delete a file, select the box to the right of the file in the **Xmodem Files Repository** list, and click the **Delete** button.
5. To send a file, select the box to the right of the file in the **Xmodem Files Repository** list, and complete the following fields:

Protocol	Select whether to use the Xmodem, Ymodem or Zmodem protocol. Xmodem is a very rudimentary protocol that sends files in 128 byte blocks, padding the resulting file if necessary. Ymodem and Zmodem expand upon Xmodem by including the file's name, size and timestamp as part of the protocol.
Device Port	Enter the device port number to send the file to. The device port that will be used must not be currently in use for any other purpose.
Transfer	Select whether to send the file as a binary file or an ASCII file.

6. Click the **Send File to Device Port** button. The send will be initiated, and the **Status** window can be opened to view the progress of the send. When the Xmodem protocol is used, the user will be prompted when to start the file receive with the message, "Give your local XMODEM receive command now."

   Note: *Ymodem transfers may display a line at the end of a successful transfer such as, "Ymodem sectors/kbytes sent: 0/ 0k", however, the transfer is successful if "Transfer complete" is displayed and the bytes sent matches the size of the file.*

7. To receive a file, complete the following fields:

Protocol	Select whether to use the Xmodem, Ymodem or Zmodem protocol. Xmodem is a very rudimentary protocol that sends files in 128 byte blocks, padding the resulting file if necessary. Ymodem and Zmodem expand upon Xmodem by including the file's name, size and timestamp as part of the protocol.
Receive File Name	When Xmodem is used, enter the name to give the file that is received.
Device Port	Enter the device port number to receive the file from. The device port that will be used must not be currently in use for any other purpose.
Transfer	Select whether to receive the file as a binary file or an ASCII file.
Receive Overwrite	Select whether to overwrite files in the repository with the same name as the received file.

8. Click the **Receive File from Device Port** button. The receive will be initiated, and the **Status** window can be opened to view the progress of the receive. If a file with the same name already exists in the repository and Receive Overwrite is not enabled, the transfer will abort without overwriting the existing file.

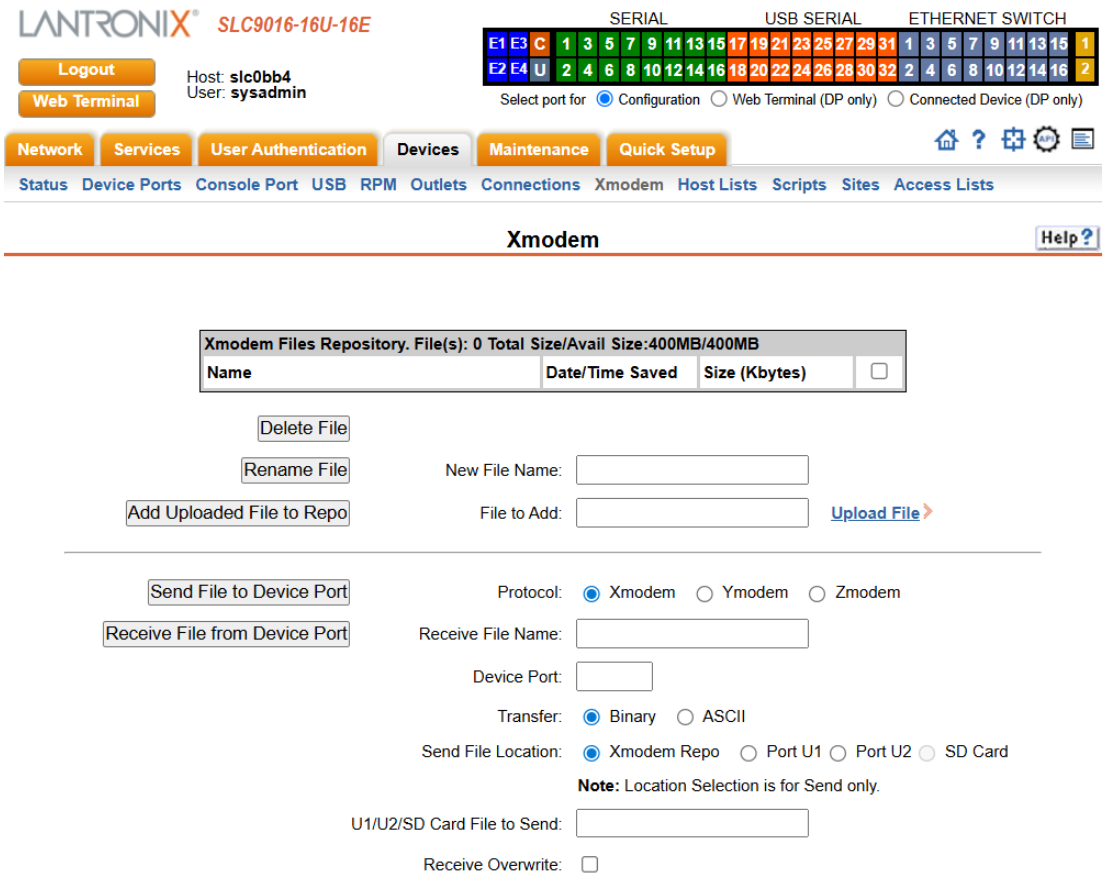
Host Lists

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 unit 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:

Figure 10-11 Devices > Host Lists



2. Enter the following:

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

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 advanced console server should attempt to retry connecting to the host list.
Authentication	Select to require authentication when the SLC unit connects to a host.

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

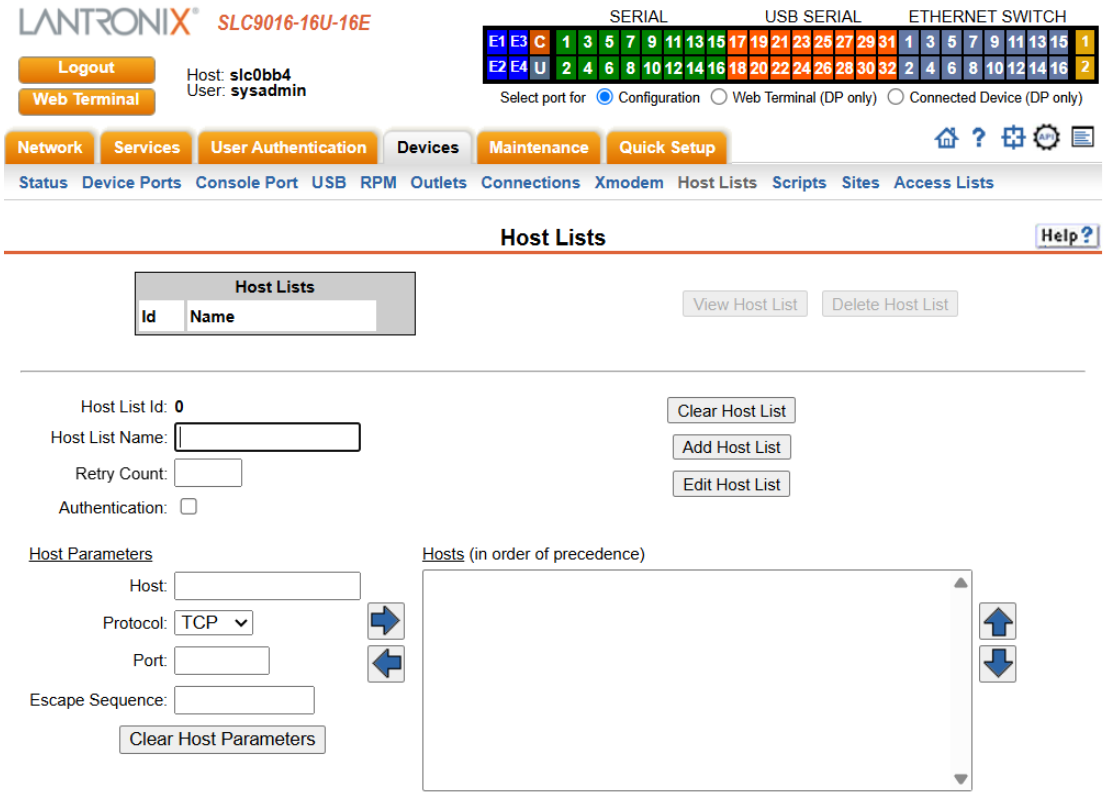
Host	Name or IP address of the host.
Protocol	Protocol for connecting to the host (TCP, SSH, or Telnet).
Port	Port on the host to connect to.
Escape Sequence	The escape character used to get the attention of the SSH or Telnet client. It is optional, and if not specified, Telnet and SSH use their default 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. ***Note:*** *When the Device Port Esc Sequence/ViewLog/PowerMenu Escape Sequence is configured, the following escape sequence precedent behavior can be expected: 1) Escape 2) PowerMenu 3) ViewLogs* *A clear/restart of the remaining escape events occurs when there is a match in any configured sequence. All the sequences should have unique sequence defined and user should avoid overlapping sequence strings. When detecting key sequences, after receiving the first character(s) of a sequence, the SLC will wait 3 or more seconds for the remaining characters, before timing out and sending all characters to the device. For example, if the Escape Sequence is ABCD, and the user types "AB", the SLC will wait at least 3 seconds for the next character ("C") before timing out and sending the "AB" characters to the device.*

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.
6. Click the **Clear Host Parameters** button to clear fields before adding the next host.
7. 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.
8. Click the **Add Host List** button. After the process completes, a link back to the *Device Ports > Settings (1 of 2)* 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.

Figure 10-12 View Host Lists



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 9000 advanced console server 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 advanced console server

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 (1 of 2)* 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 (1 of 2)* page displays.

Host List Commands

Go to *Host List Commands* to view CLI commands which correspond to the web page entries described above.

Scripts

The SLC unit supports three 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.
- **Custom Scripts** are Expect, Tcl or Python scripts which use most of the Expect/Tcl/Python scripting language, can be run against the CLI or a Device Port, and can be scheduled to run at periodic intervals, with the results from each run saved to a file in a repository. Up to 10 Custom Scripts can be created. Each Custom Script run is an operation, and the results from each operation can be viewed. Up to 50 script result files will be saved Locally in the SLC storage. Once this maximum is reached and new result files are generated, the oldest result files will automatically be deleted to accommodate the new result files.

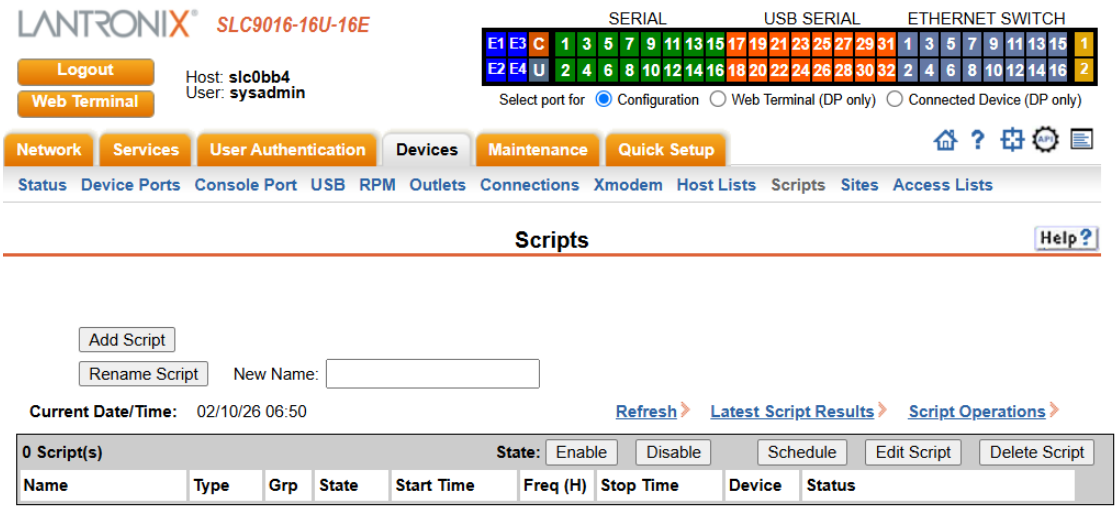
A user can create scripts at the web, view scripts at the web and the CLI, and utilize (run) scripts at the CLI. For a description of the syntax allowed in the various types of scripts, see Batch Script Syntax, Interface Script Syntax and Custom Script Syntax.

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:

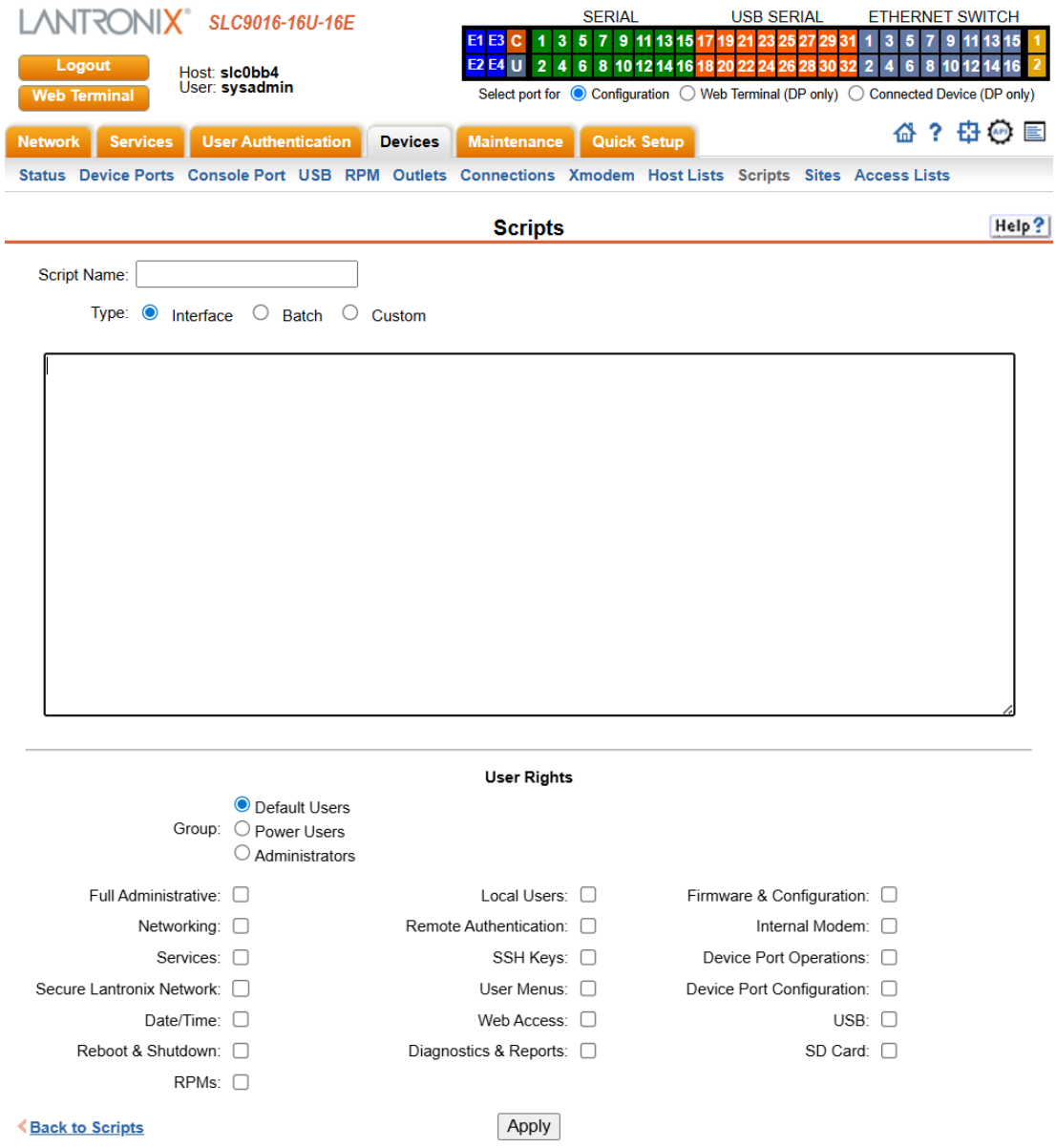
1. Click the **Devices** tab and select the **Scripts** option. This page displays.

Figure 10-13 Devices > Scripts



2. Click the **Add Script** button. The page for editing script attributes displays.

Figure 10-14 Adding or Editing New Scripts



3. Enter the following:

Scripts

Script Name	A unique identifier for the script.
Type	◆ Select **Interface** for a script that utilizes Expect/Tcl to perform pattern detection and action generation on Device Port output. ◆ Select **Batch** for a script of CLI commands. ◆ Select **Custom** for an Expect, Tcl or Python script that can be run against a CLI session or a Device Port, either manually or scheduled to run at periodic intervals.
Script Text	In the free-form editing box, enter the contents of the script. Restrictions on the script format are described in Batch Script Syntax, Interface Script Syntax, and Custom Script Syntax.
Group	Select the group to which the script will belong: ◆ **Default Users:** This group has only the most basic rights. You can specify additional rights for the individual user. ◆ **Power Users:** This group has the same rights as Default Users plus **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. You can specify additional rights for the individual user. ◆ **Administrators:** This group has all possible rights. For more information on how the group and rights are used with scripts, see To use a script at the CLI: below.

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

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., Spider, or SLC devices) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the SLC unit.
RPMs	Right to view and enter Remote Power Manager (RPM) settings.
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.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
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.
Internal Modem	Right to configure internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port configurations.

USB	Right to enter modem settings for USB modems and to control USB storage devices.

5. To save, click the **Apply** button. If the type of script is **Interface** or **Custom**, 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 10-14*).
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 schedule a custom script:

1. In the Scripts table, select the script and click the **Schedule** button. The Custom Scripts - Schedule page displays.
2. Enter the following (each Custom Script can be run against one device - CLI or Device Port - with one schedule):

Device Type	The device - either the CLI or a Device Port - that the script is connected to.
State	The state of the script's schedule. A script must be **Enabled** in order for the script scheduler to begin running the schedule. Once a script has been scheduled and enabled, it can be **Disabled**; in this state the script manager will continue to update the scheduled run time for a script, but the script will not be run or produce any results. At any point a schedule for a script can be **Deleted**.
Command Line Arguments	Optional command line arguments to pass to the script each time it is run.
Start Time	The date and time when the script should start running, either **Now** or at a specific date and time.
Frequency	How often the script will run, given in hours or days. The web UI and CLI will always display the frequency in hours.
Stop Time	The date and time when the script should stop running, either at a specified date and time, or **Forever** if it should never stop running.

4. To save, click the **Apply** button. The schedule will be validated, and the script manager will either immediately start running the script or schedule the next run of the script. The main **Scripts** page is displayed, showing the schedule status of the script (this may take a few seconds to be updated while the script manager processes the script - click **Refresh** to view the latest information).

Notes on scheduling:

- Scripts that are scheduled to start immediately and run forever will be restarted when the SLC is rebooted.
- Scripts that are scheduled to start at a specific time will be restarted when the SLC is rebooted if the script is scheduled to run forever or if the stop time has not expired.
- After the SLC has booted, there will be a short delay after launching each script before starting the next script in order to minimize the impact on system resources. Shortly after boot, if the script status shows that a script is not scheduled when the script is configured with a schedule, refreshing the status will eventually show that all scheduled scripts will be running and/or scheduled.
- If the date, time or timezone is changed on the SLC while a script is scheduled, the CLI and web UI will still show the same scheduled date and time for the script, until the next time the script is run. It is recommended that the date, time and timezone not be changed while scripts are scheduled to run.

To change the Enable/Disable state of a custom script schedule:

1. In the Scripts table, select the script to enable or disable.
2. Click the **Enable** button (this will resume running of a script at its next scheduled time if it was previously disabled) or the **Disable** button (this will suspend running of a script but continue to update the schedule). The script's state will be updated and the Scripts page redisplays.

To view the list of completed operations (runs) for a custom script:

1. In the Scripts table, select the script to view operations for, and click **Script Operations**.
2. The Custom Scripts - Operations page displays, with a list of any results that have been generated for a script, in reverse date/time order. Any of the results can be viewed by selecting the operation and clicking **Script Results**.

To delete the completed operations (runs) for a custom script:

1. In the Scripts table, select the script to view operations for, and **click Script Operations**.
2. The Custom Scripts - Operations page displays, with a list of any results that have been generated for a script, in reverse date/time order. All the results can be deleted by clicking **Delete Results**.

To view the latest results from a completed operation (run) of a custom script:

1. Click the Devices tab and select the Scripts option. The Scripts page displays.
2. In the Scripts table, select the script to view results for, and click **Latest Script Results**.

The results are displayed in a popup window.

To use a script at the CLI:

1. To run an Interface Script or a Custom Script on a device port for pattern recognition and action generation, use the `connect script <Script Name> deviceport <Device Port # or Name>` command. This action requires that a SLC user running the connect script command have Device Port Operations (do) rights and port permissions for the selected device port.
2. To run a Batch Script at the CLI with a series of CLI commands, or a Custom Script for pattern recognition and action generation, use the `set script runcli <Script Name>` command. This action requires that a SLC user running the runcli command belong to a group that is the same or greater than the group assigned to the script (e.g., if the script is assigned to the Power group, the user running the runcli command must belong to the Power or Admin group). For Batch Scripts, if this minimum group requirement is met, the SLC user will temporarily be granted all of the individual rights assigned to the script while the Batch Script is running.

   Note: *Expect Custom Scripts have a* `debug enable` *option that supports printing Expect debug information to aid in creating an Expect script. The debug option is not supported for Tcl and Python scripts.*

Script Commands

Go to *Script Commands* to view CLI commands which correspond to the web page entries described above.

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 10-15 Definitions

Term	Definition
Word	A contiguous group of characters delimited on either side by spaces. Not enclosed by double quotes.
Primary Command	One of the primary commands listed in this section.
Secondary Command	One of the secondary commands defined in this section.
Quoted String	A group of characters enclosed by double quote (") characters. A quoted string may include any characters, including space characters. If a double quote character is to be included in a quoted string it must be preceded (escaped) by a backslash character ('\').
Variable Reference	A word (as defined above) preceded by a dollar sign character ('$').
CLI Command	A quoted string containing a valid CLI `show` command.
Arithmetic Operator	A single character representing a simple arithmetic operation. The character may be one of the following: ◆ A plus sign (+) representing addition ◆ A minus sign (-) representing subtraction ◆ An asterisk sign (*) representing multiplication ◆ A forward slash (/) representing division ◆ A percent sign (%) representing a modulus

Term	Definition
Boolean Expression	An expression which evaluates to TRUE or FALSE. A Boolean expression has the following syntax: <value> <Boolean operator> <value> Each can be either a word or a variable reference.
Boolean Operator	A binary operator which expresses a comparison between two operands and evaluates to TRUE or FALSE. The following Boolean operators are valid: ◆ '<' less than ◆ '>' greater than ◆ '<=' less than or equal to ◆ '>=' greater than or equal to ◆ '==' equal to ◆ '!=' not equal to

Primary Commands

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

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

Table 10-16 Primary Commands

Command	Description
set	The `set command` assigns a value to a variable. Syntax: set <variable> <value> where <variable> is a word, and <value> can be defined in one of the following ways: ◆ A quoted string ◆ A word ◆ A variable reference ◆ A value generated via one of the string secondary commands (compare, match, first, etc.) ◆ A value generated via the `expr` secondary command ◆ A value generated via the `format` secondary command ◆ A value generated via the `expr timestamp` command
unset	This command removes the definition of a variable within a script. Syntax: unset <variable> where `<variable>` is a word.
scan	The `scan` command is analogous to the C language scanf(). Syntax: scan <variable> <format string> <value 1> <value 2> ... <value n> where `<variable>` a variable reference, and `<format string>` is a quoted string. Each of the `<value x>` elements will be a word.

Command	Description
sleep	The `sleep` command suspends execution of the script (puts it to 'sleep') for the specified number of seconds. Syntax: sleep <value> where `<value>` can be a word, a quoted string or a variable reference.
exec	The `exec` command executes a single CLI command. Currently only CLI 'show' commands may be executed via exec. Syntax: exec <CLI command>
send, send_user	The `send` command sends output to a sub-process, The `send_user` command sends output to the standard output. Both commands have the same syntax: send <string> send_user <string> where `<string>` can be either a quoted string or a variable reference.
expect, expect_user, expect_before, expect_after, expect_background	The `expect` command waits for input and attempts to match it against one or more patterns. If one of the patterns matches the input the corresponding (optional) command is executed. All `expect` commands have the same syntax: expect {<string 1> {command 1} <string 2> {command 2} ... <string n> {command n}} where `<string x>` will either be a quoted string, a variable reference or the reserved word 'timeout.' The command x is optional, but the curly braces ('{' and '}') are required. If present it must be a primary command.
return	The `return` command terminates execution of the script and returns an optional value to the calling environment. Syntax: return <value> where `<value>` can be a word or a variable reference.

Secondary Commands

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

Table 10-17 Secondary Commands

Command	Description

string	The `string` command provides a series of string manipulation operations. The `string` command will only be used with the `set command` to generate a value for a variable. There are nine operations provided by the `string` command.
	Syntax (varies by operation):
	`string compare <str 1> <str 2>`
	`Compare two strings`
	`string match <str 1> <str 2>`
	`Determine if two strings are equal`
	`string first <str needle> <str haystack>`
	`Find and return the index of the first occurrence of 'str_needle' in 'str_haystack'`
	`string last <str needle> <str haystack>`
	`Find and return the index of the last occurrence of 'str_needle' in 'str_haystack'`
	`string length <str>`
	`Return the length of 'str'`
	`string index <str> <int>`
	`Return the character located at position 'int' in 'str'`
	`string range <str> <int start> <int end>`
	`Return a string consisting of the characters in 'str' between 'int start' and 'int end'`
	`string tolower <str>`
	`Convert <str> to lowercase`
	`string toupper <str>`
	`Convert <str> to uppercase`
	`string trim <str 1> <str 2>`
	`Trim 'str 2' from 'str 1'`
	`string trimleft <str 1> <str 2>`
	`Trim 'str 2' from the beginning of 'str 1'`
	`string trimright <str 1> <str 2>`
	`Trim 'str 2' from the end of 'str 1'`
	In each of the above operations, each <str *> element can either be a quoted string or a variable reference. The <int *> elements will be either words or variable references.

expr	This command evaluates an arithmetic expression and returns the result. The `expr` command will only be used in combination with the `set command` to generate a value for a variable. Syntax: expr <value> <operation> <value> Each `<value>` will be either a word or a variable reference, and <operation> an arithmetic operation.

Command	Description
timestamp	This command returns the current time of day as determined by the SLC . The `timestamp` command will only be used in combination with the `set command` to produce the value for a variable. Syntax: timestamp <format> where `<format>` is a quoted string.
format	The `format` command is analogous to the C language sprintf(). The `format` command will only be used in combination with the `set command` to produce the value for a variable. Syntax: format <format string> <value 1> <value 2> ... <value n> where <format string> will be a quoted string. Each of the <value x> elements will be a word, a quoted string or a variable reference.

Control Flow Commands

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

Table 10-18 Control Flow Commands

Command	Description

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
	}

Command	Description

if, elseif and else	The `if` command executes an associated block of commands if its Boolean expression evaluates to TRUE. Each command within the block must be a Primary command. Syntax:
	if {<Boolean expression>} {
	command 1
	command 2
	...
	command n
	}
	The `elseif` command is used in association with an `if` command - it must immediately follow an if or `elseif` command. It executes an associated block of commands if its Boolean expression evaluates to TRUE. Each command within the block must be a Primary command. Syntax:
	elseif {<Boolean expression>} {
	command 1
	command 2
	...
	command n
	}
	The `else` command is used in combination with an if or `elseif` command to provide a default path of execution. If the Boolean expressions for all preceding if and `elseif` commands evaluate to FALSE the associated block of commands is executed. Each command within the block must be a Primary Command. Syntax:
	else {
	command 1
	command 2
	...
	command n
	}

Custom Script Syntax

This section describes the scripting syntax for Custom Scripts. The syntax is more flexible than Interactive Script syntax, but still has restrictions to prevent the creation of scripts containing potentially harmful commands. In addition, Custom Scripts can be configured to use command line parameters. Custom Scripts have the following guidelines:

1. The size of the script file cannot exceed 6 Kbytes.
2. The size of the results generated by the script cannot exceed 1 Kbyte (any results over 1Kbyte will be truncated).
3. The first line of the script must contain a Linux script style interpreter directive so that the SLC will know which interpreter to use to run the script. The format of the first line is `#! expect`, `#! tcl`, or `#! python`. When a custom script is imported, the interpreter line must match the selected script or file type (Expect, Tcl, or Python), otherwise the script will be invalid.
4. The script should include a spawn command to connect the script to either a SLC CLI session or a SLC Device Port session. Refer to the following spawn command syntax:

Note:

- *For CLI sessions, a local user name should be given*
- *For Device Port sessions, the $devicePort variable will be used by the SLC to connect the script to the appropriate Device Port. The* `-noecho` *flag may be passed to* `spawn` *command.*

- Expect script - CLI session
```
spawn clisession -U <username>
```
- Expect script - Device Port session
```
spawn portsession -p $devicePort
```
- Tcl script - CLI session
```
set io [open "| clisession -U <username>" r+]
```
- Tcl script - Device Port session
```
set io [open "| portsession -p $devicePort" r+]
```
- Python script - CLI session
```
subprocess.Popen(['clisession', '-U', '<username>'],
                 stdin=subprocess.PIPE,
                 stdout=subprocess.PIPE,
                 stderr=subprocess.PIPE)
```
- Python script - Device Port session
```
subprocess.Popen(['portsession', '-p', devicePort],
                 stdin=subprocess.PIPE,
                 stdout=subprocess.PIPE,
                 stderr=subprocess.PIPE)
```

5. It is recommended that scripts that spawn clisession only be used with the `set script runcli` command (and not the `connect script` command), and that scripts that spawn portsession only be used with the `connect script` command (and not the `set script runcli` command).
6. The script cannot contain commands which spawn or fork other commands, read or write files on the SLC filesystem, or interrogate the SLC filesystem. The list of commands that are not allowed for Expect scripts includes `"fork", "open", "exp_open", "exec", "system", "log_file", "pwd"`.
7. For scripts that return an exit code, the SLC will interpret an exit code of zero as a successful exit code, and any non-zero exit code as an error. Non-zero exit codes are displayed (at the CLI) or logged (for scripts that are run by the script scheduler).

Example Scripts

Interface Script—Monitor Port

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

```
set monPort 7
set monTime 5
```

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

```
while { $loopCtr < $loopMax } {
   #Get current time
```

The following is the screen output:

```
slc247glenn]> conn script ex4 deviceport 7
login: Logging in....
sysadmin
sysadmin
Password: PASS
Welcome to the Lantronix SLC9000 Advanced Console Manager
Model Number: SLC9016-16U-16E
Percepxion: registered to cloud: mach10-dev-01.lantronix.com
For a list of commands, type 'help'.
[SLC251glenn]> show network port 1 host
show network port 1 host
___Current Hostname Settings_____________________________________________
Hostname: SLC251glenn
Domain: support.int.lantronix.com
[SLC251glen
Device HOSTNAME: SLC 251GLENN

_____________________________________________________________________________
Monitored Port: Port 7
Monitor Interval Time: 5 Seconds
[Current Time:21:16:43]
show portcounter deviceport 7
n]> show portcounter deviceport 7
Device Port: 7 Seconds since zeroed: 1453619
Bytes input: 0 Bytes output: 0
Framing errors: 0 Flow control errors: 0
Overrun errors: 0 Parity errors: 0
[SLC251glenn]>
[Current Time:21:16:58]
show portcounter deviceport 7
show portcounter deviceport 7
Device Port: 7 Seconds since zeroed: 1453634
Bytes input: 0 Bytes output: 0
Framing errors: 0 Flow control errors: 0
Overrun errors: 0 Parity errors: 0
[SLC251glenn]>
Port Counter Monitor Script Ending......

_____________________________________________________________________________
Login Out.......
logout
Returning to command line
[slc247glenn]>
```

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:

```
[slc247glenn]> se script runcli cli
[slc247glenn]> show network port 1 host
___Current Hostname Settings_____________________________________________
Hostname: slc247glenn
Domain: <none>
[slc247glenn]>
[slc247glenn]> 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
[slc247glenn]>
[slc247glenn]> show script
___Interface Scripts______Group/Permissions_____________________________
getSLC Adm/ad,nt,sv,dt,lu,ra,um,dp,pc,rp,rs,fc,dr,sn,wb,sk,po,do
Test Adm/ad,nt,sv,dt,lu,ra,um,dp,pc,rp,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,rp
[slc247glenn]>
[slc247glenn]> connect script monport deviceport 7
login: Logging in....
sysadmin
sysadmin
Password: PASS
Welcome to the Lantronix SLC9000 Advanced Console Manager
Model Number: SLC9016-16U-16E
Percepxion: registered to cloud: mach10-dev-01.lantronix.com
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]>
[Current Time:21:25:20]
show portcounter deviceport 7
show portcounter deviceport 7
Device Port: 7 Seconds since zeroed: 1454136
Bytes input: 0 Bytes output: 0
Framing errors: 0 Flow control errors: 0
Overrun errors: 0 Parity errors: 0
[SLC251glenn]>
Port Counter Monitor Script Ending......
_____________________________________________________________________
Login Out.......
logout
Returning to command line
[slcvz249_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,rp,sn,wb,sk,po,do
[slcvz249_glenn]>
```

Expect Custom Script - SLC CLI Session

An example of an ExpectCustom Script that interacts with a SLC CLI session:

```
#! expect
# script to get the current internal temperature of the SLC
# accepts one optional command line parameter for location

set slcPrompt ">"
set slcTemp   "unknown"
set location  ""

proc myprint {str} {
    send_user -- "$str\n"
}

proc abortSession {err} {
    send_user "Error $err. Terminating session.\n"
    exit $err
}

# Are there any command line parameters?
if {$argc > 0} {
    set location [lindex $argv 0]
}

set now [clock seconds]
set date [clock format $now -format {%D %R}]
if {$argc > 0} {
    myprint "Internal temperature of the $location SLC at $date"
```

```
} else {
    myprint "Internal temperature of the SLC at $date"
}

# spawn the CLI session
if {[catch {spawn -noecho clisession -U sysadmin} result]} {
    abortSession 1
}
set sessionId $spawn_id

# Handle eof
expect_after {
    -i $sessionId eof {
        myprint "Session unexpectedly terminated."
        abortSession 2
    }
}

set timeout 10
log_user 0

# Wait for the first prompt
set loggedIn false
while {! $loggedIn} {
    expect {
    timeout {myprint "Timeout waiting to login"; abortSession 3}
    "Need to specify username" {myprint "Need to specify -U ";
abortSession 4}
    "*> " {set loggedIn true}
    } ;
}

exp_send "\n"
expect {
    timeout {myprint "Timeout waiting for CLI prompt"; abortSession 3}
    -re "\n\r(\\\[\[^\r]*]>)"
}
set slcPrompt $expect_out(1,string)

# Run the temperature command
exp_send "show temperature\n"
expect {
    timeout {myprint "Timeout waiting for temperature"; abortSession 3}
    -re "Current Internal Temperature: (.*)\r\n"
}
set slcTemp $expect_out(1,string)
myprint "Temperature: $slcTemp"

exp_send "logout\n"
sleep .5
close
exit 0
```

This script can be run manually at the CLI:

```
[slc431d] set script runcli cliExample parameters "East Data Center"
Internal temperature of the East Data Center SLC at 01/27/2019 02:07
Temperature: 48C (118F)
```

Expect Custom Script - SLC Device Port Session

An example of an Expect Custom Script that interacts with a SLC Device Port (in this example a ServerTech PDU is connected to a Device Port):

```
#! expect
#
# Script to get the load of a ServerTech PDU outlet
#

set pduPrompt ">"
set pduLoad   "unknown"

proc myprint {str} {
    send_user -- "$str\n"
}

proc abortSession {err} {
    send_user "Error $err. Terminating session.\n"
    exit $err
}

set now [clock seconds]
set date [clock format $now -format {%D %R}]
myprint "Load of ServerTech PDU outlet B1 at $date"

# spawn the port session on a device port
if {[catch {spawn -noecho portsession -p $devicePort} result]} {
    abortSession 1
}
set sessionId $spawn_id

# Handle eof
expect_after {
    -i $sessionId eof {
        myprint "Session unexpectedly terminated."
        abortSession 2
    }
}

set timeout 10
log_user 0

#
# Login to the PDU
# The "Error:*" pattern matches all error messages output by portsession
#
send "\n"
expect {
```

```
    "Username:" { send "admn\n" }
    "Error:*\r\n" { send_user $expect_out(0,string); abortSession 2 }
}
expect "Password:"
send "admn\n"

# Wait for the first prompt
set loggedIn false
while {! $loggedIn} {
    expect {
    timeout {myprint "Timeout waiting to login"; abortSession 3}
    "*CDU: " {set loggedIn true}
    } ;
}

# Detect the prompt
exp_send "\n"
expect "are:\r\n"
expect "LOGIN\r\n"
expect "REMOVE\r\n"
expect "RESTART\r\n"
expect {
    timeout {myprint "Timeout waiting for prompt"; abortSession 3}
    -re "\r\n(\[^\r]*:)"
}
set pduPrompt $expect_out(1,string)

# Run the ostat command
exp_send "ostat .b1\n"
expect "Outlet*Power\r\n"
expect "ID*Watts*\r\n"
expect {
    timeout {myprint "Timeout waiting for load"; abortSession 3}
    -re "\.B1\\s+\\S+\\s+\\S+\\s+(\\S+)"
}
set pduLoad $expect_out(1,string)
myprint "Outlet B1 Load: $pduLoad Amps"

expect $pduPrompt
exp_send "logout\n"

sleep .5
close
exit 0
```

Expect Custom Script - SLC Device Port Session

An example of an Expect Custom Script that interacts with a SLC Device Port (in this example a Cisco server is connected to a Device Port):

```
#! expect
```

```
#
# Save a copy of the running config of a Cisco server to a TFTP server
# The Cisco server is connected to a SLC/B device port
#

proc myprint {str} {
    send_user -- "$str\n"
}

proc abortSession {err} {
    send_user "Error $err. Terminating session.\n"
    exit $err
}

if {$argc < 2} {
    myprint "Usage: script_md_cisco.exp <TFTP Server> <Backup File Name>"
    abortSession 1
}

set tftp [lindex $argv 0]
set configFile [lindex $argv 1]
set enablePassword "secret"
set timeout 10

set now [clock seconds]
set date [clock format $now -format {%D %R}]
myprint "Backing up Cisco Server to $tftp:$configFile at $date"

# spawn the port session on a device port
if {[catch {spawn -noecho portsession -p $devicePort} result]} {
    abortSession 2
}
set sessionId $spawn_id

# Handle eof
expect_after {
    -i $sessionId eof {
        myprint "Session unexpectedly terminated."
        abortSession 3
    }
}

log_user 0

# Send carriage return, see if we are connected
set loggedIn false
set execMode false
set passwordPrompt false
set cnt 1
while {! $loggedIn || ! $execMode} {
    if {$cnt == 5} {
        myprint "Timeout waiting for > or # prompt"
        abortSession 4
    }
```

```
    if {! $passwordPrompt} {
        send "\r"
    }
    expect {
        "*assword: " { send "$enablePassword\r" }
       ">" { set loggedIn true; set passwordPrompt true; send "enable\r"
}
        "#" { set loggedIn true; set execMode true }
       "Error:*\r\n" { send_user $expect_out(0,string); abortSession 5 }
        timeout {set cnt [expr {$cnt + 1}] }
    }
}

myprint "Logged in."

send "copy running-config tftp://$tftp/$configFile\r"
expect "$tftp"
send "\r"
expect "$configFile"
send "\r"
myprint "Backup initiated."
expect {
    "!!" { myprint "Successfully backed up." }
    timeout { myprint "Timeout waiting for backup to complete.";
abortSession 6 }
}
send "exit\r"

sleep .5
close
exit 0
```

Python Custom Script - SLC CLI Session

An example of a Python Custom Script that interacts with a CLI session:

```
#! python
# Script to set the RADIUS authentication settings of the SLC
# Sets the first RADIUS server and secret, and enables RADIUS
# Note: passing secret as a command line parameter is a security
vulnerability
# Usage:
#   script_cli_radius.py <RADIUS server> <RADIUS secret>
#

import subprocess
import datetime
import sys

num_args = len(sys.argv) - 1
if num_args < 2:
    print("Usage: script_cli_radius.py <RADIUS server> <RADIUS secret>")
    sys.exit(1)
```

```
print("Settings RADIUS server on SLC at ", end="")
now = datetime.datetime.now()
print(now.strftime("%Y-%m-%d %H:%M"))

server = sys.argv[1]
secret = sys.argv[2]

proc = subprocess.Popen(['clisession', '-U', 'sysadmin'],
                        stdin=subprocess.PIPE,
                        stdout=subprocess.PIPE,
                        stderr=subprocess.PIPE)

# wait for prompt
while True:
    output_str = proc.stdout.readline()
    if b'list of commands' in output_str:
        proc.stdin.write(b'\n')
        proc.stdin.flush()
    if b']> ' in output_str:
        break
    if b'Invalid local user' in output_str:
        print("Invalid local user passed to clisession.")
        proc.stdin.close()
        proc.terminate()
        proc.wait()
        sys.exit(1)

# Run the RADIUS command
s = "set radius server 1 host " + server + " secret " + secret + "\n"
b = bytearray(s.encode())
proc.stdin.write(b)
proc.stdin.flush()
while True:
    output_str = proc.stdout.readline()
    if b'RADIUS settings successfully updated' in output_str:
        break
    elif b'set radius' not in output_str:
        # RADIUS command returned an error
        s1 = str(output_str)
        s2 = s1.split("\\r")[1]
        print("RADIUS command returned: " + s2.split("\\n")[0])
        proc.stdin.close()
        proc.terminate()
        proc.wait()
        sys.exit(1)

proc.stdin.write(b'set radius state enable\n')
proc.stdin.flush()
while True:
    output_str = proc.stdout.readline()
    if b'RADIUS settings successfully updated' in output_str:
        break
    elif b'set radius' not in output_str:
```

```
        # RADIUS command returned an error
        s1 = str(output_str)
        s2 = s1.split("\\r")[1]
        print("RADIUS command returned: " + s2.split("\\n")[0])
        proc.stdin.close()
        proc.terminate()
        proc.wait()
        sys.exit(1)

print("RADIUS settings updated and enabled.")
proc.stdin.close()
proc.terminate()
proc.wait()
sys.exit(0)
```

Python Custom Script - SLC CLI Session

An example of a Python Custom Script that uses the Pexpect module to interact with the CLI session and the device ports to detect the prompt on any devices connected to the SLC, and set the device port name to be the same as the device prompt:

```
#! python
# Script to detect the prompt on a device connected to a SLC or SLB
device port,
# and set the device port name to the prompt. Punctuation characters are
# removed and the device port number is appended to the name. Prompts
ending
# in '>' are detected. For example, for a Cisco device attached to device
# port 3 and displays this prompt:
#   engcisco_cat3560>
# the name for device port 3 will be set to "engcisco_cat3560-3"

import pexpect
import datetime
import time
import sys
import re

now = datetime.datetime.now()
print("Detecting devices on SLC at ", end="")
print(now.strftime("%Y-%m-%d %H:%M"))

# start the CLI session to get number of device ports
p=pexpect.spawn('clisession -U sysadmin')

slcPrompt = ""
numPorts = 0
loggedIn = False

while not loggedIn:
    i = p.expect([pexpect.TIMEOUT, pexpect.EOF,
```

```
                    'Model Number: SLC80(\d*)\r\n', 'Model Number:
SLB882\r\n',
                    '(\[.*>)'], timeout=10)
    if i == 0:   # Timeout
        print("Timeout waiting to login.")
        p.terminate(True)
        sys.exit(1)
    elif i == 1: # EOF
        print("Session unexpectedly terminated.")
        p.terminate(True)
        sys.exit(1)
    elif i == 2: # SLC9000 model number
        model = p.match.group(1)
        numPorts = int(model)
    elif i == 3: # SLB882 model number
        numPorts = 8
    elif i == 4: # prompt
        loggedIn = True
        slcPrompt = p.match.group(1).decode('utf-8')

if numPorts == 0:
    print("Cannot determine number of device ports.")
    p.terminate(True)
    sys.exit(1)

print("Number of device ports:", numPorts)

# Terminate the CLI session
p.sendline("logout")
time.sleep(.500)
p.wait()

skipPorts = False
devicePort = 1
pList = []

if numPorts == 24 or numPorts == 40:
    # Adjust port numbering for SLC8024 and SLC8040
    skipPorts = True
    numPorts = numPorts + 8

# Loop through device ports, connect and try to detect the prompt
while devicePort <= numPorts:
    if skipPorts and devicePort >= 9 and devicePort <= 16:
        devicePort = devicePort + 1
        pList.append('')
        continue
    print("Scanning device port", devicePort, "...")
    port = str(devicePort)
    p=pexpect.spawn('portsession', ['-p', port])

    # Login (if required), and wait for the first prompt
    p.sendline("")
    gotPrompt = False
```

```
    slcDevice = False
    cnt = 1
    while not gotPrompt:
        i = p.expect([pexpect.TIMEOUT, pexpect.EOF,
                      'login:', 'Error: (.*)\r\n',
                      '>'], timeout=10)
        if i == 0:     # Timeout
            cnt = cnt + 1
            if cnt == 3:
               print("Timeout waiting to connect to DP", devicePort, ".")
                p.terminate(True)
                p.wait()
                break
            # may need to send a CR to get prompt
            p.send("\r")
        elif i == 1:   # EOF
            print("portsession on DP ", devicePort, "unexpectedly
terminated.")
            break
        elif i == 2:   # login prompt
            p.sendline("sysadmin")
            p.expect("Password:")
            p.sendline("PASS")
            slcDevice = True
            gotPrompt = True
        elif i == 3:   # error from portsession
            print(p.match.group(1).decode('utf-8'))
            p.terminate(True)
            p.wait()
            break
        elif i == 4:   # prompt
            gotPrompt = True
        # end if while not gotPrompt:

    if not gotPrompt:
        devicePort = devicePort + 1
        pList.append('')
        continue

    # Detect the prompt
    devPrompt = ""
    p.send("\n")
    i = p.expect([pexpect.TIMEOUT, pexpect.EOF, '\r\n(.*)>'],
timeout=10)
    if i == 0 or i == 1:   # Timeout or EOF
        print("Timeout waiting for the prompt on DP", devicePort, ".")
        p.terminate(True)
        p.wait()
        devicePort = devicePort + 1
        pList.append('')
        continue
    if i == 2:             # prompt
        devPrompt = p.match.group(1).decode('utf-8')
```

```
    if devPrompt == "":
        print("Timeout waiting for the prompt on DP", devicePort, ".")
        devicePort = devicePort + 1
        pList.append('')
        continue

    print("Detected prompt", devPrompt, ".")
    # Strip characters not allowed in DP names
    devPromptStrip = re.sub("[^0-9A-Za-z\._\-]", "", devPrompt)
    devPromptComplete = devPromptStrip + "-" + str(devicePort)
    pList.append(devPromptComplete)

    p.terminate(True)
    p.wait()
    devicePort = devicePort + 1
    # end of while devicePort <= numPorts:

# Connect to the SLC CLI and set the device port names
p=pexpect.spawn('clisession -U sysadmin')

loggedIn = False
while not loggedIn:
    i = p.expect([pexpect.TIMEOUT, pexpect.EOF,
                  'Model Number: SLC80(\d*)\r\n', 'Model Number:
SLB882\r\n',
                  '(\[.*>)'], timeout=10)
    if i == 0:   # Timeout
        print("Timeout waiting to login.")
        p.terminate(True)
        sys.exit(1)
    elif i == 1: # EOF
        print("Session unexpectedly terminated.")
        p.terminate(True)
        sys.exit(1)
    elif i == 4: # prompt
        loggedIn = True

devicePort = 1
while devicePort <= numPorts:
    if skipPorts and devicePort >= 9 and devicePort <= 16:
        devicePort = devicePort + 1
        continue
    if len(pList[devicePort - 1]) > 0:
        # Detected a prompt; set it
       print("Setting name on DP", devicePort, "to", pList[devicePort -
1], "...")
        s = "set deviceport port " + str(devicePort) + " name " +
pList[devicePort - 1]
        p.sendline(s)
        i = p.expect([pexpect.TIMEOUT,
                      'Device Port settings successfully updated.\r\n'],
                      timeout=10)
        if i == 0:   # Timeout
            print("Timeout waiting for response.")
```

```
    devicePort = devicePort + 1

# Terminate the CLI session
p.sendline("logout")
time.sleep(.500)
p.wait()
print("Script completed.")
sys.exit(0)
```

Tcl Custom Script - SLC CLI Session

An example of a Tcl Custom Script that interacts with a CLI session:

```
#! tcl
# Script to get the current internal temperature of the SLC
# Accepts one optional command line parameter for location

set slcTemp "unknown"
set location ""

# Are there any command line parameters?
if {$argc > 0} {
    set location [lindex $argv 0]
}

set now [clock seconds]
set date [clock format $now -format {%D %R}]
if {$argc > 0} {
    puts "Internal temperature of the $location SLC at $date"
} else {
    puts "Internal temperature of the SLC at $date"
}

set io [open "| clisession -U sysadmin" r+]

set loggedIn false
while {! $loggedIn} {
    set len [gets $io line]
    if {[string first "Invalid local user" $line] != -1} {
        puts "Invalid local user passed to clisession"
        break
    }
    if {[string first "For a list of commands" $line] != -1} {
        puts $io "\n"
        flush $io
    }
    if {[string first ">" $line] != -1} {
        set loggedIn true
    }
}

if {! $loggedIn} {
    exit 1
```

```
}

puts $io "show temp"
flush $io
set gotTemp false
while {! $gotTemp} {
    set len [gets $io line]
    if {[string first "Current Internal Temperature" $line] != -1} {
       set slcTemp [string range $line [expr {[string first ":" $line] +
1}] end]
        set gotTemp true
    }
}

puts "Temperature: $slcTemp"

puts $io "logout"
flush $io
exit 0
```

Sites

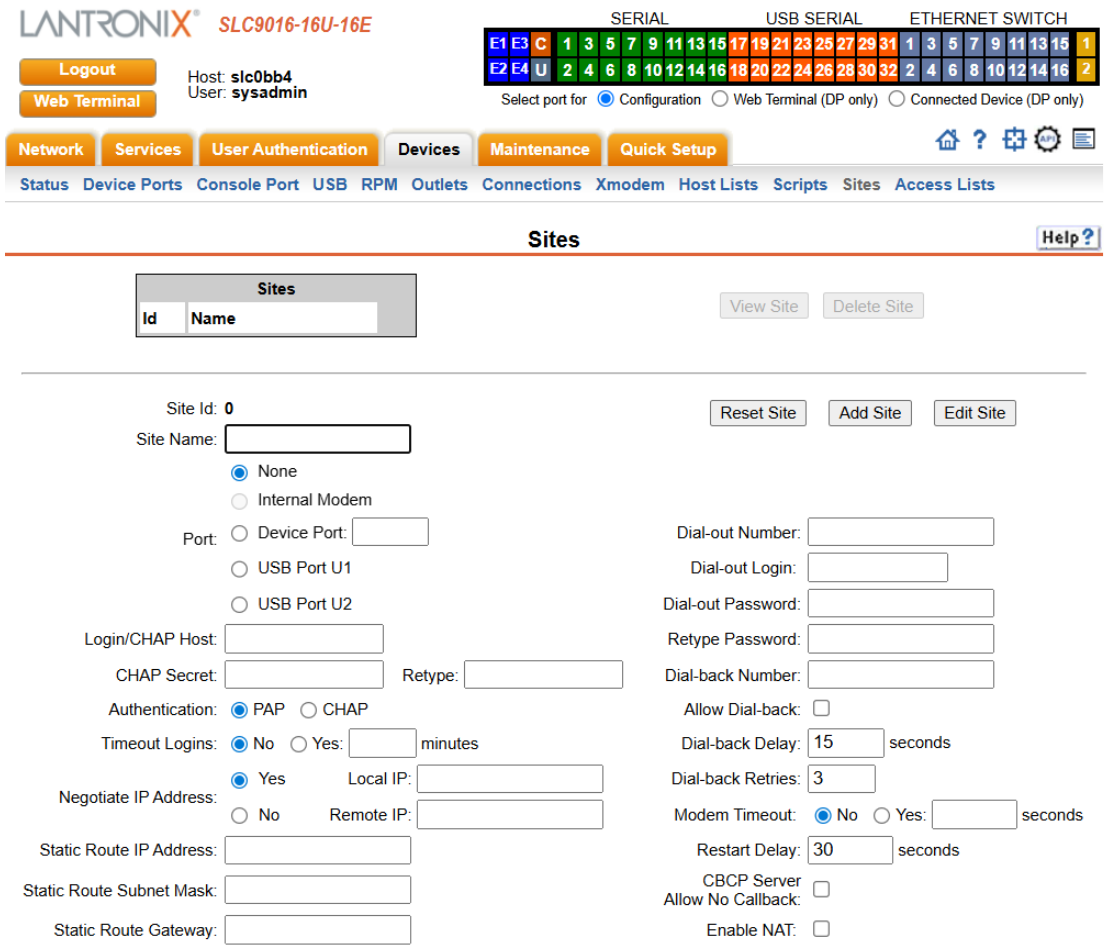
A site is a group of site-oriented modem parameters that can be activated by various modem-related events (authentication on dial-in, outbound network traffic for a dial-on-demand connection, etc.). The site parameters will override parameters that are configured for a modem.

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 234*.

To add a site:

1. Click the **Devices** tab and select the **Sites** option. The Sites page displays:

Figure 10-19 Devices > Sites



2. In the lower section of the page, enter the following:

Note: *To clear fields in the lower part of the page, click the* ***Reset Site*** *button.*

Site Id (view only)	Displays after a site is created.
Site Name	Enter a name for the site.
Port	Select the port: **None**, **Internal Modem**, **Device Port**, **USB Port U1**, or **USB Port U2** 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 234*.

Login/CHAP Host	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 & dial-on-demand, or dial-back & 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.
CHAP Secret/Retype	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 advanced console server 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 9000 advanced console server 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 unit 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, or when a remote system requests authentication from the SLC 9000 unit when it dials in. May have up to 32 characters. This ID is used for authenticating the SLC 9000 advanced console server during the dial-out portion of a dial-back (including CBCP server) and dial-on-demand.
Dial-out Password	Password for authentication when dialing out to a remote system, or if a remote system requests authentication from the SLC unit when it dials in. May have up to 64 characters
Retype Password	Re-enter password for dialing out to a remote system. May have up to 64 characters.
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 9000 advanced console server 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.
Restart Delay	The number of seconds after the modem timeout and before the SLC unit attempts another connection. The default is 30 seconds.
CBCP Server Allow No Callback	For a CBCP Server site, allows "No Callback" as an option in the CBCP handshake in addition to User-defined Number and Admin-defined Number.
Enable NAT	Select to enable Network Address Translation (NAT) for PPP connections. ***Note:*** *IP forwarding must be enabled on Network Settings for NAT to work.*

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.

Site Commands

Go to *Site Commands* to view CLI commands which correspond to the web page entries described above.

Access Lists

An access list, also known as a white list, is a list of phone numbers that will be granted access during the modem dial-in process. An access list can contain up to 100 phone numbers. This feature requires the Caller ID service be enabled for the phone line by the TelCo provider, and modem Caller ID Logging is enabled with a directive to enable caller ID for the modem in the Caller ID Logging Modem Command. This directive is usually AT+VCID=1 (refer to the AT command set for your modem).

The access list can be configured with two options for responding to a phone number that is not in the access list: hang up the call or ignore the call. If the access list is configured for ignore, the console manager dialing process will wait until the other side of the call hangs up (if the other side never hangs up, this can result in dial-in access to the console manager being blocked until the administrator resolves this issue).

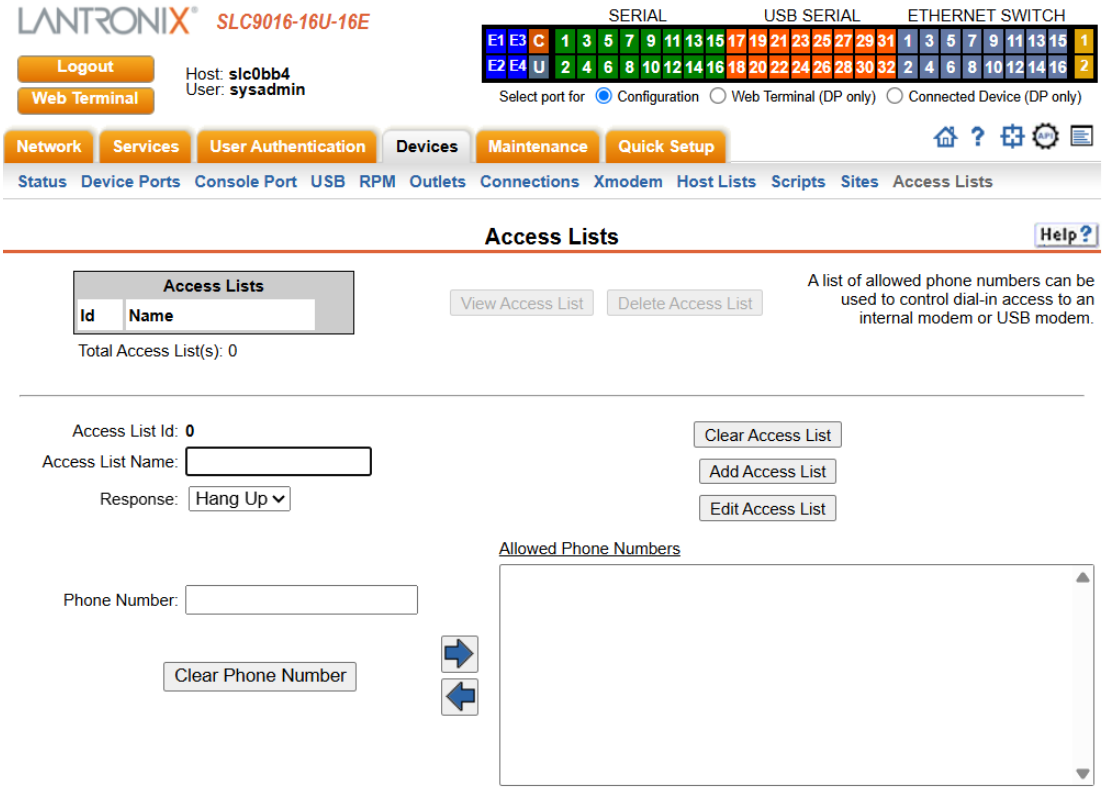
A maximum of 20 access lists can be created.

To use an access list with a modem, create one or more access lists (described below), then assign the access list to the console manager internal modem or an external USB modem.

To add an access list:

1. Click the Devices tab and select the Access Lists option. The Access Lists page displays

Figure 10-20 Devices > Access Lists.



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 Access List*** *button.*

Access List Id (view only)	Displays after an access list is created.
Access List Name	Enter a name for the access list. Valid characters are letters, numbers, hyphen and underscore. The maximum length is 40 characters.
Response	The response to phone numbers that dial-in and are not on the access list: Hang Up or Ignore. If the access list is configured for ignore, the console manager dialing process will wait until the other side of the call hangs up (if the other side never hangs up, this can result in dial-in access to the console manager being blocked until the administrator resolves this issue).

Allowed Phone Numbers	The list of phone numbers that are allowed to dial into a modem. Each access list must contain at least one phone number, and can have up to a maximum of 100 numbers. Enter numbers in the Phone Number field and click the right arrow to add numbers to the list. Click numbers in the list and use the left arrow to remove numbers from the list. The Clear Phone Number field will clear the contents of the Phone Number field.

3. Click the **Add Access List** button.

To view or update an access list:

1. In the Access Lists table, select the access list and click the **View Access List** button. The access list attributes are displayed in the bottom half of the page.
2. Update any of the access list attributes.
3. Click the **Edit Access List** button.

To delete an access list:

1. Select the access list in the Access Lists table.
2. Click the **Delete Access List** button.

Access List Commands

Go to *Access List Commands* to view CLI commands which correspond to the web page entries described above.

Modem Dialing States

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

Dial In

The SLC 9000 advanced console server 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 9000 advanced console server 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 advanced console server waits for a peer to call the SLC unit, establishes a text (command line) or PPP connection, authenticates the user, and if the SLC 9000 advanced console server 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 unit will hang up and wait **Dial-back Delay** seconds before initiating the dial-back. The SLC 9000 advanced console server 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 unit 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 9000 advanced console server, 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 9000 advanced console server 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 unit 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 9000 advanced console server 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.

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 **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 advanced console server, 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 9000 advanced console server 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 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 **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 9000 advanced console server will hang up and wait **Dial-back Delay** seconds before initiating the dial-back. The SLC unit 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 9000 advanced console server 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 and CBCP Client

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. 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 9000 advanced console server waits for a client to call the SLC unit, establishes a PPP connection, authenticates the user, and negotiates a dial-back number with the client using CBCP. If the SLC 9000 advanced console server 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/Remote 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 CHAP Challenge response sent by the PPP peer. If the remote peer requests PAP or CHAP authentication from the SLC unit, the **Remote/Dial-out Login** and **Remote/Dial-out Password** will be provided as authentication tokens. Once 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 the authenticated user is a Local/Remote 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 unit can determine a dial-back number to use, it will hang up and wait **Dial-back Delay** seconds before initiating the dial-back (if the dial-back fails, the SLC will try **Dial-back Retries** times to dial-back). The SLC unit will call back the previously authenticated remote peer, and if the remote peer requests PAP or CHAP authentication, provide the **Remote/Dial-out Login** and **Remote/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 unit 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 unit dials the **Dial-out Number**, and if the remote peer requests PAP or CHAP authentication, provides the **Remote/Dial-out Login** and **Remote/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 unit will provide the **Fixed Dial-back Number** as the number to call). If the CBCP handshake is successful, the SLC unit will terminate the PPP connection, hang up, and wait for the server to dial back. When the remote server calls back the SLC unit and the PPP connection is established, the user will be authenticated via PAP or CHAP (configured with the **Authentication** setting). For PAP, the Local/Remote 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 CHAP Challenge response 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 unit answers after the 2nd ring.*
- *Any text or PPP connection can be terminated by setting the modem state to disabled.*

Key Sequences

The default values for the various key sequences (Escape Sequence, Break Sequence, View Port Log Sequence, Power Menu Sequence) are set to different key sequences, and it is recommended that they always be set to different key sequences so that the SLC can properly handle each of the functions accessed by the key sequence while connected to a device.

For example, if the View Port Log Sequence is set to the same sequence as the Power Menu Sequence, and this sequence is typed while connected to a device port, both the Power Menu and the option to display Port Log will be displayed, with the Power Menu taking precedence and processing user input.

If any of the key sequences are set to the same value, the precedence used to process the key sequences is:

- Escape Sequence
- Power Management Sequence
- View Port Log Sequence

It is also recommended that the key sequences not share a significant amount of overlap other than the first character. For example, if the View Port Log Sequence is set to **ABCD** and the Power Management Sequence is set to **ABCE**, the first three characters of both sequences are the same - this is not recommended.

When any portion of key sequences overlap, typing a complete escape sequence for one of the sequences will reset recognition of the other sequences back to the beginning of the key sequence. For example, with the default View Port Log sequence of **ESC-V** and the default Power Management sequence of **ESC-P**, if the user types "ESC-V" and views the port log and then returns to interacting with the device, they need to type "ESC-P" to view the Power Menu, and not just "P".

When detecting key sequences, after receiving the first character(s) of a sequence, the SLC will wait 3 or more seconds for the remaining characters, before timing out and sending all characters to the device. For example, if the Escape Sequence is **ABCD**, and the user types "AB", the SLC will wait at least 3 seconds for the next character ("C") before timing out and sending the "AB" characters to the device.

11: Managed Devices Automation

Managed Device Automation is a built-in system for onboarding Cisco, Arista, and other network devices connected to the console manager serial ports, then running scheduled operations against them automatically. This feature is only available on SLC9000 models. Configuration is available at the CLI only; see help set managedfor the supported configuration options. Currently Cisco IOS and IOS-XE models are supported.

Once a device has been onboarded, a managed device name can be used with `connect direct ssh` or `connect direct telnet` to access the managed device CLI via the configured management IP address.

The following features are available for managed devices:

- **Onboarding**: manually identify the device to be managed or discover the device (future capability); this requires providing authentication credentials for the device. When a device is onboarded, the managed device settings and operations schedule will be auto-configured.
- **Settings**: configure the managed device name, update authentication credentials, labels and management IP address.
- **Operations**: managed and update default schedules, and create new tasks to monitor and control the device.
- **Files**: repository of configuration, log and monitoring files maintained for the managed device. **Diagnostics**: view managed device logs and update the logging level.

Example of onboarding and managing a Cisco IOS-XE device on device port 9:

1. **Onboarding**: this is an example of manually specifying the device type and providing the serial port setting for the device port that the device is connected to. If the serial port settings are not specified, the default settings **9600/8/N/1** will be used. After onboarding, device health and details are automatically collected.

```
[slc0b34]> set managed onboard 9 method manual login admin serial 9600/8/N/1
1:Cisco
Select Make (1-1): 1
Enter Cisco model: 9200L
1: IOS
2: IOS-XE
Select OS (1-2): 2
Enter password for user 'admin':
Retype password:
Enter privileged user password:
Retype password:
Enter Management IPv4 Address: 10.0.1.163
Onboarding of device connected to port 9 initiated (may take up to 5 minutes).
Do not reboot the SLC during this time.
See 'show managed onboard port 9' and 'show managed port 9 display status' for
results.
[slc0b34]> show managed onboard
Ports with onboarded managed devices:
Port 9 device onboarded at 06/15/26 16:07:
cisco C9200L-24P-4G, iosxe/17.12.04, hostname knoxcisco
1 onboarded managed device(s).
[slc0b34]> show managed port 9 display status
       Managed Device Information_____________________________________
Status of knoxcisco/Port 9
==================================================
Details  - Description: <none>
```

```
Make: cisco
       Model: C9200L-24P-4G
       OS/Version: iosxe / 17.12.04 Serial Number: FVH29111LR0 Label(s):
<none>,<none>,<none>
Network  - Hostname: knoxcisco
       Management IPv4 Address: 10.0.1.163 Ping IPv4 Address: 10.0.1.196
Resource - CPU Utilization (1 minute, 5 minute avg): 5.0%, 5.0%
       Total  Memory: 2020675584 bytes
       Used Memory: 860565504 bytes
       Used Memory Percentage: 43%
       Total Flash: 1956839424 bytes
       Used Flash: 646328320 bytes
       Used Flash Percentage: 33%
       Temperature: 35C (95F) (state: normal)
Auth   - User Login: admin
       User Password: <set> Priv
       User Login: <none>
       Priv Password: <set>
Serial - Settings: 9600/8/1/N
       DSR/DTR/CTS: No/Yes/Yes
       Bytes Input/Output: 32215705/415658
       Errors: No
Status - Onboarded: 2026-06-15 20:06:00.682570
       Time of Last Update: 2026-06-18T02:20:12.734Z
       Uptime: 2 days, 6 hours, 18 minutes
```

There should not be any active connections to the device port during onboarding and while the device is being managed with the device automation functionality. The device console port is frequently in use to monitor the health of the device and run operations (tasks). The operations can be paused in order to connect to the device console and interact directly with the device.

2. **Settings**: configuration settings for a managed device can be updated, including labels (used to identify classes of managed devices, used when filtering devices), the managed IPv4 address (used for accessing the CLI of the device via Telnet or SSH if these protocols are enabled), and the ping IPv4 address (used to test connectivity between the device and another host that should be reachable from the device).

```
[slc0b34]> set managed settings 9 label switch Managed Device settings
successfully updated.
[slc0b34]> show managed settings port 9
       Managed Device Setting - Port  9
Name: knoxcisco
Description: <none>
Label(s): switch,<none>,<none>
Management IPv4 Address: 10.0.1.163
Ping IPv4 Address: 10.0.1.196
User Login: admin
User Password: <set>
Priv User Login: <none>
Priv Password: <set>
Serial Settings: 9600/8/1/N
```

3. **Operations**: default tasks configured after onboarding, and single or repeating tasks can be created and updated. Some operations may prompt for additional inputs. A task can be configured to start immediately or at a later time, and can be performed once or repeated at a specified frequency. The operations that are supported are:

```
clear_counters            Reset interface counters
clear_logs                Clear system logs
```

```
device_status              Retrieve heartbeat, monitor the chassis and health
status
device_tech                Retrieve detailed tech support report (no repeat
option)
device_ping                Ping a device to test connectivity
interface_on               Turn a network interface on
interface_off              Turn a network interface off
interface_cycle           Turn a network interface off, then on
monitor_interfaces         Monitor network interface
pull_config                Pull configuration, save in file repository
pull_startup_config        Pull startup configuration, save in file repository
pull_vlan_config           Pull VLAN configuration, save in file repository
push_config                Push configuration from file repository
push_config+reboot         Push configuration followed by reboot
```

Once a device has been onboarded, a set of default operations are created:

```
[slc0b34]> show managed operations
       Managed Device Schedule and Jobs
Schedule for knoxcisco/Port 9

  Operation           Op Create Time   Freq min         Enabled         Last Run Time
                                                                        Status

  ==================    ============================    ==========      =================

  Device Heartbeat     06/15/26 16:07 4                Yes             PENDING

  Monitor Chassis      06/15/26 16:07 5                Yes             PENDING

  Monitor Status       06/15/26 16:07 7                Yes             PENDING

  Monitor Interfaces  06/15/26 16:07 15                Yes             PENDING

  Pull Running Config   06/15/26 16:07 180             Yes             PENDING

  Pull Startup Config   06/15/26 16:07 1440            Yes             PENDING

  Pull VLAN Config     06/15/26 16:07 1440             Yes             PENDING

  8 Operation(s).
```

The operations are run according to their schedule, and the status is updated:

```
[slc0b34]> show managed operations
       Managed Device Schedule and Jobs
Schedule for knoxcisco/Port 9
Operation     Op Create Time Freq min Enabled Last Run Time Status
============ ============== ======== ========= ============= ============
Device Heartbeat    06/15/26 16:07 4    Yes    06/15/26 18:02 COMPLETED
Monitor Chassis     06/15/26 16:07 5    Yes    06/15/26 18:05 DISPATCHED
Monitor Status      06/15/26 16:07 7    Yes    06/15/26 18:02 COMPLETED
Monitor Interfaces  06/15/26 16:07 15   Yes    06/15/26 17:55 COMPLETED
Pull Running Config 06/15/26 16:07 180Yes                     PENDING
Pull Startup Config 06/15/26 16:07 1440Yes                    PENDING
Pull VLAN Config    06/15/26 16:07 1440Yes                     PENDING
```

New tasks can be scheduled as needed:

```
[slc0b34]> set managed operations 9 operation device_ping starttime now
Operation device_ping 10.0.1.196 on device connected to port 9 initiated (5 pings
sent each time operation is run).
[slc0b34]> show managed operations
       Managed Device Schedule and Jobs
Schedule for knoxcisco/Port 9
Operation  Op Create Time Freq min Enabled Last Run Time  Status
============ ============ ======== ======= ============== ============
Device Heartbeat06/15/26 16:07 4       Yes    06/16/26 11:40 COMPLETED
```

```
Monitor Chassis    06/15/26 16:07 5      Yes   06/16/26 11:42   COMPLETED
Monitor Status     06/15/26 16:07 7      Yes    06/16/26 11:41  COMPLETED
Monitor Interfaces 06/15/26 16:07 15     Yes    06/16/26 11:42   COMPLETED
Pull Running Config 06/15/26 16:07 180   Yes  06/16/26 10:11    COMPLETED
Pull Startup Config     06/15/26 16:07 1440  Yes               PENDING
Pull VLAN Config   06/15/26 16:07 1440    Yes                  PENDING
Device Ping        06/16/26 11:43 N/A     Yes                  PENDING
9 Operation(s).
```

Any errors encountered for an operation with status **FAIL** can be displayed with show managed operations port 9 display detailed.

4. **Files Repository**: as operations are run, they generate log files from the operation and possibly additional artifacts (for example, a device configuration). The files can be viewed (if a text file), compared to another file in the repository, downloaded off the SLC via scp or sftp, and used for an operation on the managed device (for example, pushing a configuration to the device at a scheduled time). Files can also be uploaded to the repository and version labels associated with each file:

```
[slc0b34]> show managed files
       Managed Device File Repository
Device knoxcisco/Port 9
Generated by: U=user generated file, S=default schedule files
Type: R/S=config, L=log file, O=OS, P=POST, T=tech report, U=user file, V=VLAN
```

Id	File Category	Create Time	Version	Size (KB)	Generated|Type|Name
1	Monitor Status	06/15/26 16:06	<none>	6	S|L|facts.collect.ba
2	Inventory	06/15/26 16:06	<none>	1	S|L|facts.collect.in
3	Monitor Interfaces	06/15/26 16:06	<none>	5	S|L|facts.collect.in
4	Monitor Chassis	06/15/26 16:07	<none>	29	S|L|telemetry.health
5	Device Heartbeat	06/17/26 22:49	<none>	10	S|L|device.heartbeat
6	Monitor Chassis	06/17/26 22:50	<none>	29	S|L|telemetry.health
7	Monitor Status	06/17/26 22:47	<none>	6	S|L|facts.collect.ba
8	Monitor Interfaces	06/15/26 16:06	<none>	5	S|L|facts.collect.in
9	Pull Running Config	06/15/26 19:10	17.12	7	U|R|cfg.read.running
10	Pull Running Config	06/15/26 19:10	<none>	1	S|L|cfg.read.running
11	Device Ping	06/16/26 11:43	<none>	1	U|L|device.ping
12	Device Ping	06/16/26 11:45	<none>	1	U|L|device.ping
13	Pull Startup Config	06/16/26 16:09	17.12	5	U|S|cfg.read.startup
14	Pull Startup Config	06/16/26 16:09	<none>	1	S|L|cfg.read.startup
15	Pull VLAN Config	06/16/26 16:11	<none>	1	U|V|vlan.pull
16	Pull VLAN Config	06/17/26 16:11	<none>	1	S|L|vlan.pull

```
16 File(s).
```

Displaying the contents of the file with ID #2:

```
[slc0b34]> show managed files port 9 contents 2 display head numlines 10
       Managed Device File Repository Contents Files for knoxcisco/Port 9 -
File ID 2 / Inventory:
### show inventory show inventory
NAME: "c92xxL Stack", DESCR: "c92xxL Stack"
PID: C9200L-24P-4G, VID: V06  , SN: FVH29111LR0
```

```
NAME: "Switch 1", DESCR: "C9200L-24P-4G"
PID: C9200L-24P-4G, VID: V06  , SN: FVH29111LR0

NAME: "Switch 1 - Power Supply A", DESCR: "Switch 1 - Power Supply A"
PID: PWR-C5-600WAC, VID: V02  , SN: QCS29056KMW
```

Assigning a version label to a file:

```
[slc0b34]> set managed files 9 version 2 string baseline File
facts.collect.inventory assigned version 'baseline'.
[slc0b34]> show managed files
       Managed Device File Repository
Device knoxcisco/Port 9
Generated by: U=user generated file, S=default schedule files
Type: R/S=config, L=log file, O=OS, P=POST, T=tech report, U=user file, V=VLAN
```

ID	File Category	Create	Time	Version	Size (KB)	Generated|Type|Name
1	Monitor Status	06/15/26	16:06	<none>	6	S|L|facts.collect.in
2	Inventory	06/17/26	22:59	baseline	N/A	S|L|facts.collect.in
3	Monitor Interfaces	06/15/26	16:06	<none>	5	S|L|facts.collect.in
4	Monitor Chassis	06/15/26	16:07	<none>	29	S|L|telemetry.health
5	Device Heartbeat	06/17/26	22:57	<none>	10	S|L|device.heartbeat
6	Monitor Chassis	06/17/26	22:55	<none>	28	S|L|telemetry.health
7	Monitor Status	06/17/26	22:54	<none>	6	S|L|facts.collect.ba
8	Monitor Interfaces	06/15/26	16:06	<none>	5	S|L|facts.collect.in
9	Pull Running Config	06/15/26	19:10	17.12	7	U|R|cfg.read.running
10	Pull Running Config	06/15/26	19:10	<none>	1	S|L|cfg.read.running
11	Device Ping	06/16/26	11:43	<none>	1	U|L|device.ping
12	Device Ping	06/16/26	11:45	<none>	1	U|L|device.ping
13	Pull Startup Config	06/16/26	16:09	17.12	5	U|S|cfg.read.startup
14	Pull Startup Config	06/16/26	16:09	<none>	1	S|L|cfg.read.startup
15	Pull VLAN Config	06/16/26	16:11	<none>	1	U|V|vlan.pull
16	Pull VLAN Config	06/17/26	16:11	<none>	1	S|L|vlan.pull

```
   16 File(s).
```

12: Containers (Docker)

The SLC9000 supports Docker containers to run pre-built applications for automation and monitoring on the console manager. Images can be pulled from public repositories, including Docker hub, and run one or more container instances of the image. It is recommended that only trusted containers be downloaded to the console manager.

Containers are currently only configurable in the CLI; see help set container for the supported configuration options. Containers are stored in a large filesystem with separate storage for each boot bank; it is important to monitor the space used by containers (see the CLI command admin system show).

- Docker containers have the following limitations:
- Memory usage for each container is limited to 256MB
- CPU usage for each container is limited to 1 CPU
- Containers cannot gain new privileges via setuid or setgid
- Docker containers options that are not permitted are: --privileged, --security-opt, --ipc=host, --device, --userns=host, --cap-add, --memory, --cpus

Example of downloading and running Glances to monitor console manager resources:

1. **Enable Containers**: by default, containers are disabled; enable containers so that images can be downloaded, and containers that are created will be re-launched after reboot.

```
[slc0b34]> show container
   Current Container Settings
Container State: disabled
0 Image(s).
[slc0b34]> set container state enable Container settings successfully updated.
[slc0b34]> show container
   Current Container Settings
Container State: enabled
0 Image(s).
```

2. **Download Image**: download an image from Docker hub.

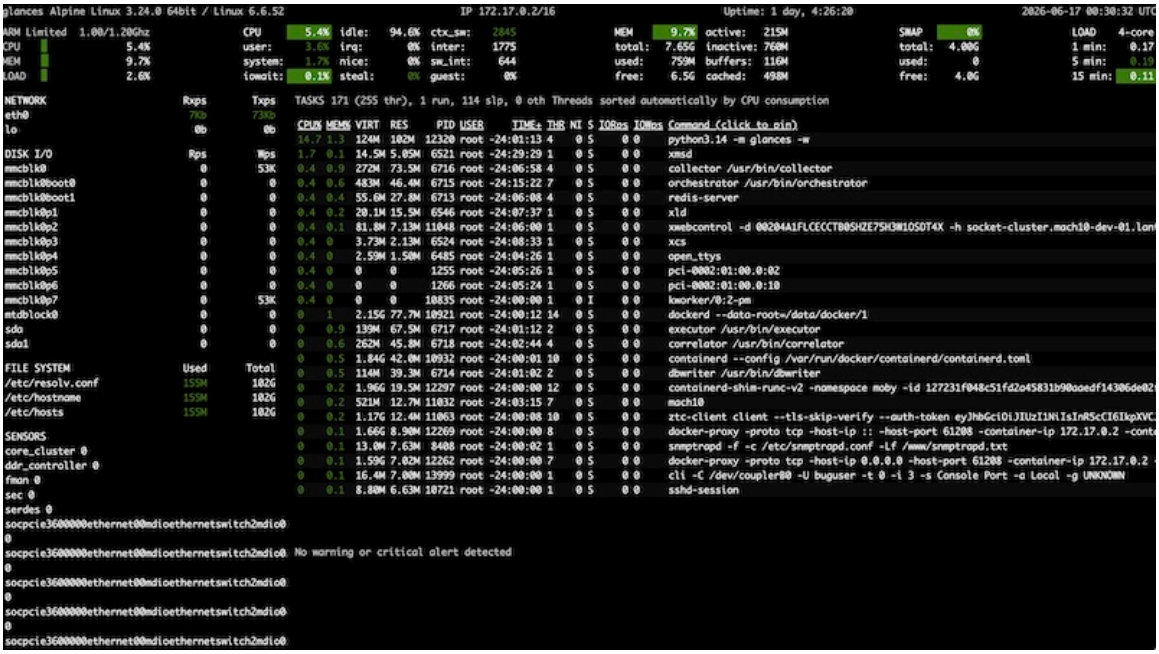
```
[slc0b34]> set container pull nicolargo/glances
Image download times from docker hub may vary based on network speed.
Please wait, downloading image 'nicolargo/glances'...
Container settings successfully updated.
[slc0b34]> show container display images
   Current Container Settings
Container State: enabled
Image 1:
Image Name: nicolargo/glances
Platform:              Tag Name:
Referenced Container:
1 Image(s).
```

3. Launch a runtime instance of the image (container):

```
[slc0b34]> set container run nicolargo/glances hostname glances otheropts "--pid
host -p 61208:61208 -e GLANCES_OPT=-w" name slcGlances
Container 'slcGlances' created successfully.
[slc0b34]> show container status display running
   Current Containers Status
CONTAINER ID  IMAGE     COMMAND       CREATED       STATUS     PORTS
```

```
127231f048c5  nicolargo/glances   "/bin/sh -c '/venv/b..."28 seconds agoUp 28
seconds0.0.0.0:61208->61208/tcp, :::61208->61208/t
```

4. **Test Container**: test that the container is running by accessing **http://<SLC9000 IP address>:61208/**:



5. **Stop Container**: stop the running container:

```
[slc0b34]> set container containerstate slcGlances action stop
Do you want to stop container slcGlances? [no] yes
Container state settings successfully updated.
[slc0b34]> show container status display exited
   Current Containers Status
CONTAINER ID  IMAGE  COMMAND          CREATED    STATUS     PORTS  NAMES
127231f048c5  nicolargo/glances"/bin/sh -c '/venv/b..."   21 minutes ago   Exited
(0) 23 seconds ago  slcGlances
```

6. **Delete the Container and Image:**

```
[slc0b34]> set container containerstate slcGlances action delete
Do you want to delete container slcGlances? [no] yes
Container state settings successfully updated. [
slc0b34]> set container delete nicolargo/glances
Do you want to delete container image nicolargo/glances? [no] yes
Container image 'nicolargo/glances' deleted successfully.
[slc0b34]> show container
   Current Container Settings
Container State: enabled
0 Image(s).
```

13: Power Management

The SLC9000 supports two power management modes: Integrated PDU Management for directly connected PDUs via a device port, and Remote Power Managers (RPMs) for network-connected power devices.

Integrated PDU Management

The console manager supports a single integrated external PDU to manage power for devices that may (or may not be) connected to the console manager via a serial port. This feature allows the administrator to view outlet status, turn outlets on or off, reboot outlets, view outlet current, set outlet wake (power on) state, and view PDU status. Multiple integrated external PDUs are not supported.

Integrated PDUs are connected to the console manager via a Device Port or USB Port (U1 or U2). Supported integrated PDUs:

- Synaccess SP-1004A Switched Pro+ ATS PDU
- Synaccess SP-1004B Single Phase Switched ATS PDU
- APC APC7900B NetShelter Rack PDU Switched 1U
  (Note: in rare cases controlling the APC PDU may require resetting the PDU to synchronize with the APC PDU state; when this is required the message "cannot login to the PDU; try again after one minute." is displayed.)

To setup a PDU for management via the console manager:

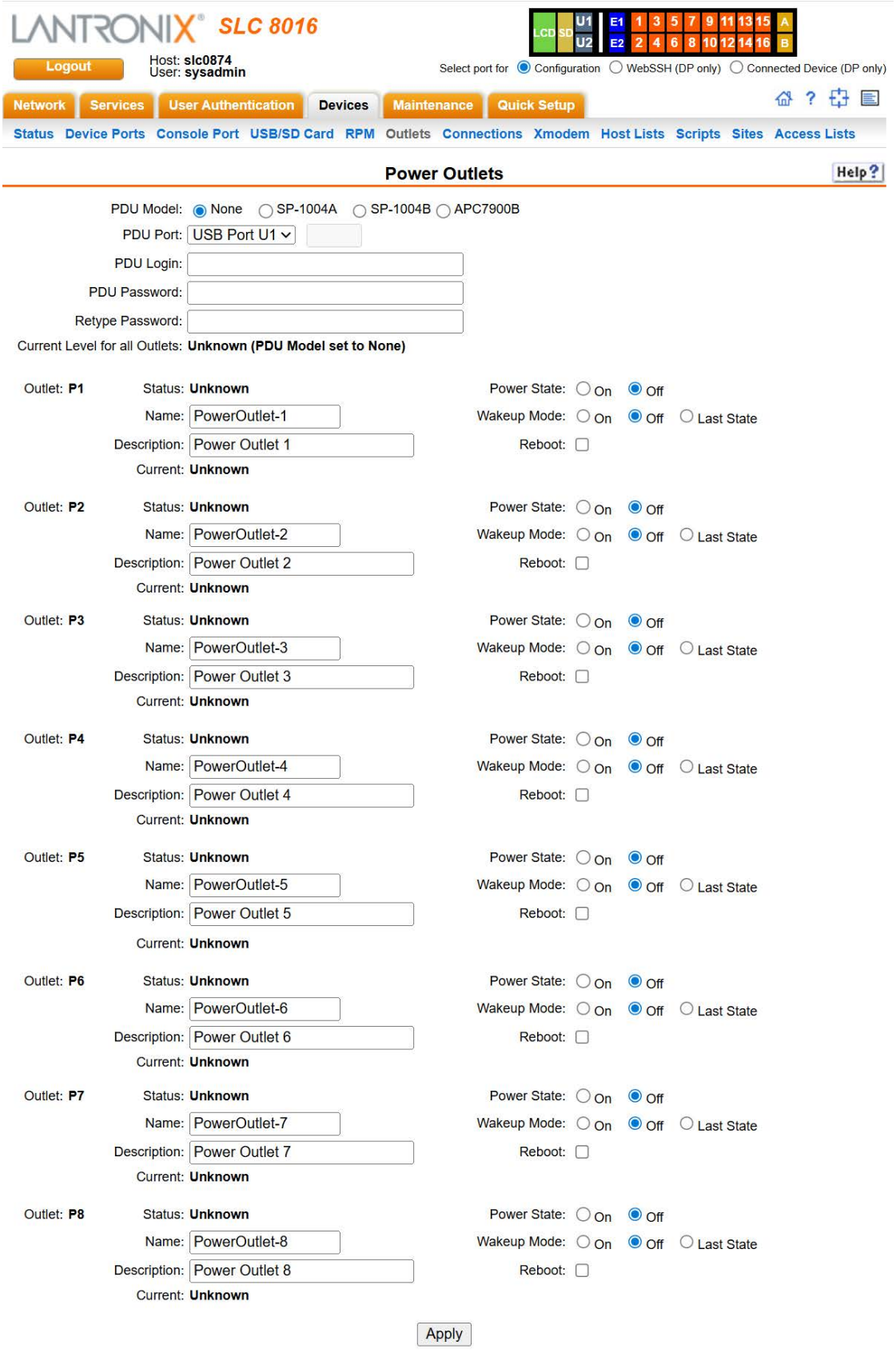
1. Connect the console port of the PDU to the desired serial port (front USB, USB device port or RJ45 device port) on the console manager.
2. On the console manager, configure the serial port settings to be compatible with the serial settings for the PDU console port. Use the CLI command **connect direct** to verify that the serial connection is correctly configured. See **PDU Port** below for more details.
3. In the Power Outlets settings, select the appropriate **PDU Model**, configure the **PDU Port** selected in step 2, and enter the PDU login credentials with **PDU Login** and **PDU Password**.
4. CLI **show power** or the web UI **Power Outlets** page should now display the status of the PDU outlets. Note that there will be a delay displaying the page while the PDU is queried.

At boot, the console manager will configure the on/off state and wakeup mode for each outlet on the PDU to match what is configured in the console manager Power Outlets configuration.

To manage an integrated PDU:

1. Click **Devices > Outlets** option (it may take a few moments for the console manager to query the PDU for status). The following page displays

Figure 13-1 Devices > Power Outlets:



2. Configure the following fields:

PDU Model	Select the model of the integrated PDU. The console manager will automatically determine what PDU features are available to the administrator based on the selected model. Supported models are **SP-1004A, SP-1004B,** and **APC7900B**.
PDU Port	Select the RJ45 or USB Device Port or USB Port (U1, or U2 on console managers that have 2 USB ports) which is connected to the console port of the PDU. The default value is **USB Port U1**. It is recommended that the serial settings for the PDU Port be configured with the correct serial settings for the PDU console port. For Synaccess PDUs, the default USB console port and RJ45 Port A settings are **Baud Rate: 115200, Data Bits: 8, Stop Bits: 1, Parity: None, Hardware Handshaking: None** (RJ45 Port A must be placed in **COM** mode before it can be used for PDU management via the console manager). In order to control or monitor a PDU, a user must have rights and permissions to access the configured USB or serial PDU port. For example, for USB Port U1, a user must have **USB** user permissions as well as **U1** data ports rights.
PDU Login	The user login that will be used to access the PDU CLI for commands and status. There is no default value; however if the PDU Login is not defined when the **PDU Model** is changed from **None** to a supported model, the default administrator username for the selected model will be auto-filled in for the PDU Login. The maximum length is 32 characters and valid characters are letters, numbers, !, @, #, $, % and ^. For Synaccess PDUs, the default username is **admin**. For APC PDU, the default username is **apc**.
PDU Password	The user password that will be used to access the PDU CLI for commands and status. There is no default value; however if the PDU Password is not defined when the **PDU Model** is changed from **None** to a supported model, the default administrator password for the selected model will be auto-filled in for the PDU Password. The maximum length is 64 characters and valid characters are letters, numbers, !, @, #, $, % and ^. For Synaccess PDUs, the default password for the **admin** username is **admin**. For APC PDU, the default password for the **apc** username is **apc**.
Current Level for All Outlets	The total load carried by the outlets in Amps. If the **PDU Model** is set to None, this will be blank. If there is an issue communicating with the PDU due to incorrect serial settings or login credentials, this will be displayed as **Unknown** along with an error message.

3. For each outlet, configure:

Outlet	Displays the number of the outlet being configured.
Status	Displays the current state of the outlet as reported by the integrated PDU. If there is an issue communicating with the PDU due to incorrect serial settings or login credentials, this will be displayed as **Unknown**.
Name	User-configurable name identifying the outlet. If the PDU supports configuring a name for each outlet, this value will be pushed to the PDU configuration. The outlet name can be up to 20 characters long and may contain alphanumeric characters, hyphen "-", period ".", or underscore "_" (this name length and character set may be more restrictive than what is supported on the integrated PDU).
Description	User-configurable text describing the outlet. The description can be up to 50 characters long and can contain any characters.

Current (some models)	Displays the load, in Amps, for the outlet as reported by the integrated PDU. If there is an issue communicating with the PDU due to incorrect serial settings or login credentials, this will be displayed as **Unknown**. If per-outlet current status if not available for the selected PDU model, this field will show **N/A**. For Synaccess PDUs, only the SP-1004A supports per-outlet current status, and APC7900B PDU does not support per-outlet current status.
Power State	Select whether the power should be on or off. Note that a Power State change and Reboot cannot be performed at the same time. If the **PDU Model** is changed from **None** to a supported model, the default Power State will be set to reflect the default state for the selected model. For Synaccess PDUs, the factory default setting for outlets is On. For APC7900B PDU, the factory default setting for outlets is On. If a PDU is connected to the console manager which is not in a factory default state, it may take multiple changes to outlet power states to synchronize the console manager configuration with the PDU configuration.
Wakeup Mode	Select whether, after a reboot, the power state for the outlet should be on, off, or returned to the state it was in before the reboot. For APC7900B PDU, the wakeup mode setting for outlet is not supported.
Reboot	To power cycle the outlet, select the checkbox. Note that a Power State change and Reboot cannot be performed at the same time. On outlet reboot APC7900B PDU makes the outlet's power state to On.

4. To save, click **Apply**.

Power Commands

Go to *Power Commands* to view CLI commands which correspond to the web page entries described above.

Remote Power Managers

The SLC supports managing remote power managers (RPMs) for devices from over 140 vendors. The RPMs can be either PDUs or UPSes, and can be managed via SNMP, serial port, network and USB connections. The RPMs web page displays a list of all currently managed RPMs with an overview of their current status, with options to control and view detailed status for each RPM, depending on its supported capabilities.

Network and SNMP managed RPMs are disabled in FIPS mode. The only action that can be performed on a network or SNMP managed RPM in FIPS mode is that it can be deleted via the CLI.

For a complete list of RPM models, drivers and driver options, refer to the *Network UPS Tools Hardware Compatibility List*.

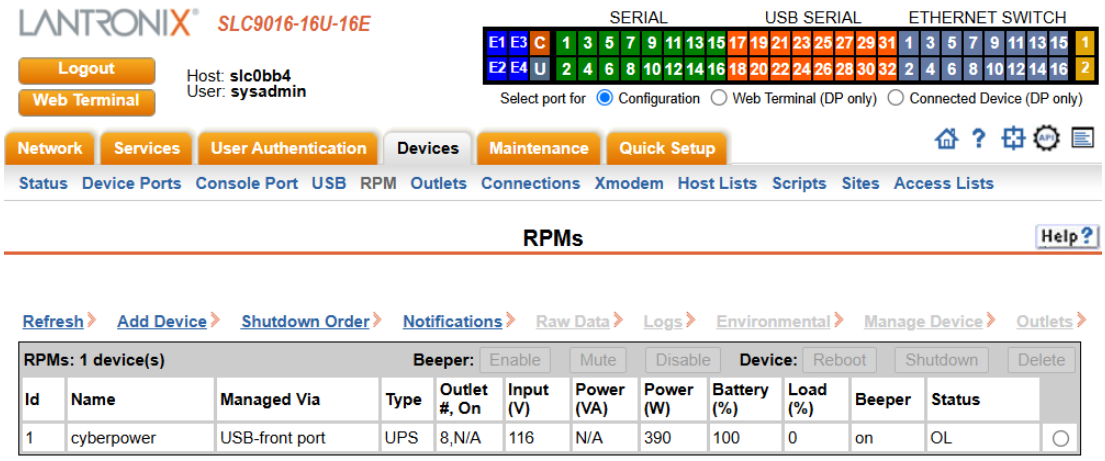
For notes on optimizing the management of specific devices, see *Optimizing and Troubleshooting RPM Behavior*.

Devices - RPMs

To control or view status for an RPM:

1. Click the **Devices** tab and select the **RPM** option. The RPMs page displays.

Figure 13-2 Devices > RPMs



2. In the lower section of the page, select an RPM by clicking on the radio button to the far right in the RPM's row. The options that are available for that RPM will be available (ungreyed). Select one of the following options:

Refresh	Refreshes the information in the RPMs table.
Add Device	Displays the *Device Ports > RPMs - Add Device* page to add a new managed PDU or UPS.
Shutdown Order	Displays the order in which all UPS devices are shutdown in the event that a UPS reaches a low battery state. See *Figure 13-3*. For more information, see *RPM Shutdown Procedure*.
Notifications	Displays the notifications configured for each PDU and UPS. See *Figure 13-4*.
Raw Data	Displays a window with all of the information returned by the driver when a query for status is requested. This option is available for all RPMs. See *Figure 13-5*.
Logs	Displays a window with any logging information that has been accumulated for the selected RPM, if logging is enabled for the RPM. This option is available for all RPMs. See *Figure 13-6*.
Environmental	Displays a window with any environmental (humidity and temperature) information that may be available for the selected RPM, if sensors are installed for the RPM. This option is available for all RPMs. See *Figure 13-7*.
Managed Device	Displays the *RPMs - Manage Device* page, with the complete status and configuration for the selected RPM. This option is available for all RPMs.
Outlets	Displays the *RPMs - Outlets* page for RPMs that support individual outlet control and status.
Beeper: Enable, Mute, Disable	If the RPM has a beeper than can be controlled, these options allow the administrator to **Enable**, **Mute**, or **Disable** the beeper. If you try to use **Mute** to silence a beeper and the beeper continues to sound, the UPS most likely does not support mute, and the **Disable** option will be the only way to silence the beeper.

Reboot	Reboots the RPM immediately, which may interrupt the power provided by the RPM while it is rebooting. Some PDUs and UPSes have a default delay that they will wait before initiating a reboot; this setting may be visible in the raw data (see above) as "ups.delay.reboot".
Shutdown	Shutsdown the RPM immediately, which will interrupt the power provided by the RPM. Some PDUs and UPSes have a default delay that they will wait before initiating a shutdown; this setting may be visible in the raw data (see above) as "ups.delay.shutdown".
Delete	Deletes the selected RPM, after a confirmation.

Figure 13-3 RPM Shutdown Order

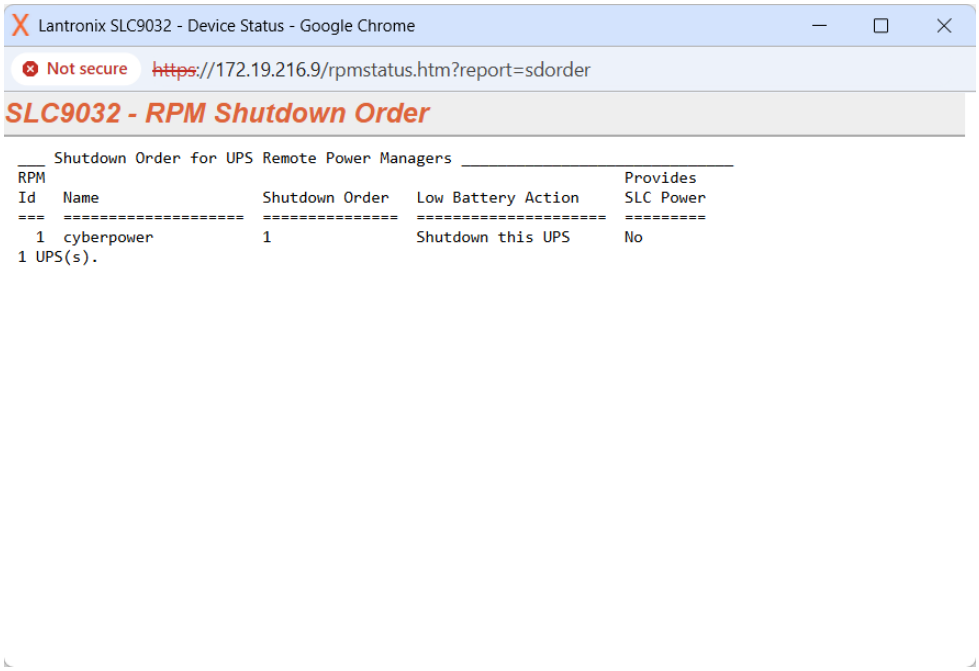


Figure 13-4 RPM Notifications

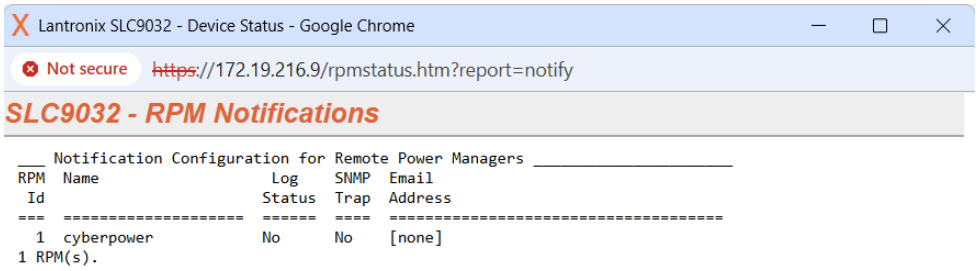


Figure 13-5 RPM Raw Data Log

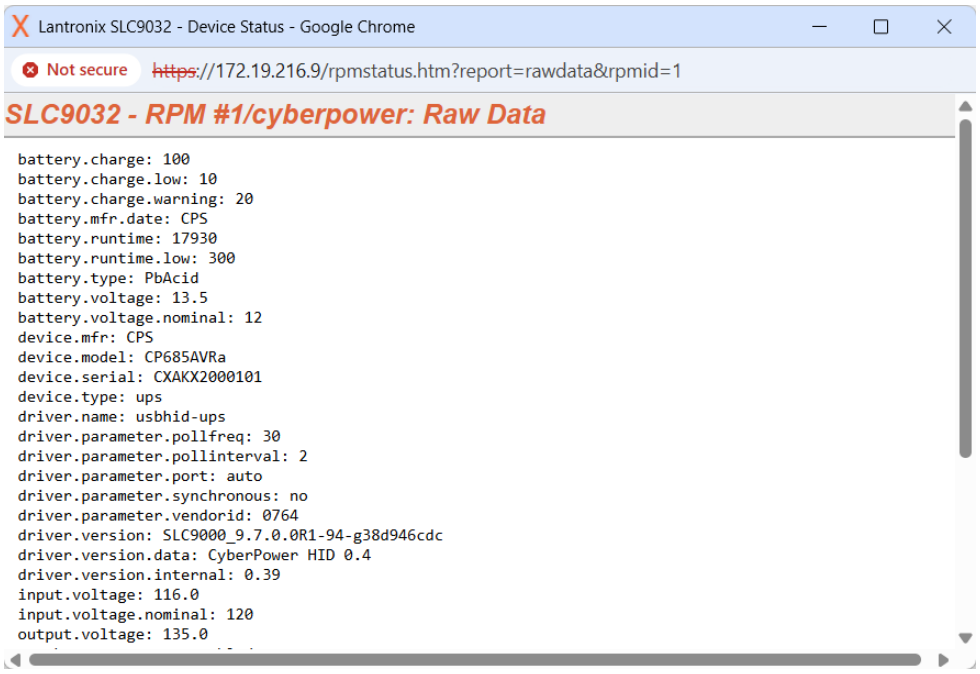


Figure 13-6 RPM Logs

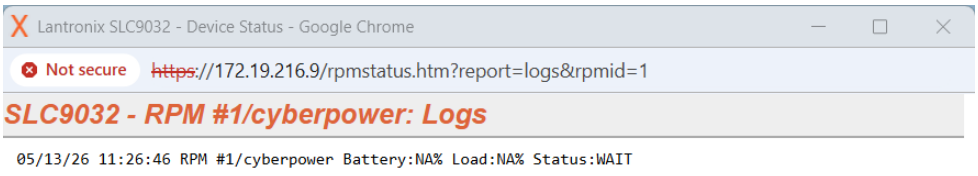


Figure 13-7 RPM Environmental Log



RPMs - Add Device

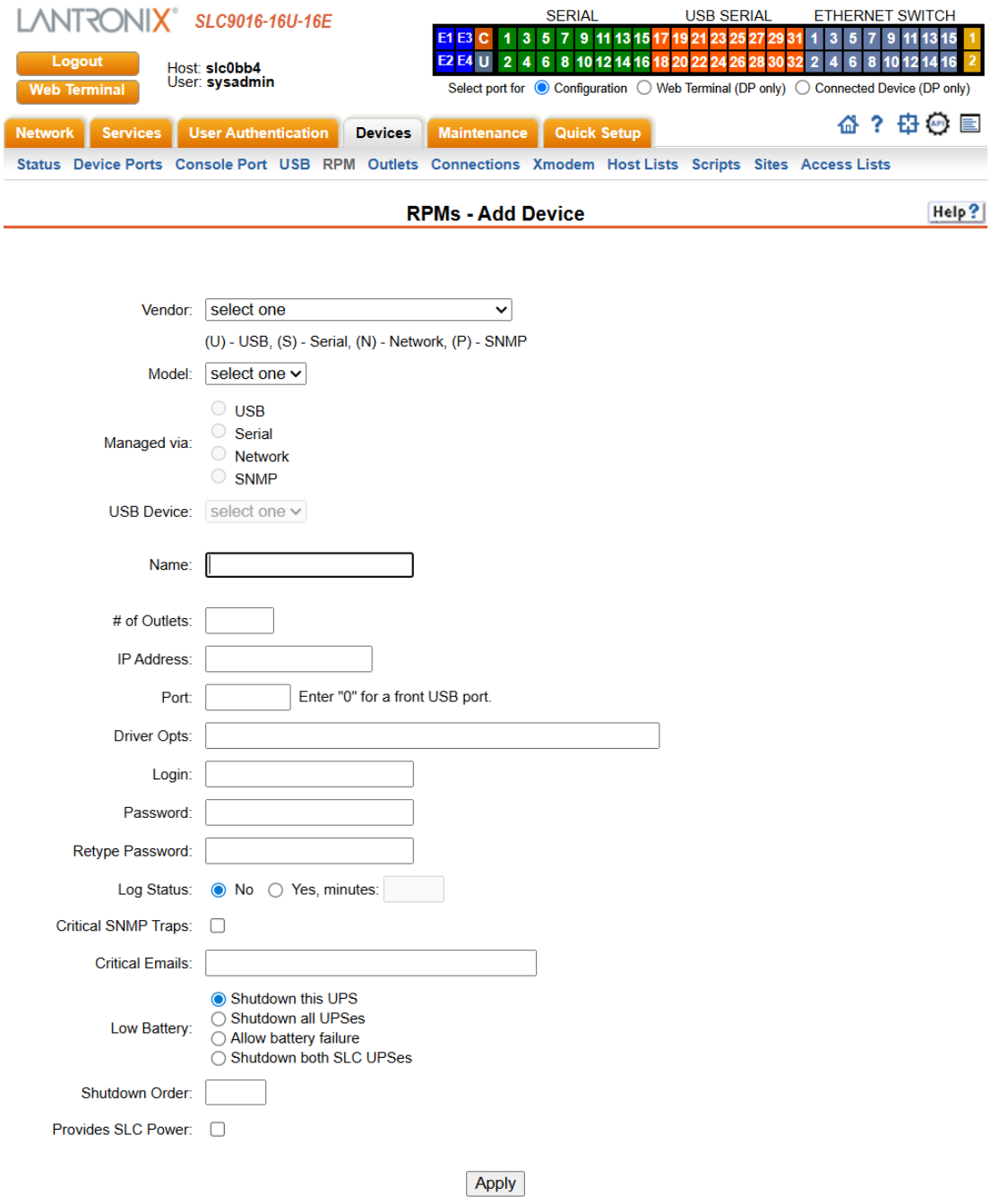
The **Add Device** page assists the administrator with adding a new managed RPM to the SLC configuration. With over 140 different vendors and nearly 1000 different models that are supported, the key to ensuring the SLC can properly manage a PDU or UPS is selecting the right model (with its associated driver) and any required driver options, especially for USB managed devices. On the *Devices > RPMs* page, access the *Device Ports > RPMs - Add Device* page to configure a new managed remote power manager (RPM) for the SLC configuration.

Note: *The Device Ports > RPMs - Add Device page with the same functionality can also be accessed through the Devices > Device Ports page.*

To add a new managed RPM :

1. Click the **Devices** tab and select the **RPMs** option. *Figure 13-2* shows the page that displays.
2. Click the **Add Device** link on the Devices > RPMs page. The following page displays.

Figure 13-8 Device Ports > RPMs - Add Device



3. Enter the following:

Vendor	Select the correct vendor from the drop-down menu.

Model	Select the Model in the drop-down menu. The drop-down menu will be populated with models supported for the selected vendor above. To the left of each model name is one or two letters in parentheses that indicate the type of control available for the selected model: P - SNMP, S - serial port, U - USB port, N - network. Some of the model names in the dropdown may be truncated because the list of models is very long - in this case, hover over the model name and the complete model name(s) will be displayed.
Managed via	If there is more than one way to manage the selected model, select the appropriate management method.
USB Device	For USB controlled devices, if the RPM is connected to a USB port, the device should be displayed in the USB Device dropdown. Select the correct device. This will automatically fill in the **Port** with the correct port number and the **Driver Opts** with the USB vendor and product ID (see below).
Name	Specify the unique name of the RPM (up to 20 characters).
# of Outlets	Specify the number of outlets on the RPM (maximum of 120 outlets).
IP Address	For SNMP and Network (Telnet) managed RPMs, specify the IP address of the RPM.
Port	For network (Telnet) managed RPMs, this is assumed to be port 23 (if left blank), or it can be filled in with an alternate TCP port. For USB managed RPMs, this is one of the front USB ports ("0") or the device port that the RPM is connected to on the SLC (this may be automatically filled in when the **USB Device** is selected). For serially controlled RPMs, this is the device port that the RPM is connected to on the SLC.
Driver Opts	For the driver associated with the RPM device, these are extra options which may be required to make the driver work. The most frequent use of the driver options is for USB devices (the vendor and product ID may be required so that the SLC can find the correct device on the USB bus), or in the event that the default driver options do not work with the RPM. The vendor and product ID may be automatically filled in if a USB Device is selected. There may also be other driver options that are filled in by the SLC from an internal table - these will be automatically set and can be viewed after the RPM has been added, and can always be overridden by driver options set by the user. The format of the driver options setting is one or more comma-separated parameters-value pairs, e.g. `<parameter name>=<value>`.
Login	For Network and serially managed RPMs, this is the administrator login.
Password/Retype Password	For Network and serially managed RPMs, this is the administrator password.
Read Community	For SNMP managed RPMs, this is the SNMP read (get) community.
Write Community/Retype Write Comm	For SNMP managed RPMs, this is the SNMP write (set) community.
Log Status	Indicates if the status of the RPM is periodically logged. Select Yes, minutes to log the status periodically and enter a value between 1 and 60 minutes. The logs can be viewed by viewing the *Devices > RPMs* page and clicking on "Logs".
Critical SNMP Traps	If enabled, under critical conditions (UPS goes onto battery power, UPS battery is low, UPS forced shutdown in progress, UPS on line power, UPS battery needs to be replaced, RPM is unavailable, communications with RPM lost, communications with RPM established), a `slcEventRPMAction` trap will be sent to the NMS configured in the *SNMP* settings. This requires that SNMP traps be enabled.

Critical Emails	If an email address is specified, under critical conditions (see Critical SNMP Traps above), an email notification will be sent to the email address. The Server and Sender configured in the *SSH* settings will be used to send the email.
Low Battery	For UPS devices only. Indicates the behavior to take when the UPS reaches a low battery state. Options are to **Shutdown this UPS** - shutdown only the UPS that has reached a low battery state; **Shutdown all UPSes** - shutdown all UPSes managed by the SLC; **Allow battery failure** - allow the battery to completely fail, which may result in the unsafe shutdown of the devices it provides power to; **Shutdown both SLC UPSes** - shutdown both UPSes that provide power to the SLC, including the UPS with that has reached a low battery state (some SLCs have dual power supplies). For more information, see *RPM Shutdown Procedure*.
Shutdown Order	For UPS devices only. If any of the UPSes managed by the SLC reaches a low battery state AND is configured for **Shutdown all UPSes** for its Low Battery setting, this indicates the order in which this UPS will be shutdown. All UPSes with a shutdown order of "1" will be shutdown first, followed by all UPSes with a shutdown order of "2", etc. Shutdown orders are in the range of 1 to 49, with 50 being reserved for UPSes that provide power to the SLC - they will always be shutdown last (see **Provides SLC Power** below).
Provides SLC Power	For UPS devices only. Indicates if this UPS provides power to the SLC.

4. Click **Apply** to Save.

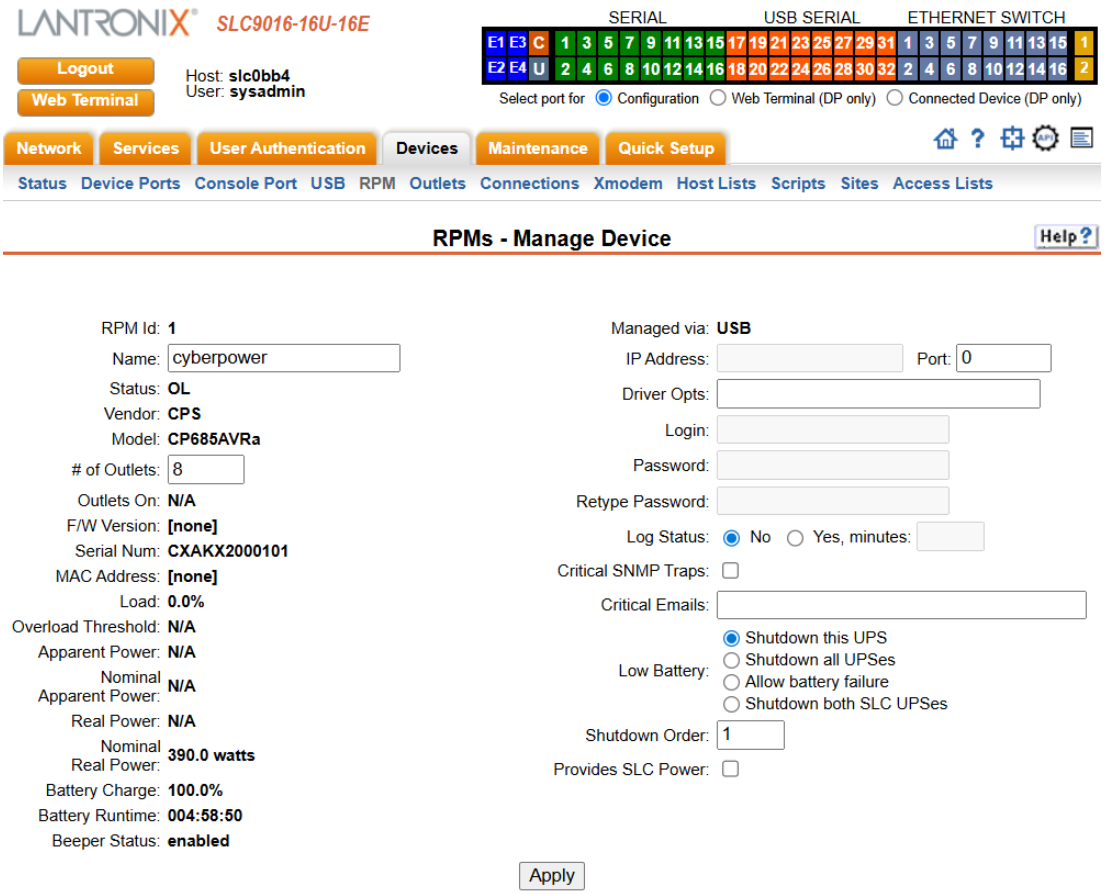
RPMs - Manage Device

The **Manage Device** page allows the administrator to modify the settings for a managed RPM.

To modify a managed RPM:

1. Click the **Devices** tab and select the **RPMs** option. *Figure 13-2 Devices > RPMs* shows the page which displays.
2. Select an RPM and click the **Manage Device** link. *Figure 13-9 RPMs - Managed Device* shows the page which displays.

Figure 13-9 RPMs - Managed Device



3. Enter the following:

RPM Id (view only)	The unique number associated with the RPM.
Name	Specify the unique name of the RPM (up to 20 characters).
Status (view only)	The current status of the RPM. Any error status will be shown here.
Vendor (view only)	The manufacturer of the RPM.
Model (view only)	The model of the RPM. The model is read from the device, if it is provided; not all RPMs provide a model string. If the device normally provides the device model and becomes unreachable, or does not provide a model string, the Model is derived from the supported model list strings.
# of Outlets	Specify the number of outlets on the RPM (maximum of 120 outlets).
Outlets On (view only)	The number of outlets that are currently turned on, if this information is provided by the RPM.
F/W Version (view only)	The firmware version of the RPM, if this information is provided by the RPM.
Serial Num (view only)	The serial number of the RPM, if this information is provided by the RPM.
MAC Address (view only)	The MAC address of the RPM, if this information is provided by the RPM.

Current (view only)	The total current value for the RPM in Amperes, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own current value, both current values will be displayed, separated by a slash.
Input Voltage (view only)	The input voltage for the RPM in Volts, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own input voltage value, both voltage values will be displayed, separated by a slash.
Apparent Power (view only)	The apparent power value for the RPM in Volt-Amperes, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own apparent power value, both power values will be displayed, separated by a slash.
Nominal Apparent Power (view only)	The nominal apparent power value for the RPM in Volt-Amperes, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own nominal apparent power value, both power values will be displayed, separated by a slash.
Real Power (view only)	The real power value for the RPM in Watts, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own real power value, both power values will be displayed, separated by a slash.
Battery Charge (view only)	For UPS devices only. Displays the current charge level for the battery, as a percentage.
Battery Runtime (view only)	For UPS devices only. Displays the amount of time remaining in the UPS battery life.
Beeper Status (view only)	For UPS devices only. Displays the current state of the UPS beeper.
Managed via (view only)	Displays the method used to control the RPM device (SNMP, Network, Serial Port, USB port).
IP Address	For SNMP and Network (Telnet) managed RPMs, specify the IP address of the RPM.
Port	For network (Telnet) managed RPMs, this is assumed to be port 23 (if left blank), or it can be filled in with an alternate TCP port. For USB managed RPMs, this is one of the front USB ports ("0") or the device port that the RPM is connected to on the SLC. For serially controlled RPMs, this is the device port that the RPM is connect to on the SLC.
Driver Opts	For the driver associated with the RPM device, these are extra options which may be required to make the driver work. The most frequent use of the driver options is for USB devices (the vendor and product ID may be required so that the SLC can find the correct device on the USB bus), or in the event that the default driver options do not work with the RPM. There may also be other driver options that are filled in by the SLC from an internal table - these will be automatically set and can be viewed after the RPM has been added, and can always be overridden by driver options set by the user. For a complete list of RPM models, drivers and driver options, refer to *Network UPS Tools Hardware Compatibility List*. The format of the driver options setting is one or more comma-separated parameters-value pairs, e.g. "<parameter name>=<value>".
Login	For Network and serially managed RPMs, this is the administrator login.
Password/Retype Password	For Network and serially managed RPMs, this is the administrator password.
Read Community	For SNMP managed RPMs, this is the SNMP read (get) community.
Write Community/ Retype Write Comm	For SNMP managed RPMs, this is the SNMP write (set) community.

Log Status	Indicates if the status of the RPM is periodically logged. Select Yes, minutes to log the status periodically and enter a value between 1 and 60 minutes. The logs can be viewed by viewing the RPMs web page and clicking on "Logs".
Critical SNMP Traps	If enabled, under critical conditions (UPS goes onto battery power, UPS battery is low, UPS forced shutdown in progress, UPS on line power, UPS battery needs to be replaced, RPM is unavailable, communications with RPM lost, communications with RPM established), a slcEventRPMAction trap will be sent to the NMS configured in SNMP settings. This requires that SNMP traps be enabled.
Critical Emails	If an email address is specified, under critical conditions (see Critical SNMP Traps above), an email notification will be sent to the email address. The Server and Sender configured in the *SSH* settings will be used to send the email.
Low Battery	For UPS devices only. Indicates the behavior to take when the UPS reaches a low battery state. Options are to Shutdown this UPS - shutdown only the UPS that has reached a low battery state; Shutdown all UPSes - shutdown all UPSes managed by the SLC; Allow battery failure - allow the battery to completely fail, which may result in the unsafe shutdown of the devices it provides power to; Shutdown both SLC UPSes - shutdown both UPSes that provide power to the SLC, including the UPS with that has reached a low battery state (some SLCs have dual power supplies). For more information, see *RPM Shutdown Procedure*
Shutdown Order	For UPS devices only. If any of the UPSes managed by the SLC reaches a low battery state AND is configured for Shutdown all UPSes for its Low Battery setting, this indicates the order in which this UPS will be shutdown. All UPSes with a shutdown order of "1" will be shutdown first, followed by all UPSes with a shutdown order of "2", etc. Shutdown orders are in the range of 1 to 49, with 50 being reserved for UPSes that provide power to the SLC - they will always be shutdown last (see **Provides SLC Power** in the next field below).
Provides SLC Power	For UPS devices only. Indicates if this UPS provides power to the SLC.

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

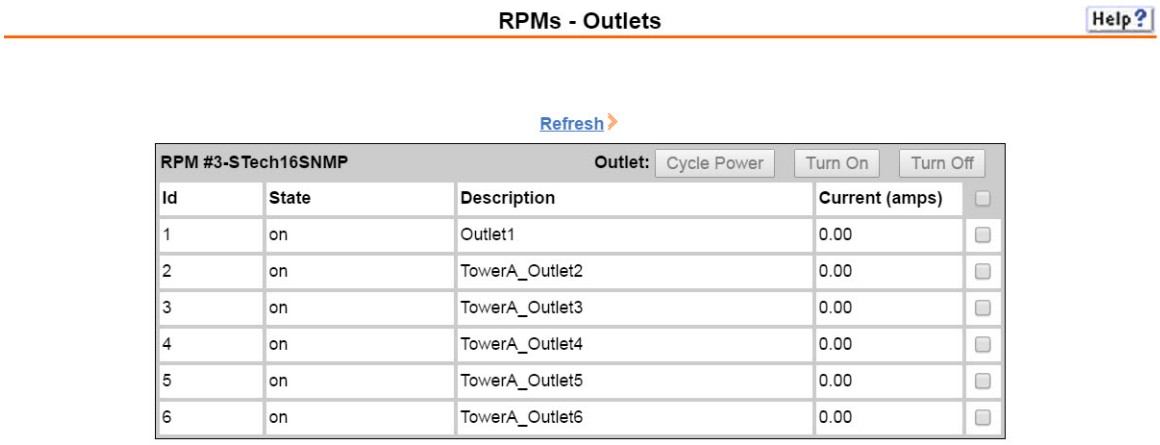
RPMs - Outlets

The **Outlets** page allows the administrator to view the current status of each individual outlet on an RPM, and change the state of the outlets. Not all RPMs support individual outlet status and control.

To control and view status for RPM outlets:

1. Click the **Devices** tab and select the **RPMs** option. *Figure 13-2 Devices > RPMs* shows the page which displays.
2. Select an RPM and click the **Outlets** link. *Figure 13-10 RPMs - Outlets* shows the page which displays. This page will, at a minimum, list the outlet numbers and their state - **On** or **Off**. If the RPM provides additional information for the outlets, the custom name and the current reading in Amperes will also be displayed for each outlet.

Figure 13-10 RPMs - Outlets



3. To change the state of one or more outlets, select the outlets, and click the **Cycle Power**, **Turn On** or **Turn Off** buttons. The command will be sent to the RPM and the page will refresh. It may take one or two minutes before the new outlet state(s) are reflected on the Outlets page.

RPM Shutdown Procedure

This section applies to UPS-type RPMs only, and does not apply to PDU-type RPMS. This section describes the shutdown process when a UPS managed by the SLC reaches a low battery state.

Caution: ***The shutdown procedure initiates a controlled shutdown and cuts power to connected outlets. Verify all connected devices are prepared to lose power before proceeding.***

When one UPS reaches a low battery state, the SLC can be configured to allow the UPS to continue to run until its battery fails completely, to shutdown just the UPS with the low battery, or to shutdown one or more UPSes. UPS-type RPMs can report the following states:

- **OL** - On line power
- **OB** - On battery power
- **LB** - Low battery
- **HB** - High battery
- **RB** - The battery needs to be replaced
- **CHRG** - The battery is charging
- **DISCHRG** - The battery is discharging (inverter is providing load power)
- **BYPASS** - UPS bypass circuit is active - no battery protection available
- **CAL** - UPS is currently performing runtime calibration (on battery)
- **OFF** - UPS is offline and is not supplying power to the load
- **OVER** - UPS is overloaded
- **TRIM** - UPS is trimming incoming voltage
- **BOOST** - UPS is boosting incoming voltage

- **FSD** - UPS is in forced shutdown due to a critical condition

Once a UPS is on line power (status is **OL**) and goes off of line power and onto battery power (status is **OB**), it may reach a low battery state (status is **OB**, **LB** or **LB**). Switching from line power to battery power, and reaching a low battery state are critical states that can result in syslog, email and SNMP trap notifications. The exact point at which a UPS reaches a low battery state is device dependent and is related to the **battery.charge**, **battery.charge.low**, **battery.runtime** and battery.runtime.low settings which can be viewed in the "Raw Data" report.

Once a UPS reaches a low battery state, the **Shutdown Order**, **Low Battery Action** and **Provides SLC Power** settings determine which UPSes to shutdown, and in what order. The UPS with the low battery will be placed into **FSD** (Forced Shutdown) mode. The following actions will be performed based on the **Low Battery Action** setting for the UPS with the failed battery:

- **Allow Battery Failure** - The UPS battery will be allowed to run until it fails completely. If the UPS provides power to the SLC and the battery fails, the SLC will not be cleanly shutdown. In this scenario, the **Shutdown Order** setting will be ignored. The **Shutdown Order** setting may be used if another UPS reaches the low battery state (see **Shutdown all UPSes** below).
- **Shutdown This UPS** - If the UPS provides power to the SLC, the SLC will begin shutdown procedures, shutting down the UPS last. If the UPS does not provide power to the SLC, the UPS will be shutdown, but will continued to be monitored in case it comes back online.
- **Shutdown all UPSes** - The SLC will begin shutting down all UPSes with a non-zero **Shutdown Order**, shutting down UPSes with a shutdown order of "1" first, UPSes with a shutdown order of "2" second, etc. Any UPS which provides power to the SLC is always forced to have its **Shutdown Order** set to 50, which the highest (and last) Shutdown Order. If the UPS with the failed battery provides power to the SLC (and thus has a Shutdown Order set to 50), the SLC will also begin shutdown procedures, shutting down the failed UPS last. If none of the UPSes provide power to the SLC, after they are all shutdown their drivers will remaining running in case the UPS comes back online. In this case, any queries to an RPM while it is still offline may report "RPM driver data is stale". If the **Low Battery Action** for a UPS is set to **Allow Battery Failure**, but the UPS has a non-zero **Shutdown Order**, the UPS will still be shutdown if another UPS reaches the low battery state and has its **Low Battery Action** set to **Shutdown all UPSes**.
- **Shutdown Both SLC UPSes** - This setting should only be used on dual-power SLC units which have each power supply connected to separate (different) UPS devices, and both UPS devices are being managed by the SLC. If a UPS is configured for **Shutdown Both SLC UPSes** but does not have **Provides SLC Power** enabled, this is an ambiguous configuration, and no shutdown action will occur.

  For this configuration, when one of the UPSes providing power to the SLC reaches a low battery state, the event will be noted in the system log, and the SLC will continue to run with no further actions until the second UPS providing power to the SLC reaches a low battery state. At this point the SLC will begin shutdown procedures, shutting down both failed UPSes last.

Optimizing and Troubleshooting RPM Behavior

This section gives tips on how to optimize the management of specific PDUs and UPSes, and how to troubleshoot any problems with the SLC connecting to and managing an RPM.

- **Sentry3 - Network and Serially Managed PDUs** - Some Sentry3 PDUs have a CLI timeout, with a default setting of 5 minutes. This timeout may cause frequent query errors when requesting information from the Sentry3 PDU. It is recommended that the timeout be set as high as possible to reduce the frequency of the query errors.

- **Serially Managed RPMs with Administrator Logins** - Some serially managed devices will have an administrator login for the console port. It is recommended that any active sessions be logged out before adding the device as an RPM, otherwise the RPM may experience query errors.

If the SLC is unable to communicate with an RPM, or an RPM is displaying the error "driver is not running", the following steps can be used to troubleshoot the driver issues:

- **Correct Driver** - The CLI command `set rpm driver <RPM Id or Name> action show` can be used to display the current running driver for the RPM. Some serially and network managed RPMs do not have drivers; if this is the case for the RPM, the CLI command will indicate this. Otherwise it will display the driver that is running for the RPM, and it should match the driver listed for the device at *Network UPS Tools Hardware Compatibility List*. If the wrong driver is shown, the RPM will need to be deleted and re-added, with the correct vendor and model selected. If no driver is shown, the driver may not be able to start for a variety of reasons; see remaining steps.
- **SNMP Settings** - For SNMP managed devices, verify the **IP Address**, **Read Community** and **Write Community** settings are correct.
- **Reverse Pinout Setting** - For serially managed devices, verify the **Reverse Pinout** setting (located in the *Device Port Settings* page) is set correctly.
- **VendorId and ProductId Driver Options** - For USB managed devices, verify the `vendorid` and `productid` shown in the RPM driver options are correct. These can be set automatically by the SLC from an internal table, set by the user by selecting a specific USB device when adding a USB-managed RPM, or changed by the user at any time. The CLI command `show usb devices` displays all connected USB devices with their port, Product ID and Vendor ID.
- **Extra Driver Options** - The driver documentation at *Network UPS Tools Hardware Compatibility List* may indicate that extra driver options are required for the RPM. Select the driver name link under the Driver column to see any special requirements for the UPS or PDU.
- **Driver Debug Mode** - The driver can be run in debug mode at the CLI and the output examined to determine why the driver is not starting or is unable to communicate with the RPM. The CLI command `set rpm driver <RPM Id or Name> action debug [level <1|2|3>]` will stop any currently running driver and restart the driver in debug mode with output sent to a local file. Running `set rpm driver <RPM Id or Name> action show` should show a driver running with one or more **-D** flags. The debug output can be examined or emailed with the `set rpm driver <RPM Id or Name> action viewoutput [email <Email Address>] [display <head|tail>] [numlines <Number or Lines>]` command. To return the driver to its normal non-debug state, run `set rpm driver <RPM Id or Name> action restart`. Note that drivers running in debug mode will generate copious output, and for disk space reasons should not be left running in debug mode for long periods of time (e.g. more than an hour).

RPM Commands

Go to *RPM Commands* to view CLI commands which correspond to the web page entries described above.

14: Connections

Chapter 10: Device Ports described how to configure and interact with an SLC advanced console server 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.

An SLC unit 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 reestablished until the specified data passes through the connection.

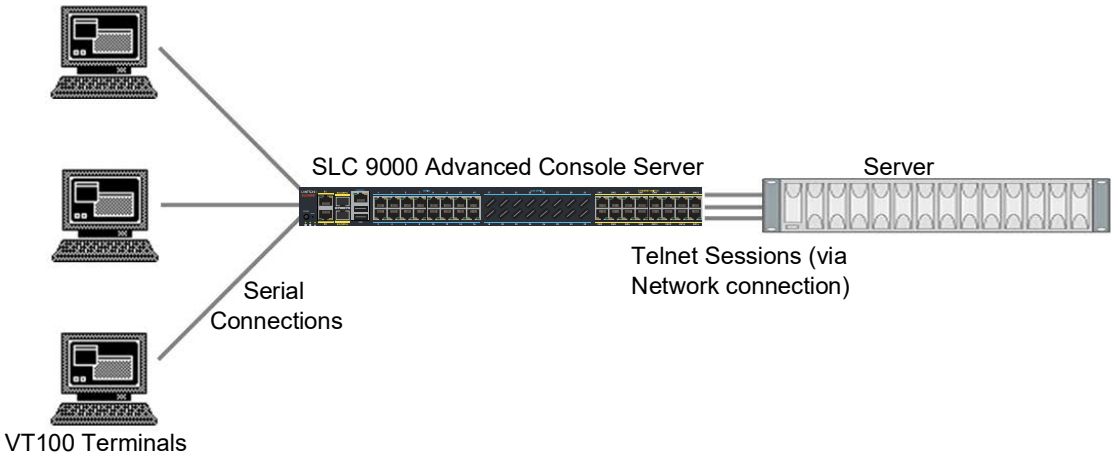
Typical Setup Scenarios for the SLC Unit

Following are typical configurations in which SLC connections can be used, with references to settings on the *Devices > Connections* and *Device Ports > Settings (1 of 2)* web pages.

Terminal Server

In this setup, the SLC 9000 advanced console server acts as a multiplexer of serial data to 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.

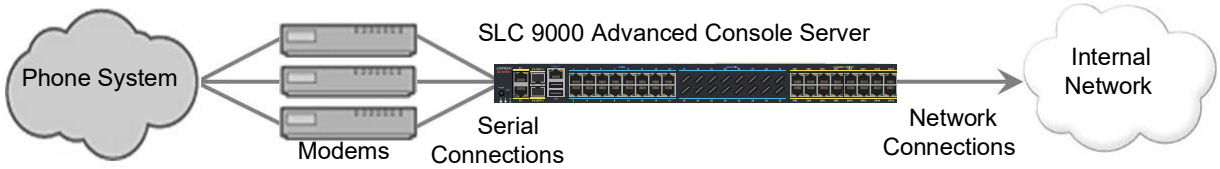
Figure 14-1 Terminal Server



Remote Access Server

In this setup, the SLC 9000 advanced console server is connected to one or more modems by its device ports. Configure the device ports on the *Device Ports > Settings (1 of 2)* 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 9000 advanced console server. 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.

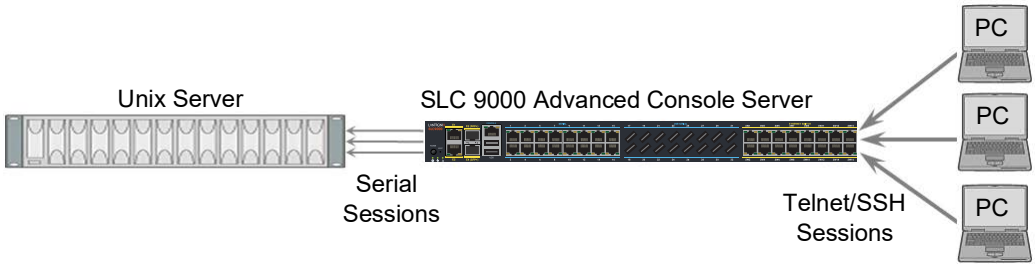
Figure 14-2 Remote Access Server



Reverse Terminal Server

In this scenario, the SLC 9000 advanced console server 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 unit. To configure the SLC console manager, select the **Enable Telnet In** or **Enable SSH In** option on the *Device Ports > Settings (1 of 2)* page.

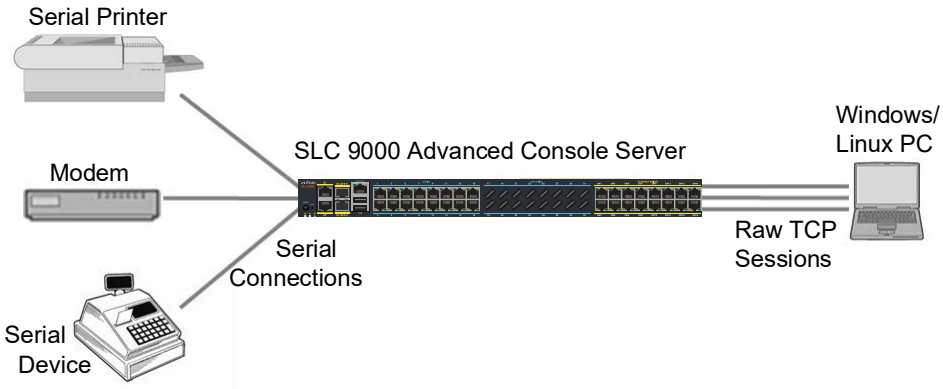
Figure 14-3 Reverse Terminal Server



Multiport Device Server

A PC can use the device ports on the SLC unit as virtual serial ports, enabling the ports to act as if they are local ports to the PC. To use the SLC 9000 advanced console server in this setup, the PC requires special software, for example, Com Port Redirector (available on www.lantronix.com) or similar software).

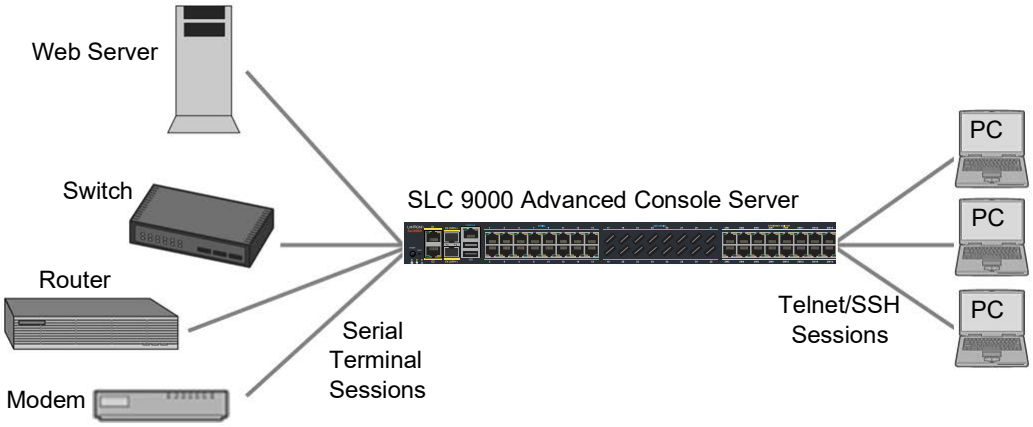
Figure 14-4 Multiport Device Server



Console Server

For this situation, the SLC unit 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 9000 advanced console server 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 unit 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 (1 of 2)* 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 (1 of 2)* page. A user could then dial into the SLC 9000 advanced console server using another modem and terminal emulation program at a remote location.

Figure 14-5 Console Server



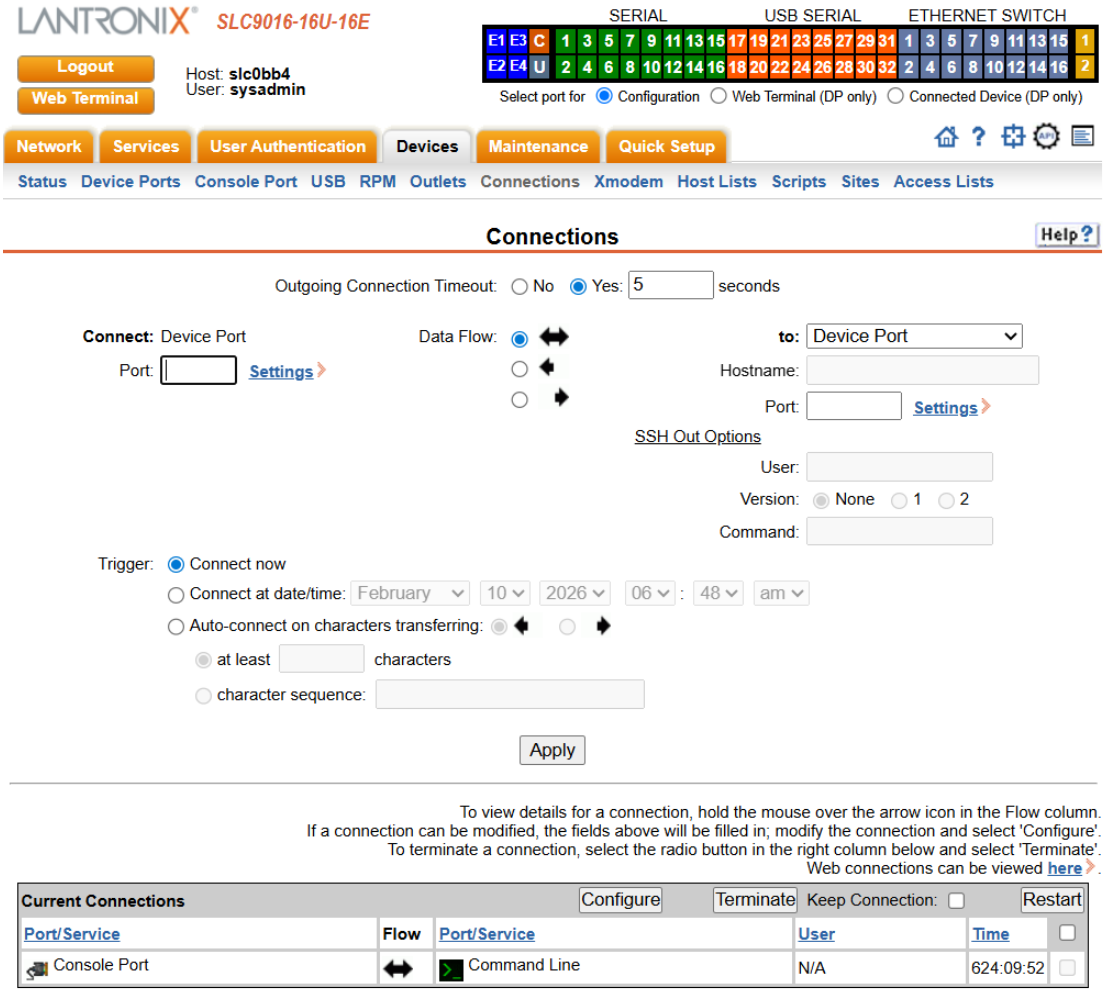
Connection Configuration

Note: *These are advanced connection settings for specific applications. If the SLC 9000 advanced console server is being used as a console or device server it is unlikely that you will need any of the Connection settings described below.*

To create a connection:

1. Click the **Devices** tab and select **Connections**. The following page displays:

Figure 14-6 Devices > Connections



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.

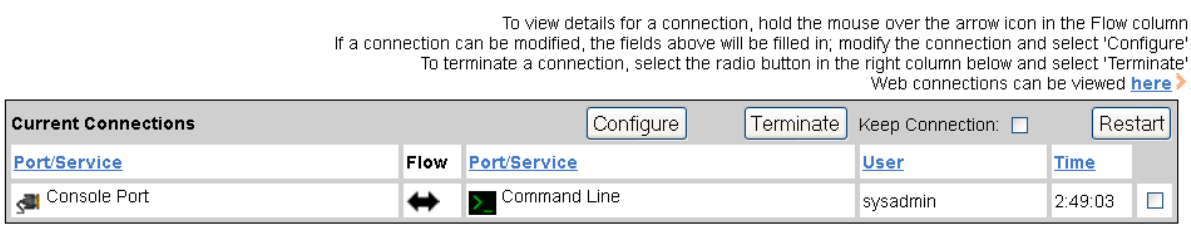
Port	The number of the device port you are connecting. This device port must be connected to an external serial device and must not have command line interface logins enabled, be connected to a modem, or be running a loopback test. ***Note:*** *To see the current settings for this device port, click 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.
to	From the drop-down list, select a destination for the connection: a device port connected to a serial device, a device port connected to a modem, or an outbound network connection (**Telnet out**, **SSH out**, **TCP Port**, or **UDP Port**). ***Note:*** *To see the current settings for a selected device port, click the* ***Settings*** *link.*
Hostname	The host name or IP Address of the destination. This entry is required if the **to** field is set to Telnet out, SSH out, TCP port, or UDP port.
Port	If the **to** field is set to **Device Port** or **Modem on Device Port**, enter the number of the device port. For all other options, this is the TCP/UDP port number, which is optional for Telnet out and SSH out, but required for TCP Port and UDP Port. ***Note:*** *If you select* ***Device Port****, it must not have command line interface logins enabled or be running a loopback test. To view the device port's settings, click the* ***Settings*** *link to the right of the port number.*
SSH Out Options	Select one of the following optional flags to use for the SSH connection. ◆ **User:** Login ID to use for authenticating on the remote host. ◆ **Version:** Version of SSH. Select 1 or 2. ◆ **Command:** Enter a specific command on the remote host (for example, reboot).
Trigger	Select the condition that will trigger a connection. Options include: ◆ **Connect now:** Connects immediately, or if you reboot the SLC 9000 advanced console server, immediately on reboot. ◆ **Connect at date/time:** Connects at a specified date and time. Use the drop-down lists to complete the date and time. Upon rebooting, the SLC unit reestablishes the connection if the date/time has passed. ◆ **Auto-connect on characters transferring:** Select the arrow indicating the direction of the data transfer and either the minimum number of characters or a specific character sequence that will trigger the connection. You can select the direction of the data transfer only if **Data Flow** is bidirectional. Upon rebooting, the SLC 9000 advanced console server does not reestablish the connection until the specified data has passed through one of the endpoints of the connection.

3. 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 14-7 Current Connections



1. To view details about a connection, hold the mouse over the arrow 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 & Configurations* page displays.

Connection Commands

Go to *Connection Commands* to view CLI commands which correspond to the web page entries described above.

15: User Authentication

Authentication Methods

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

By default, Local user authentication is always enabled and is the first method the SLC uses to authenticate users. The User Authentication page provides a submenu of other methods (LDAP, RADIUS, TACACS+) you can select to authenticate users attempting to log in. Use this page to assign the order in which the SLC will use the methods.

Two-factor authentication (2FA) is supported with LDAP and RADIUS authentication. Only one method of generating the secure token (SMS, smartphone app, etc) is supported (e.g., the user cannot choose between different methods to generate a secure token at login). Note: 2FA cannot be used with the Percepxion **Web Connect** feature, as this connection is handled via Percepxion (cloud or on-premise).

Note: *Even if Local user authentication is disabled or last in the authentication order, the local user sysadmin will always be enabled and granted access first (before any other authentication methods); this ensures that there is always a method to authenticate to the console server in the event that all remote authentication methods are unreachable.*

For security purposes, full administrative access to the SLC via the default **sysadmin** local user account can be limited to only the front console port of the SLC device. To configure this: (1) enable the **Sysadmin access limited to Console Port** option on the Local/Remote Users web page; (2) enable a remote authentication method (such as TACACS+ or LDAP) and configure the remote authentication method to be first in the order of methods used; (3) create a remote user account with full administrative rights; and (4) uncheck the **Attempt next method on authentication rejection** checkbox on the Authentication Methods web page. This will prevent any local users from logging in, restrict the default **sysadmin** local user to the front console port, and allow a user with administrative rights to login, as long as remote authentication is working. To completely disable **sysadmin** user access with this configuration, the console port can be disabled.

If you enable multiple authentication methods, and a user has a login ID for more than one of these methods, the login defaults to the highest priority authentication method based on the settings made on this web page.

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

Example:

There is an LDAP user "joe" and a TACACS+ user "joe" and the order of authentication methods is:

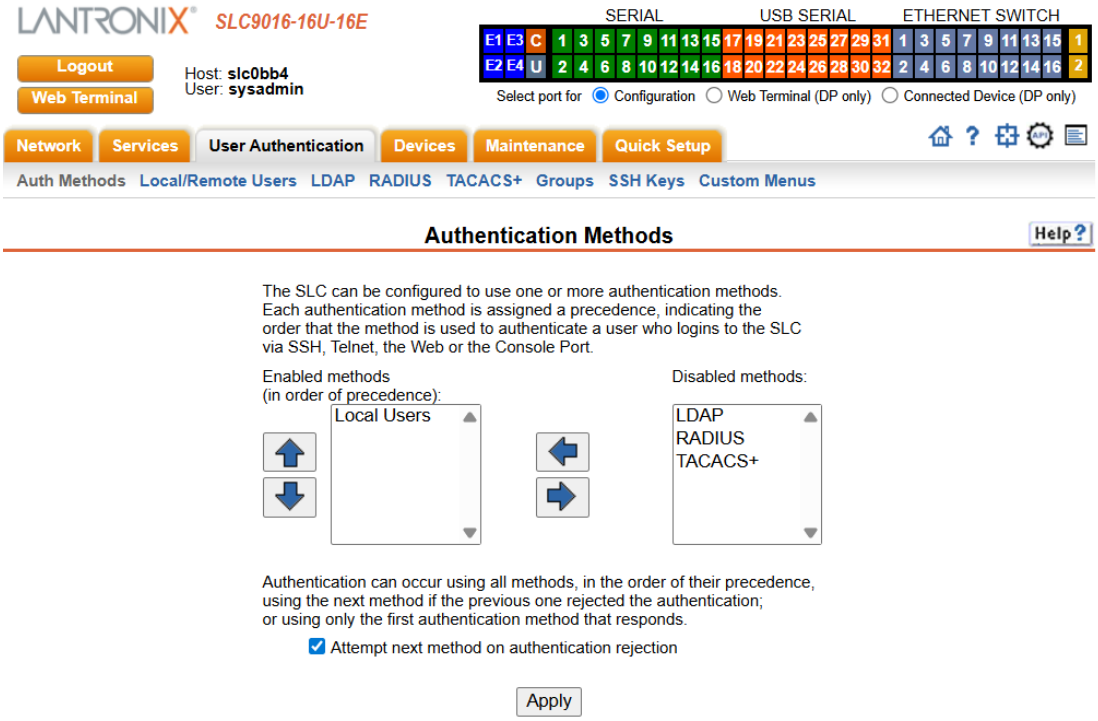
1. Local Users
2. LDAP
3. TACACS+

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 unit may (or may not) try to authenticate him against his TACACS+ "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:

Figure 15-1 User Authentication > Authentication Methods



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:

LDAP (Lightweight Directory Access Protocol)	A set of protocols for accessing information directories, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection-oriented transfer services.
RADIUS (Remote Authentication Dial-In User Service)	An authentication and accounting system used by many Internet Service Providers (ISPs). A client/server protocol, it enables remote access servers to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It increases security, allowing a company to set up a policy that can be applied at a single administered network point.
TACACS+ (Terminal Access Controller Access Control System)	TACACS+ allows a remote access server to communicate with an authentication server to determine whether the user has access to the network. TACACS+ is a completely new protocol and is not compatible with TACACS or XTACACS. The SLC 9000 advanced console server supports TACACS+ only.
Local Users	Local accounts on the SLC unit used to authenticate users who log in using SSH, Telnet, the web, or the console port.

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 unit 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 unit to use only the first authentication method that responds (in case a server is down or unavailable), clear the check box.

     Note: *When limiting accessibility of the sysadmin login to the physical SLC 9000 unit, make sure to uncheck* ***Attempt next method on authentication rejection****.*
6. Click **Apply**.

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

Authentication Commands

Go to *Authentication Commands* to view CLI commands which correspond to the web page entries described above.

User Rights

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

- `connect direct/listen`
- `set locallog/password/history/cli`
- `show datetime/deviceport/locallog/portstatus/portcounters/`
- `history/cli/user`

The table below shows the mapping of groups and user rights.

Table 15-2 User Types and Rights

User Right	Administrator	Power Users	Default Users
Full Administrative Rights	**X**		
Networking	**X**	**X**	
Services	**X**		
Date/Time	**X**	**X**	
Local Users	**X**		
Remote Authentication	**X**		
SSH Keys	**X**		
User Menus	**X**		
Device Port Operations	**X**		
Device Port Configuration	**X**		
RPMs	**X**		

USB	**X**		
Reboot/Shutdown	**X**	**X**	
Firmware/Configuration	**X**		
Diagnostics and Reports	**X**	**X**	
Secure Lantronix Network	**X**		
Web Access	**X**	**X**	
Internal Modem	**X**		
Ethernet Switch	**X**		

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

By default, the system assigns new users to the Default Users group, but you can change their group membership at any time. If you change a user's rights while the user is logged into the web or CLI, the results do not take effect until the next time the user logs in. The default sysadmin password will be the last 8 characters of the Device ID if it is set, or the last 8 characters of the serial number if the Device ID is not set

To assign user rights:

1. Enter the following:

Login (view only)	User ID of selected user.
Group	Select the group to which the local or remote user will belong: ◆ **Default Users:** This group has only the most basic rights. ◆ **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.

2. 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., Spider, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the SLC unit.
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.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.

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**.
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
RPMs	Right to manage and control remote power managers.

3. Click **Apply**.

Local and Remote Users

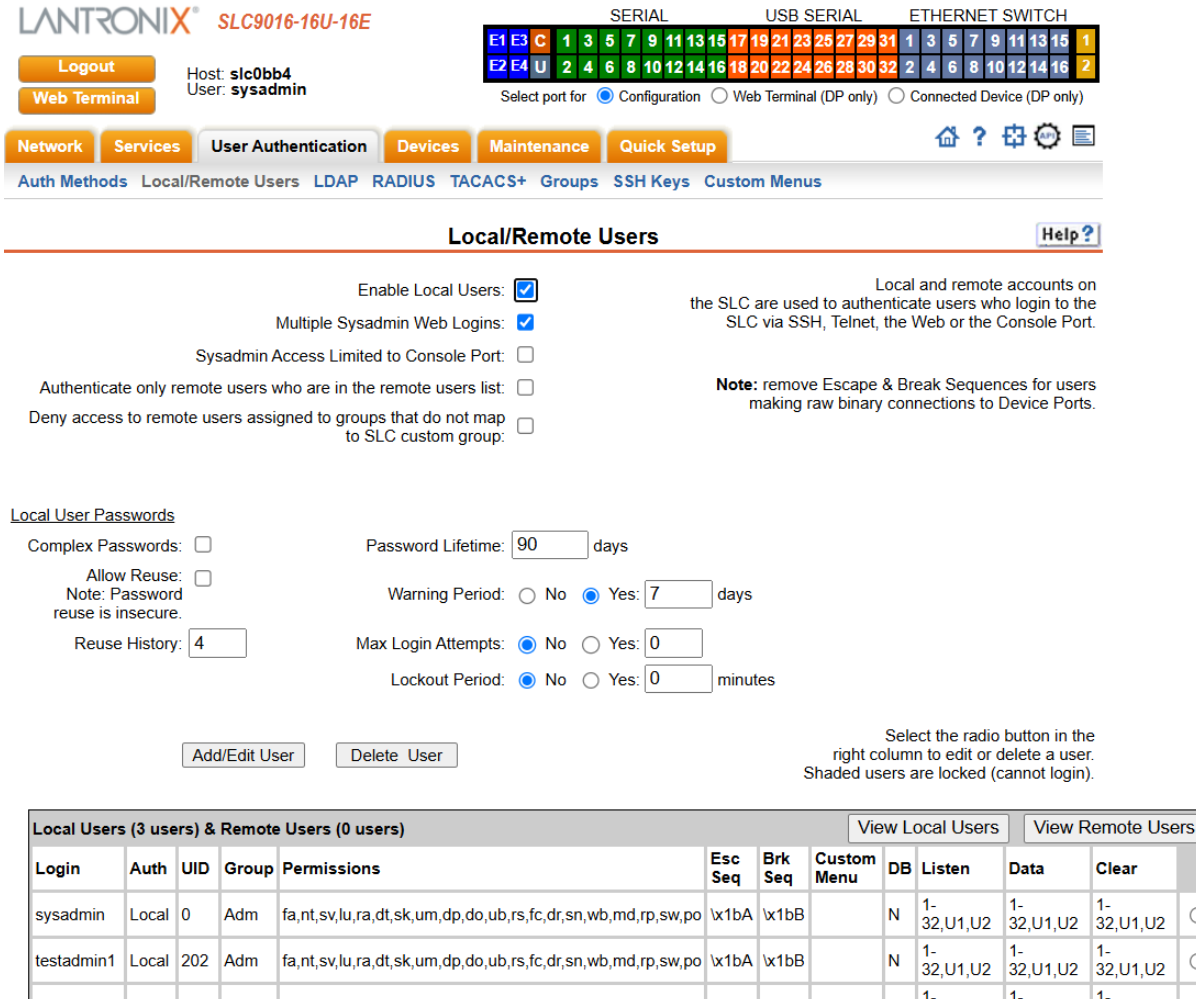
The system administrator can configure the SLC unit to use local accounts and remote accounts to authenticate users.

Note: *The default sysadmin password will be the last 8 characters of the Device ID if it is set, or the last 8 characters of the serial number if the Device ID is not set.*

To set local and/or remote users attributes:

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

Figure 15-3 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.

2. Enter the following:

Enable Local Users	Select to enable all local users except sysadmin. The sysadmin user is always available regardless of how you set the check box. Enabled by default.
Multiple Sysadmin Web Logins	Select to allow the sysadmin to have multiple simultaneous logins to the web interface. Disabled by default.
Sysadmin Access Limited to Console Port	Select to limit sysadmin logins to the physical SLC 9000 console port only. Disabled by default.
Authenticate only remote users who are in the remote users list	Select the check box to authenticate only remote users listed in the Remote Users list in the lower part of the page. All other users who can be authenticated by remote authentication servers are denied access. Disabled by default.
Deny access to remote users assigned to groups that do not map to SLC custom group	Select the check box to authenticate remote users whose LDAP group or TACACS+ priv_lvl map to a SLC custom group, allow SLC access if matched. Disabled by default.

3. Click the **Apply** button.

To set password requirements for local users:

Local User Passwords:

Complex Passwords	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. **Complexity rules:** Passwords must be at least eight characters long. They must contain one upper case letter (A-Z), one lower case letter (a-z), one digit (0-9), and one punctuation character (()`~!@#$%%^&*-+=\{}[]:;'"<>,.?/_).
Allow Reuse	Select to enable users to continue to reuse old passwords. If you disable the check box, they cannot use any of the **Reuse History** number of passwords. Enabled by default.
Reuse History	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.
Password Lifetime (days)	The number of days until the password expires. The default setting is **90**.
Warning Period (days)	The number of days ahead that the system warns that the user's password will expire. The default setting is **7**.
Max Login Attempts	The number of times (up to 8) the user can attempt to log in unsuccessfully before the system locks the user out. The default setting is **0** (disabled).
Lockout Period (minutes)	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).

4. Click the **Apply** button.

To add, edit, or delete a user:

You can delete a user listed in the table on this page or open the page for adding or editing a user.

You have the following options:

- To add a user, click the **Add/Edit User** button. The Local/Remote User Settings page displays.
- To edit a user, select the user in the table and click the **Add/Edit User** button. The Local/Remote User Settings page displays.
- To delete a user, select the user in the table, click the **Delete** button and then the **Apply** button.

Sysadmin Account Default Login Values

On factory default SLC units, the local user sysadmin account has the following default login values.

- username: **sysadmin**

- password: the last 8 characters of the Device ID (Percepxion ID). If the Device ID is not set, the password is the last 8 characters of the serial number.

Note: *It is recommended that you change the default passwords on initial setup. The sysadmin password should be recorded and stored in a secure place accessible by at least two authorized system administrators. Recovering an SLC if both of these passwords are unknown is cumbersome and time consuming.*

To restore the SLC unit to factory defaults, see *Firmware & Configurations*.

Limiting Sysadmin User Access

For security purposes, full administrative access to the SLC via the default sysadmin local user account can be limited to only the front console port of the SLC device.

To configure this:

1. Enable the Sysadmin access limited to Console Port option on the Local/Remote Users web page.'
2. Enable a remote authentication method (such as TACACS+ or LDAP) and configure the remote authentication method to be first in the order of methods used.
3. Create a remote user account with full administrative rights.
4. Uncheck the **Attempt next method on authentication rejection** checkbox on the Authentication Methods web page.

These steps will prevent any local users from logging in, restrict the default sysadmin local user to the front console port, and allow a user with administrative rights to login, as long as remote authentication is working.

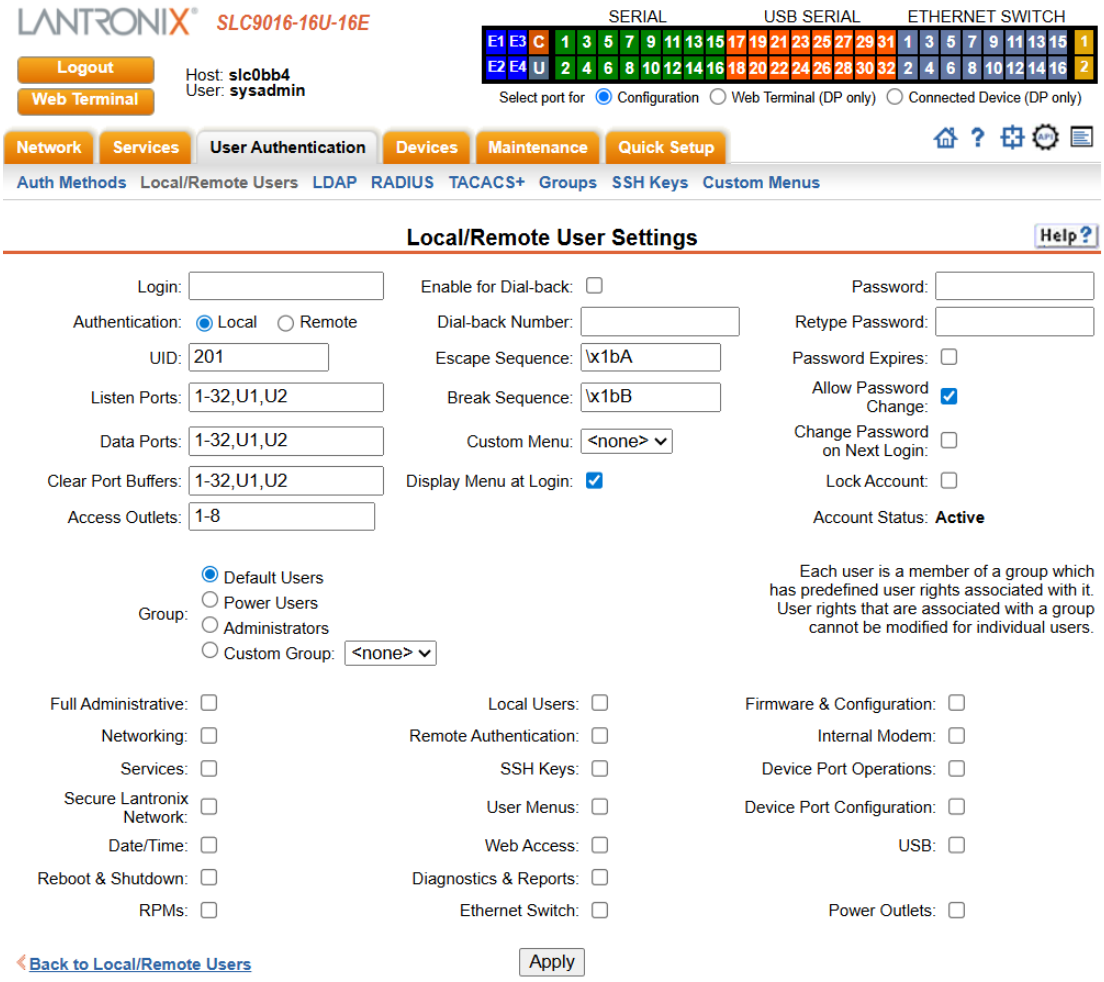
Local/Remote User Settings

On this page, you can add, edit, or delete a local or remote user.

To add a user:

1. On the *User Authentication > Local/Remote Users*, click the **Add/Edit User** button. The *Local/Remote User Settings* page displays.

Figure 15-4 User Authentication > Local/Remote User > Add/Edit User



2. Enter the following information for the user:

Login	User ID of selected user.
Authentication	Select the type of authenticated user: ◆ **Local:** User listed in the SLC database. ◆ **Remote:** User not listed in the SLC database.
UID	A unique numeric identifier the system administrator assigns to each user. Valid UIDs are 101-4294967295. ***Note:*** *The UID must be unique. If it is not, SLC unit automatically increments it. Starting at 101, the SLC 9000 advanced console server finds the next unused UID.*
Listen Ports	The device ports that the user may access to view data using the connect listen command. Enter the port numbers or the range of port numbers (for example, 1, 5, 8, 10-15). U1 and U2 denote the USB upper and lower ports on the front of the SLC unit.
Data Ports	The device ports with which the user may interact using the connect direct command. Enter the port numbers or the range of port numbers.
Clear Port Buffers	The device port buffers the users may clear using the `set locallog clear` command. Enter the port numbers or the range of port numbers.

Enable for Dial-back	Select to grant a local user dial-back access. Users with dial-back access can dial into the SLC unit and enter their login and password. Once the SLC 9000 advanced console server authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number (specified on the Device Port - Settings page), or on a number that is associated with the user's login (specified here).
Escape Sequence	A single character or a two-character sequence that causes the SLC 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`. See *Key Sequences on page 238* for notes on key sequence precedence and behavior.
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**. See *Key Sequences on page 238* for notes on key sequence precedence and behavior.
Custom Menu	If custom menus have been created, you can assign a default custom menu to the user. The custom menu will display at login. ***Note:*** *In the Local Users table, if the menu assigned to a local user no longer exists, it is marked with an asterisk (*).*
Display Menu at Login	If custom menus have been created, select to enable the menu to display when the user logs into the CLI.
Password / Retype Password	When a user logs into the SLC 9000 advanced console server, the SLC unit prompts for a password (up to 64 characters). The sysadmin establishes that password here.
Password Expires	If not selected, allows the user to keep a password indefinitely. If selected the user keeps the password for a set period. (See the section, *Local and Remote Users (on page 274)* for information on specifying the length of time before the password expires.)
Allow Password Change	Select to allow the user to change password.
Change Password on Next Login	Indicate whether the user must change the password at the next login.
Lock Account	Select to lock the account indefinitely.
Account Status	Displays the current account status: ◆ Active ◆ Locked ◆ Locked (invalid logins)

3. In the **User Rights** section, Assign rights to users. You can assign or remove additional rights

of the individual user.

Group	Select the group to which the local or remote user will belong: ◆ **Default Users:** This group has only the most basic rights. You can specify additional rights for the individual user. ◆ **Power Users:** This group has the same rights as Default Users plus **Web Access, Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. ◆ **Administrators:** This group has all possible rights. ◆ **Custom Group:** Select a custom group from the drop-down menu.

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., Spider, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the SLC unit.
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.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
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**.
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
RPMs	Right to manage and control remote power managers.
Ethernet Switch	Right to view and enter settings for the managed Ethernet Switch.

5. Click the **Apply** button.
6. Click the **Back to Local/Remote Users** link to return to the Local/Remote User Settings page.
7. 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.*

Shortcuts

To add a user based on an existing user:

1. Display the existing user on the *User Authentication > Local/Remote Users* 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 *User Authentication > 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 *User Authentication > 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 *User Authentication > 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

Go to *Local Users Commands* to view CLI commands which correspond to the web page entries described above.

Remote User Rights Commands

Go to *Remote User Commands* to view CLI commands which correspond to the web page entries described above.

LDAP

The system administrator can configure the SLC 9000 advanced console server to use LDAP to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

LDAP allows SLC unit 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.

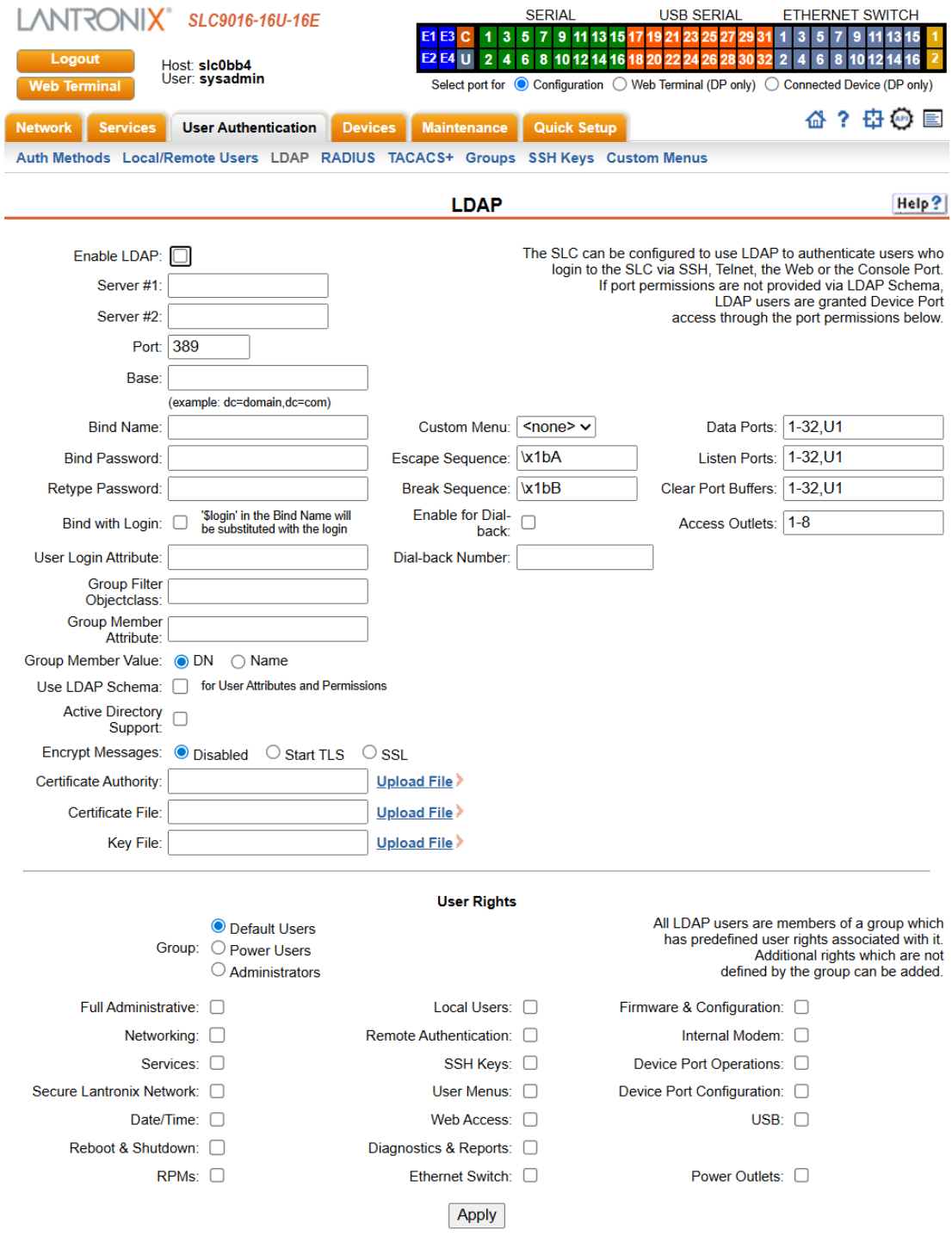
Users who are authenticated through LDAP are granted device port access through the port permissions on this page.

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.

Figure 15-5 User Authentication > LDAP



2. Enter the following:

Enable LDAP	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.

Server #1 (or Server #2)	The IPv4 or IPv6 address or host name of the primary and secondary LDAP servers. The secondary LDAP server will be used for authentication in the event that the primary LDAP server cannot be reached.
Port	Number of the TCP port on the LDAP server to which the SLC talks. The default is **389**.
Base	The name of the LDAP search base (e.g., dc=company, dc=com). May have up to 80 characters.
Bind Name	The name for a non-anonymous bind to an LDAP server. This item has the same format as LDAP Base. One example is cn=administrator,cn=Users,dc=domain,dc=com
Bind Password / Retype Password	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.
Bind with Login	Select to bind with the login and password that a user is authenticating with. This requires that the Bind Name contain the `$login` token, which will be replaced with the current login. For example, if the Bind Name is `uid=$login,ou=People,dc=lantronix,dc=com`, and user `roberts` logs into the SLC 9000 advanced console server, LDAP will bind with `uid=roberts,ou=People,dc=lantronix,dc=com` and the password entered by roberts.
User Login Attribute	The attribute used by the LDAP server for user logins. If nothing is specified for the user filter, the SLC unit will use "uid". For AD LDAP servers, the attribute for user logins is typically "sAMAccountName".
Group Filter Objectclass	The objectclass used by the LDAP server for groups. If nothing is specified for the group filter, the SLC 9000 advanced console server will use "posixGroup". For AD LDAP servers, the objectclass for groups is typically "Group".
Group Member Attribute	The attribute used by the LDAP server for group membership. This attribute may be use to search for a name (ie, "msmith") or a Distinguished Name (ie, "uid=msmith,ou=People,dc=lantronix,dc=com"). 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 "memberUID" for name and "uniqueMember" for DN. For AD LDAP servers, the Group Membership Value is typically DN, with the Group Membership Attribute of "member".
Group Member Value	The attribute used by the LDAP server for group membership. This attribute may be use to search for a name (ie, "msmith") or a Distinguished Name (ie, "uid=msmith,ou=People,dc=lantronix,dc=com"). Select either Name or DN as appropriate for the LDAP server. If nothing is specified for the group membership attribute, the SLC 9000 advanced console server will use "memberUID" for name and "uniqueMember" for DN. For AD LDAP servers, the Group Membership Value is typically DN, with the Group Membership Attribute of "member".
Use LDAP Schema	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”. For more information, see *User Attributes & Permissions from LDAP Schema or RADIUS VSA*. This option is disabled by default.
Active Directory Support	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- compliant. Disabled by default.

Encrypt Messages	Select **Start TLS** or **SSL** to encrypt messages between the SLC 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.

Certificate Authority
Certificate File
Key File
	A certificate can be uploaded to the SLC unit for peer authentication. The uploaded certificate may contain a Certificate Authority file, a Certificate file (with an optional Key file), or both. A Key file alone is not a valid certificate. The Certificate Authority and Certificate File are in PEM format, for instance:
	`-----BEGIN CERTIFICATE-----`
	`(certificate in base64 encoding)`
	`-----END CERTIFICATE-----`
	The Key File is in PEM format, eg:
	`-----BEGIN RSA PRIVATE KEY-----`
	`(private key in base64 encoding)`
	`-----END RSA PRIVATE KEY-----`

Custom Menu	If custom menus have been created, you can assign a default custom menu to LDAP users. See *Custom Menus*.
Escape Sequence	A single character or a two-character sequence that causes the SLC 9000 advanced console server 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. See *Key Sequences on page 238* for notes on key sequence precedence and behavior.
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 9000 advanced console server 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. **U1** and **U2** denote the USB upper and lower ports on the front of the SLC unit.
Listen Ports	The ports users are able to monitor using the `connect listen` command.
Clear Port Buffers	The ports whose port buffer users may clear using the `set 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 **Web Access**, **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. ◆ **Administrators:** This group has all possible rights.

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure Lantronix units (e.g., Spider, or SLC devices) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the SLC unit.
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.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
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**.
Internal Modem	Right to configure internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port configurations.
USB	Right to enter modem settings for USB.
RPM	Right to manage and control remote power managers.
Ethernet Switch	Right to view and enter settings for the managed Ethernet Switch.

5. Click the **Apply** button.

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

LDAP Commands

Go to *LDAP Commands* to view CLI commands which correspond to the web page entries described above.

RADIUS

The system administrator can configure the SLC 9000 advanced console server to use RADIUS to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

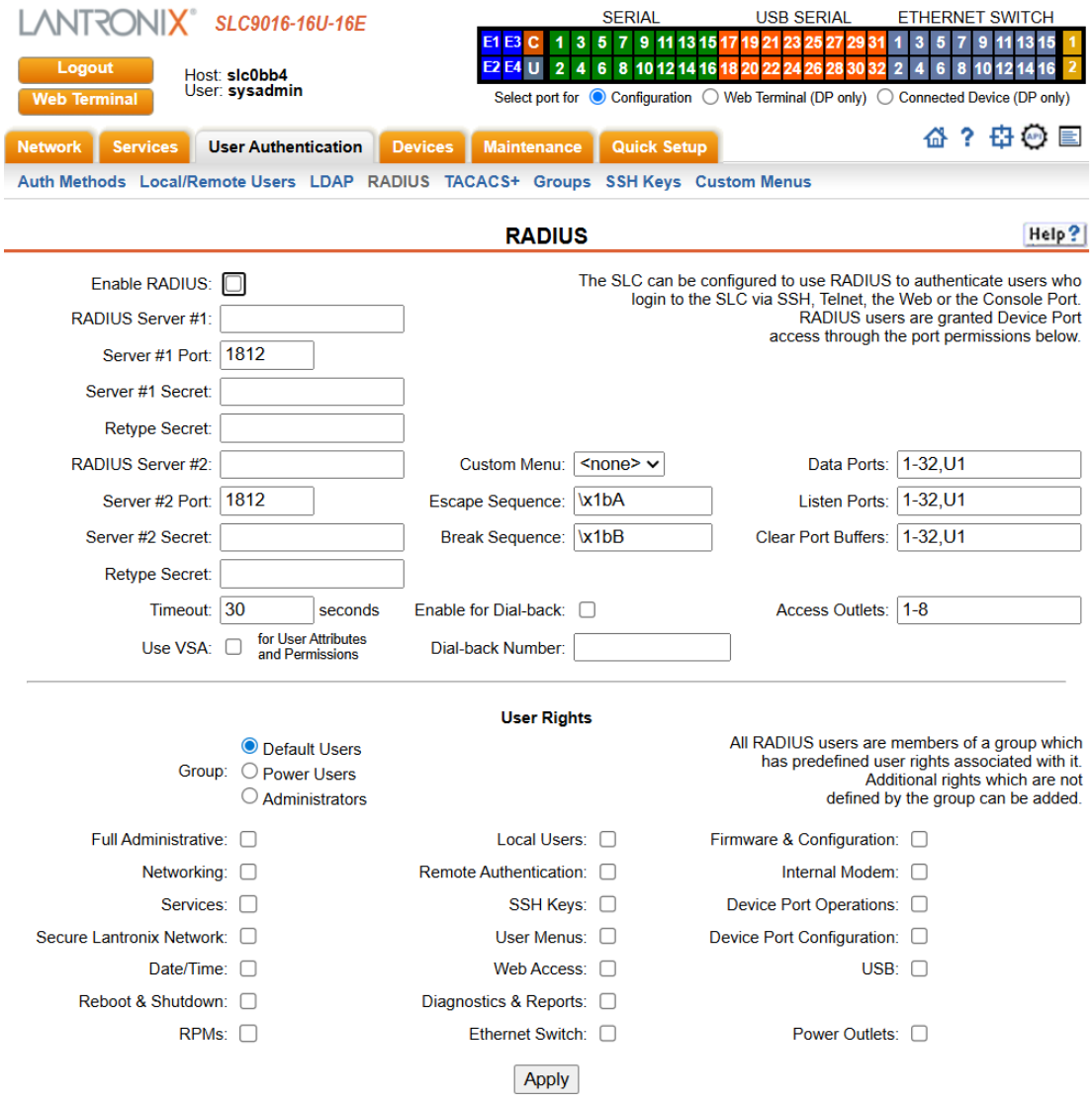
Users who are authenticated through RADIUS are granted device port access through the port permissions on this page.

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.

Figure 15-6 User Authentication > RADIUS



2. Enter the following:

Enable RADIUS	Displays selected if you enabled this method on the User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox. ***Note:*** *You can enable RADIUS here or on the first User Authentication page. If you enable RADIUS here, it automatically displays at the end of the order of precedence on the User Authentication page.*
RADIUS Server #1	IPv4 or IPv6 address or hostname of the primary RADIUS server. This RADIUS server may be a proxy for SecurID. SecurID is a two-factor authentication method based on the user's SecurID token and pin number. The SecurID token displays a string of digits called a token code that changes once a minute (some tokens are set to change codes every 30 seconds).
Server #1 Port	Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the SLC unit uses the default RADIUS port (**1812**).
Server #1 Secret	Text that serves as a shared secret between a RADIUS client and the server (SLC unit). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.
RADIUS Server #2	IPv4 or IPv6 address or host name of the secondary RADIUS server. This server can be used as a SecurID proxy.
Server #2 Port	Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the SLC 9000 advanced console server uses the default RADIUS port (**1812**).
Server #2 Secret	Text that serves as a shared secret between a RADIUS client and the server (SLC unit). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.
Timeout	The number of seconds (1-30) after which the connection attempt times out. The default is **30** seconds.
Use VSA	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 & Permissions from LDAP Schema or RADIUS VSA on page 290*.
Custom Menu	If custom menus have been created, you can assign a default custom menu to RADIUS users. See *Custom Menus*.
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`. See *Key Sequences on page 238* for notes on key sequence precedence and behavior.
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 9000 advanced console server 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. **U1** and **U2** denote the USB upper and lower ports on the front of the SLC unit.
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.

Group	Select the group to which the RADIUS 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 **Web Access**, **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. ◆ **Administrators:** This group has all possible rights.

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage Secure Lantronix units (e.g., Spider, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the SLC unit.
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.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
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**.
Internal Modem	Right to update internal modem settings.

Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
RPM	Right to manage and control remote power managers.
Ethernet Switch	Right to view and enter settings for the managed Ethernet Switch.

5. Click the **Apply** button.

RADIUS Commands

Go to *RADIUS Commands* to view CLI commands which correspond to the web page entries described above.

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,U1,U2".
- **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 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.

```
# dictionary.lantronix
#
# Lantronix SLC Console Manager
# Provides SLC-specific user attributes
#
VENDOR Lantronix 244

BEGIN-VENDOR Lantronix

ATTRIBUTE Lantronix-User-Attributes 1 string

END-VENDOR Lantronix
```

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"
```

TACACS+

Similar to RADIUS, the main function of TACACS+ is to perform authentication for remote access. The SLC 9000 advanced console server 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 TACACS+ are granted device port access through the port permissions on this page.

All TACACS+ users are members of a group with associated predefined user rights. You may add additional user rights that are not defined by the group.

TACACS+ Groups

This section describes how a priv_lvl assigned to a TACACS+ user can be mapped to a SLC custom *Groups*, which will set the permissions and port rights for a TACACS+ user when they login to the SLC.

TACACS+ users are typically configured to have a privilege level 0-15, with each level representing a privilege level that is a superset of the next lower value. The privilege level can be assigned to individual users, or to groups that the user is a member of. When the SLC authenticates a TACACS+ user, it will first send an authentication request to the TACACS+ server, and wait for an authentication reply. If the user is successfully authenticated, the SLC will next send an authorization request to the TACACS+ server with the **Service** and optional **Protocol**. The SLC will wait for an authorization response that will indicate if the user was successfully

authorized for the requested service and protocol, and also contains a set of attribute-value pairs which define the attributes associated with the TACACS+ user.

The **priv_lvl** or **priv-lvl** is the only attribute sent from the TACACS+ server that the SLC will recognize and utilize. The privilege level number will be used to map to a SLC custom user group by finding a group with a name that ends in the same number as the priv_lvl. For example, a SLC group called "admin15" will map to any TACACS+ users with priv_lvl equal to 15; a SLC group called "manager8" will map to any TACACS+ users with priv_lvl equal to 8, and a SLC group called "readonly0" will map to any TACACS+ users with priv_lvl equal to 0. If two SLC groups ending with the same number exist, the SLC will select the first matching group it finds while searching the group list; for consistency it is recommended that only one SLC group exist for each priv_lvl.

When a TACACS+ user authenticates to the SLC, the Authentication Log will record any priv_lvl attribute-value pair returned by the TACACS+ server:

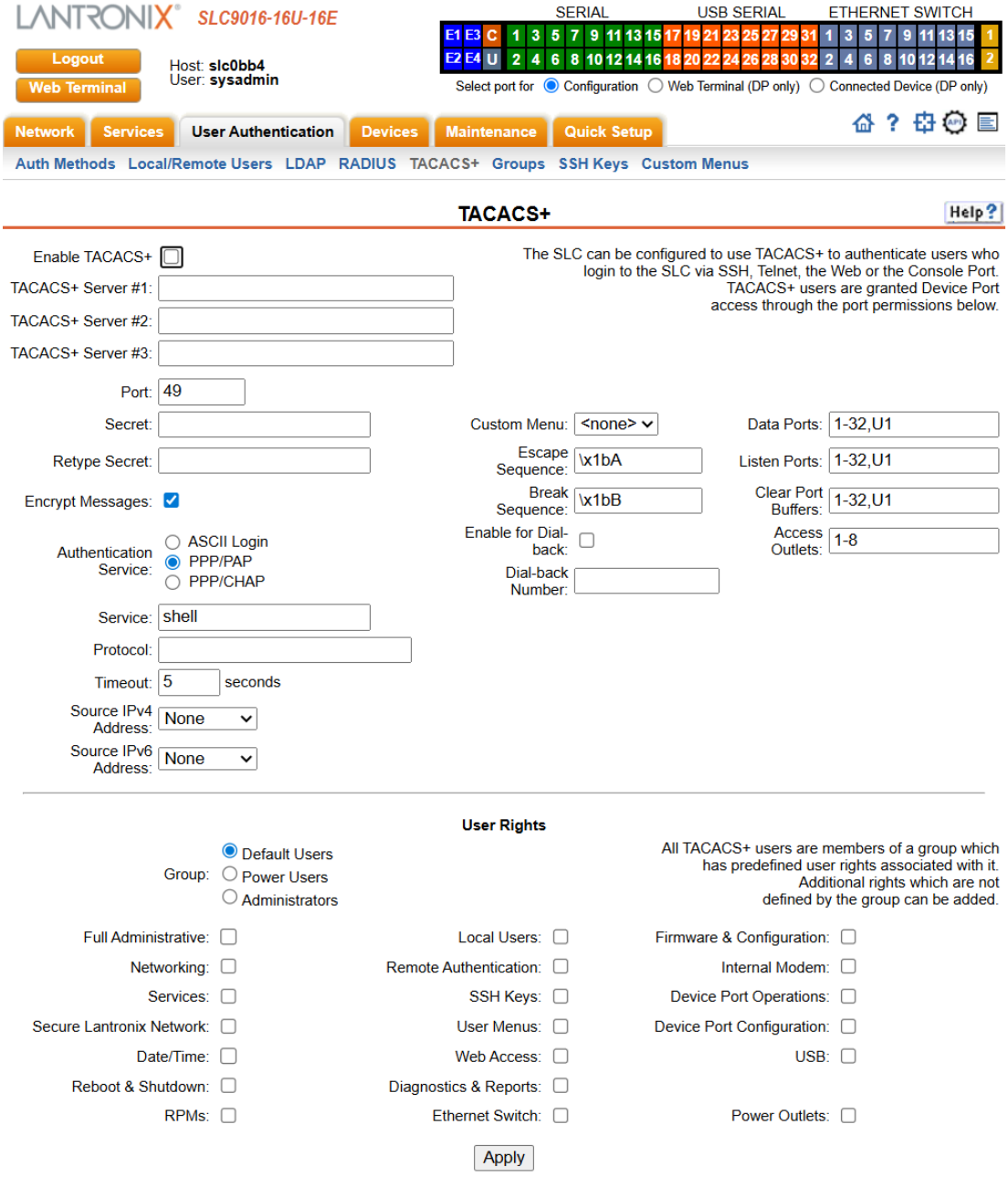
```
May 21 15:44:38 2026 slc431d SLC-SLB/x15login[2839]:
pam_sm_authenticate: server returned attribute `PRIV_LVL=14'
```

Any priv_lvl obtained for a TACACS+ user can also be viewed at the CLI with the `show user` command.

To configure the SLC unit to use TACACS+ to authenticate users:

1. Click the **TACACS+** tab and select **TACACS+**. The following page displays.

Figure 15-7 User Authentication > TACACS+



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	IPv4 or IPv6 address or host name of up to three TACACS+ servers.

Port	Number of the TCP port on the TACACS+ server to which the console manager talks. The default is 49.
Secret/Retype Secret	Shared secret for message encryption between the SLC 9000 advanced console server 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.
Authentication Service	The type of service used to pass the authentication tokens (e.g., login and password) between the SLC and the TACACS+ server. Options are: **ASCII Login** (login and password are transmitted in clear, unencrypted text), **PPP/PAP** (login and password are transmitted in clear, unencrypted text via a PAP protocol packet), and **PPP/CHAP** (the TACACS+ server sends a challenge that consists of a session ID and an arbitrary challenge string, and the user name and password are encrypted before they are sent back to the server). PPP/PAP is the default.
Service	The service to use when sending a TACACS+ authorization message to the server to obtain an authenticated user's priv_lvl. The priv_lvl is used to assign a SLC custom group to the authenticated user for permissions and port rights (see TACACS+ Groups). Suggested values are "slip", "ppp", "arap", "shell", "tty-daemon", "connection", "system" and "firewall". The default is "shell".
Protocol	The optional protocol associated with the Service, which is included in the TACACS+ authorization message sent to the server to obtain an authenticated user's priv_lvl. The priv_lvl is used to assign a SLC custom group to the authenticated user for permissions and port rights (see TACACS+ Groups). Suggested values are "lcp", "ip", "ipx", "atalk", "vines", "lat", "xremote", "tn3270", "telnet", "rlogin", "pad", "vpdn", "ftp", "http", "deccp", "osicp" and "unknown".
Timeout	The timeout in seconds when attempting to connect to a TACACS+ server. Timeout range is 1 to 10 seconds. 5 seconds is the default.
Source IPv4 Address	The Source IPv4 Address can be used to configure which interface (and source IPv4 address) is used for sending TACACS+ packets. By default, the source IP address for sending TACACS+ traffic is not specified, and the source address of a TACACS+ packet is selected according to the routing table. S**ource IPv4 Address** can be used to select the IPv4 address of Eth1, Eth2, VEth1 or VEth2 as the source IPv4 address for packets sent to all TACACS+ servers defined with an IPv4 address or a name which resolves to an IPv4 address. Before selecting an interface, make sure the interface is enabled and has a valid IPv4 address.
Source IPv6 Address	The Source IPv6 Address can be used to configure which interface (and source IPv6 address) is used for sending TACACS+ packets. By default, the source IP address for sending TACACS+ traffic is not specified, and the source address of a TACACS+ packet is selected according to the routing table. **Source IPv6 Address** can be used to select the IPv6 address of Eth1, Eth2, VEth1 or VEth2 as the source IPv6 address for packets sent to all TACACS+ servers defined with an IPv6 address or a name which resolves to an IPv6 address. Before selecting an interface, make sure the interface is enabled and has a valid IPv6 address.
Custom Menu	If custom menus have been created, you can assign a default custom menu to TACACS+ users. See *Custom Menus*.

Escape Sequence	A single character or a two-character sequence that causes the SLC 9000 advanced console server 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**. See *Key Sequences* for notes on key sequence precedence and behavior.
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 9000 advanced console server 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 *Dial-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. **U1** and **U2** denote the USB upper and lower ports on the front of the SLC unit.
Listen Ports	The ports users are able to monitor using the `connect listen` command.
Clear Port Buffers	The ports whose port buffer users may clear using the `set locallog clear` command.

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

Group	Select the group to which the TACACS+ 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 **Web Access**, **Networking**, **Date/Time**, **Reboot & Shutdown**, and **Diagnostics & Reports**. ◆ **Administrators:** This group has all possible rights.

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure Lantronix units (e.g., Spider, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the SLC unit.
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.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
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**.
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
RPM	Right to manage and control remote power managers.
Ethernet Switch	Right to view and enter settings for the managed Ethernet Switch.

5. Click the **Apply** button.

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

TACACS+ Commands

Go to *TACACS+ Commands* to view CLI commands which correspond to the web page entries described above.

Groups

The SLC 9000 advanced console server 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 9000 advanced console server 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.

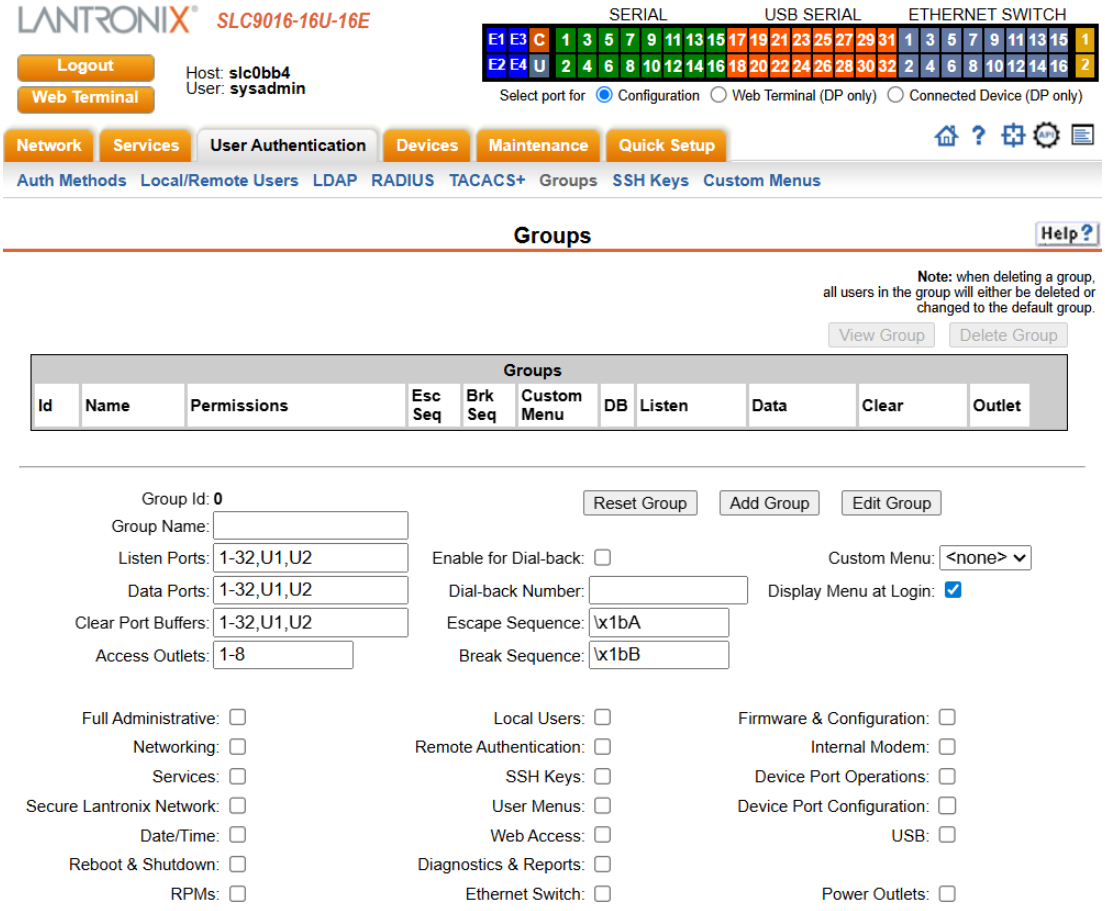
A custom group cannot be given the name of one of the pre-defined groups: "Admin", "Power" or "Default" (or any version of these names where the case of the letters is different) since these names are used for the SLC pre-defined groups. Any LDAP group that matches one of these pre-defined group names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

To configure Groups in the SLC unit:

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.

Figure 15-8 User Authentication > Groups



2. Enter the following:

Group Name	Enter a name for the group.
Listen Ports	The ports users are able to monitor using the `connect listen` command.
Data Ports	The ports users are able to monitor and interact with using the connect direct command. **U1** and **U2** denote the USB upper and lower ports on the front of the SLC unit.
Clear Port Buffers	The ports whose port buffer users may clear using the `set locallog clear` command.
Enable for Dial-back	Select to grant a user. Users with dial-back access can dial into the SLC unit and enter their login and password. Once the SLC 9000 advanced console server 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 on a fixed number, or on a number that is associated with the user's login (specified here).

Escape Sequence	A single character or a two-character sequence that causes the SLC 9000 advanced console server 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 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**.
Custom Menu	If custom menus have been created you can assign a default custom menu to the group. See *Custom Menus*.
Display Menu at Login	Check the checkbox to display the menu at login.

3. 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., Spider, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the SLC unit.
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.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
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**.
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
RPM	Right to manage and control remote power managers.
Ethernet Switch	Right to view and enter settings for the managed Ethernet Switch.

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.

Group Commands

Go to *Group Commands* to view CLI commands which correspond to the web page entries described above.

SSH Keys

Overview

The SLC 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 supports RSA and ECDSA keys, and can import and export keys in OpenSSH and SECSH formats. Imported and exported keys are saved with the console manager configuration, and the administrator has the option of retaining the SSH keys during a reset to factory defaults.

The SLC can also update the SSH host keys that the SSH server uses with site-specific host keys or reset them to the default values.

Imported Keys

Imported SSH keys can be used for SLC local users, NIS users and LDAP users. The key can be generated on host "MyHost" for user "MyUser," and when the key is imported into the console manager, it must be associated with either "MyUser" (if "MyUser" is an existing console manager local user) or an alternate SLC local user, NIS user or LDAP user. Once imported, the key can be used to access the console manager from any host, not just the host associated with the key. The public key file can be imported via SCP, SFTP, FTP or Copy/Paste; once imported, you can view or delete the public key. Any SSH connection into the console manager from the designated host/user combination uses the SSH key for authentication.

Using RSA or ECDSA keys with the SHA1 signature algorithm is no longer supported; attempting to login to to the SLC with a SHA1 RSA or SHA1 ECDSA key will fail (the user will be prompted for a password).

Exported Keys

The SLC can generate SSH keys for SSH connections out of the SLC 9000 advanced console server for any user. The SLC 9000 advanced console server retains both the private and public key on the SLC unit, and makes the public key available for export via SCP, SFTP, 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 for the designated host/user combination uses the SSH key for authentication.

Create an SSH Key

The SLC can import and export SSH keys to facilitate shared key authentication (or public key authentication) for all incoming and outgoing SSH connections. A public-private key pair is generated on a host that is the SSH client (both keys should be stored secure manner), and the public key is imported into the host that the user wants to SSH to, eg, the SSH server.

An example of how to create a 3072 bit RSA SSH key on a Linux host:

```
% ssh-keygen -t rsa -b 3072
Generating public/private rsa key pair.
Enter file in which to save the key (/home/username/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/username/.ssh/id_rsa.
Your public key has been saved in /home/username/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:cCWA3ydbTYUAqPtJQ3I8UY7Cyhieri5zNbB56Cc27z0 username@emg0000
The key's randomart image is:
+---[RSA 3072]----+
|     ..++.o. o.  |
|   .. oo o  o    |
|.   o+ooo  o     |
|.+o.o.*oo o .    |
|.oo= = .S=       |
|. + = o .        |
| o o + o         |
|+ * ..E          |
|+= *o ..         |
+----[SHA256]-----+
```

It is recommended to use secure bit sizes (-b); for example, at least 2048 bits for RSA keys. The passphrase is optional, and will be used to encrypt the key. Once the key is generated, add the contents of the id_rsa.pub file into the user's .ssh/authorized_keys file on the SSH server.

The SLC can import keys generated by OpenSSH or keys in SECSH format (a format used by other SSH tools); when importing a key in SECSH format it will automatically be converted to OpenSSH format, and require the user to specify the user and host if this is not included with the key file. For example, the public key below from a public-private key pair generated by PuTTY can be imported into the SLC, but will require the user and host associated with the key to be specified:

```
---- BEGIN SSH2 PUBLIC KEY ----

Comment: "rsa-key-20200320"

AAAAB3NzaC1yc2EAAAABJQAAAQEAv37tfnOKNcMPLFOA69gPhVk5A1ieKCPywzwK

uQsyMGOdCeFabfgtFu5WwnYZG9IzvWR12KTCfOz18EYisUyldoONmsHLf+TNwrho

ktI/Vfq+V4oh9u6Oz/6AI40XqmO3LxEDF1sMqA19+uE30sU0kxvbrEYYsAHk9KLH

QZj/w/2f5Ftgl8yL2kxbNEAfqLYjB/FV62SJ5ne+1/1HI2Ave1gsp0P9Lr9TbJq3
```

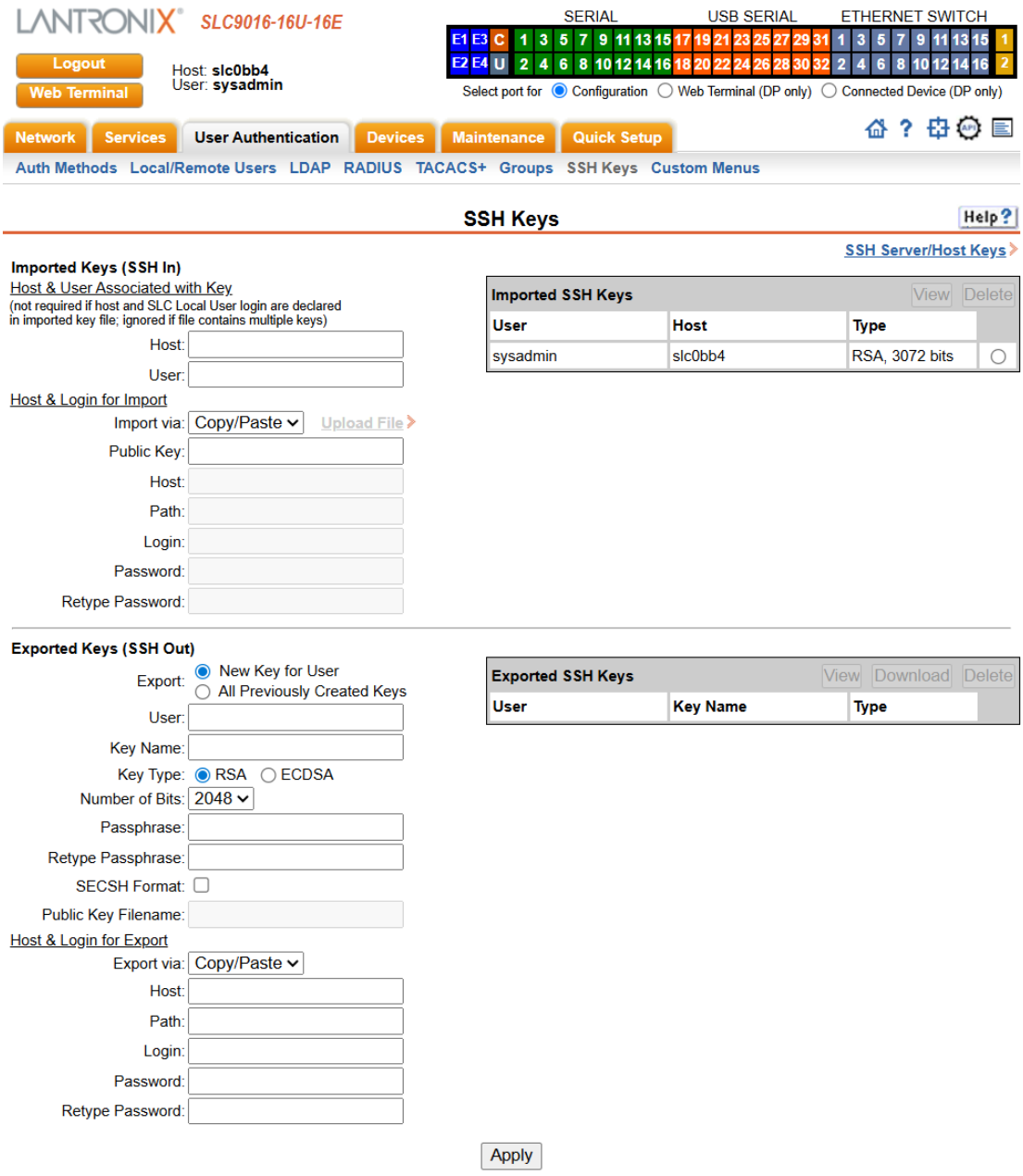
```
r8rnZWy1iSX0f2OGsLehA3ummcSEevwsE2HiPeo2C+oBM8tTPztJEIBv8dtzidH0
gPh4ZRBoUr2nnMCCCsJ1NLFZ+cV0i7GwTCcm/+rix8O6H1b16w==
---- END SSH2 PUBLIC KEY ----
```

SSH/Telnet/Logging provides information on enabling 'Require SSH Public Key for Authentication'. If enabled, the remote user needs a public key in addition to a password to login to the console manager.

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.

Figure 15-9 User Authentication > SSH Keys



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 any 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 AAAAB3NzaC1yc2EAAAABIwAAAEEApUHCX9EWsHt+jmUGXa1YC3us
ABYxIXUhSU1N+NU9HNaUADUFfd8LYz8/gUnUSH4Ksm8GRT7/8/Sn9jCVfGPh
UQ== asallaway@winserver
```

Host	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 from any host, not just the host associated with the key.
User	The User ID of the user being given secure access to the SLC unit.

Host & Login for Import

Import via	Select **SCP**, **SFTP**, **FTP**, **HTTPS**, or **Copy/Paste** as the method for importing the SSH keys. SCP is the default. If SCP, SFTP 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.
Filename Public Key	The name of the file that was uploaded via HTTPS, or to be copied via SCP, SFTP or FTP (may contain multiple keys); or the public key (optionally including "user@host" at the end) if Copy/Paste is used.
Host	IP address of the remote server from which to SCP, SFTP or FTP the public key file.
Path	Optional pathname to the public key file.
Login	User ID to use to SCP, SFTP or FTP the file.
Password / Retype Password	Password to use to SCP, SFTP or FTP the file.

Exported Keys (SSH Out)

Note: *Only RSA and ECDSA keys are supported.*

Export	Enables you to export created public keys. Select one of the following: ◆ **New Key for User:** Enables you to create a new key for a user and export the public key in a file. ◆ **All Previously Created Keys:** Does not create any keys, but exports all previously created public keys in one file.
User	User ID of the person given secure access to the remote server.
Key Name	Name of the key. This will generate the public key filename (e.g., <keyname>.pub).
Key Type	Select either the **RSA** or **ECDSA** encryption standard. RSA is the default.
Number of Bits	Select the number of bits in the key (**1024**, **2048**, **3072**, or **4096**). The default for RSA is **2048**; the default for ECDSA is **384**

Passphrase / Retype Passphrase	Optionally, enter a passphrase associated with the key. The passphrase may have up to 50 characters. The passphrase is an optional password that can be associated with an SSH key. It is unique to each user and to each key. See *Key Sequences* for notes on key sequence precedence and behavior.
SECSH Format	Indicate whether the keys will be exported in **SECSH** format (by default the key is exported in **OpenSSH** format).
Public Key Filename	Filename of the public host key.

Host and Login for Export

Export via	Select the method (**SCP**, **SFTP**, **FTP**, **HTTPS**, or **Copy/Paste**) of exporting the key to the remote server. **Copy/Paste**, the default, requires no other parameters for export.
Host	IP address of the remote server to which the SLC 9000 advanced console server will SCP, SFTP or FTP the public key file.
Path	Optional path of the file on the host to SCP, SFTP or FTP the public key too.
Login	User ID to use to SCP, SFTP or FTP the public key file.
Password / Retype Password	Password to use to SCP, SFTP or FTP the public key file.

To view or delete a key:

1. Select the key from the appropriate table. The **View** and **Delete** buttons become active.
2. To view the key, click the **View** button. A pop-up page displays the key.

```
Imported key for sysadmin@DaveSLM:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxGxPGY9HsG9VqroDo98B89Cf
haqB6jG//0tTMKkb3zrpPu0HHAXaiVXHAvv7lAte31VTpoXdLAXN0uCvuJLf
aL/LvvGmoEWBuBSu505lQHfL70ijxZWOEVTJGFqUQTSq8Ls3/v3lkUJEX5ln
2AlQx0F40I5wNEC0+m3d5QE+FKc= sysadmin@DaveSLM
```

3. To delete the key, click the **Delete** button.

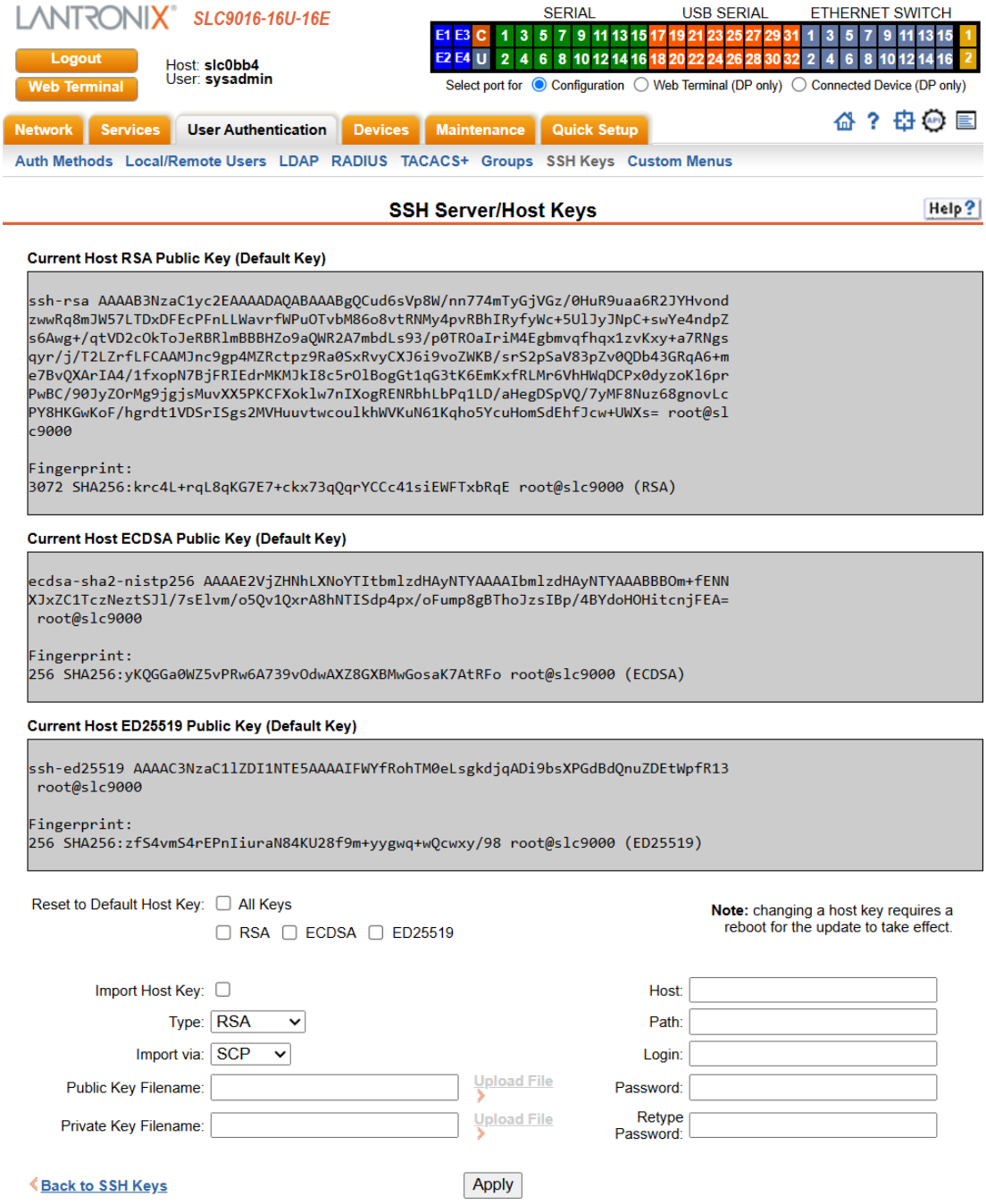
SSH Server/Host Keys

This page allows the user to view information about SSH server host keys, import new host kys, and reset the keys back to the default keys. The CLI provides a command to remove the SSH server host keys; the keys will be regenerated when the console manager is rebooted (rebooting the console manager immediately after removing SSH server host keys is highly recommended).

To view, reset, or import SSH RSA, ECDSA, and ED25519 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.

Figure 15-10 Current Host Keys



2. View or enter the following:

Reset to Default Host Key	Select **All Keys** to reset all default key(s), or select one or more check boxes to reset defaults for **RSA**, **ECDSA,** or **ED25519** keys. By default, the check boxes are clear.
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. The default is **RSA**.

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

Go to *SSH Key Commands* to view CLI commands that correspond to the web page entries described above.

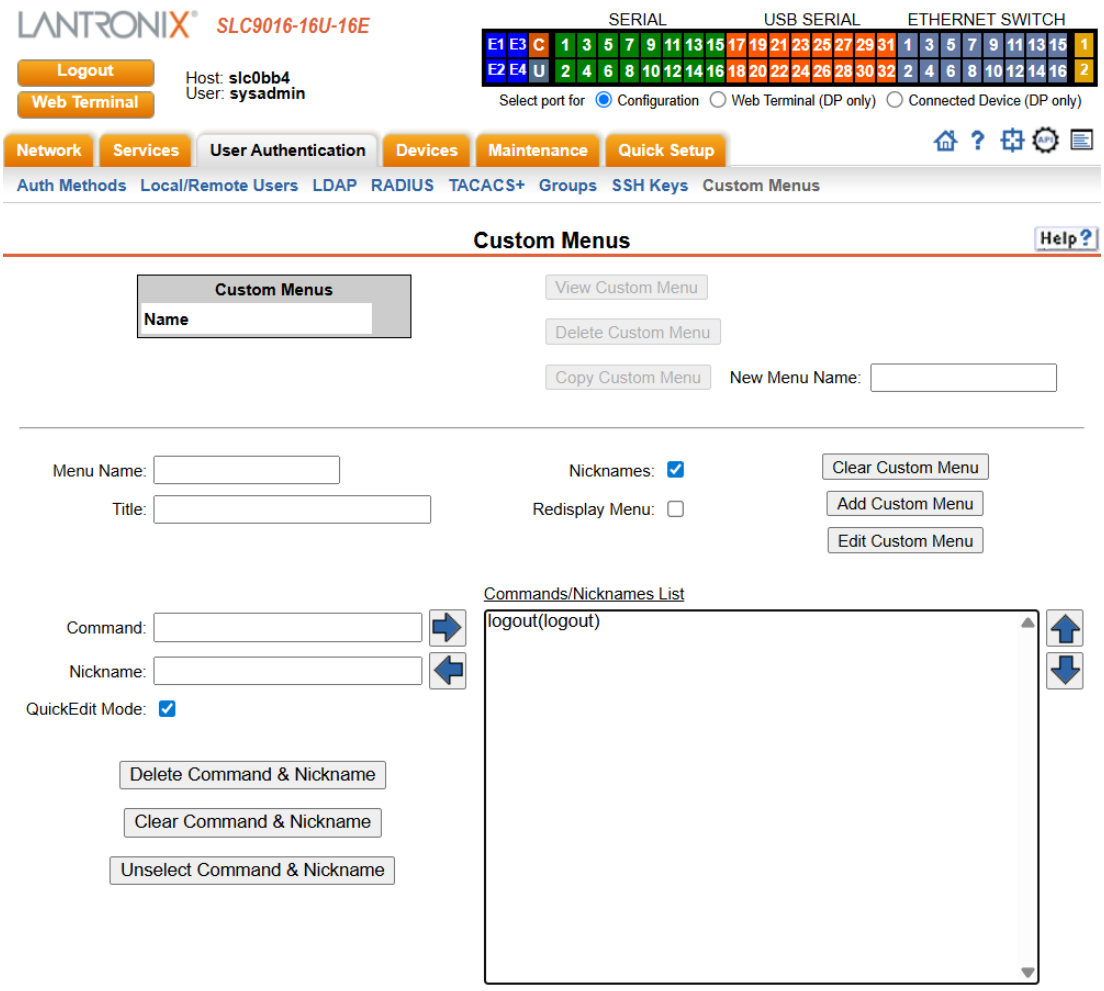
Custom Menus

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:

Figure 15-11 User Authentication > Custom Menus



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.*

Menu Name	Enter a name for the custom menu.
Title	Enter an optional title which will be displayed about the menu at the CLI.
Nicknames	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.
Redisplay Menu	Select to redisplay the custom menu each time before the CLI prompt is displayed.

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** 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.)

Go to *Custom User Menu Commands* to view CLI commands which correspond to the web page entries described above.

16: Maintenance

The system administrator performs maintenance activities and operates the SLC advanced console server using the options for the Maintenance tab and additional commands on the command line interface.

Firmware & Configurations

The Firmware & Configuration 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 and configurations restored via DHCP/TFTP *Provision via Zero Touch Provisioning*.)
- Set up the location or method that will be used to save or restore configurations (Local Disk, FTP, SFTP, NFS, CIFS, USB, HTTPS). Update the version of the firmware running on the SLC unit.
- Save a snapshot of all settings on the SLC device (save a configuration).
- Restore the configuration, either to a previously saved configuration, or to the factory defaults.
- Factory default can also be initiated by using an external storage device or the reset button.
- As part of configuration management, configurations can be:
  - Pushed to the console manager via the HTTPS Push Configuration feature.
  - Pulled from TFTP, FTP, HTTP or HTTPS servers via Zero Touch Provisioning (ZTP) or Bootstrapping.

Firmware Update Policy:

Do not rename the firmware file - it must retain the same filename in order for the firmware upgrade to complete successfully.

The firmware can be updated via either the 'Firmware & Configurations' web page, or with the 'admin ftp' and 'admin firmware' CLI commands. Updating firmware via tftp does not use the FTP login, password, or path settings. The firmware update will be applied to the alternate boot bank.

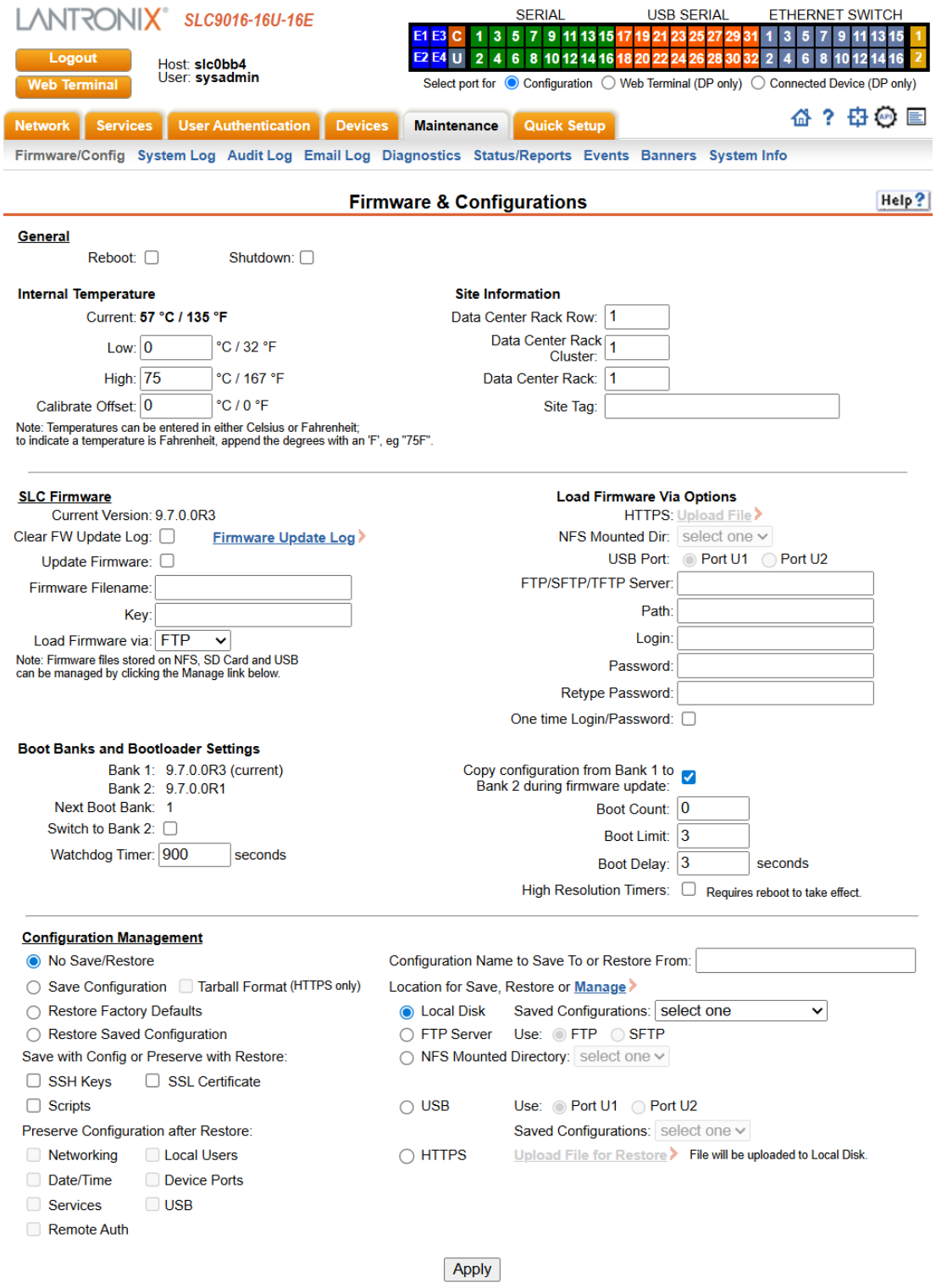
Downgrading firmware versions is not supported.

Avoid skipping more than three major releases at once.

To configure settings:

1. Click the **Maintenance** tab. The *Maintenance > Firmware & Configurations* page displays.

Figure 16-1 Maintenance > Firmware & Configurations



2. Enter the following:

Reboot	Select this option to reboot the SLC 9000 advanced console server immediately. The default is **No**. ***Note:***
Shutdown	Select this option to shut down the SLC unit. The default is **No**.

Internal Temperature

Current	Displays current temperature.
Low	Sets the acceptable minimum for the internal temperature of the SLC 9000 advanced console server. If the temperature of the SLC unit changes to be outside of this range, the SLC console manager will issue an SNMP trap.
High	Sets the acceptable maximum for the internal temperature of the SLC unit. If the temperature of the SLC 9000 advanced console server changes to be outside of this range, the SLC unit will issue an SNMP trap.
Calibrate Offset	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.

Site Information

Data Center Rack Row	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.
Data Center Rack Cluster	Set these fields to define the rack cluster the SLC 9000 advanced console server is located within a large data center. The default for these fields is 1.
Data Center Rack	Set these fields to define the rack the SLC unit is located within a large data center. The default for these fields is 1.
Site Tag	Tag or description used to identify the location or some other attribute of the SLC.

SLC Firmware

Note: *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.*

Current Version	Displays the current firmware version.
Clear ZTP Onboarding Log (checkbox)	Clears the contents of the ZTP & Bootstrap Onboarding log file. To view a log of all prior ZTP & Bootstrap onboarding updates, click the **ZTP Onboarding Log** link.
Clear FW Update Log (checkbox)	Clears the contents of the Firmware Update log file.
Firmware Update Log (link)	To view a log of all prior firmware updates, click the **Firmware Update Log** link.
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.

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**, **TFTP**, **HTTPS, NFS, USB**. **FTP** is the default. ◆ If you select **HTTPS**, the **Upload File** link becomes active. Select the link to open a popup window that allows you to browse to a firmware update file to upload. ◆ If you select NFS, the mount directory must be specified. ***Note:*** *Connections available depend on the model of the SLC unit.*

Boot Banks and Bootloader Settings

Note: *The SLC9000 stores two independent firmware images (Bank 1 and Bank 2). Firmware updates are applied to the inactive bank, allowing rollback to the previous firmware if the update fails.*

Bank 1	Displays the version of SLC firmware in bank 1. ***Note:*** *The word "current" displays next to the bank from which the SLC booted.*
Bank 2	Displays the version of SLC firmware in bank 2.
Next Boot Bank	Displays the current setting for bank to boot from at next reboot.
Switch to Bank 2	If desired, select the alternate bank to boot from at next reboot.
Copy configuration from Bank 1 to Bank 2 during firmware update	If checked, will copy the configuration from the current bank to the bank being updated. The two numbers are automatically generated so that the first number is the current bank.
Boot Count, Boot Delay, Boot Limit	Parameters that control how the SLC boots and when it switches to the alternate boot bank. ◆ **Boot Delay -** how many seconds the bootloader pauses before booting the SLC. Default is 3 seconds, range is 3 - 1800 seconds. ◆ **Boot Limit -** how many times the SLC will fail to boot before switching to the alternate boot bank. After the SLC fails to boot 2 times Boot limit (so it has attempted to boot **Boot Limit** times on each bank), the SLC will go into advanced recovery mode, which may require support from Technical Support to resolve so that the SLC can be booted again. Default is 3 boots, range is 3 - 20. ◆ **Boot Count -** how many times the SLC has failed to boot. If this value reaches Boot Limit, the SLC will switch to the alternate boot bank. The SLC will switch to the alternate boot bank only once. For example, if it fails to boot Boot Limit times on bank 1, it will automatically switch to bank 2; if it fails to boot Boot Limit times on bank 2, it will enter advanced recovery mode. If Boot Count has reached Boot Limit, setting this value to 0 will enable the SLC to boot again. Default is 0, range is 0 - 1.
High Resolution Timers	Enables or disables timers with a high degree of accuracy. High resolution timers are required for *Performance Monitoring*, but may affect SLC performance if they are enabled. Off by default. Changing this value requires a reboot for the change to take effect.
Panic Reboot	Enables or disables SLC auto-reboot on a kernel panic.
Watchdog Timer	Timer that will reboot the SLC if the boot fails to properly complete. If the timer expires without a successful boot of the SLC, the timer will automatically reboot the SLC. The default is 300 seconds. A value of zero will disable the watchdog timer.

Load Firmware Via Options

Note: *Prior to firmware update, the current configuration is saved to the Local Disk location with the name "before_MMDDYY_HHMM".*

HTTPS	Click **Upload File** to update the SLC firmware.
NFS Mounted Dir	Select the NFS mounted directory from the drop-down menu.
USB Port	Click to select USB port.
FTP/SFTP/TFTP Server	The IP address or host name of the server used for obtaining updates and saving or restoring configurations. May have up to 64 alphanumeric characters; may include hyphens and underscores.
Path	The default path on the server for obtaining firmware update files and getting and putting configuration save files.
Login	The userid for accessing the FTP server. May be blank.
Password / Retype Password	The FTP user password.
One time Login/ Password	If checked, the FTP Username and Password will not be saved. This is useful in scenarios where an OTP token is used to perform a firmware update or configuration save or restore. This checkbox is only applicable for firmware update and configuration save and restore; it has no effect for other operations (for example when the FTP/SFTP/TFTP Server, Path, Login and Password are being configured apart from firmware update and configuration save/restore).

Configuration Management

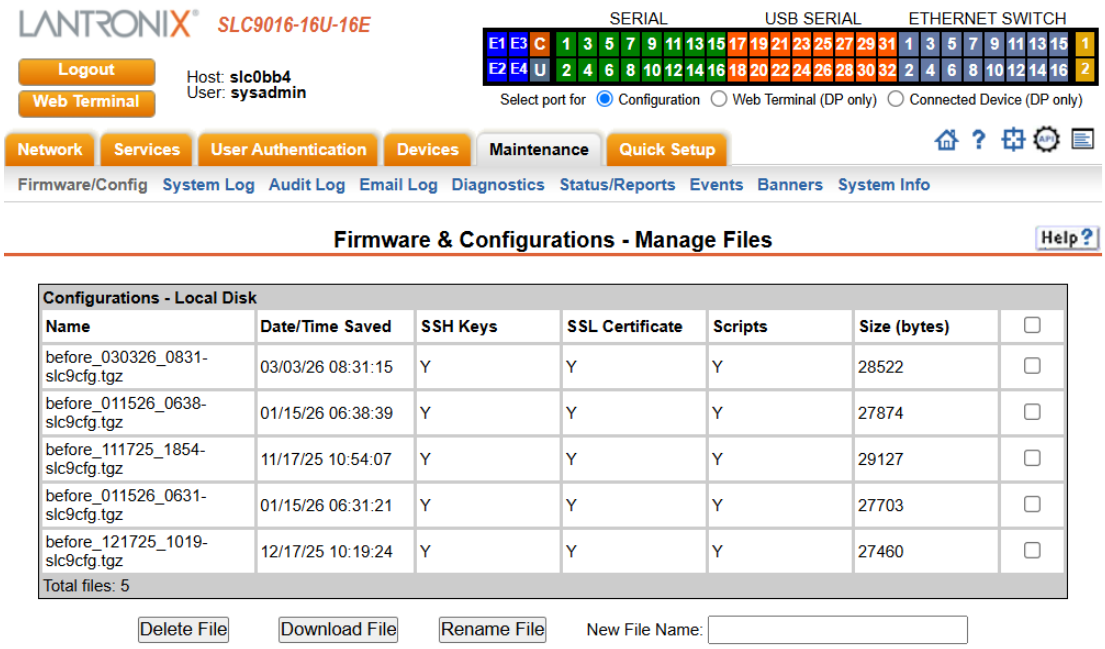
Configuration Management	From the option list, select one of the following: ◆ **No Save/Restore:** Does not save or restore a configuration. ◆ **Save Configuration:** Saves all settings to file, which can be backed up to a location that is not on the SLC 9000 advanced console server. If **Tarball Format** is checked, the configuration will be saved in the old (insecure) compressed tar file format, instead of the password protected zip file format. ◆ **Restore Factory Defaults:** Restores factory defaults. If you select this option, the SLC unit reboots after you apply the update.**WARNING:** This erases all settings and cannot be undone. ◆ **Restore Saved Configuration:** Returns the SLC settings to a previously saved configuration. If you select this option, the SLC console manager reboots after you apply the update. ***Note:*** *After the SLC reboots, verify key settings (network addresses, device port configuration) to confirm the restore completed successfully.*
Save with Config or Preserve with Restore	◆ Select the **SSH Keys** checkbox to save any imported or exported SSH keys. ◆ Select the **SSL Certificate** checkbox to save an imported certificate. ◆ Select the **Scripts** checkbox to save any interface or batch scripts. Disabled by default.
Preserve Configuration after Restore	Allows the user to keep a subset of the current configuration after restoring a configuration or resetting to factory defaults. Select the checkbox for each part of the current configuration you want to keep, for example, Networking, Services, or Device Ports.
Configuration Name to Save to or Restore From	If you selected to save or restore a configuration, enter a name for the configuration file (up to 12 characters).

Location for Save, Restore, or Manage	If you selected to save or restore a configuration, select one of the following options: ◆ **Manage:** This link allows you to view and delete all configurations saved to the selected location. This feature is available for the Local Disk, NFS Mounts, and USB locations. See *Provision via Zero Touch Provisioning*. ◆ **Local Disk – Saved Configurations:** If restoring, select a saved configuration from the drop-down list. ◆ **FTP Server:** The FTP server specified in the FTP/SFTP/TFTP section. If you select this option, select **FTP** or **SFTP** to transfer the configuration file. ◆ **NFS Mounted Directory:** Local directory of the NFS server for mounting files. ◆ **USB:** If a USB device is loaded into one of the USB ports of the SLC 9000 advanced console server, and properly mounted, the configuration can be saved to or restored from this location.If you select this option, select the port in which the USB thumb drive is mounted; then click a saved configuration from the drop-down list. ◆ **HTTPS:** For saving, the browser will prompt the user to save the configuration. For restoring, the configuration will be uploaded to the Local Disk location.

3. To view a log of all prior firmware updates, click the **Firmware Update Log** (blue link near the center of the web page).
4. Click **Apply**.

Note: *If you selected an option that forces a reboot (restore configuration, update firmware, or reset factory defaults), the SLC unit automatically reboots at the end of the process. To confirm the save succeeded, click **Manage** and verify the configuration file appears with a current timestamp.*

Figure 16-2 Network > Firmware/Config > Manage



Administrative Commands

Go to *Access List Commands* to view CLI commands which correspond to the web page entries described above.

HTTPS Push Configuration Restore

The HTTPS Push Configuration feature allows a saved configuration to be pushed to a SLC via a command line tool such as "curl" that includes the configuration to upload:

```
% curl --insecure --request POST --form "file=@/home/users/admin/
current-slccfg.tgz" 'https://myslc.company.com/
cfgupdate.htm?login=sysadmin&password=PASS&config=all&comment=FirmwareUp
date'
```

The arguments that are passed with the URL are:

- **login** - Login token to use for authentication. This must be a local user with firmware/config and reboot/shutdown rights.
- **password** - Clear text password for the login token.
- **config** - Indicates the portion of the configuration to restore, either all, or any combination of the following separated by commas: network, datetime, services, localusers, devports, usb, rpms, remoteauth, connections, events, ipfilter, groups, hostlist, nfscifs, maintenance, sites, scripts, slcnetwork, consoleport, menus, sshkeys, or sslcerts.
- **comment** - optional comment to include in the system log and audit log. If spaces are included in the comment they should be URL encoded as shown in this bash script:

```
#!/bin/bash

url="https://myslc.company.com/
cfgupdate.htm?login=sysadmin&password=PASS&config=all&comment=Update
myslc.company.com with default configuration"

curl --insecure --request POST --form "file=@/home/users/admin/current-
slccfg.tgz" "$( echo $url | sed 's/ /%20/g' )"
```

If an HTTPS Push Config command is accepted and initiated by the SLC, the SLC will respond with "Configuration restore initiated; SLC will reboot.", the restore will be performed, a message will be logged to the audit log and the system log, and the SLC will reboot. Any errors in the process will result in an error message being displayed.

Factory Reset with External Storage Device

In the event that a reset to factory defaults cannot be performed via the web UI or CLI, a factory reset can be initiated by attaching an external storage device to the console manager with a file in the top level directory of the storage device:

Warning: ***This procedure permanently erases all device configuration. Back up your configuration before proceeding.***

To perform a factory reset using external storage device:

1. Create a file called FACTORY_DEFAULT in the top level directory of an external storage device (USB thumb drive or SD card). The file should contain one line with the MAC address of the Eth1 Ethernet port, with or without colons (case insensitive). If the file is created on a Windows device, the file type should be of type **File** and not a **.txt** or **Text Document** file type.
2. Insert the external storage device into the console manager.
3. Boot the console manager. After the message “Starting <model>...” the console manager attempts to mount an external storage device. The console manager first searches for an external storage device in the upper USB port, then lower USB port (if present). The first external storage device that the console manager identifies and is successfully mounted is expected to have the `FACTORY_DEFAULT` file (any other external storage devices will be ignored). If it successfully mounts a storage device, and finds the appropriate `FACTORY_DEFAULT` file in the top level directory, it will perform a reset to factory defaults. A message appears on the console indicating that the `FACTORY_DEFAULT` file is detected in the external storage and the device is performing a factory reset.
4. If the external storage device with the `FACTORY_DEFAULT` file is left connected to the console manager and it is rebooted, a reset to factory default will be performed again. Therefore, we recommend you remove the storage device after a reset to factory defaults.

Factory Reset with Reset Button

The console manager can be factory reset (followed by an immediate reboot) with the reset button:

1. Locate the reset button above and between the Warning and Status LEDs.
2. Press and hold the reset button for 30 seconds with a small pointed tool (or paper clip); the status LED (LED in the middle) will begin to blink green more rapidly (three times per second) when the reset button is pressed.
3. After 30 seconds (continue to press the button) factory reset mode will be initiated; the warning LED (triangle with exclamation symbol) will begin to blink green three times per second at the same rate as the status LED.
4. Once factory reset is complete, the console manager will reboot.

Zero Touch Provisioning and Bootstrapping

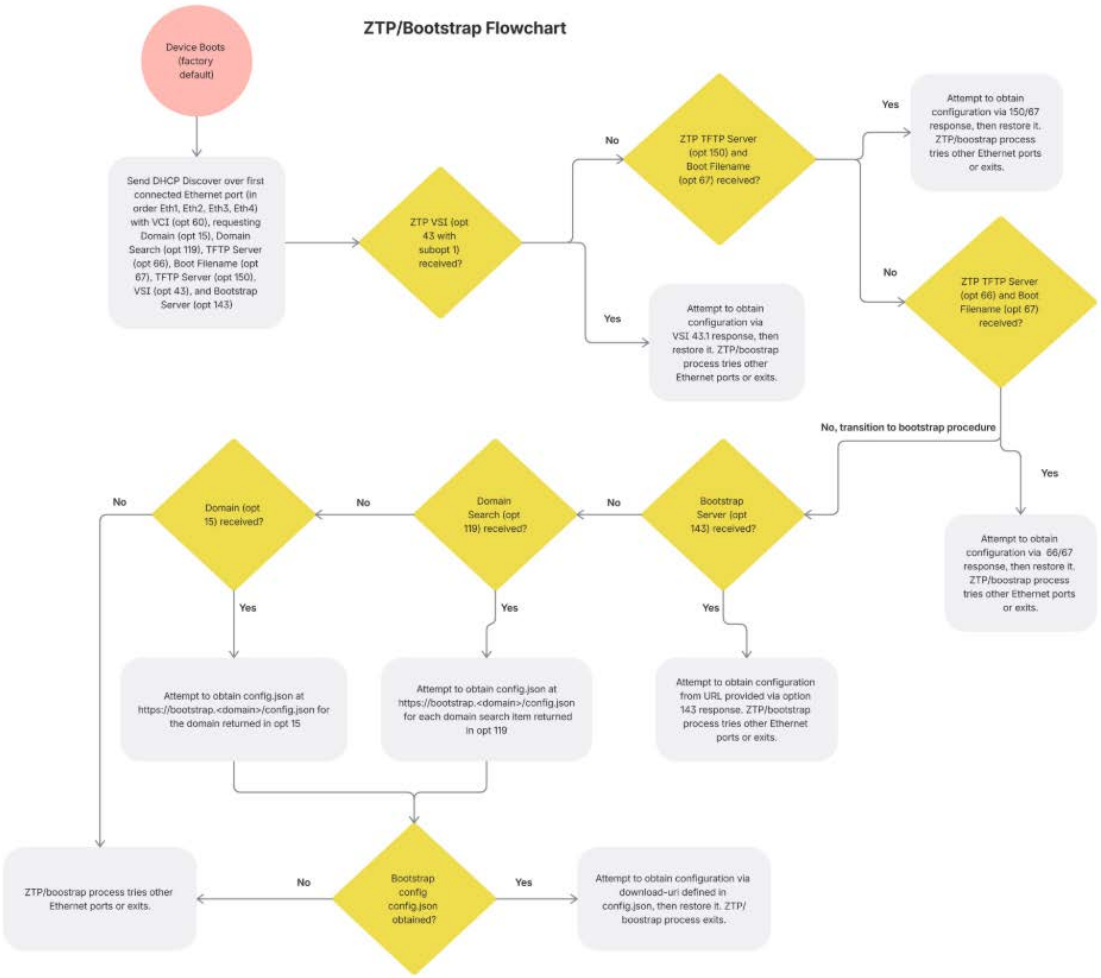
Console managers that are in a factory default state can be provisioned (acquire an initial configuration) through Zero Touch Provisioning (ZTP), bootstrapping (establishing identity and downloading an initial configuration from a bootstrap server) or Percepxion. Both ZTP and bootstrapping require that the device acquire network information from a DHCP server. In this way, the console manager can be deployed without manual intervention. At first boot, the console manager proceeds through a set of steps to acquire an initial configuration:

1. On the first connected Ethernet interface in order: Eth1, Eth2, Eth3, Eth4 , send a DHCP Discover requesting DHCP options 43 (Vendor Specific Information), 66 (TFTP Server), 67 (Boot Filename), 119 (Domain Search List), and 143 (Bootstrap Server, also known as ZTP Redirect), 150 (TFTP Server - Cisco). These options are in addition to the options requesting network configuration: option 1 (Subnet Mask), 3 (Router), 6 (Domain Name Server), 12 (Host Name), 15 (Domain Name), 28 (Broadcast Address), and (42) NTP Servers.
2. The ZTP process first attempts to acquire a configuration using options 43, 66, 67 and 150

(see diagram and ZTP description below).

3. If ZTP does not acquire a configuration, the console manager uses several methods to locate a bootstrap server that provides a configuration (see diagram and bootstrap description below).
4. If ZTP or bootstrapping succeeds (a configuration is acquired) on an Ethernet interface, the process terminates and the console manager reboots with the new configuration; otherwise, the process is repeated on the next connected Ethernet interface. Note: if a configuration is acquired in the bootstrap phase and the hash-value given in the config.json payload and used to verify the configuration image is incorrect, the process will stop and not continue to the next Ethernet interface.
5. If the console manager connects to Percepxion and is able to acquire a configuration update or a firmware update, the console manager will apply the update(s), and the initial connection and provisioning actions will be logged in the ZTP & Bootstrap Onboarding Log.
6. Any configuration acquired during onboarding (via ZTP, bootstrap or Percepxion) will be saved to the local configuration location with the name baseline; if multiple configurations are acquired, the most recent configuration acquired will the saved as the baseline configuration.
7. Logs for the onboarding process can be retrieved by filtering the system log at the CLI with grep: show syslog level warning grepi RE:ZTP|Bootstrap or by viewing the ZTP & Bootstrap Onboarding Log on the Maintenance page.

Figure 16-3 ZTP/Bootstrap Flowchart



Provision via Zero Touch Provisioning

The Zero Touch Provisioning (ZTP) feature allows a factory defaulted SLC 9000 to acquire a default configuration from a DHCP server and TFTP server when it is booted. If ZTP will be performed in an untrusted network, it is recommended that the Vendor Specific Information option using HTTPS and X.509 certificates be used. At boot-time, before the normal startup process, a unit will attempt to acquire network parameters and a configuration file, first over Eth1, and then over Eth2, followed by SFP Eth3 and SFP Eth4.

- The SLC unit will broadcast a DHCP Discover request on the Eth1 network port for a DHCP server on the local subnet, requesting DHCP options:
  - **Vendor Specific Information** (option 43)
  - **TFTP Server IP address list** (option 150, a Cisco proprietary option)
  - **TFTP Server Name or IP address** (option 66)
  - **Boot Filename** (option 67)

  For more information on these options see RFC 2132 and RFC 5859. To obtain Vendor Specific Information (VSI), the console manager sends a **Vendor Class Identifier** (option 60) of LantronixSLC 9000. The console manager will use VSI suboption 1 (see format below) to

determine the location of the ZTP file.

- If the DHCP Offer received from a DHCP server contains multiple options, they will be utilized in this order:

  a. Option **VSI/43** with suboption 1 (ZTP file location) will be used, and all other DHCP options will be ignored.

  b. Option **TFTP Server IP/150 and Boot Filename/67** - if both of these are received, they will be used, and all other DHCP options will be ignored.

  c. Option **TFTP Server IP or Name/66** and **Boot Filename/67** - if both of these are received, they will be used.

  Any configuration file specified by VSI/43 or Boot Filename/67 must be a valid console manager configuration filename ending in "-slc9cfg.tgz". For TFTP Server IP/150, the first IP address in the IP address list will be used; all other IP addresses will be ignored.

- **VSI/43 suboption 1 format:** the format of this suboption is a string consisting of tokens separated by spaces. The following tokens are supported: a URL indicating where to download the ZTP configuration file from, and the optional **validatecert** and **preserve_ethname** tokens. The URL can use the HTTPS, HTTP, FTP or TFTP protocol. The **validatecert** token indicates that the HTTPS protocol will be used and that a client side X.509 certificate and certificate authority files will be provided on an external USB drive or SD card; if the certificate files cannot be located, ZTP will terminate and not attempt to location a ZTP file with any other methods. The **preserve_ethname** token indicates that the current Eth1, Eth2 and hostname settings on the console manager should be preserved and not over-written with the Eth1, Eth2 and hostname settings from the configuration being restored. Examples of suboption 1 strings are "ftp://ftplogin:ftppassword@myserver.mynetwork.com/ztp2-slccfg.tgz preserve_ethname" and "https://10.0.1.131/config/ztp2-emgcfg.tgz validatecert".

  For **validatecert**, 3 certificate files are required to be in the top level directory of an external storage device: **cacert.pem** (certificate authority file for validating the HTTPS server), **cert.pem** (client side certificate file), and **key.pem** (client side key file). The console manager will search external storage devices in this order: upper USB port, lower USB port (if present) and SD card. The first external storage device that is found and successfully mounted is expected to be the source for the certificate files; if they are not located in the top level directory, ZTP will terminate and not attempt to locate a ZTP file with any other methods. See *Provision via Zero Touch Provisioning* for instructions to create a self-signed certificate with OpenSSL.

- If the console manager is able to download the configuration file, it will restore the configuration onto the console manager, and begin the normal startup process.
- If any of these steps fail for the Eth1 network port, it will repeat the process of trying to acquire a configuration over the Eth2 network port.
- After attempting to acquire a configuration over the Eth2 network port, the unit will begin the normal startup process.

Any results of attempting to acquire and restore a configuration file will be output to the console port and the system log. ZTP system log messages can be filtered from the system log with the CLI command `show syslog level warning grepi ZTP`. Configurations for firmware versions that are newer than the firmware version running on the unit will not be restored. Spaces are not supported in either the directory or filename portion of the **Boot Filename** path.

Creating a Certificate

You can create self-signed root certificate authority (CA) using OpenSSL, and use it to sign a client certificate that is used in the console manager and a server certificate that is installed in a web server responding to Zero Touch Provisioning (ZTP) requests.

To create certificate:

1. Setup an OpenSSL environment as follows (Perform this step only when you do not have an existing OpenSSL environment):
   a. Create a new directory and copy existing openssl.cnf file (or create a new `openssl.cnf`):

      ```
      cd /root
      mkdir ztp-cert
      cd ztp-cert
      mkdir newcerts
      cp /etc/ssl/openssl.cnf .
      export OPENSSL_CONF=/root/ztp-cert/openssl.cnf
      ```

   b. Under the `CA_default` section in openssl.cnf, change the directory where everything is kept to ".":

      ```
      [ CA_default ]
      dir = . # Where everything is kept
      ```

   c. Update the `[ req ]` and `[ req_distinguished_name ]` sections of `openssl.cnf` with specific certificate requests; otherwise, use the default values.
   d. Create the `index.txt` and serial files, which is a flat file database to keep track of signed certificates:

      ```
      touch index.txt
      echo 1000 > serial
      echo 1000 > crlnumber
      ```

2. Create the root certificate as follows:
   a. Create the private key for the root CA. Use longer bit sizes for the private key, such as 8192 instead of 4096

      ```
      openssl genrsa -out ca.key 4096
      ```

   b. Create the certificate for the root CA (the common name (CN) overrides the value in openssl.cnf, and can be set to any allowed certificate name).

      ```
      openssl req -new -x509 -days 3650 -key ca.key -out cacert.pem -subj
      /CN=ztpExampleCA
      ```

   c. Copy the output `cacert.pem` file of the previous step to the top-level directory of the external storage device, which will be used for ZTP.
   d. Verify the information in the certificate, such as the algorithms, validity date, and CN at using the following command:

      ```
      openssl x509 -noout -text -in cacert.pem
      ```

3. Create the server certificate and sign it with the root CA as follows:

a. Create the private key of the server certificate. Use longer bit sizes for the private key, such as 8192 can be used instead of 4096

```
openssl genrsa -out server.key 4096
```

b. Create the Certificate Signing Request (CSR) of the server certificate (the CN must match the IP address or name used in the URL to access the ZTP configuration file. Also, the CN cannot be the same as the CN of the root CA).

```
openssl req -new -key server.key -out server.csr -subj
/CN=example.ztp.com
```

c. Create the server certificate by signing the CSR with the root CA. `policy_match` can be used in place of `policy_anything` to use a different rule in `openssl.cnf` for controlling attributes of the certificate are required to match those given in the CA; by default `policy_anything` requires only CN:

```
openssl ca -days 365 -in server.csr -out server.crt -keyfile
ca.key -policy policy_anything -batch -notext
```

d. Install the output files, `server.key` and `server.crt` in the web server that will provide the ZTP configuration file.

e. Verify the information in the certificate, such as the algorithms, validity date and CN using the following command:

```
openssl x509 -noout -text -in server.crt
```

4. Create the client certificate and sign it with the root CA as follows:

a. Create the private key of client certificate. Use longer bit sizes for the private key, such as 8192 can be used instead of 4096

```
openssl genrsa -out client.key 4096
```

b. Create the Certificate Signing Request (CSR) of client certificate (The CN cannot be the same as the CN of the root CA).

```
openssl req -new -key client.key -out client.csr -subj
/CN=ztpExampleClient
```

c. Create the client certificate by signing the CSR with the root CA. `policy_match` can be used in place of `policy_anything` to use a different rule in openssl.cnf for controlling which attributes of a certificate are required to match those given in the CA; by default `policy_anything` requires only CN:

```
openssl ca -days 365 -in client.csr -out client.crt -keyfile
ca.key -policy policy_anything -batch -notext
```

d. Copy the output files `client.key` and `client.crt` to the top-level directory of the external storage device, which will be used for ZTP.

e. Update the name `client.key` to `key.pem` and `client.crt` to cert.pem).

f. Verify the information in the certificate, such as the algorithms, validity date and CN using the following command:

```
openssl x509 -noout -text -in client.crt
```

Provision via Bootstrap Server

If provisioning via ZTP process on an Ethernet interface fails, the console manager will transition to a bootstrap procedure for provisioning:

- The DHCP Discover request for both ZTP and bootstrapping included requests for the following DHCP options:

  Bootstrap Server (also known as ZTP Redirect) (option 143)

  Domain Search List (option 119)

  Domain Name (option 15)

For more information on these options see RFC 2132 and RFC 3397.

- If the DHCP Offer received from a DHCP server contains multiple options, they will be utilized in this order:

  a. Option **Bootstrap Server/143** will be used as a URL pointing to the configuration file, and all other DHCP options will be ignored.

  b. Option **Domain Search List/119** will be used to look for a provision JSON payload called config.json, and all other DHCP options will be ignored.

  c. Option **Domain Name/15** will be used to look for a provision JSON payload called **config.json**, and all other DHCP options will be ignored.

     Any configuration filenames in the DHCP server responses must be a valid console manager configuration filename ending in "-slc9cfg.tgz".

- Bootstrap Server/option 143 format: The response for this option is expected to be an URL for the config file to download and install on the console manager. The URL can use the HTTPS, FTP or TFTP protocol. Subdirectories can be included in the path. Examples are

  "https://bootserver.lantronix.com/initial-slc9cfg.tgz"

  "tftp://10.0.1.131/provision-slc9cfg.tgz"

  "ftp://10.0.1.131/provision-slc9cfg.tgz".

  Domain Search List/option 119 format: The response for this option is expected to be a list of domain names (see RFC 3397 for how to format the response). The console manager will attempt to download a config.json file from each domain name in the order they are given; for example, if the domain search list is **sales.lantronix.com, ops.lantronix.com** and **engr.lantronix.com**, the console manager will attempt to acquire config.json at **https://bootstrap.sales.lantronix.com/config.json, https://bootstrap.ops.lantronix.com/config.json** and **https://bootstrap.engr.lantronix.com/config.jso**n. The first URL that is accessible will be used. The format of config.json contains a URL for the config file to download and install on the console manager:

```
{
  "onboard": {
    "configuration" : {
      "download-uri": [ "https://example.com/configs/slc9000/provision-
slc9cfg.tgz" ],
      "image-verification" : [
        {
          "hash-algorithm" : "sha256",
          "hash-value" :
"baeccfa56782b41077c667a622ab7d5004a78b8f0edb028bf47555fbc113b233"
        }
```

```
            ]
         }
      }
   }
```

The image-verification block is used to verify the file given in the **download-uri**. Only **https** is supported for the download-uri protocol. The supported hash algorithms are md5, sha1, sha224, sha256, sha384 and sha512.

- **Domain Name/option 15 format**: The response for this option is expected to be a single domain name (see RFC 2132 for how to format the response). The console manager will attempt to download a **config.json** file from the domain name; for example, if the domain name is hq.lantronix.com, the console manager will attempt to acquire config.json at **https://bootstrap.hq.lantronix.com/config.json**. The format of **config.json** is the same as the format for Domain Search List.

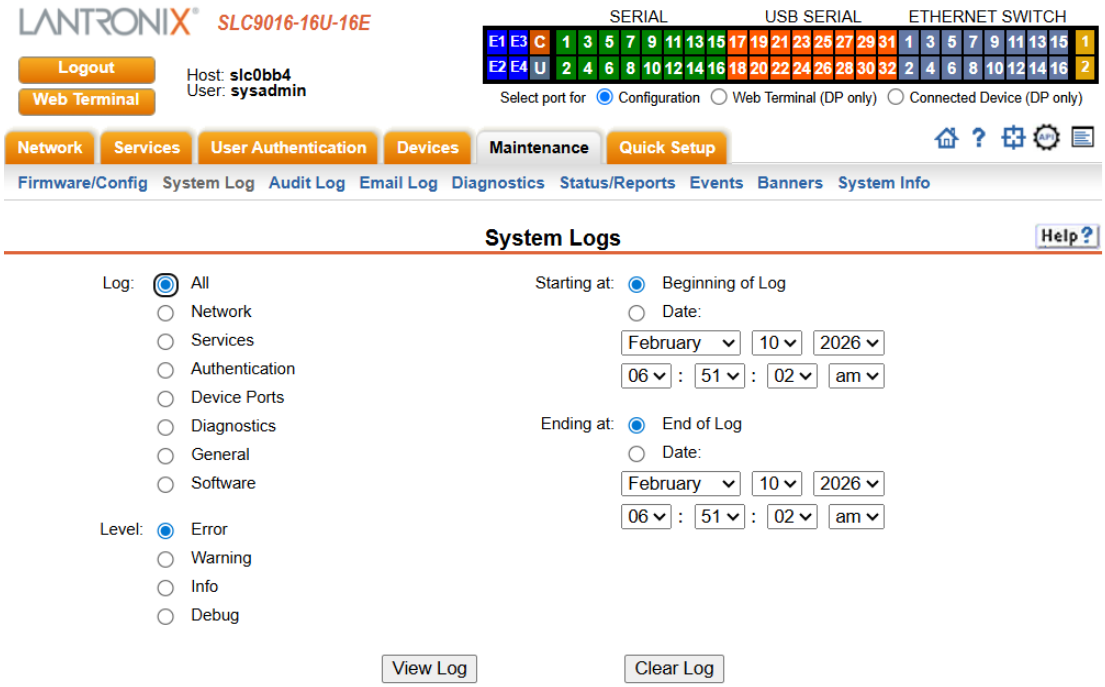
System Logs

The *Maintenance > System Logs* page allows you to view various system logs. (See *Chapter 7: Services on page 116* 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:

Figure 16-4 Maintenance > System Logs

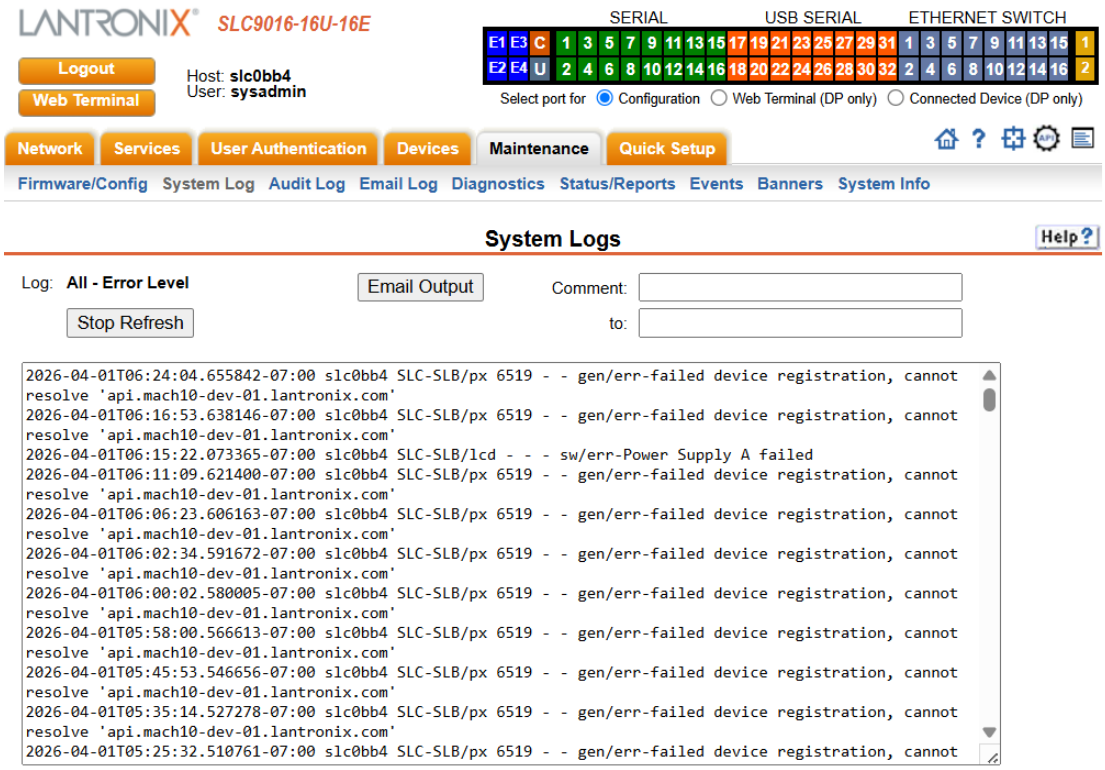


2. Enter the following to define the parameters of the log you would like to view:

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 unit displays a log similar to this:

Figure 16-5 System Logs



From a queried system log (e.g., *Figure 16-5*), you may email this information to a specific individual or to Lantronix Technical Support. See *Emailing Logs and Reports (on page 335)*.

To clear system logs:

1. From the *Maintenance > System Logs* page, select **Maintenance - System Logs**.
2. Click the **Clear Log** button to clear all log information.

System Log Commands

Go to *System Log Commands* to view CLI commands which correspond to the web page entries described above.

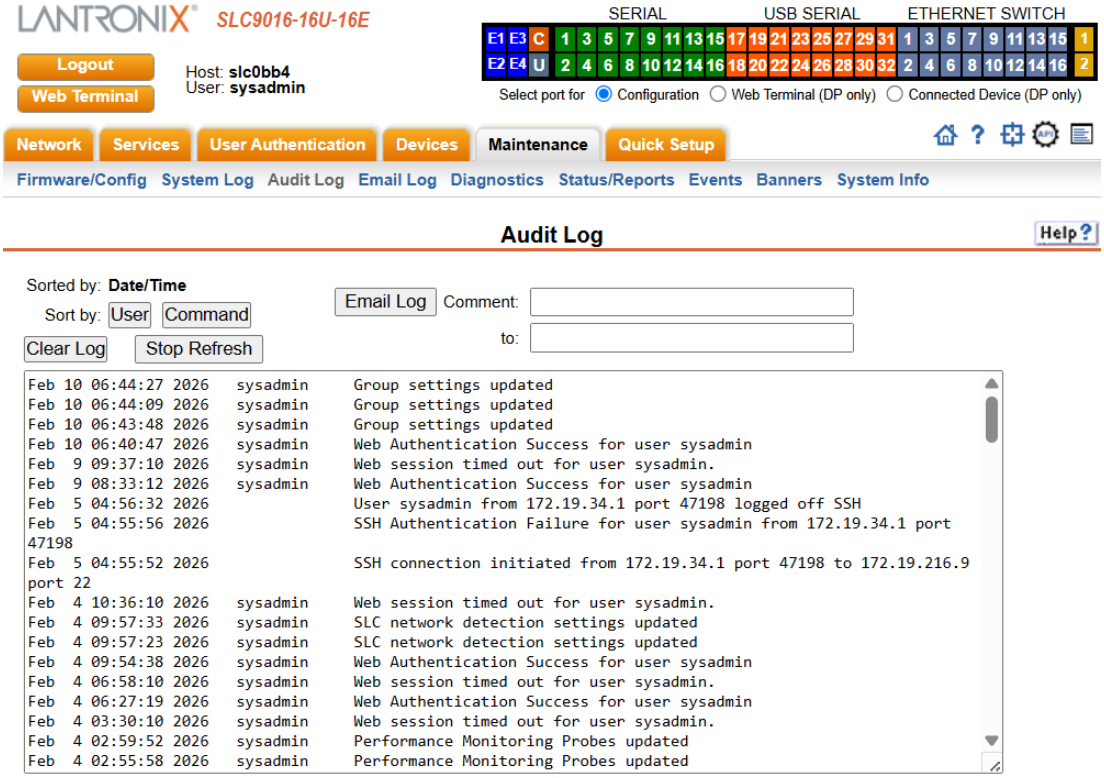
Audit Log

The *Maintenance > Audit Log* page displays a log of all actions that have changed the configuration of the SLC 9000 advanced console server. The audit log is disabled by default. Use the *Services > SSH/Telnet/Logging* 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 reboots.

1. Click the **Maintenance** tab and select the **Audit Log** option. The following page displays:

Figure 16-6 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 sort by **Command** button.
3. To email this log, follow the instructions in *Emailing Logs and Reports (on page 335)*.
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.

Audit Log Commands

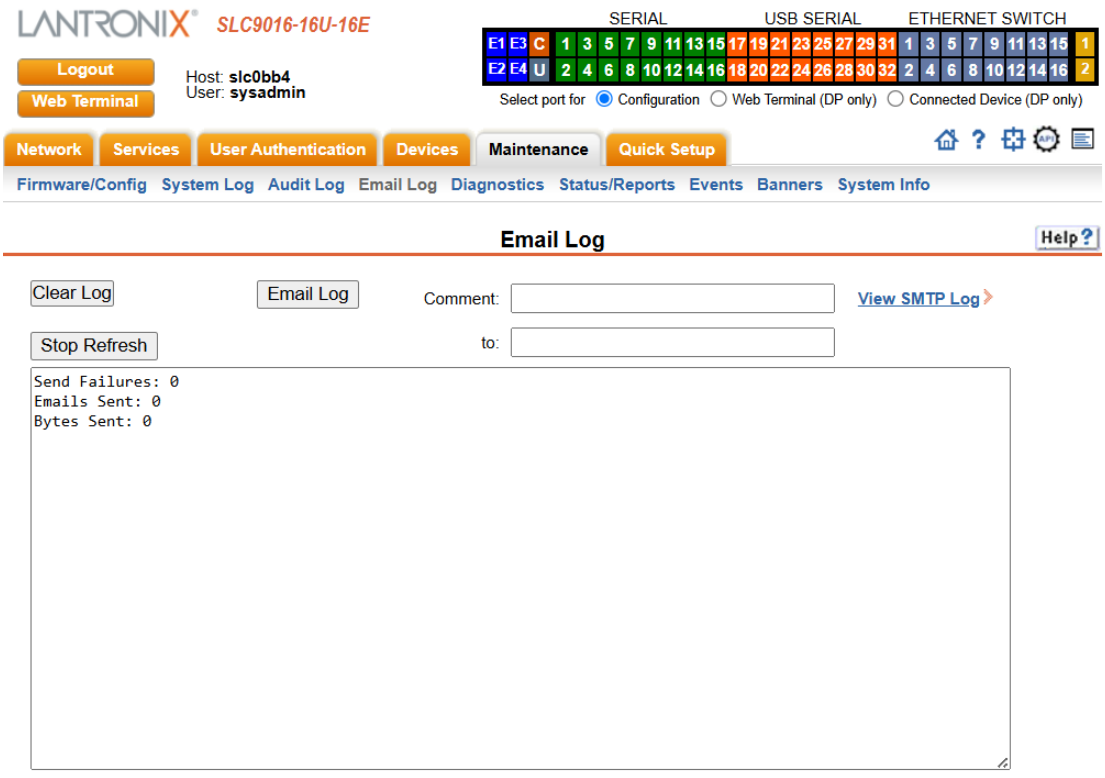
Go to *Audit Log Commands* to view CLI commands which correspond to the web page entries described above.

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 reboots.

1. Click the Maintenance tab and select the Email Log option. The following page displays:

Figure 16-7 Maintenance > Email Log



2. To email this log, follow the instructions in *Emailing Logs and Reports (on page 335)*.

3. To clear the log, click the **Clear Log** button.

Logging Commands

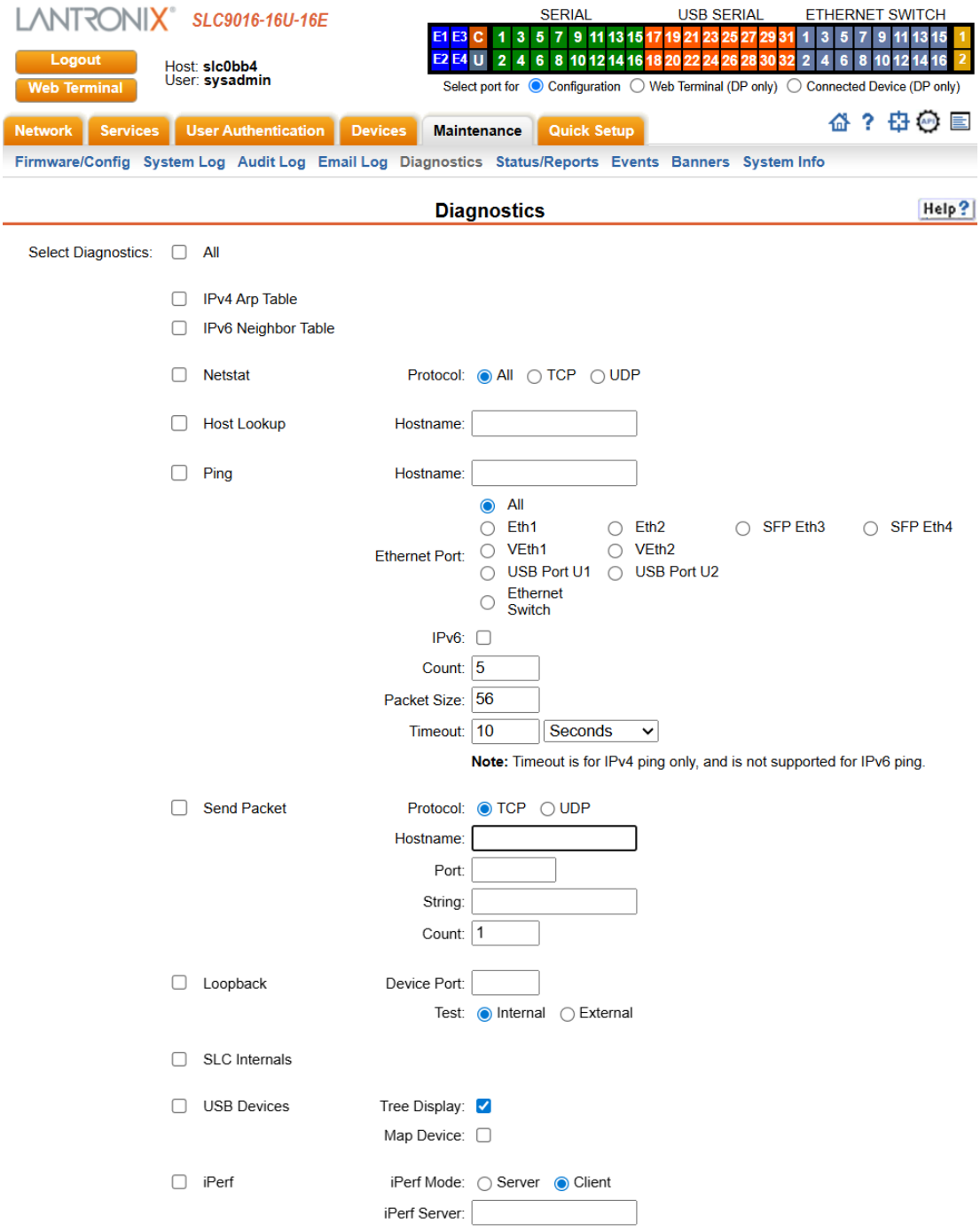
Go to *Logging Commands*, *USB Device Commands*, *USB Device Commands*, and *USB Modem Commands* to view CLI commands which correspond to the web page entries described above.

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.

1. Click the **Maintenance** tab and select the **Diagnostics** option. The following page displays:

Figure 16-8 Maintenance > Diagnostics



2. Select **Diagnostics** from checklist (one or more diagnostic methods you want to run, or select **All** to run them all):

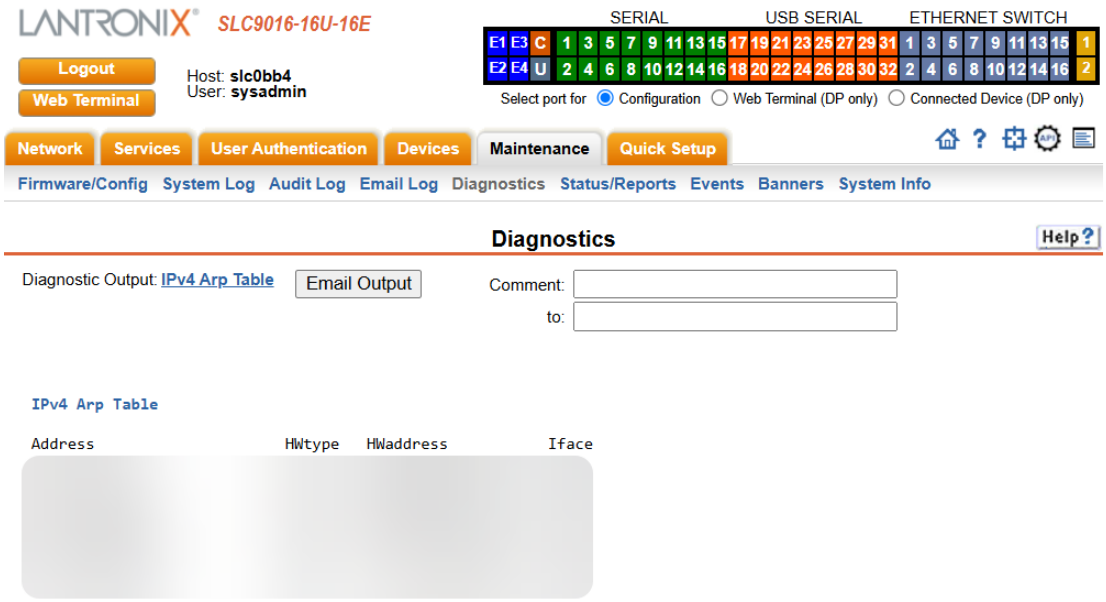
IPv4 ARP Table	The IPv4 Address Resolution Protocol (ARP) table used to view the IP address-to-hardware address mapping.
IPv6 Neighbor Table	The IPv6 Neighbor table is used to view a list of neighbor's IPv6 addresses on the same network, and their corresponding MAC addresses.

Netstat	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.
Host Lookup	Select to verify that the SLC 9000 advanced console server 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,
Ping	Select to verify that the host is up and running. If selected, also do the following: ◆ **Hostname:** Specify a host name or IP address of the host to send the packet. ◆ **Ethernet Port:** Select **All** (to not bind to any interface) or select a specific interface to bind to (e.g. select as the source interface) when sending the ping packets. ◆ **Packet Size:** Specify the size of the packet. ◆ **Timeout:** Specify the number of seconds to wait for the first response. ***Note:*** *Timeout is for IPv4 ping only, and is not supported for IPv6 ping.*
Send Packet	This option sends an Ethernet packet out one of the Ethernet ports, mainly as a network connectivity test. For UDP, the number of times the string is sent is equal to the number of packets sent. For TCP, the number of times the string is sent may (or may not) be equal to the number of packets sent, because TCP controls how data is packetized and sent out. Enter the following: ◆ **Protocol:** Select the type of packet to send (**TCP** or **UDP**). ◆ **Hostname:** Specify a host name or IPaddress of the host to send the packet to. ◆ **Port:** Specify a **TCP** or **UDP** port number of the host to send the packet to. ◆ **String:** Enter a set of up to 64 characters. The string is encapsulated in the packet (so you could use a network sniffer to track the packet and, by looking at its contents, verify that it was sent). ◆ **Count:** The count is the number of times the string is sent.
Loopback	Specify loopback information: ◆ **Device Port** ◆ Select either an **Internal** or **External** test ***Note:*** *The External test is currently not supported for USB device ports*
SLC Internals	Select to display information on the internal memory, storage and processes of the SLC 9000 advanced console server.
USB Devices	Select to display information about USB buses and the devices connected to them, including a mapping between a USB device and the SLC ports.

iPerf	Select to start an iPerf3 server or client to measure network throughput. The server will run in “one-off” mode. This means that it will handle one client connection and then terminate. The server will wait indefinitely for the client to connect. The client will time out if a connection is not made to a server within 15 seconds. For more information, visit the iPerf website. ◆ **iPerf Mode:** Select the mode (**Server** or **Client**). Two SLCs can be used to measure network throughput, one running in server mode and one running in client mode. ◆ **iPerf Server:** Specify the server name or IP address that the client connects to. ◆ **iPerf Options:** Enter options to configure the packets sent by the server or client. If no options are specified, the server or client will run with a default set of TCP packets. ➢ Set server port to listen on/connect to (default 5201): -p, --port n ➢ Format to report: -f, --format [kmgtKMGT] ➢ Pause n seconds between reports: -i, --interval n ➢ Bind to a host, an interface or multicast address: -B, --bind ➢ More detailed output: -V, --verbose ➢ Output in JSON format: -J, --json ***Note:*** *The options below are supported on the client only:* ➢ Set length of buffer to n (default 8 KB): -l, --length n[KMG] ➢ Use UDP rather than TCP: -u, --udp ➢ TCP window size (socket buffer size): -w, --window n[KMG] ➢ Set TCP/SCTP maximum segment size (MTU): -M, --set-mss n ➢ Set TCP/SCTP no delay, disabling Nagle’s Algorithm: -N, --no-delay ➢ Set bandwidth to n bits/sec (default 1Mbit/sec, unlimited for TCP): -b, --bitrate n[KMG] ➢ Number of bytes to transmit (instead of -t): -n, --bytes n[KMG] ➢ Time in seconds to transmit for (default 10 secs): -t, --time n ➢ Set the IPv6 flow label: -L, --flowlabel n ➢ Omit the first n seconds: -O, --omit n ➢ Prefix every output line with this string: -T, --title str ➢ Number of blocks (packets) to transmit (instead of -t/-n): -k, --blockcount ➢ Set the IP type of service, 0-255. The usual prefixes for octal and hex can be used, i.e. 52, 064 and 0x34 all specify the same value: -S, --tos n ➢ Set the IP dscp value, either 0-63 or symbolic: --dscp n ***Note:*** *The SLC uses iPerf version 3.x, which is incompatible with older iPerf versions.*

3. Click the **Run Diagnostics** button. The *Maintenance > Diagnostics* page displays.

Figure 16-9 Maintenance > Diagnostics



4. To view a report, click the link for that report.
5. To email this report, follow the instructions in *Emailing Logs and Reports*.

Additional diagnostics available at the CLI:

Dmesg	Displays kernel logs.
Ethtool	Displays Ethernet interface ethtool diagnostic information.
Nettrace	Display all network traffic, applying optional filters. The output can be saved to a Wireshark pcap file on external storage, or to a Wireshark pcap file on local storage (located in the sysinfo files repository; a maximum of 3 local pcap files of up to 50MB can be saved; if a file reaches 50MB it will be truncated). The local pcap files can be downloaded from the web UI System Info files repository.
Speedtest	Runs a network performance test over the default gateway to speedtest.net and outputs the results (speedtest.net must be reachable in order to perform the test). This tool is useful for testing performance of various network configurations, including performance of a cellular connection.
Top	Displays CPU usage, memory usage and tasks
Traceroute	Displays the route packets take to get to a network host.

Diagnostic Commands

Go to *Diagnostic Commands* to view CLI commands which correspond to the web page entries described above.

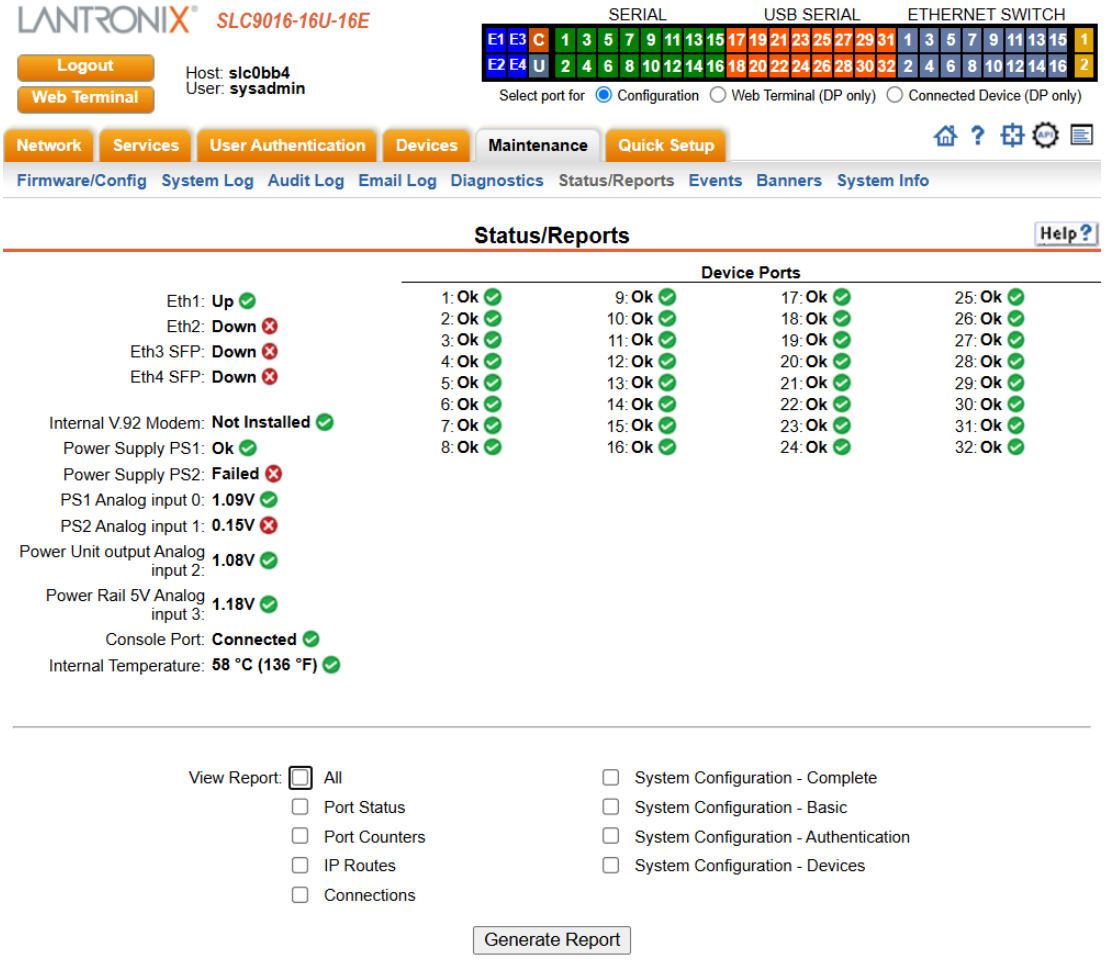
Status/Reports

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 16-10 Maintenance > Status/Reports



The top half of the page displays the status of each port, power supply, and the internal modem:

- **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**:

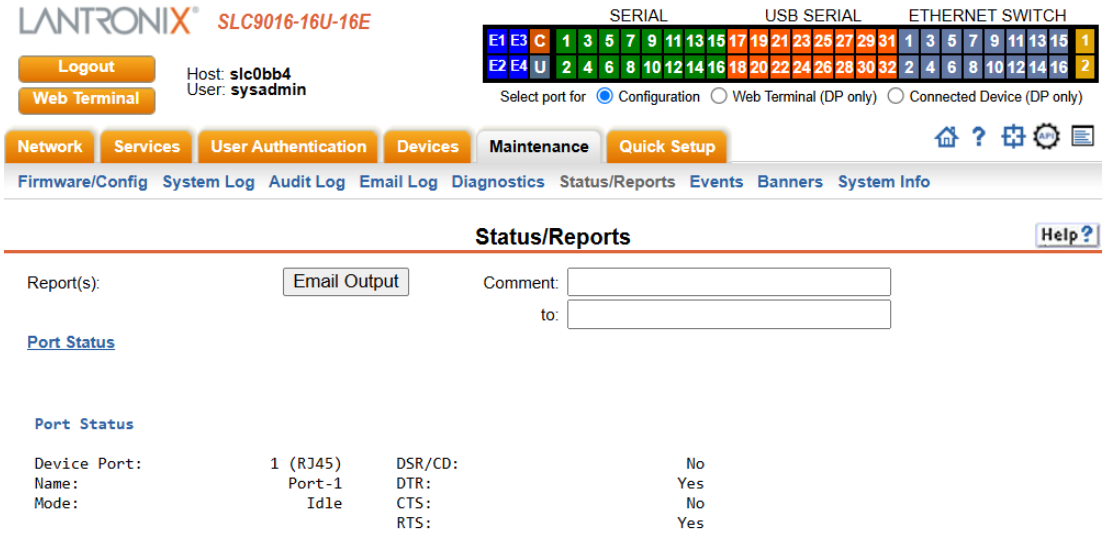
View Report

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.
IP Routes	Displays the routing table.
Connections	Displays all active connections for the SLC unit: Telnet, SSH, TCP, UDP, device port, and modem.
System Configuration – Complete	Displays a complete snapshot of the SLC settings.
System Configuration – Basic	Displays a snapshot of the SLC unit's basic settings (for example, network, date/time, routing, services, console port).
System Configuration – Authentication	Displays a snapshot of authentication settings only (including a list of all localusers).
System Configuration - Devices	Displays a snapshot of settings for each device port, USB Port, Modem, and Host Lists.

3. Click the **Generate Report** button. In the upper left of the *Generated Status/Reports* page displays a list of reports generated.

Figure 16-11 Generated Status/Reports



4. To email these report(s), follow the instructions in *Emailing Logs and Reports (on page 335)*.

Status Commands

Go to *Status Commands* to view CLI commands which correspond to the web page entries described above.

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 (*Figure 16-5*)
- Audit Log (*Figure 16-6*)
- Email Log (*Figure 16-7*)
- Diagnostic Reports (*Figure 16-9*)
- Status/Reports (*Figure 16-11*)

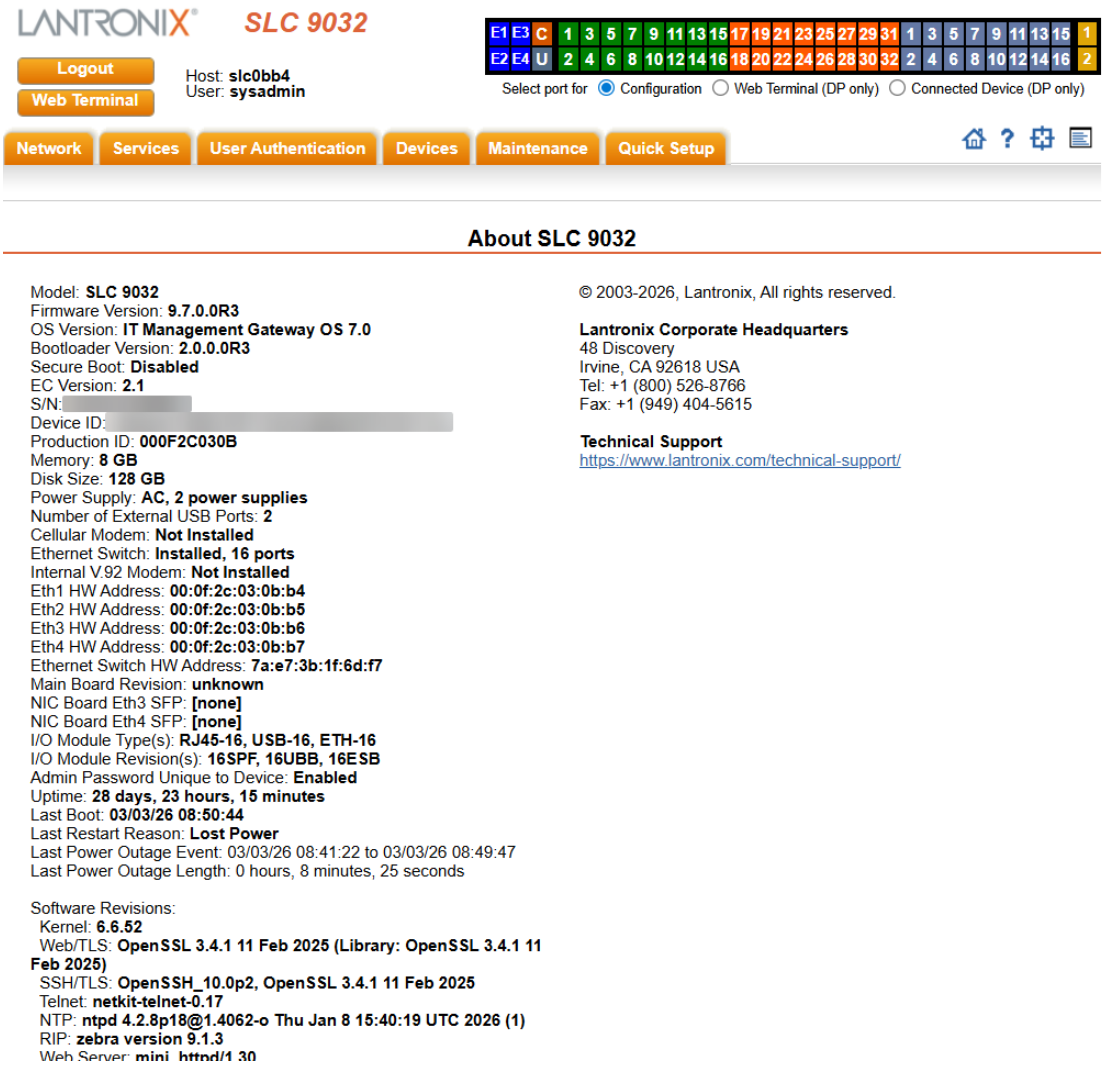
To email a log to an individual:

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 Log** button. An email is immediately sent out and a confirmation appears on the screen.

To view information about the SLC unit and contact information for Lantronix:

1. Click the ? button on the upper right portion of any web page to access the **About SLC** page (see *Figure 16-12*).

Figure 16-12 About SLC

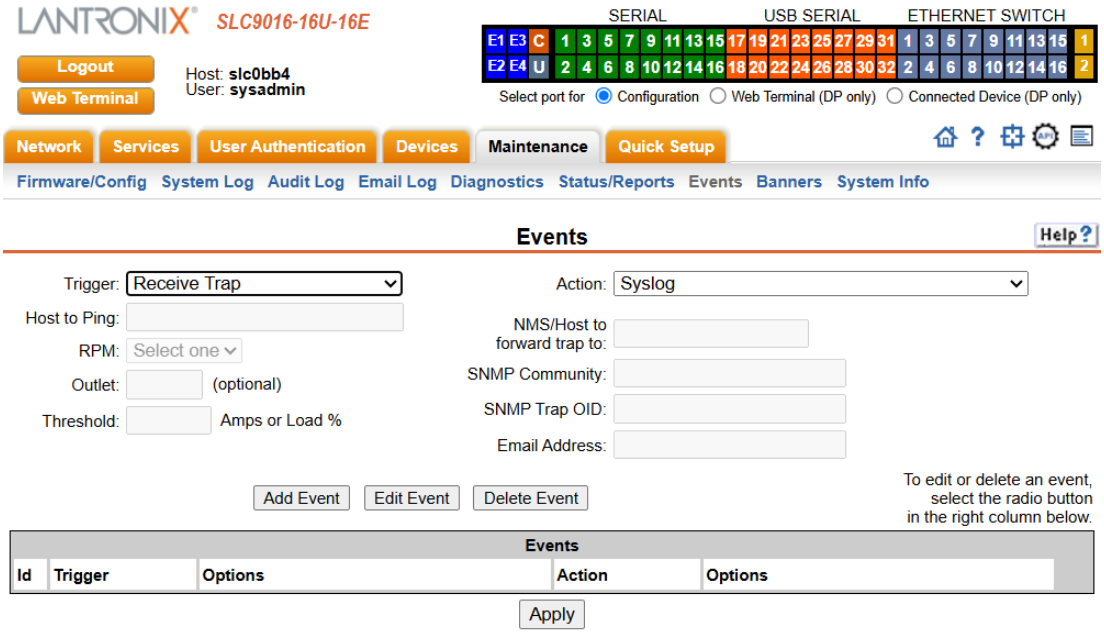


Events

On this *Maintenance > Events* page, you can define what action you want to take for events that may occur in the SLC unit.

1. Click the **Maintenance** tab and select the **Events** option. The following page displays:

Figure 16-13 Maintenance > Events



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 ◆ No Internal Modem Dial Tone ◆ Ping Host Fails ◆ RPM Load Over Threshold
Host to Ping	When the trigger is set to **Ping Host Fails**, enter the hostname, IPv4 address or IPv6 address of the host to ping. The host will be pinged every 2 minutes.
RPM	When the trigger is set to **RPM Load over Threshold**, select the RPM that will be monitored for a current that exceeds a defined threshold. The RPM needs to support providing a current level as part of its status information. The RPM current will be checked every 2 minutes.
Outlet	When the trigger is set to **RPM Load over Threshold**, select the outlet that will be monitored for a current that exceeds a defined threshold. The RPM needs to support providing a current level for the selected outlet as part of its status information. If an outlet is not specified, the current level for the entire device will be monitored. The RPM current will be checked every 2 minutes.
Threshold	When the trigger is set to **RPM Load over Threshold**, specify the maximum allowable threshold for the current; any current readings over this threshold will trigger the selected action. The threshold can be specified in Amps (e.g. 8.5) or as a percentage (e.g. 90%).

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. ◆ Syslog ◆ Forward All Traps to Ethernet ◆ Forward Selected Trap to Ethernet ◆ Forward all Traps to a Modem Connection ◆ Forward Selected Trap to a Modem Connection ◆ Email Alert ◆ SNMP Trap
Ethernet	For actions that require an Ethernet connection (for example, **Forward All Traps to Ethernet**), select the Ethernet port to use.
Modem Connection on	For actions that require a modem connection (for example, **Forward All Traps to a Modem Connection**, select which modem connection to use (**Device Port**, **USB Port U1**, **USB Port U2**, or the **Internal Modem**). Connections available depend on the model of the SLC unit.
NMS/Host to forward trap to	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.
SNMP Community	Forwarded traps are sent with this SNMP community value There is no default.
SNMP Trap OID	Enter a unique identifier for an SNMP object. (An SNMP object is anything that can hold a value and can be read using an SNMP "get" action.) The OID consists of a string of numbers separated by periods (for example, 1.1.3.2.1). Each number is part of a group represented by the number on its left.
Email Addresses	Enter an email address to receive email alerts.

3. 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

Go to *Events Commands* to view CLI commands which correspond to the web page entries described above.

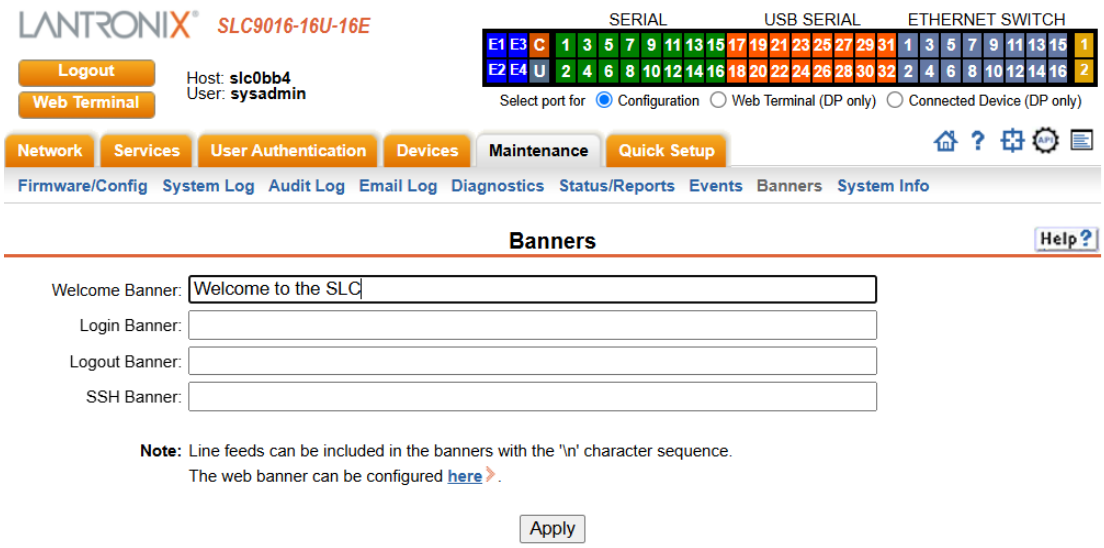
Banners

The 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 16-14 Maintenance > Banners



2. Enter the following fields.

Welcome Banner	The text to display before the user logs in to the command line interface. This banner is displayed for Telnet and Console Port sessions; for SSH sessions the **SSH Banner** is used to show a welcome message before user authentication. May contain up to 1350 characters (banners that contain both quotes and spaces may not be configurable at the CLI due to CLI syntax requirements for values that contain spaces). Depending on your console manager, the default banner text is "Welcome to the console manager." ***Note:*** *To create more lines use the* ***\n*** *character sequence.*
Login Banner	The text to display on the command line interface after the user logs in. May contain up to 1350 characters (banners that contain both quotes and spaces may not be configurable at the CLI due to CLI syntax requirements for values that contain spaces). Blank by default. ***Note:*** *To create more lines, use the* ***\n*** *character sequence.*
Logout Banner	The text to display on the command line interface after the user logs out. May contain up to 1350 characters (banners that contain both quotes and spaces may not be configurable at the CLI due to CLI syntax requirements for values that contain spaces). Blank by default. ***Note:*** *To create more lines use, the* ***\n*** *character sequence.*

SSH Banner	The text to display when a user logs into the console manager via SSH, prior to authentication. May contain up to 1350 characters (banners that contain both quotes and spaces may not be configurable at the CLI due to CLI syntax requirements for values that contain spaces). Blank by default. ***Note:*** *To create more lines use the* ***\n*** *character sequence.*

3. Click **Apply** to save.

Administrative Banner Commands

Go to *Administrative Commands* to view CLI commands which correspond to the web page entries described above.

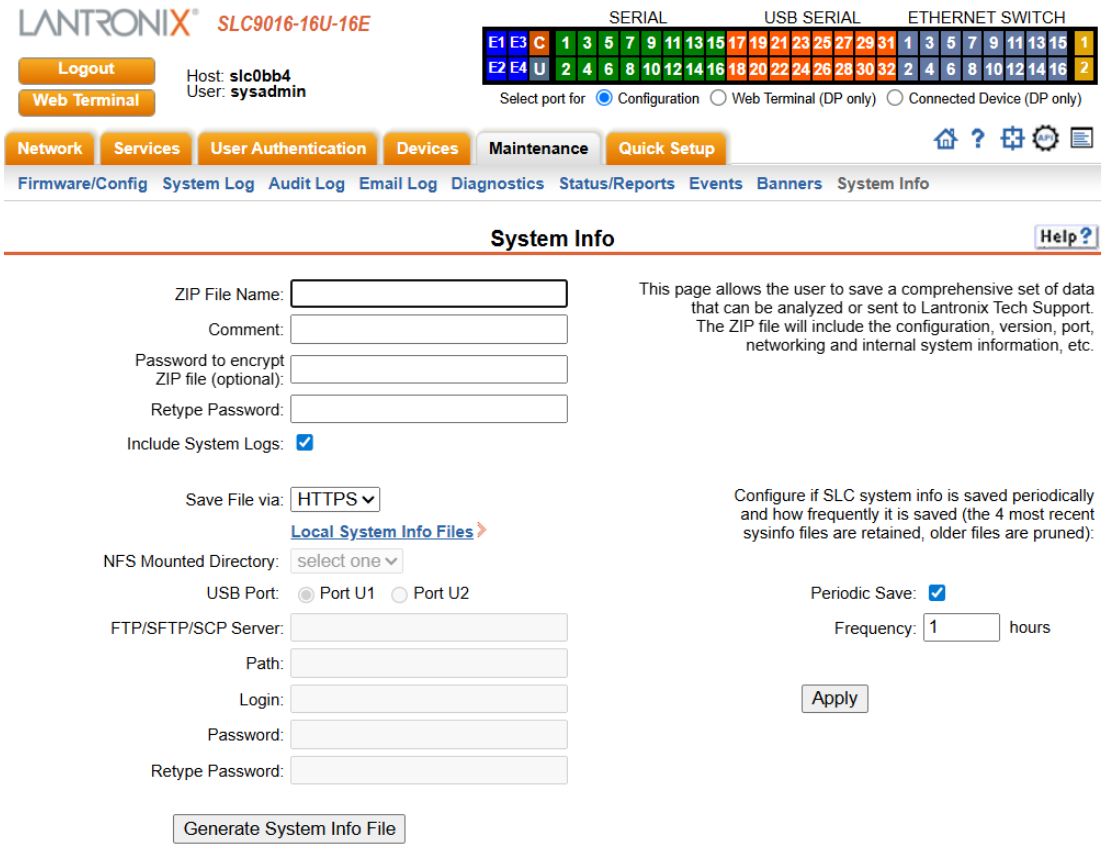
System Info

The **System Info** page allows you to generate a ZIP file containing log data that can be used for debugging SLC or for sending to Lantronix Tech Support. The ZIP file contains network information, current configuration, logs, port information, and internal diagnostic information.

To generate the System Info file:

1. Click **Maintenance** and then click **System Info**. The **System Info** page appears.

Figure 16-15 System Info



2. Enter the following information:

ZIP File Name	The name of the System Info ZIP file, without the .zip extension. Up to 40 characters can be entered.
Password to encrypt ZIP file/ Retype Password	An optional password that can be used to encrypt the ZIP file, and will be required to unpack the ZIP file.
Include System Logs	If selected, will include all of the system log files in the ZIP file. This can significantly increase the size of the ZIP file.
Save File via	The method of saving the ZIP file. The available options are **FTP**, **SFTP**, **SCP**, **HTTP**, **NFS**, and **USB**. By default, **FTP** is the default selected. For NFS, a NFS share needs to be configured and mounted on the console manager. For information about NFS, see *NFS Commands*. For USB, external media needs to be present and mounted on the console manager. For information about USB, see *Chapter 9: USB Port on page 155*.
NFS Mounter Directory	The mount directory of NFS. This option is available only when you select the **NFS** option in **Save File via**.
USB Port	Select the USB port to save the System Info file.
FTP/SFTP/TFTP Server	The IP address or host name of the server used for saving the System Info file. It may consist of 64 alphanumeric characters, hyphens, and underscores.
Path	The optional directory on the FTP/SFTP/SCP server to use for saving the ZIP file,..
Login/Password/ Retype Password	The user login credentials of the FTP/SFTP/SCP server.

3. Click **Generate System Info File**. The **System Info ZIP** file is saved.

To configure auto System Info files:

Complete the following fields:

Periodic Save	Check this field to enable periodic save of System Info files. Enabled by default.
Frequency	Enter how ofter the auto System Info files are generated, in hours (1 to 999 hours). The default is once an hour.

To save the auto system info settings, select **Apply**.

Manage Files

The **Manage Files** web page allows you to view the firmware and configuration files saved to the selected location and rename, download or delete any of the files. This feature is available for the Local Disk, NFS Mounts, and USB locations.

To manage files:

1. On the *Maintenance > Firmware & Configurations* page, click the **Manage** link. The *Network > Firmware/Config > Manage (on page 315)* page appears and displays the name and the time and date the file was saved.
2. To rename a file, select a file, enter the **New File Name**, and click the **Rename File** button.
3. To download a file, select a file and click the **Download File** button.

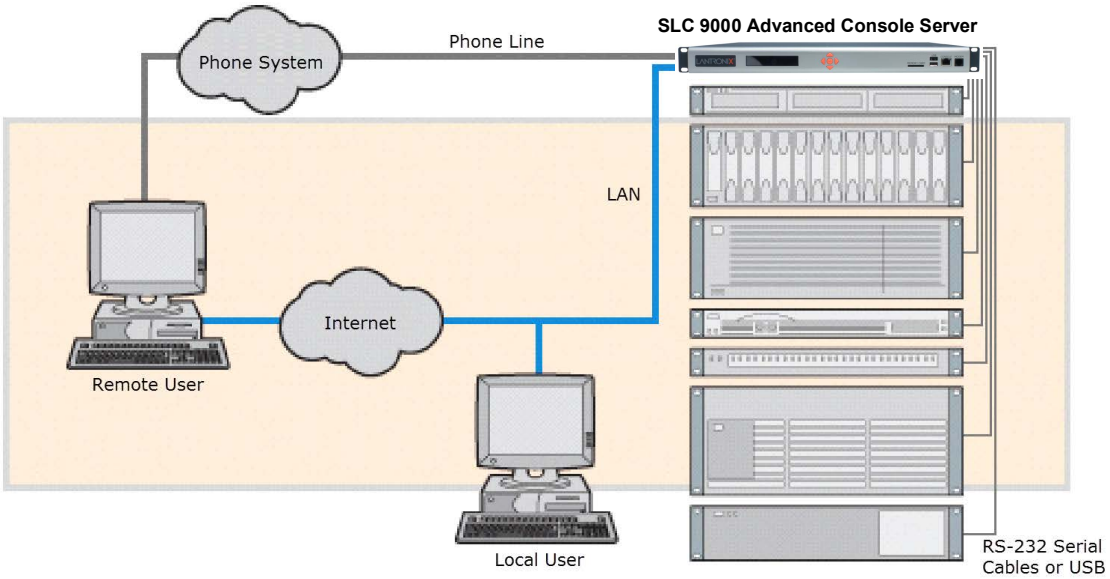
4. To delete files, select one, multiple files, or all files, and click the **Delete File** button. A verification message showing files deleted will appear. Click **Back to Manage Files** to return to the *Network > Firmware/Config > Manage (on page 315)* page.

   Note: *When deleting multiple files with a single command, the list of files that have been deleted will only be shown if 10 or fewer files are deleted.*

17: Application Examples

Each SLC advanced console server has multiple serial ports and two network ports. Each serial port can be connected to the console port of an IT device. Using a network port (in-band) or a modem (out-of-band) for dial-up connection, an administrator can remotely access any of the connected IT devices using Telnet or SSH.

Figure 17-1 SLC - Console Manager Configuration

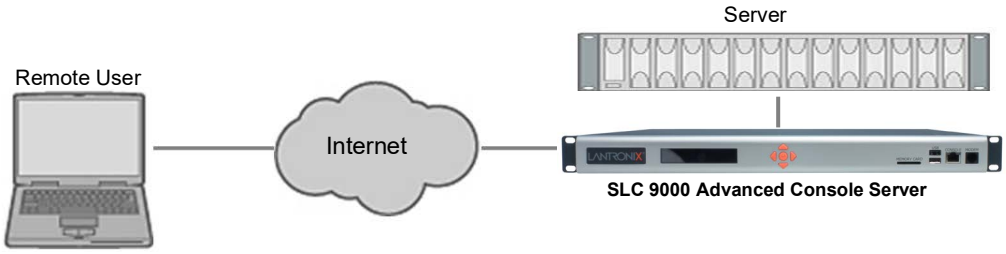


This chapter includes three typical scenarios for using the SLC unit. The scenarios assume that the SLC 9000 advanced console server is connected to the network and has already been assigned an IP address. In the examples, we use the command line interface. You can do the same things using the web page interface except for directly interacting with the SLC unit (`direct` command).

Telnet/SSH to a Remote Device

The following figure shows a server connected to port 2 of the SLC 9000 advanced console server.

Figure 17-2 Remote User Connected to a UNIX Server via the SLC unit



In this example, the sysadmin would:

1. Display the current settings for device port 2:

```
[SLC]> show deviceport port 2
___Current Device Port
Settings_____________________________________________________
Number: 2  Name: Port-2

Modem Settings-------------Data Settings----------IP Settings-------
Modem State: disabled      Baud Rate: 9600         Telnet: disabled
Modem Mode: text           Data Bits: 8            Telnet Port: 2002
Timeout Logins: disabled   Stop Bits: 1            SSH: disabled
Local IP: negotiate        Parity: none            SSH Port: 3002
Remote IP: negotiate       Flow Control: xon/xoff  IP: <none>
Authentication: PAP        Logins: disabled
CHAP Host: <none>          Break Sequence: \x1bB
CHAP Secret: <none>        Check DSR: disabled
NAT: disabled              Close DSR: disabled
Dial-out Login: <none>
Dial-out Password: <none>
Dial-out Number: <none>
Dial-back Number: usernumber
Initialization Script: <none>

Logging Settings-----------------------------------------------------
Local Logging: disabled    USB Logging: disabled
Email Logging: disabled    Log to: upper slot
Byte Threshold: 100        Max number of files: 10
Email Delay: 60  seconds   Max size of files: 2048
Restart Delay: 60  seconds
Email To: <none>
Email Subject: Port %d Logging
Email String: <none>
NFS File Logging: disabled
Directory to log to: <none>
Max number of files: 10
Max size of files: 2048
```

2. Change the baud to 57600 and disable flow control:

```
[SLC]> set deviceport port 2 baud 57600 flowcontrol none
Device Port settings successfully updated.
```

3. Connect to the device port:

```
[SLC]> connect direct deviceport 2
```

4. View messages from the server console:

```
Mar 15 09:09:44 tssf280r sendmail[292]: [ID 702911 mail.info] starting
daemon (8.12.2+Sun): SMTP+queueing@00:15:00
Mar 15 09:09:44 tssf280r sendmail[293]: [ID 702911 mail.info] starting
daemon (8.12.2+Sun): queueing@00:15:00
Mar 15 14:44:40 tssf280r sendmail[275]: [ID 702911 mail.info] starting
daemon (8.12.2+Sun): SMTP+queueing@00:15:00
Mar 15 14:44:40 tssf280r sendmail[276]: [ID 702911 mail.info] starting
daemon (8.12.2+Sun): queueing@00:15:00
```

5. Reboot the server:

```
Reboot
```

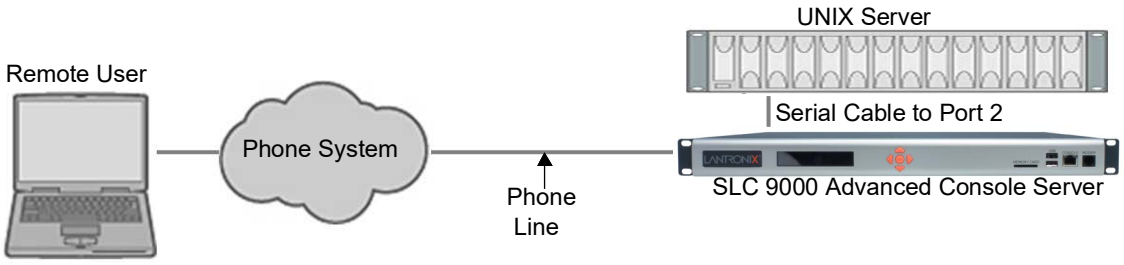
```
<shutdown messages>
```

6. Use the escape sequence to escape from direct mode back to the command line interface.

Dial-in (Text Mode) to a Remote Device

This example shows a phone line connection to the internal modem of the SLC, and a UNIX server connected to a device port. 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 UNIX server.

Figure 17-3 Dial-in (Text Mode) to a Remote Device



In this example, the sysadmin would:

1. Configure the device port that the modem is connected to for dial-in:

```
[SLC]> set deviceport port 1 modemmode text
Device Port settings successfully updated.
[SLC]> set deviceport port 1 initscript "AT&F&K3&C1&D2%C0A"
Device Port settings successfully updated.
[SLC]> set deviceport port 1 auth pap
Device Port settings successfully updated.
[SLC]> set deviceport port 1 localsecret "password"
Device Port settings successfully updated.
[SLC]> set deviceport port 1 modemstate dialin
Device Port settings successfully updated.
[SLC]>
```

2. Configure the device port that is connected to the console port of the UNIX server:

```
[SLC]> set deviceport port 2 baud 57600 flowcontrol none
Device Port settings successfully updated.
```

3. Dial into the SLC 9000 advanced console server via the modem using a terminal emulation program on a remote PC. A command line prompt displays.

4. Log into the SLC unit.

```
CONNECT 57600
Welcome to the SLC9000 Advanced Console Manager
login: sysadmin
Password:
Welcome to the Lantronix SLC9000 Advanced Console Manager
Model Number: SLC9016-16U-16E
Percepxion: registered to cloud: mach10-dev-01.lantronix.com
For a list of commands, type 'help'.
```

```
[SLC]>
```

5. Connect to the UNIX server using the direct command.

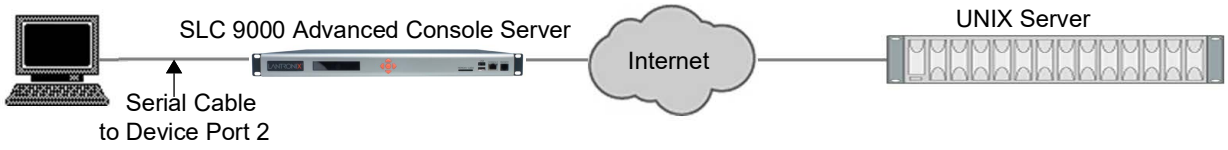
```
[SLC]> connect direct deviceport 2
SunOS 5.7
login: frank
Password:
Last login: Wed Jul 14 16:07:49 from computer
Sun Microsystems Inc.SunOS 5.7Generic October 1998
SunOS computer 5.7 Generic_123485-05 sun4m sparc SUNW,SPARCstation-20
$
```

6. Use the escape sequence to escape from direct mode back to the command line interface.

Local Serial Connection to Network Device via Telnet

This example shows a terminal device connected to an SLC device port, and a UNIXserver connected over the network to the SLC unit. When a connection is established between the device port and an outbound Telnet session, users can access the UNIX server as though they were directly connected to it. (See *14: Connections on page 264*).

Figure 17-4 Local Serial Connection to Network Device via Telnet



In this example, the sysadmin would:

1. Display the current settings for device port 2:

```
[SLC]> show deviceport port 2
___Current Device Port
Settings_____________________________________________________
Number: 2  Name: Port-2
Modem Settings-------------Data Settings-----------IP Settings-------
Modem State: disabled      Baud Rate: 9600         Telnet: disabled
Modem Mode: text           Data Bits: 8            Telnet Port: 2002
Timeout Logins: disabled   Stop Bits: 1            SSH: disabled
Local IP: negotiate        Parity: none            SSH Port: 3002
Remote IP: negotiate       Flow Control: xon/xoff  IP: <none>
Authentication: PAP        Logins: disabled
CHAP Host: <none>          Break Sequence: \x1bB
CHAP Secret: <none>        Check DSR: disabled
NAT: disabled              Close DSR: disabled
Dial-out Login: <none>
Dial-out Password: <none>
Dial-out Number: <none>
Dial-back Number: usernumber
Initialization Script: <none>
```

```
Logging Settings-----------------------------------------------------
Local Logging: disabled    USB Logging: disabled
Email Logging: disabled    Log to: upper slot
Byte Threshold: 100        Max number of files: 10
Email Delay: 60  seconds   Max size of files: 2048
Restart Delay: 60  seconds
Email To: <none>
Email Subject: Port %d Logging
Email String: <none>
NFS File Logging: disabled
Directory to log to: <none>
Max number of files: 10
Max size of files: 2048
```

2. Change the serial settings to match the serial settings for the vt100 terminal - changes baud to 57600 and disables flow control:

```
[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. (The IP address of the server is 192.168.1.1):

```
[SLC]> connect bidirection 2 telnet 192.168.1.1
Connection settings successfully updated.
```

4. At the VT100 terminal, hit <return> a couple of times. The Telnet prompt from the server displays:

```
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.

Sun OS 8.0
login:
```

At this point, a user can log in and interact with the UNIX server at the VT100 terminal as if directly connected to the server.

18: Command Reference

After an introduction to using commands, this chapter lists and describes all of the commands available on the SLC command line interface accessed through Telnet, SSH, or a serial connection. The commands are in alphabetical order by category.

Introduction to Commands

Following is some information about command syntax, command line help, and tips for using commands.

Command

Syntax

Commands have the following format:

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

where

```
<action> is set, show, connect, admin, diag, 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:
```

`<parameter name> <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.
`<parameter name> <Value>`	User must specify an appropriate value, for example, an IP address. The parameter values are in mixed case. Square brackets [ ] indicate optional parameters.

Table 18-1 Actions and Category Options

Action	Category
set	accesslist|auth|cellular|cli|command|consoleport|container|datetime|deviceport|dhcp|groups|history|hostlist|ipfilter|ldap|localusers|log|managed|menu|network|nfs|ntp|password|perfmon|power|px|radius|remoteusers|routing|rpm|script|security|services|site|slcnetwork|snmp|sshkey|switch|tacacs+|temperature|usb|virtual|vpn|xmodem
show	accesslist|auth|auditlog|cellular|cli|connections|consoleport|datetime|deviceport|dhcp|emaillog|groups|history|hostlist|ipfilter|ldap|localusers|log|managed|menu|network|nfs|ntp|perfmon|portcounters|portstatus|power|px|radius|remoteusers|routing|rpm|script|security|services|site|slcnetwork|sshkey|switch|sysconfig|syslog|sysstatus|tacacs+|temperature|usb|user|virtual|vpn|xmodem
connect	bidirection|direct|forward|global|listen|restart|script|terminate|unidirection

Action	Category
diag	arp|arp6|dmesg|ethtools|internals|iperf|lookup|loopback|netstat|nettrace|perfstat|ping|ping6|sendpacket|speedtest|top|traceroute|usb
admin	banner|clear|config|events|feature|firmware|ftp|quicksetup|reboot|shutdown|site|sysinfo|version|web
logout	Terminates CLI session.

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 release notes for the current firmware release, type:

```
help release
```

For more information about a specific command, type help followed by the command, for example:

`help set network` or `help admin firmware`

Tips

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

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

  to

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

- Use the Tab key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** either to complete the name if only one is possible, or to display the possible names if more than one is possible. Following a space after the preceding name, Tab displays all possible names.
- Should you make a mistake while typing, backspace by pressing the Backspace key and/or the Delete key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the left and right arrow keys to move within a command.
- Use the up and down arrows to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.
- To clear an IP address, type 0.0.0.0, or to clear a non-IP address value, type CLEAR.

- When the number of lines displayed by a command exceeds the size of the window (the default is 25), the command output is halted until 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.
- Keyboard Shortcuts:

  Control-a: move to the start of the line

  Control-e: move to the end of the line

  Control-b: move back to the start of the current word

  Control-f: move forward to the end of the next word

  Control-u: erase from cursor to the beginning of the line

  Control-k: erase from cursor to end of the line
- Show Commands Output Filtering (grep, with Posix Extended Regex functionality, see https://www.man7.org/linux/man-pages/man7/regex.7.html):

  show <category> <parameters> grepi|grepic|grepe|grepec <Token|RE:Regex Token>

  - grepi - show output containing token (case sensitive)
  - grepic - show output containing token (case insensitive)
  - grepe - show output not containing token (case sensitive)
  - grepec - show output not containing token (case insensitive)

  For example:

  - 'show network all grepi Bytes' displays lines containing the string 'Bytes'
  - 'show network all grepi RE:[0-9]' displays lines containing digits 0-9
  - 'show network all grepi "RE:^Gateway "' displays lines starting with 'Gateway '

Access List Commands

set accesslist add|edit

Syntax

```
set accesslist add|edit <Access List Name> [<parameters>]
```

Parameters

```
name <New Access List Name>
response <hangup|ignore>
```

Description

Configure an access list of phone numbers to be granted access for modem dial-in connections.

Create or edit an access list (when creating a list, the user will be prompted for the list entries):

set accesslist add|edit

Syntax

```
set accesslist add|edit <Access List Name>
               entry <Entry Number> phonenumber <Phone Number>
```

Description

Add a phone number entry to a list or edit an existing entry:

set accesslist delete

Syntax

```
set accesslist delete <Access List Name> [entry <Entry Number>]
```

Description

Delete an access list, or a single phone number entry from an access list:

show accesslist

Syntax

show accesslist <all|names|Access List Name>

Description

Show access list settings.

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 logout0

Syntax

```
admin banner logout <Banner Text>
```

Description

Configures the banner displayed after the user logs out.

Note: *To go to the next line, type* ***\n*** *and press* ***Enter****.*

admin banner show

Syntax

```
admin banner show
```

Description

Displays the welcome, SSH, 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 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 <resource_name>
```

Description

Resets various system resources. For example,

To clear the directory holding temporary files:

```
admin clear tmpdir
```

To remove the SSH Known Hosts Keys:

```
admin clear sshknownhosts
```

To clear the dmesg kernel log buffer:

```
admin clear dmesg
```

admin config copy

Syntax

```
admin config copy <current|Config Name>
             [location <local|nfs|usb|>
             [nfsdir <NFS Mounted Directory>] [usbport <U1|U2>] ]
```

Description

Copies the current configuration (or optionally, a configuration from another location) to the other bank (for dual-boot SLCs).

admin config rename|delete

Syntax

```
admin config rename|delete <Config Name>
             location <local|nfs|usb>
             [nfsdir <NFS Mounted Directory>][usbport <U1|U2>]
```

Description

Deletes or renames a configuration.

admin config factorydefaults

Warning: ***This command permanently erases all configuration.***

Syntax

```
admin config factorydefaults [savesshkeys <enable|disable>]
           [savesslcert <enable|disable>][savescripts <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
`dp`	Device Ports
`ra`	Remote Authentication
`ub`	USB Port
`po`	Power outlets

Description

Restores the SLC unit to factory default settings.

Note: *A reboot will automatically be done after a successful config restore or factorydefaults.*

admin config restore

Syntax

```
admin config restore <Config Name>
            location <local|ftp|sftp|nfs|usb>
            [nfsdir <NFS Mounted Directory>] [usbport <U1|U2>]
            [preserveconfig <Config Params to Preserve>]
            [savesshkeys <enable|disable>][savesslcert <enable|disable>]
            [savescripts <enable|disable>]
            [onetimepassword <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 Port
`po`	Power Outlets

Description

Restores a saved configuration to the SLC 9000 advanced console server.

Note: *A reboot will automatically be done after a successful config restore or factorydefaults.*

admin config save

Syntax

```
admin config save <Config Name>
            location <local|ftp|sftp|nfs|usb>
            [nfsdir <NFS Mounted Dir>] [usbport <U1|U2>]
            [savesshkeys <enable|disable>][savesslcert <enable|disable>]
            [savescripts <enable|disable>]
            [onetimepassword <enable|disable>]
```

Description

Saves the current SLC configuration to a selected location.

admin config checksum

Syntax

```
admin config checksum
```

Description

Displays a checksum for the current configuration.

admin config commands

Syntax

```
admin config commands <sftp|scp|usb|copypaste>
             [escapechar <enable|disable>][host <IP Address or Name>]
             [login <User Login>][path <Directory>]
             [file <CLI Commands Filename>][usbport <U1|U2>]
```

Note: *The "admin config commands" will output passwords in cleartext.*

Note: *The 'escapechar' option will prepend every "\" in the output with a "\".*

Description

Exports the current configuration as a text file containing CLI commands. The file can be saved as a backup, optionally modified, and restored to the SLC.

admin config batch

Syntax

```
admin config batch <sftp|scp|usb|copypaste>
```

```
            [escapechar <enable|disable>][host <IP Address or Name>]
            [login <User Login>][path <Directory>]
            [file <CLI Commands Filename>] [usbport <U1|U2>]
```

Note: *The 'escapechar' option will remove the prepended '\' in the input, before running the CLI command.*

Description

Imports a previously saved configuration text file containing CLI commands and applies it to the SLC.

admin config show

Syntax

```
admin config show <local|ftp|sftp|nfs|usb>
            [nfsdir <NFS Mounted Dir>] [usbport <U1|U2>]
            [sort <filename|date]
```

Description

Lists the configurations saved to a location.

admin firmware update

Syntax

```
admin firmware update <ftp|tftp|sftp|nfs|usb>
              file <Firmware File> key <Checksum Key>
              [nfsdir <NFS Mounted Dir>] [usbport <U1|U2>]
              [onetimepassword <enable|disable>]
              [verbose <enable|disable>]
Note: the verbose flag will enable debug output for sftp and ftp.
```

Description

Updates SLC firmware to a new revision.

You should be able to access the firmware file using the settings `admin ftp show` displays if FTP, TFTP or SFTP are used to load the firmware file. The SLC 9000 advanced console server automatically reboots after successful update.

admin firmware bootbank

Syntax

```
admin firmware bootbank <1|2>
```

Description

Sets the boot bank to be used at the next SLC reboot.

admin firmware show

Syntax

```
admin firmware show [viewlog <enable|disable>][ztplog <enable|disable>]
```

Description

Lists the current firmware revision, the boot bank status, and optionally displays the log containing details about ZTP and Bootstrap onboarding and firmware updates:

admin firmware clearlog

Syntax

```
admin firmware clearlog
```

Description

Clears the firmware update log.

admin firmware bootcount

Syntax

```
admin firmware bootcount <0|1>
```

Description

Configures bootcount parameter that control how many times the SLC has failed to boot. If this value reaches Boot Limit, the SLC will switch to the alternate boot bank. The SLC will switch to the alternate boot bank only once. For example, if it fails to boot Boot Limit times on bank 1, it will automatically switch to bank 2; if it fails to boot Boot Limit times on bank 2, it will enter advanced recovery mode. If Boot Count has reached Boot Limit, setting this value to 0 will enable the SLC to boot again. Default is 0, range is 0 - 1.

admin firmware bootlimit

Syntax

```
admin firmware bootlimit <3-20>
```

Description

Configures bootlimit parameters that control how many times the SLC will fail to boot before switching to the alternate boot bank. After the SLC fails to boot 2 times Boot limit (so it has attempted to boot Boot Limit times on each bank), the SLC will go into advanced recovery mode, which may require support from Technical Support to resolve so that the SLC can be booted again. Default is 3 boots, range is 3 - 20.

admin firmware bootdelay

Syntax

```
admin firmware bootdelay <3-1800>
```

Description

Configures bootcount parameters that control how seconds the bootloader pauses before booting the SLC. The default is 3 seconds and the range is between 3 and 1800 seconds.

admin firmware highrestimers

Syntax

```
admin firmware highrestimers <enable|disable>
```

Description

Enables high resolution timers required for Performance Monitoring or disables high resolution timers (the default). Changing this setting requires a reboot in order for the change to take effect.

admin firmware uniquepassword

Syntax

```
admin firmware uniquepassword <enable|disable>
```

Description

Enables or disables default sysadmin password that is unique to each device.

admin firmware watchdog

Syntax

```
admin firmware watchdog <disable|180-1800 seconds>
```

Description

Configures how long the SLC waits for boot completion before forcing a reboot.

admin firmware panicreboot

Syntax

```
admin firmware panicreboot <enable|disable>
```

Description

Enables auto-reboot on a kernel panic.

admin firmware hwwatchdog

Syntax

```
admin firmware hwwatchdog <enable|disable>
```

Description

Enables SLC Hardware Watchdog.

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 Hostname> [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 memory show

Syntax

```
admin memory show
```

Description

Displays information about SLC memory usage.

admin memory swap add

Syntax

```
admin memory swap add <Size of Swap in MB> usbport <U1|U2>
```

Description

Creates a swap space from an external storage device.

admin memory swap delete

Syntax

```
admin memory swap delete
```

Description

Deletes the swap space from an external storage device.

admin quicksetup

Syntax

```
admin quicksetup
```

Description

Runs the quick setup script.

admin reboot

Syntax

```
admin reboot
```

Description

Immediately terminates all connections and reboots the SLC 9000 advanced console server.

admin shutdown

Syntax

```
admin shutdown
```

Description

Prepares the SLC 9000 advanced console server to be powered off.

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>
```

```
admin site tag <Site Description>
admin site show
```

Description

Configures information about the site where the SLC 9000 advanced console server is located.

admin sysinfo

Syntax

```
admin sysinfo save <ZIP File Name> location
              <local|ftp|sftp|scp|nfs|usb>
              [nfsdir <NFS Mounted Directory>] [usbport <U1|U2>]
              [host <IP Address or Name>] [login <User Login>]
              [path <Path to Save File>]
              [comment <Comment Included in the System Info File>]
              [auto <enable|disable>]
```

Note: *The 'auto' option includes the logs, does not prompt for an encryption password for the sysinfo file, and appends a date-time stamp to the filename; this supports automating sysinfo generation from a CLI btach script.*

Example:

A script that saves a sysinfo file every 60 seconds.

```
[slc]> show script type batch name auto_sysinfo
  ___Batch Script
'auto_sysinfo'_____________________________________________________
  Group/Perms: Adm/
ad,nt,sv,dt,lu,ra,um,dp,ub,rs,fc,dr,sn,wb,sk,do,sd,md,rp,di
  set cnt 5
  while { $cnt >= 1 } {
      admin sysinfo save SLCsysinfo location usb auto enable
      sleep 60
      set cnt [expr $cnt - 1]
  }
```

Note: *For ftp and sftp, the host login and path parameters may be omitted and the parameters set via 'admin ftp server' (including the password) can be used.*

Description

Saves the current SLC system info to a selected location in ZIP format.

admin sysinfo save

Syntax

```
admin sysinfo periodicsave <enable|disable> frequency <1-999> hours
```

Description

Configure if SLC system info is saved periodically and how often it is saved; the 4 most recent sysinfo files are retained, older files are pruned (any extra sysinfo save parameters are ignored):

admin version

Syntax

```
admin version
```

Description

Displays current hardware and firmware information.

admin web certificate import

Syntax

```
admin web certificate import via <sftp|scp> [rootfile <Cert Auth File>]
     certfile <Certificate File> privfile <Private Key File>
     host <IP Address or Name> login <User Login> [path <Path to Files>]
```

Description

Imports an SSL certificate.

admin web certificate reset

Syntax

```
admin web certificate reset
```

Description

Resets the web server to the default SSL certificate.

admin web certificate custom

Syntax

```
admin web certificate custom
```

Description

Generates a custom self-signed SSL certificate. The SHA256 hashing algorithm will be used to generate the certificate.

admin web certificate show

Syntax

```
admin web certificate show
```

Description

Displays the web server SSL certificate.

admin web group

Syntax

```
admin web group <Local or Remote Group Name>
```

Description

Configures the group that can access the web.

admin web server

Syntax

```
admin web server <enable|disable>
```

Description

Enables or disables running the web server (TCP ports 80 and 443).

admin web sha2

Syntax

```
admin web sha2 <enable|disable>
```

Description

Enables using only SHA2 and higher ciphers.

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. Use 'admin web show' to view the current sessions and their ID.

admin web show

Syntax

```
admin web show [viewcipherlist <enable|disable>]
```

Description

Displays the current sessions, with optional extra sessions or current ciphers.

admin web banner

Syntax

```
admin web banner
```

Description

Configures the banner displayed on the web home page.

admin web iface

Syntax

```
admin web iface <none,eth1,eth2,eth3,eth4,veth1,veth2,ppp>
```

Description

Defines a list of network interfaces the web is available on.

admin web ciphers

Syntax

```
admin web ciphers <prompt|Comma Separated List of Disabled Ciphers>
```

Description

Defines the set of TLS ciphers that are enabled, either by prompting for each cipher or by specifying a complete list of disabled ciphers.

admin web tlsv10

Syntax

```
admin web tlsv10 <enable|disable>
```

Description

Enables or disables TLS v1.0.

admin web tlsv11

Syntax

```
admin web tlsv11 <enable|disable>
```

Description

Enables or disables TLS v1.1.

admin web tlsv12

Syntax

```
admin web tlsv12 <enable|disable>
```

Description

Enables or disables TLS v1.2.

admin web restart

Syntax

```
admin web restart
```

Description

Restarts the web server.

Warning: ***The following admin chip commands should only be used under the direction of Lantronix Technical Support.***

admin chip resetmodem

Description

Resets the internal modem chip in key system chips.

Syntax

```
admin chip resetmodem
admin chip reseti2cmux
```

Description

Resets the I2C Mux chip in key system chips.

Syntax

```
admin chip reseti2cmux
admin chip resetsfp ethport <1|2>
```

Description

Resets the SFP chip in key system chips.

Syntax

```
admin chip resetsfp ethport <1|2>
```

Warning: ***The following admin eeprom command should only be used under the direction of Lantronix Technical Support.***

admin eeprom

Syntax

```
admin eeprom slot <integer> [id <string> | mac <mac addr>]
```

Parameters

```
slot:
       1 for first slot
       2 for second slot
       3 for third slot
id:
       "16SPE" for 16 Port Exar RJ45 FRU
       "16SPF" for 16 Port Exar RJ45 Reverse Pinout FRU
       "16UBB" for 16 Port Etron USB FRU
       "16UBC" for 16 Port Renesas USB FRU
       "16ESB" for 16 Port Ethernet Switch FRU
```

Description

Show/Update EEPROM ID of the attached FRU.

Audit Log Commands

show auditlog

Syntax

```
show auditlog <parameters>
```

Parameters

```
sort <date|command|user>
display <head|tail> [numlines <Number of Lines>]
starttime <MMDDYYhhmm[ss]>
endtime <MMDDYYhhmm[ss]>
email <Email Address>
Defaults:    sort=date, numlines=40
```

Note: *Display and time parameters cannot be used simultaneously.*

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.

`show auditlog clear`

Syntax

```
show auditlog clear
```

Description

Clears the auditlogs.

Authentication Commands

`set auth`

Syntax

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

Parameters

```
authusenextmethod <enable|disable>
ldap <1-6>
localusers <1-6>
radius <1-6>
tacacs+ <1-6>
```

Description

Sets ordering of authentication methods.

Local user accounts (including sysadmin) are always checked first regardless of configured order. Remote methods are tried in sequence if local authentication fails. 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.

LDAP Commands

set ldap

Syntax

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

Parameters

```
state <enable|disable>
server1 <IP Address or Name>
server2 <IP Address or Name>
port <TCP Port>
base <LDAP Base>
bindname <Bind Name>
bindwithlogin <enable|disable>
useldapschema <enable|disable>
adsupport <enable|disable>
filteruser <User Login Attribute>
filtergroup <Group Objectclass>
grmemberattr <Group Membership Attribute>
grmembervalue <dn|name>
encrypt <starttls|ssl|disable>
dataports <Port List>
listenports <Port List>
clearports <Port List>
escapeseq <1-10 Chars>
breakseq <1-10 Chars>
custommenu <Menu Name>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
group <default|power|admin>
permissions <Permission List>
```

Note: *See User Permissions Commands (on page 376) for information on groups and user rights.*

Description

Configures the SLC 9000 advanced console server to use LDAP to authenticate users who log in via the Web, SSH, Telnet, or the console port.

set ldap bindpassword

Description

Set the LDAP bind password.

Syntax

```
set ldap bindpassword
```

set ldap certificate import

Description

To upload X.509/PEM certificate for Start TLS encrypted connections:

Syntax

```
set ldap certificate import via <sftp|scp> rootfile <Cert Auth File>
      certfile <Certificate File> keyfile <Key File>
      host <IP Address or Name> login <User Login> [path <Path to Files>]
```

set ldap certificate delete

Description

To delete an LDAP certificate.

Syntax

```
set ldap certificate delete
```

show ldap

Syntax

```
show ldap
```

Description

Displays LDAP settings.

Local Users Commands

set localusers add|edit

Syntax

```
set localusers add|edit <User Login> <one or more parameters>
```

Parameters

```
allowdialback <enable|disable>
breakseq <1-10 Chars>
changenextlogin <enable|disable>
changepassword <enable|disable>
clearports <Port List>
dataports <Port List>
dialbacknumber <Phone Number>
displaymenu <enable|disable>
escapeseq <1-10 Chars>
listenports <Port List>
custommenu <Menu Name>
uid <User Identifier>
group <default|power|admin|Custom Group Name>
passwordexpires <enable|disable>
permissions <Permission List>
```

Note: *See User Permissions Commands (on page 376) for information on groups and user rights. Remove Escape & Break Sequences for users making raw binary connections to Device Ports.*

Description

Configures local accounts (including sysadmin) who log in to the SLC 9000 advanced console server by means of the Web, SSH, Telnet, or the console port.

set localusers allowreuse

Syntax

```
set localusers allowreuse <enable|disable>
```

Description

Sets whether a login password can be reused.

set local users complexpasswords

Syntax

```
set localusers complexpasswords <enable|disable>
```

Description

Sets whether a complex login password is required. Complex passwords require at least one uppercase character, one lowercase character, one digit, and one non-alphanumeric character.

set localusers state

Syntax

```
set localusers state <enable|disable>
```

Description

Enables or disables authentication of local users.

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 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 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 multipleadminlogins

Syntax

```
set localusers multipleadminlogins <enable|disable>
```

Description

Allows multiple admin logins among local users to the web server.

set localusers consoleonlyadmin

Syntax

```
set localusers consoleonlyadmin <enable|disable>
```

Description

Sets local users. to console only admin setting. If enabled, the admin user can only log into the SLC via the console, and will be prevented from logging in via the web, SSH or Telnet.

show localusers

Syntax

```
show localusers [display <brief|extended>] [user <User Login>]
```

Description

Displays local users.

set localusers lock

Syntax

```
set localusers lock <User Login>
```

Description

Blocks (locks) a user's ability to login.

set localusers unlock

Syntax

```
set localusers unlock <User Login>
```

Description

Allows (unlocks) a user's ability to login.

set localusers permissions

Syntax

```
set localusers add|edit <user> permissions <Permission List>
```

where

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

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

Description

Sets a local user's permissions (not defined by the user group).

RADIUS Commands

set radius

Syntax

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

Parameters

`state <enable|`**`disable`**`>`
`allowdialback <enable|disable>`

```
clearports <Port List>
custommenu <Menu Name>
dataports <Port List>
dialbacknumber <Phone Number>
breakseq <1-10 Chars>
escapeseq <1-10 Chars>
group <default|power|admin>
listenports <Port List>
permissions <Permission List>
```

Note: *See User Permissions Commands on page 376 for information on groups and user rights.*

```
timeout <enable|3-60>
```

Note: *Sets the number of seconds after which the connection attempt times out. It may be 3-60 seconds.*

Description

Configures the SLC 9000 advanced console server 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(s), the text secret, and the number of the TCP port on the RADIUS server.

Note: *The default port is 1812.*

show radius

Syntax

```
show radius
```

Description

```
Displays RADIUS settings.
```

TACACS+ Commands

set tacacs+

Syntax

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

Parameters

```
state <enable|disable>
server1 <IP Address or Name>
server2 <IP Address or Name>
server3 <IP Address or Name>
port <TCP Port>
encrypt <enable|disable>
authservice <login|pap|chap>
service <Service to Authorize>
protocol <Protocol for Service>
timeout <1-10 seconds>
srcipaddr <none|eth1|eth2|veth1|veth2>
srcipv6addr <none|eth1|eth2|veth1|veth2>
dataports <Port List>
listenports <Port List>
clearports <Port List>
escapeseq <1-10 Chars>
breakseq <1-10 Chars>
custommenu <Menu Name>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
group <default|power|admin>
permissions <Permission List>
```

Note: *See User Permissions Commands (on page 376) for information on groups and user rights.*

Set the TACACS+ secret (any extra parameters will be ignored):

```
set tacacs+ secret
```

Description

Configures the SLC 9000 advanced console server 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.

User Permissions Commands

set localusers group

Syntax

```
set localusers add|edit <user> group <default|power|admin|custom group name>
```

Description

Adds a local user to a user group or changes the group the user belongs to.

set localusers lock

Syntax

```
set localusers lock <User Login>
```

Description

Blocks (locks) a user's ability to login.

set localusers unlock

Syntax

```
set local users unlock <User Login>
```

Description

Allows (unlocks) a user's ability to login.

set localusers permissions

Syntax

```
set localusers add|edit <user> permissions <Permission List>
```

where

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

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

Description

Sets a local user's permissions (not defined by the user group).

set <ldap|radius|tacacs+> permissions

Syntax

```
set <ldap|radius|tacacs> permissions <Permission List>
```

where

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

Description

Sets permissions not already defined by the assigned permissions group.

show user

Syntax

```
show user
```

Description

Displays the rights of the currently logged-in user.

Remote User Commands

set remoteusers add|edit

Syntax

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

Parameters

```
dataports <Port List>
breakseq <1-10 Chars>
escapeseq <1-10 Chars>
listenports <Port List>
clearports <Port List>
custommenu <Menu Name>
displaymenu <enable|disable>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
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, do,
ub, rp, rs, rc, dr, wb, sn, ad, md
```

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

Note: *See 'help user permissions' for information on groups and user rights.*

Description

Sets attributes for users who log in by a remote authentication method. Access to authenticated remote users whose LDAP group or TACACS+ priv_lvl map to a Local Manager custom group.

set remoteusers listonlyauth

Syntax

```
set remoteusers listonlyauth <enable|disable>
```

Description

Configure whether remote users who are not part of the remote user list will be authenticated.

set remoteusers denyaccessnocustomgroup

Syntax

```
set remoteusers denyaccessnocustomgroup <enable|disable>
```

Description

Access to authenticated remote users whose LDAP group or TACACS+ priv_lvl map to a Local Manager custom group:.

set remoteusers lock|unlock

Syntax

```
set remoteusers lock|unlock <User Login>
```

Description

Allow (unlock) or block (lock) a user's ability to login.

set remoteusers delete

Syntax

```
set remoteusers delete <User Login>
```

Description

Removes a remote user.

show remoteusers

Syntax

```
show remoteusers [display <brief|extended>] [user <User Login>]
```

Description

Displays settings for all remote users.

set <ldap|radius|tacacs+> group

Syntax

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

Description

Sets a permission group for remotely authorized users.

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

Configures the current command line session. Allows you to use SCS-compatible commands as shortcuts for executing commands. It is disabled by default.

Note: *Settings are retained between CLI sessions for local users and users listed in the remote users list.*

set cli terminallines

Syntax

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

Description

Sets the number of lines in the terminal for paging through text one screenful at a time, if the size of the terminal cannot be automatically detected.

set cli allusers

Syntax

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

Description

Globally enable or disable the terminallines feature for all users.

Note: *Only sysadmin users or users with full administrative rights can modify the allusers parameter.*

set cli menu

Syntax

```
set cli menu <start|Menu Name>
```

Description

If a menu is associated with the current user and the menu was not displayed at login, 'start' will run the menu. Users with full administrative or menu user rights can also specify the name of any menu to run.

Note: *Settings are retained between CLI sessions for local users and users listed in the remote users list.*

show cli

Syntax

```
show cli
```

Description

Displays current CLI settings.

show user

Syntax

```
show user
```

Description

Displays attributes of the currently logged in user.

set history

Syntax

```
set history clear
```

Description

Clears the commands that have been entered during the command line interface session.

show history

Syntax

```
show history
```

Description

Displays the last 100 commands entered during the session.

Cellular Modem Commands

set cellular

Syntax

```
set cellular <parameters>
Parameters: state <dhcp|disable>
            apn <APN of Mobile Carrier>
            apnauto <enable|disable>
            preferrednet <AUTO|4G|3G>
            band <Frequency Band>
            roam <enable|disable>
            carrier <Cellular Carrier Name>
            cellauth <none|pap|chap>
            celluser <Cellular Carrier Username>
            simlock <enable|disable>
            ipv6 <enable|disable>
            mtu <Maximum Transmission Unit>
Note: if apnauto is enabled, any predefined APN will be cleared and any
APN set with the 'apn' parameter will be overridden; the SLC will try to
perform the initial LTE connection without an APN.

Note: Configure band as 'AUTO' to reset band settings. Refer to 'show
cellular status' to see supported band values.

set cellular simpin
set cellular factoryreset
set cellular reboot
set cellular cellpass
set cellular admin <Cellular Modem Admin Username>
set cellular adminpw
set cellular dpass
set cellular px <enable|disable>
```

Description

Configure cellular modem. Transfer file to initiate a firmware update on the cellular modem.

Note: *If apnauto is enabled, any predefined APN will be cleared and any APN set with the 'apn' parameter will be overridden; the LM will try to perform the initial LTE connection without an APN.*

Note: *Configure band as 'Auto' to reset band settings. Refer to 'show cellular detail' to see supported band values.*

set cellular update

Syntax

```
set cellular update <ftp|sftp|scp|usb> fwfile <Firmware File (.star)>
            [host <IP Address or Name>] [login <User Login>] [path <File
Path>]
```

Description

Transfer file to initiate a firmware update on the cellular modem:

show cellular

Syntax

```
show cellular [basic|config|status]
```

Description

Displays cellular modem configuration and status.

Connection Commands

connect bidirection

Syntax

```
connect bidirection <Port # or Name> <endpoint> <one or more Parameters>
```

Parameters

```
Endpoint is one of:
charcount <# of Chars>
charseq <Char Sequence>
charxfer <toendpoint|fromendpoint>
date <MMDDYYhhmm[ss]>
deviceport <Device 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>
```

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.

```
udp <IP Address> [port <UDP Port>]
```

Description

Connects a device port to another device port or an outbound network connection (data flows in both directions).

connect direct

Syntax

```
connect direct <endpoint>
```

Parameters

```
<endpoint> is one of:
           deviceport <Device Port # or Name | U1 | U2>
           telnet <IP Address or Name> [port <TCP Port>]
           ssh <IPv4/IPv6 Address or Name> [port <TCP Port>][<SSH flags>]
           tcp <IP Address> port <TCP Port>
           udp <IP Address> port <UDP Port>
           hostlist <Host List>
<SSH flags> are:
            user <Login Name>
            iface <eth1|eth2|veth1|veth2|eth1v6|eth2v6|veth1v6|veth2v6>
            command <Command to Execute>
```

Description

Connects to a device port to monitor and/or interact with it, or establishes an outbound network connection.

connect forward

Syntax

```
connect forward iface <eth1|eth2> inport <TCP Port>
                ipaddr <IP Address> outport <TCP Port>
```

Description

Configures a port on Eth1 or Eth2 to listen for incoming connections and redirect traffic to an IP address:Port on the Ethernet switch or local subnet.

Note: *This requires that SSH logins to the CLI be enabled.*

connect global outgoingtimeout

Syntax

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

Description

Sets the amount of time the SLC 9000 advanced console server will wait for a response (sign of life) from an SSH/Telnet server that it is trying to connect to.

Note: *This is not a TCP timeout.*

connect listen deviceport

Syntax

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

Description

Monitors a device port.

connect terminate

Syntax

```
connect terminate <Connection ID>
```

Description

Terminates a connection.

connect unidirection

Syntax

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

Parameters

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>
```

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.

```
udp <IP Address> [port <UDP Port>]
```

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

```
access <enable|disable>
mode <dce|dte|auto>
baud <300-115200>
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>
```

Description

Configures console port settings.

show consoleport

Syntax

```
show consoleport
```

Description

Displays console port settings.

Container Commands

Provides support for Docker containers to run pre-built applications on the SLC. Images can be pulled from public repositories, and one or more container instances of the image can be run. It is recommended that only trusted containers be downloaded to the SLC.

For more information, see *Chapter 12: Containers (Docker) on page 245*.

set container state

Syntax

```
set container state <enable|disable>
```

Description

Enable or disable the use of containers:

set container pull

Syntax

```
set container pull <Image Name>
              [platform <Platform Name (ex: 'os/architecture[/
variant]')>]
              [tagname <Name of a Tag>]
```

Description

Download an image from a registry to the SLC:

set container run

Syntax

```
set container run <Image Name> <one or more parameters>
```

Parameters

```
             name <Container Name>
             [detachmode <enable|disable>]
             [port <Port Number>]
             [interactive <enable|disable>] [tty <enable|disable>]
             [network <none|bridge>]
             [hostname <Container Host Name>]
             [readonly <enable|disable>]
             [user <User Name or UID> (format: <name|uid>[:<group|gid>])]
             [otheropts <Options String>]
Note: Append any custom or missing arguments into 'otheropts'.
```

Description

Run an image, to create a container:

set container containerstate

Syntax

```
set container containerstate <Container Name>
              action <start|stop|restart|pause|unpause|delete>
```

Description

Set a container state with start, stop, restart, pause, unpause and delete:

set container delete

Syntax

```
set container delete <Image Name>
```

Description

Delete a container image:

show container search

Syntax

```
show container search <Search String> [official <enable|disable>]
               [limit <Number of Entries>] [stars <Number of Stars>]
```

Description

Search Docker hub or an alternate registry for external images:

show container status

Syntax

```
show container status [ancestor <Image Name|all>] [lastcreated <1-15>]
           [display <created|restarting|running|removing|paused|exited>]
```

Description

Display the running status of one or all containers:

show container

Syntax

```
show container [display <containers|images>] [otheropts <options
string>]
```

Description

Display information for images and containers:

Custom User Menu Commands

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 localusers

Syntax

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

Syntax

```
set menu edit <Menu Name> <parameter>
```

Parameters

```
command <Command Number>
nickname <Command Number>
redisplaymenu <enable|disable>
shownicknames <enable|disable>
title <Menu Title>
```

Description

Changes a command within an existing custom user menu. Changes a nickname within an existing custom user menu. Enables or disables the redisplay of the menu before each prompt. Enables or disables the display of command nicknames instead of commands. 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.

set <ldap|radius|tacacs+> custommenu

Syntax

```
set <ldap|radius|tacacs> custommenu <Menu Name>
```

Description

Assigns a custom menu to users who authenticate via LDAP, Radius, or TACACS+.

set remoteusers add|edit

Syntax

```
set remoteusers add|edit <User Login> custommenu <Menu Name>
```

Description

Sets a default custom menu for remotely authorized users.

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 parameter>
```

Parameters

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

Note: *If you do not know a valid <Time Zone>, enter 'timezone <invalid time zone>' and you will be guided through selecting one from the available time zones.*

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 ntp parameters>
```

Parameters

```
state <enable|disable>
sync <broadcast|poll>
poll <local|public>
localserver1 <IP Address or Hostname>
localserver2 <IP Address or Hostname>
localserver3 <IP Address or Hostname>
localserver4 <IP Address or Hostname>
localserver5 <IP Address or Hostname>
localserver6 <IP Address or Hostname>
publicserver <IP Address or Hostname>
srcipaddr <none|eth1|eth2|veth1|veth2>
srcipv6addr <none|eth1|eth2|veth1|veth2>
```

Description

Synchronizes the SLC 9000 clock with a remote time server using NTP.

set ntp localserverid

Syntax

```
set ntp localserverid <1-6> [keyindex <1-65535>]
        [hash <disable|aes128cmac|ripemd160|sha1|md5>]
```

Description

Configure NTP authentication for local servers 1-6; for each server, configure a key index and the message digest algorithm:

set ntp localserverkey

Syntax

```
set ntp localserverkey <1-6> format <hex|ascii>
```

Description

Configure HEX or ASCII key for NTP authentication for local servers 1-6:

show ntp

Syntax

```
show ntp
```

Description

Displays NTP settings.

The CLI 'show ntp' command and Date and Time web page will display the current NTP status if NTP is enabled. The currently selected peer is marked with a "*", while additional peers designated acceptable for synchronization, but not currently selected, are marked with a "+". Peers marked * and + are included in the weighted average computation to set the local clock; the data produced by peers marked with other symbols are discarded.

For information about the displayed columns, see *Date and Time*.

Device Commands

set command

Syntax

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

Parameters

`sensorsoft lowtemp <Low Temperature>`

Sets the lowest temperature permitted for the port.

`sensorsoft hightemp <High Temperature>`

Sets the hightest temperature permitted for the port.

`sensorsoft lowhumidity <Low Humidity %>`

Sets the lowest humidity pemitted for the port.

`sensorsoft highhumidity <High Humidity %>`

Sets the lowest humidity permitted for the port.

`sensorsoft degrees <celsius|fahrenheit>`

Enables or disables temperature settings as celcius or fahrenheit.

`sensorsoft traps <enable|disable>`

Enables or disables traps when specified conditions are met.

`sensorsoft status`

Displays the status of the port.

`sensorsoft showall`

Displays the status for all connected Sensorsoft devices and ignores the device port\nlist.

Note: *The Sensorsoft lowtemp and hightemp settings are given in the scale specified by the degrees setting.*

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 Sensorsoft devices.*

Device Port Commands

set deviceport global

Syntax

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

Parameters

```
telnetport <TCP Port>
sshport <TCP Port>
tcpport <TCP Port>
autorefreshcounters <enable|disable>
```

Description

Configures settings for all or a group of device ports.

set deviceport port

Description

Sets the dialout password.

Syntax

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

Example: `set deviceport port 2-5,6,12,15-16 baud 2400`

Parameters

```
actiondelay <Action Delay>
actionrestart <Restart Delay>
assertdtr <enable|disable>
auth <pap|chap>
banner <Banner Text>
baud <300-230400>
breakseq <1-10 Chars>
bytethreshold <# of Characters>
calleridcmd <Modem Command String>
calleridlogging <enable| disable>
cbcptype <admin|user>
cbcpnocallback <enable|disable>
chapauth <chaphost|localusers>
```

```
chaphost <CHAP Host or User Name>
checkdsr <enable|disable>
closedsr <enable|disable>
connectedmsg <enable|disable>
databits <7|8>
device <none|sensorsoft|rpm>
detectname <enable|disable>
detecttokens <Name Detection Tokens>
dialbackdelay <PPP Dial-back Delay>
dialbacknumber <usernumber|Phone Number>
dialbackretries <1-10>
dialinlist <Host List for Dial-in>
dialoutlogin <Remote User Login>
dialoutnumber <Phone Number>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
dtrcontrol <none|toggledtr|autodtr>
emailsubj <Email Subject>
emailto <Email Address>
flowcontrol <none|xon/xoff|rts/cts>
group <Local or Remote Group Name>
idletimeoutmsg <enable|disable>
initscript <Modem Initialization Script>
ipaddr <IP Address[/Mask Bits]>
locallogging <enable|disable>
maxdirect <1-15>
localipaddr <negotiate|IP Address>
logins <enable|disable>
minimizelatency <enable|disable>
modemmode <text|ppp>
modemstate <disable|dialin|dialout|dialback|dialinhostlist|dialondemand|
   dialin+ondemand|dialback+ondemand|cbcpclient|cbcpserver>
modemtimeout <disable|1-9999 seconds>
name <Device Port Name>
nat <enable|disable>
newusermsg <enable|disable>
nfsdir <Logging Directory>
nfslogging <enable|disable>
nfsmaxfiles <Max # of Files>
nfsmaxsize <Size in Bytes>
numsessionsmsg <enable|disable>
parity <none|odd|even>
portlogseq <1-10 Chars>
poweraction <on|off|cycle>
powermgmtseq <1-10 Chars>
powersupply <Managed Power Supply Name>
remoteipaddr <negotiate|IP Address>
restartdelay <PPP Restart Delay>
reversepinout<enable|disable>
sendstring <String to Send|QUOTEDSTRING>sendtermstr <enable|disable>
showlines <disable|1-50 lines>
slmlogging <enable|disable>
slmnms <NMS IP Address>
slmthreshold <Threshold>
```

```
slmtime <Time Frame>
sshauth <enable|disable>
sshdatadir <netin|netout|both>
sshin <enable|disable>
sshport <TCP Port>
sshtimeout <disable|1-3600 seconds>
stopbits <1|2>
sysloglogging <enable|disable>
tcpauth <enable|disable>
tcpdatadir <netin|netout|both>
tcpin <enable|disable>
tcpport <TCP Port>
tcptimeout <disable|1-3600 seconds>
telnetauth <enable|disable>
telnetdatadir <netin|netout|both>
telnetin <enable|disable>
telnetport <TCP Port>
telnetsoftiac <enable|disable>
telnettimeout <disable|1-3600 sec>
termstr <Termination String>
timeoutlogins <disable or 1-30 minutes>
tokenaction <List of none,log,trap,email,string,power>
tokendatadetect <enable|disable>
tokenstring <Regex String>
tokentrigger <bytecnt|charstr>
usbchannel <1-2>
usblogging <enable|disable>
usbmaxfiles <Max # of Files>
usbmaxsize <Size in Bytes>
usbport <U1|U2|SD>
usbvbus <enable|disable>
usesites <enable|disable>
viewportlog <enable|disable>
```

Description

Configures a single port or a group of ports.

Set the modem password and CHAP secrets (any extra parameters will be ignored):

```
set deviceport port <Device Port # or List or Name> dialoutpassword
set deviceport port <Device Port # or List or Name> chapsecret
set deviceport port <Device Port # or List or Name> dodchapsecret
```

Configure up to 4 managed power supplies for device connected to a device port:

```
set deviceport port <Device Port # or Name> managepower
```

Reset a device port, terminating and restarting all relevant connections:

```
set deviceport port <Device Port # or List or Name> reset
```

Reset a device port, terminating and restarting all relevant connections:

```
set deviceport port <Device Port # or List or Name> reset
```

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. It is recommended that the 'initscript' be prepended with 'AT' and include 'E1 V1 x4 Q0' so that the SLC may properly control the modem.

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 deviceport types

Syntax

```
show deviceport types
```

Description

Displays the list of port types (RJ45 or USB) for all 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.

DHCP Commands

set dhcp

Syntax

```
set dhcp <switch> <one or more parameters>
```

Parameters

```
mode <disable|server|relay>
ip <Eth Switch Port IP Address>
mask <Eth Switch Port Subnet Mask>
DHCP Server Mode Parameters:
            serverstartip <Server Start IP Address>
            serverendip <Server End IP Address>
            serverprimarydns <Server Primary DNS>
            serversecondarydns <Server Secondary DNS>
            servergw <Server Gateway>
            domain <Domain Name>
            leasetime <1-336 hours>
DHCP Relay Mode Parameters:
            relayserverip1 <DHCP Server IP Address>
            relayserverip2 <DHCP Server IP Address>
```

Description

Configure the DHCP settings for the Ethernet Switch.

show dhcp

Syntax

```
show dhcp
show dhcp display clients
```

Description

Displays the DHCP settings.

Diagnostic Commands

diag arp

Syntax

```
diag arp|arp6 [email <Email Address>]
```

Description

Displays the Address Resolution Protocol table (for IPv4) or the Neighbor table (for IPv6) for mapping IP Addresses to hardware addresses.

diag dmesg

Syntax

```
diag dmesg [email <Email Address>]
```

Description

Displays kernel logs

Note: The output can optionally be emailed, and the log can be cleared with 'admin clear dmesg'.

diag ethtool

Syntax

```
diag ethtool <eth1|eth2|eth3|eth4>
             [display <all|driver|eeprom|features|statistics]
```

Description

Displays Ethernet ethtool information:

diag internals

Syntax

```
diag internals [email <Email Address>]
```

Enable debug printing on the next SLC reboot:

```
diag internals [printapplication <enable|disable>
   printconnection <enable|disable>
   printmanagement <enable|disable>
```

Description

Displays information on the internal memory, storage and processes of the SLC 9000 advanced console server. You can optionally email the displayed information.

diag iperf

Syntax

```
diag iperf mode <server|client> [host <iPerf Server IP Address or Name>]
     [options <iPerf options>] [email <Email Address>]
```

Options

iPerf Options (enclose all options in quotes):

```
Set server port to listen on/connect to (default 5201): -p, --port n
Format to report:                                        -f, --format [kmgtKMGT]
Pause n seconds between reports:                         -i, --interval n
Bind to a host, an interface or multicast address        -B, --bind <host>
More detailed output:                                    -V, --verbose
Output in JSON format:                                   -J, --json
Options below are supported on client only:
Set length of buffer to n (default 8 KB):               -l, --length n[KMG]
Use UDP rather than TCP:                                -u, --udp
TCP window size (socket buffer size):                   -w, --window n[KMG]
Set TCP/SCTP maximum segment size (MTU):                -M, --set-mss n
Set TCP/SCTP no delay, disabling Nagle's Algorithm:     -N, --no-delay
Set bandwidth to n bits/sec (default 1Mbit/sec, unlimited for TCP);
                                                         -b, --bitrate n[KMG]
Number of bytes to transmit (instead of -t):            -n, --bytes n[KMG]
Time in seconds to transmit for (default 10 secs):      -t, --time n
Set the IPv6 flow label:                                -L, --flowlabel n
Use a 'zero copy' method of sending data:               -Z, --zerocopy
Omit the first n seconds:                               -O, --omit n
Prefix every output line with this string:              -T, --title str
# of blocks (packets) to transmit (instead of -t/-n):   -k, --blockcount
Set the IP type of service, 0-255.
The usual prefixes for octal and hex can be used,
i.e. 52, 064 and 0x34 all specify the same value:       -S, --tos n
```

```
Set the IP dscp value, either 0-63 or symbolic:        --dscp n
```

Description

Runs an iPerf server or client to measure network throughput. You can optionally email the output.

The SLC uses iPerf version 3.X, which is incompatible with older versions (2.x).

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>
Defaults: test=external, xferdatasize=1K
```

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 9000 advanced console server. 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. The External test is currently not supported for USB device ports.

diag netstat

Syntax

```
diag netstat [protocol <all|tcp|udp>] [email <Email Address>]
Defaults: protocol=all
```

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>
protocol <tcp|udp|icmp|esp>
host <IP Address or Name>
numpackets <Number of Packets>
verbose <low|medium|high|disable>
pcapfile <File Name> location <usb> [usbport <U1|U2>]
```

Description

Displays all network traffic, applying optional filters (the output can be saved to a Wireshark pcap file on external storage). This command is available in the CLI but not the web.

diag perfstat

Syntax

```
diag perfstat [ethport <1|2>] [deviceport <Device Port # or Name>]
```

Description

Display performance statistics for an Ethernet Port or Device Port, averaged over the last 5 seconds. Must specify an Ethernet Port or Device Port.

diag ping|ping6

Syntax

```
diag ping|ping6 <IP Address or Name> [<parameters>]
```

Parameters

```
count <Number Of Times To Ping>
packetsize <Size In Bytes>
ethport <eth1|eth2|veth1|veth2|U1|U2>
timeout <Seconds to Wait for the First Response>
Defaults:    count=5, packetsize=64, timeout=10
Note: Timeout is for IPv4 ping only, and is not supported for IPv6 ping.
Defaults:    count=5, packetsize=64
```

Description

Verifies if the SLC can reach a host over the network.

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>]
```

Description

Generate and send Ethernet packets.

diag speedtest

Syntax

diag speedtest [email <Email Address>]

Description

Runs a network performance test over the default gateway to speedtest.net and outputs the results (speedtest.net must be reachable in order to perform the test). This tool is useful for testing performance of various network configurations, including performance of a cellular connection.

diag top

Syntax

```
diag top [parameters]
```

Parameters

```
continuous <enable|disable>
count <Number of Iterations to Display>
delay <Delay in Seconds>
numlines <Number of Lines to Display>
```

Defaults:

```
count=1, delay = 5 seconds
```

Description

Displays CPU usage, memory usage and tasks.

diag traceroute

Syntax

```
diag traceroute <IP Address or Hostname>
```

Description

Displays the route that packets take to get to a network host.

diag traceroute6

Syntax

```
diag traceroute6 <IP Address or Name>
```

Description

Displays the route that packets take to get to a network host.

diag usb

Syntax

```
diag usb [<parameters>]
```

Parameters

```
treedisplay <enable|disable>
mapdevice <enable|disable>
email <Email Address>
Defaults: treedisplay=enable
```

Description

To display information about USB buses and the devices connected to them, including the mapping between a USB device and the SLC port. For "mapdevice enable", the port numbers will be displayed at the end of the line in square brackets.

Events Commands

admin events add

Syntax

```
admin events add <trigger> <response>
```

<trigger> is one of:

```
dpdatadrop, humidlimit, pingfails, receivetrap, rpmload, nomodemdialor
templimit.
```

<response> is one of:

```
action syslog
action emailalert emailaddress <destination email address>
action snmptrap nms <SNMP NMS> community <SNMP Community>
action <fwdalltrapseth|fwdseltrapeth> ethport <1|2> nms <SNMP NMS>
     community <SNMP Community> [oid <SNMP OID>]
action <fwdalltrapsmodem|fwdseltrapmodem> deviceport <Device Port # or
Name> nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap OID>]
action <fwdalltrapsmodem|fwdseltrapmodem> usbport <U1|U2>
     nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap OID>]
```

```
action <fwdalltrapsmodem|fwdseltrapmodem> internal modem
     nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap OID>]
```

Description

Defines events.

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>
host <IP Address or Name>
oid <SNMP Trap OID>
outlet <Outlet #>
rpm <RPM Id or Name>
threshold <Load Percentage|Current in Amps>usbport <u1|u2>
internal modem
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>
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.*

Rename a group:

```
set groups rename <Group Name> newname <New Group Name>
```

Delete a group:

```
set groups delete <Group Name>
```

Show one or more groups:

```
show groups [name <Group Name>] members <enable|disable>
```

Host List Commands

set hostlist add|edit <Host List Name>

Syntax

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

Parameters

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

Default: retrycount=3, auth=enable.

```
auth <enable|disable>
```

Description

Configures a prioritized list of hosts to be used for modem dial-in connections.

set hostlist add|edit <Host List Name> entry

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 edit <Host List Name> move

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.

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.

show hostlist

Syntax

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

Description

Displays the members of a host list.

IP Filter Commands

set ipfilter state

Syntax

```
set ipfilter state <enable|disable> [testtimer <disable|1-120 minutes>]
```

Description

Enables or disables IP filtering for incoming network traffic.

set ipfilter mapping

Syntax

```
set ipfilter mapping <parameters>
```

Parameters

```
ethernet <1|2|bond0> state <disable>
ethernet <1|2|bond0> state <enable> ruleset <Ruleset Name>
deviceport <1..48> state <disable>
deviceport <1..48> state <enable> ruleset <Ruleset Name>
usbport <U1|U2> state <disable>
usbport <U1|U2> state <enable> ruleset <Ruleset Name>
internal modem state <disable>
internal modem state <enable> ruleset <Ruleset Name>
```

Description

Maps an IP filter to an interface.

set ipfilter rules

Syntax

```
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>
```

Description

Sets IP filter rules.

set ipfilter delete

Syntax

```
set ipfilter delete all
```

Description

Delete all rulesets and mappings.

show ipfilter

Syntax

```
show ipfilter
show ipfilter ruleset <all|Ruleset Name>
show ipfilter mapping
show ipfilter status <all|Ruleset Name>
```

Description

Show ipfilter.

Logging Commands

set deviceport port

Syntax

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

Parameters

```
actiondelay <Action Delay>
actionrestart <Restart Delay>
bytethreshold <# of Characters>
emailsubj <Email Subject>
emailto <Email Address>
locallogging <enable|disable>
nfsdir <Logging Directory>
nfslogging <enable|disable>
nfsmaxfiles <Max # of Files>
nfsmaxsize <Size in Bytes>
poweraction <on|off|cycle>
powersupply <Managed Power Supply Name>
sendstring <String to Send|QUOTEDSTRING>
tokenaction <List of none,log,trap,email,string,power>
tokendatadetect <enable|disable>
```

```
tokenstring <Regex String>
tokentrigger <bytecnt|charstr>
usblogging <enable|disable>
usbmaxfiles <Max # of Files>
usbmaxsize <Size in Bytes>
usbport <u1|u2|sd>
sysloglogging <enable|disable>
```

Description

Configures logging settings for one or more device ports.

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 15: User Authentication on page 270*.)

Example

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

show locallog

Syntax

```
show locallog <Device Port # or Name> [bytes <Bytes To Display>]
      [startbyte <Byte Index>]
```

Description

Displays a specific number of bytes of data for a device port. **1**K is the default.

set locallog clear

Syntax

```
set locallog clear <Device Port # or Name>
```

Description

Clears the local log for a device port.

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 15: User Authentication on page 270*).

set log clear modem

Syntax

```
set log clear modem
```

Description

Clear the modem log (the modem log is automatically pruned when it reaches 50K):

set log modem ppplog

Syntax

```
set log modem ppplog <enable|disable>
```

Description

Enables PPP activity messages in the modem log.

set log modem ppplog <enable|disable>

Syntax

```
set log modem pppdebug
```

Description

Enables PPP debugging messages in the modem log:

set log modem pppdebug <enable|disable>

Syntax

```
show log modem
```

Description

View the modem activity log for external modems and USB modems:

```
show log modem [display <head|tail>][numlines <Number of Lines>]
```

show log local

Syntax

```
show log local
```

Description

View the log for local, NFS, or USB logging (NFS and USB use the current logging settings for the Device Port). Default is to show the log tail:

```
show log local|nfs|usb <Device Port # or Name> [<parameters>]
```

Parameters

```
display <head|tail>
numlines <Number of Lines>
bytes <Bytes to Display>
startbyte <Byte Index>
logfile <NFS, USB Log File>
Defaults: bytes=1000, startbyte=1, numlines=40
```

Lists the NFS, USB log files, either for a specific device port, or all log files in a USB, NFS location:

```
show log files nfs|usb [localdir <NFS Mount Local Directory>]
[usbport <U1|U2>]
[deviceport <Device Port # or name>]
```

Managed Device (Automation) Commands

Onboard, configure, monitor and automate management of devices connected to serial ports.

See individual features (enter 'help set managed <feature>'):

- onboard Initiate MD onboarding and display onboarded status
- settings Configure managed device attributes, including authentication
- operations Manually run or schedule actions to monitor or pull/push data
- files Maintain repository of managed device files
- diag Diagnostics

For more information, see *Chapter 11: Managed Devices Automation on page 240*.

show managed

Syntax

```
show managed [name <Managed Device Name>] [port <Device Port # or Name>]
             [label <Managed Device Label>] [display
<status|post|tech|all>]
```

Description

Display managed device information (high level status, POST output, or detailed tech support report), filtering by name, port or label:

A MD name can be used with 'connect direct ssh' or 'connect direct telnet' to connect to the management IP of a managed device.

Note: *There should not be any active connections to the device port during onboarding and while the device is being managed with the device automation functionality. The device console port is frequently in use to monitor the health of the device and run operations (tasks). The operations can be paused in order to connect to the device console and interact directly with the device.*

set managed onboard

Initiate onboarding and display onboarded status. A device can be onboarded:

- Manually: the user is prompted for the model, IP address, etc. of the device
- Discover All: discovery is performed on all specified ports
- Discover New: discovery is performed on all specified ports that do not already have a managed device associated with the port
- Discover Moved: determine if managed devices have moved to a different port

The device port cannot have any active connections (e.g. 'connect direct') during onboarding. A user login and password must be given to onboard a device (all onboarding methods will prompt for the login password). The default serial settings to access a device console are 9600/8/N/1, but can be overridden. The managed device name will automatically be set to the device hostname.

Syntax

```
set managed onboard <all|Device Port # or Name>
            method <all|new|moved|manual>
           login <User Login> [serial <Baud[/DataBits/Parity/StopBits]>]
Note: if the device model and OS is determined during onboarding, the
managed device settings and operations schedule will be auto-configured.

Remove managed devices with 'set managed settings <MD Name|Port #>
remove'.

Display the onboarding status for all ports or a single port (displaying
a single port which is being onboarded will also display the onboard
log):
show managed onboard [port <Device Port # or Name>]
```

set managed settings

Configure settings for a managed device, including user login and password, and privileged user and password:

Syntax

```
set managed settings <Managed Device Name|Device Port # or Name|Label>
Parameters: newname <Managed Device Name>
            description <Device Description>
            login <User Login>
            privlogin <Privileged User Login>
            label <Comma Separated List Of Up To 3 Labels>
            serial <Baud[/DataBits/Parity/StopBits]>
            managementipv4 <IPv4 Address to Access Managed Devices>
            pingipv4 <IPv4 Address to Ping for Connectivity Test>
Note: the label parameter sets (or clears) all 3 labels simultaneously.
set managed settings <MD Name|Device Port # or Name|Label> password
set managed settings <MD Name|Device Port # or Name|Label> privpassword

Remove a managed device and all associated data:
set managed settings <MD Name|Device Port # or Name> remove

Display settings, filtering by name, port or label:
show managed settings [name <MD Name>] [port <Device Port # or Name>]
                      [label <MD Label>]
```

set managed operations

Manually run or schedule periodic operations and monitoring on the MD, and view results of an operation run. Some operations may prompt for additional inputs. The starttime parameter is ignored when updating a default scheduled operation for a device.

Operations Status:

- PENDING operation run waiting for next scheduled time
- DISPATCHED operation run in progress
- SUSPENDING operation schedule suspended
- OK operation completed successfully
- COMPLETED operation completed all jobs successfully
- SUSPENDED operation is temporarily suspended
- FAIL operation run failed; see Reason in detailed schedule output

Syntax

```
set managed operations <Managed Device Name|Device Port # or Name|Label>
                       operation <Operation> <Schedule>
<Operation> is one of:
  clear_counters       Reset interface counters
  clear_logs           Clear system logs
  device_status       Retrieve heartbeat, monitor the chassis and health
status
  device_tech          Retrieve detailed tech support report (no repeat
option)
  device_ping          Ping a device to test connectivity
  interface_on         Turn a network interface on
  interface_off        Turn a network interface off
  interface_cycle      Turn a network interface off, then on
  monitor_interfaces   Monitor network interface
  pull_config          Pull configuration, save in file repository
  pull_startup_config  Pull startup configuration, save in file
repository
  pull_vlan_config     Pull VLAN configuration, save in file repository
  push_config          Push configuration from file repository
  push_config+reboot   Push configuration followed by reboot
  reboot               Reboot device
  suspend              Pause all running operations for a specified
duration
  resume               Resume paused operations
<Schedule> is one of:
  starttime            <now|HH:MM[MMDD]|afterHH:MM>
                           [repeat <Minutes>M|<Hours>H|<Days<D>]
  delete               Delete operation (default schedules are returned
to their original repeat frequency)

This creates an operation to run immediately, or at a given time and
optionally repeat; this will replace any previous schedule for the
operation.
```

```
Each instance of an operation run is called a 'job'; each job has a
success or failure status.
As each job requires use of the managed device console port, operations
should not be scheduled in a manner that causes them to compete for use
of the console port; competing jobs will be rescheduled for a later time.

Display operations schedule or jobs, filtering by name, port or label. An
operation has a start time (time that the operation was initially
created, either automatically after onboarding or when a user creates an
operation); a frequency (in minutes if the operation repeats); an Enabled
flag indicating if the operation is enabled or disabled due to being
paused; and a Last Run Time, which is the time that the operation last
ran.

show managed operations [port <Device Port # or Name>] [label <MD Label>]
                        [name <MD Name>] [display
<schedule|detailed|jobs|all>]
```

set managed files

View, transfer and manage log, config and miscellaneous files in a repository for each MD:

Syntax

```
set managed files <Managed Device Name|Device Port # or Name>
Parameters: delete <File ID>
            diff <Text File ID> compare <Text File2 ID>
            download <File ID> via <sftp|scp> host <IP address or Name>
                login <User Login> [path <Remote Directory>]
            upload <Filename> via <sftp|scp> host <IP address or Name>
                login <User Login> [path <Remote Directory>] [version
<Version>]
            version <File ID> string <Custom Version for File ID>

Display files in a MD repository:
show managed files [name <MD Name>] [port <Device Port # or Name>]
                   [detailed <enable|disable>]

Display contents of file in a MD repository (text files only):
show managed files name <MD Name>|port <Device Port # or Name>
                   contents <File ID>
Parameters: display <head|tail> [numlines <Number of Lines>]
```

set managed diag

MD diagnostic tools:

Change the log level for managed device logs; the default is log level is Info. The log level will reset back to Info after a reboot.

Syntax

```
set managed diag loglevel <info|debug|trace>

Clear the managed device logs:
```

```
set managed diag clear logs

Display current log level:
show managed diag loglevel

Display the log of console activity for a managed device:
show managed diag consolelog <Managed Device Name|Device Port # or Name>
Parameters: display <head|tail> [numlines <Number of Lines>]
            email <Email Address>

Display the collector, correlator, dbwriter, executor or orchestration
logs:
show managed diag collector|correlator|dbwriter|executor|orchestrator
             <all|Managed Device Name|Device Port # or Name>
Parameters: display <head|tail> [numlines <Number of Lines>]
            level <error|warning|info>
            email <Email Address>
Note: the level and display parameters cannot be used simultaneously.

Display internal automation information:
show managed diag internals [email <Email Address>]
```

Network Commands

set network port

Syntax

```
set network port <1|2|3|4> <parameters>

Parameters: state <dhcp|bootp|static|disable> [ipaddr <IP Address> mask
   <Mask>]
   ipv6addr <IPv6 Address/Prefix>
   mode <auto|10mbit-half|100mbit-half|10mbit-full|100mbit-full|
      1000mbit-full>
   mtu <Maximum Transmission Unit>
set network ipv6 <enable|disable>
```

Description

Configure Ethernet Port 1 or 2, or SFP Port 3 or 4

set network

Syntax

```
set network <parameters>
```

Parameters

```
startprobes <1-99999 Seconds>
probes <Number of Probes>
interval <1-99999 Seconds>
ipforwarding <enable|disable>
ip6forwarding <enable|disable>
reversepathfilter <enable|disable>
```

Description

Sets TCP Keepalive and IP Forwarding network parameters.

set network bonding

Syntax

```
set network bonding <disabled|active-backup|802.3ad|load-balancing>
```

Description

Configure Ethernet Bonding.

set network dns

Syntax

```
set network dns <1-10> ipaddr <IP Address>
```

Description

Configures up to 10 DNS servers.

set network dnsipv4prec

Syntax

```
set network dnsipv4prec <enable|disable>
set network dnssrcipaddr <none|eth1|eth2|veth1|veth2>
set network dnssrcipaddr <none|eth1|eth2|veth1|veth2>
```

Description

Configures IPv4/IPv6 lookup precedence.

set network gateway

Syntax

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

Parameters

```
default <IP Address>
```

```
ipv6default <IPv6 Address>
precedence <dhcp|default>
failover <IP Address>
pingip <IP Address>
ethport <1|2|bond0>
failoverport <eth2|intmodem>
pingdelay <1-250 seconds>
failedpings <1-250>
faildevice <none|hspa|sierra|g52x>
faildevapn <Fail-over Device: APN of Mobile Carrier>
faildevlockpin <enable|disable>
faildevlogin <Fail-over Device: Admin Login(Default HSPA+:admin,
Sierra:user, Lantronix G52x:admin)>
faildevcelluser <Fail-over Device: SIM Login>
faildevcellpwd <Fail-over Device: SIM Password>
faildevcelldialstr <Fail-over Device: Dialup Str>
faildevcellroam <enable|disable>
faildevpassthru <enable|disable>
faildevethip <IP Address>
faildevdhcp <enable|disable>
```

Transfer firmware update files to the SLC to initiate a firmware update on the fail-over device:

```
set network gateway faildevupdate <ftp|sftp|scp|usb>
         gwfile <Firmware File> radiofile <Radio File> [usbport <U1|U2>]
         [host <IP Address or Name>] [login <User Login>] [path <File
Path>]
```

Reboot the fail-over device, or set the fail-over device SIM Card PIN #, SIM Personal Unblocking Key or Admin Password (any extra parameters will be ignored):

```
set network gateway reboot
set network gateway faildevpin
set network gateway faildevpuk
set network gateway faildevcellpwd
set network gateway faildevpassword
    (Default faildevpassword HSPA+:PASS, Sierra:12345, Lantronix
G52x:admin)
```

Description

Set default and fail-over gateway configuration parameters. The fail-over gateway is a backup default gateway, used when it is determined through a fail-over trigger, that the primary default gateway is no longer a viable route. A fail-over event happens when a Ping device reachable via an Ethernet interface and the default gateway, becomes unreachable. Fail-back is when the Ping device becomes reachable again, causing the primary default route to be restored.

set network host

Syntax

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

Description

Sets the SLC host name and domain name.

set network fqdnlist

Syntax

```
set network fqdnlist <1-15> ipaddr <IP Address> fqdn <hostname>
```

Description

Updates the local hosts table for DNS lookup of FQDNs.

show network

Syntax

```
show network port <1|2|3|4>
show network bonding
show network dns
show network gateway
show network host
show network fqdnlist
show network ipv6
show network sfp
show network all
```

Description

Displays network settings.

NFS Commands

set nfs mount

Syntax

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

Parameters

```
locdir <Directory>
mount <enable|disable>
remdir <Remote NFS Directory>
rw <enable|disable>
Enables or disables read/write access to remote directory.
```

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 nfs

Syntax

```
show nfs
```

Description

Displays NFS share settings.

Percepxion Commands

set px client

Syntax

```
set px client <enable|disable>
```

Description

Configure interaction with Percepxion management server. The communication with the server is enabled by default, and can be disabled.

set px statusinterval

Syntax

```
set px statusinterval <1-60 minutes> fwconfiginterval <1-72 hours>
```

Description

Set interval between status updates, and firmware and configuration checks.

set px fwupdate

Syntax

```
set px fwupdate <enable|disable> configupdate <enable|disable>
```

Description

Enable or disable firmware and configuration updates via Percepxion.

set px rebootafterupdate

Syntax

```
set px rebootafterupdate <enable|disable>
```

Description

Enable or disable reboots after firmware or configuration updates.

set px allowremoteconnection

Syntax

```
set px allowremoteconnection <enable|disable>
```

Description

Enable or disable remote connections.

set px auditlogmessages

Syntax

```
set px auditlogmessages <enable|disable>
```

Description

Enable or disable sending audit log messages.

set px connection

Syntax

```
set px connection <cloud|onpremise> [<one or more parameters>]
```

Parameters

```
host <FQDN>
port <TCP Port>
secureport <enable|disable>
validatecerts <enable|disable>
mqttstate <enable|disable>
```

Description

Configure Percepxion Cloud or On-Premise settings.

set px devicename

Syntax

```
set px devicename <Device Name> description <Device Description>
```

Description

Configure the device name and description used for registration.

set px timeoutcli

Syntax

```
set px timeoutcli <1-1800 seconds>
set px timeoutdp <1-1800 seconds>
```

Description

Configure the timeout for the Percepxion Web Terminal sessions.

set px digitalprobe

Syntax

```
set px digitalprobe <Device Port # or List or Name>
          frequency <disable|60-3600 seconds>
```

Description

Configures the device port digital probe for determining managed device connection status.

set px id

Syntax

```
set px id
```

Description

Set the device ID.

set px key

Syntax

```
set px key
```

Description

Set the Percepxion key

set px useproxy

Syntax

```
set px useproxy <enable|disable> [<one or more parameters>]
```

Parameters

```
proxy type <socks5|http>
proxy host <FQDN or IP Address>
proxyport <Port Number>
proxylogin <User Name>
```

Description

Enables or disables the use of a proxy server to act as a gateway between the Percepxion client and the Percepxion server.

set px proxypassword

Syntax

```
set px proxypassword
```

Description

Set the Proxy Server password.

set px clear updatelog

Syntax

```
set px clear updatelog
```

Description

Clear the Firmware/Config updates log,

show px

Syntax

```
show px
show px status
show px perfmon
show px scripts
show px probes
show px clicommands
show px connecttest
```

Description

Show Percepxion settings.

Use “show px connecttest” to test the connection to the Percepxion server (with proxy settings if configured).

Performance Monitoring Commands

show perfmon

Syntax

```
show perfmon
```

Parameters

```
show perfmon [probe <all|Probe Id or Name>]
```

Description

Display global settings and all probes, or a selected probe.

show perfmon status

Syntax

```
show perfmon status
```

Parameters

```
show perfmon status [probe <Probe Id or Name>]
```

Description

Display the running status of all probes or a selected probe.

show perfmon operations

Syntax

```
show perfmon operations
```

Parameters

```
show perfmon operations <Probe Id or Name>
```

Description

Display list of completed operation sets for a probe.

set perfmon results

Syntax

```
set perfmon results
```

Parameters

```
show perfmon results <Probe Id or Name> [set <Operation Set Number>]
```

```
                    [display <head|tail>] [numlines <Number of Lines>]
                    [email <Email Address>]
```

Description

Display round trip times (RTT) for last completed operation set or selected set, and optionally email the complete results.

show perfmon accumulated

Syntax

```
show perfmon accumulated
```

Parameters

```
show perfmon accumulated <Probe Id or Name> [set <Operation Set Number>]
                    [email <Email Address>]
```

Description

Display accumulated statistics for last completed operation set or selected set, and optionally email the statistics.

set perfmon repo

Syntax

```
set perfmon repo <local|usb> [usbport <U1|U2>]
```

Description

Set repository where probe operations are stored.

set perfmon keep

Syntax

```
set perfmon keep <Number of Operations to Keep>
```

Description

Set number of operations stored for each probe.

set perfmon udpjitterresp

Syntax

```
set perfmon udpjitterresp <enable|disable>
```

Description

Enable responders for UDP jitter.

set perfmon udpechoresp

Syntax

```
set perfmon udpechoresp <UDP Port Number|disable>
```

Description

Enable responders for UDP echo.

set perfmon tcpconnectresp

Syntax

```
set perfmon tcpconnectresp <TCP Port Number|disable>
```

Description

Enable responders for TCP connect.

set perfmon add

Syntax

```
set perfmon add <Probe Name>
type <dns|http|icmp|tcpconnect|udpecho|udpjitter|udpjittervoip>
```

Parameters

```
name <Probe Name>
            starttime <now|HH:MM[:SS][MMDD]|afterHH:MM:SS>
            operations <Number of Operations to Perform>
            frequency <Seconds between Operations>
            packets <Number of Packets to Send>
            interval <Milliseconds between Packets>
            timeout <Milliseconds to Wait for Response>
            host <Destination IP Address or Name>
            port <Destination Port>
            precision <milli|micro>
            datasize <Payload Data Size in Bytes>
            verifydata <enable|disable>
            codec <g729a|g711alaw|g711mulaw>
            tos <none|Type of Service>
            interface <none|eth1|eth2>
            nameserver <IPv4 Address>
```

Description

Add a new probe.

set perfmon edit

Syntax

```
set perfmon edit <Probe Id or Name> [<parameters>]
```

Parameters

```
name <Probe Name>
            starttime <now|HH:MM[:SS][MMDD]|afterHH:MM:SS>
            operations <Number of Operations to Perform>
            frequency <Seconds between Operations>
            packets <Number of Packets to Send>
            interval <Milliseconds between Packets>
            timeout <Milliseconds to Wait for Response>
            host <Destination IP Address or Name>
            port <Destination Port>
            precision <milli|micro>
            datasize <Payload Data Size in Bytes>
            verifydata <enable|disable>
            codec <g729a|g711alaw|g711mulaw>
            tos <none|Type of Service>
            interface <none|eth1|eth2>
            nameserver <IPv4 Address>
```

Description

Edit an existing probe.

set perfmon delete

Syntax

```
set perfmon delete <Probe Id or Name> [data <all|# of Sets to Keep>]
```

Description

Delete a probe, or delete all operation data for a probe, or delete all but the most recent operation sets for a probe.

set perfmon state

Syntax

```
set perfmon state <all|Probe Id or Name> action <restart>
```

Description

Set the running state of all probes or a single a probe.

Power Commands

set power

Syntax

```
set power model <none|sp1004a|sp1004b|apc7900b>
set power port <U1|U2|Device Port # or Name>
set power pdulogin <PDU Username>
set power pdupassword
set power outlet <Outlet # or List or Name> <one or more parameters>
Parameters:  name <Outlet Name>
             description <Outlet Description>
             state <on|off>
             wakeup <on|off|laststate>
             reboot
```

Description

Configure and control power outlets on an integrated PDU.

show power

Syntax

```
show power [outlet <Outlet # or Name>]
           [pduinfo  <devicestatus|networkstatus|inletstatus|
            userlogs|eventlogs>]
```

Description

Show power settings

Routing Commands

set routing

Syntax

```
set routing [parameters]
```

Parameters

```
rip <enable|disable>
version <1|2|both>
static <enable|disable>
route <1-64> ipaddr <IP Address> mask <Netmask> gateway <IP Address>
ipv6route <1-64> ipv6addr <IPv6 Address/Prefix> ipv6gateway <IPv6
Address>
```

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

Description

Sets the routing table to display IP addresses (disable) or the corresponding host names (enable). You can optionally email the displayed information.

RPM Commands

set rpm add

Syntax

```
set rpm add <RPM Name>
```

Description

Adds an RPM to be managed (prompts will guide selection of RPM vendor and model).

set RPM command

Syntax

```
set rpm command <RPM Id or Name>
        outlet <all|Outlet # or List> state <on|off|cyclepower>
```

Description

Sends a command to control one or more outlets on an RPM.

Syntax

```
set rpm command <RPM Id or Name> device <reboot|shutdown>
```

Description

Sends a command to control an RPM device.

Syntax

```
set rpm command <RPM Id or Name> beeper <mute|enable|disable>
```

Description

Sends a command to control an RPM beeper.

set rpm delete

Syntax

```
set rpm delete <RPM Id or Name>
```

Description

Deletes an RPM.

set rpm driver

Syntax

```
set rpm driver <RPM Id or Name> action restart
set rpm driver <RPM Id or Name> action debug [level <1|2|3>]
set rpm driver <RPM Id or Name> action show
set rpm driver <RPM Id or Name> action viewoutput [email <Email Address>]
               [display <head|tail>] [numlines <Number of Lines>]
```

Description

Control and debug the RPM driver if the driver is not properly communicating with the PDU or UPS: restart the driver; restart the driver with debug output to a file; show the running driver; view and email the driver debug output.

Note: *Drivers running in debug mode will generate copious output and for disk space reasons should not be left running in debug mode for long periods of time.*

set rpm edit

Syntax

```
set rpm edit <RPM Id or Name> <one or more parameters>
```

Parameters

```
name <New RPM Name>
outlets <# of Outlets>
ipaddr <IP Address>
port <TCP or Device Port>
login <RPM Admin Login>
rocommunity <SNMP Read-Only Community>
rwcommunity <SNMP Read-Write Community>
logstatus <disable|1-60 minutes>
snmptraps <enable|disable>
emailaddress <Email Address>
upslowbattery <shutdown|shutdownall|shutdownboth|allowfailure>
sdorder <disable|1-49>
```

```
powertoslc <enable|disable>
driveropts <Driver Options Override>
```

Description

Configure and control Remote Power Managers (RPMs), including PDUs and UPSes.

set rpm password

Syntax

```
set rpm password <RPM Id or Name>
```

Description

Set RPM administrative password.

show rpm

Syntax

```
show rpm [type <ups|pdu>]
         [config <sdorder|notify>]
         [device <RPM Name or Id> [data <raw|logs|envmon>]]
```

Note: *The show rpm envmon command for RPM-configured ServerTech Serial/Network Mode is not supported by NUT/Powerman.*

Description

Display a list of all RPMs, RPMs of a specific type, UPS shutdown and notification configuration, or details and outlets for a single RPM device.

Script Commands

set script import

Syntax

```
set script import <interface|batch|custom> via <ftp|scp|copypaste>
           [file <Script File>] [name <Script Name>] [host <IP Address
              or Name>]
           [login <User Login>] [path <Path to Script File>]
           [filetype <expect|tcl|python>]
```

Note: *Interface scripts will be given default/do user rights; Batch and Custom scripts will be given admin/ad user rights. The name of the script will be 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 update

Syntax

```
set script update <interface|batch|custom> name <Script Name>
           [group <default|power|admin>] [permissions <Permission List>]
```

Note: *See 'help user permissions' for information on groups and user rights.*

Description

Update a script.

set script rename

Syntax

```
set script rename <interface|batch|custom> name <Script Name>
           newname <New Script Name>
```

Description

Rename a script.

set script delete

Syntax

```
set script delete <interface|batch|custom> name <Script Name>
           [data <all|# of Sets to Keep>]
```

Description

Delete a script.

set script runcli

Syntax

```
set script runcli <Script Name> [parameters <Command Line Parameters>]
           [prompt <Prompt String>][debug <enable|disable>]
```

Description

Run a CLI batch or custom script one time (script output will be displayed in the current terminal; custom script output will be saved in the repository).

connect script

Syntax

```
connect script <Script Name> deviceport <Device Port # or Name>
           [parameters <Command Line Parameters>]
           [debug <enable|disable>]
```

Description

Connect an interface or custom script to a Device Port and run it one time (script output will be displayed in the current terminal; custom script output will be saved in the repository).

set script schedule

Syntax

```
set script schedule <Script Name> [device <cli|Device Port # or Name>]
           [state <enable|disable|delete>] [parameters
               <Cmd Line Parameters>]
           [starttime <now|HH:MM[MMDD]|afterHH:MM>]
           [frequency <Hours/Days between each operation>]
           [stoptime <forever|HH:MM[MMDD]|afterHH:MM>]
```

Description

Schedule a custom script to be run at a certain time, either once or recurring; frequency is specified as hours (4H for 4 hours) or days (2D for 2 days).

show script

Syntax

```
show script [type <interface|batch|custom> [name <Script Name>]]
```

Description

Display list of scripts, or view the details and contents of a script.

show script status

Syntax

```
show script status [script <Script Name>]
```

Description

Display the running status of all custom scripts or a single custom script.

show script operations

Syntax

```
show script operations <Script Name>
```

Description

Display list of completed results for a custom script.

show script results

Syntax

```
show script results <Script Name> [set <all|Operation Set Number>]
            [display <head|tail>] [numlines <Number of Lines>]
            [email <Email Address>]
```

Description

Display the results for the last completed custom script operation or a selected operation, and optionally email the results.

Security Commands

set security

Syntax

```
set security <parameters>
Parameters:  fipsmode <enable|disable>
```

Description

Configure SLC security and FIPS settings.

show security

Syntax

```
show security
```

Description

Display security settings and current status.

Services Commands

set services

Syntax

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

Parameters

auditlog <enable|disable>	ssh <enable|disable>
auditsize <1-500 Kbytes>	timeoutssh <disable|1-30 minutes>
clicommands <enable|disable>	sshdatadir <netin|netout|both>
includesyslog <enable|disable>	portssh <TCP Port>
netlog <off|error|warning|info|debug>	requiresshpublickey <enable|disable>
servlog <off|error|warning|info|debug>	telnet <enable|disable>
authlog <off|error|warning|info|debug>	timeouttelnet <disable|1-30 minutes>
devlog <off|error|warning|info|debug>	telnetdatadir <netin|netout|both>
diaglog <off|error|warning|info|debug>	escapeseqtelnet <1-10 Chars>
genlog <off|error|warning|info|debug>	outgoingtelnet <enable|disable>
syslogserver1 <IP Address or Name>	discoveryserver <enable|disable>
syslogserver2 <IP Address or Name>	
syslogsrcipaddr <none|eth1|eth2|eth3|eth4|veth1|veth2>	
syslogsrcipv6addr <none|eth1|eth2|eth3|eth4|veth1|veth2>	
rpmlogsize <5-40 Kbytes>	smtpserver <IP Address or Name>
otherlogsize <5-400 Kbytes>	smtpsender <Email Address>
webterminal <enable|disable>	smtpport <SMTP TCP Port>
webermtimeout <disable|1-1800 seconds>	smtplogin <Username or Email Address>
webtermrequirelogin <enable|disable>	smtpsecurity <none|starttls|tls>
	smtpauth <none|auto|plain|cram-md5|login>

Description

Configures services (system logging, SSH and Telnet access, SSH and Telnet timeout, email [SMTP] server, and audit log.)

set services sshalgorithms

Syntax

```
set services sshalgorithms <prompt|List of Disabled SSH Algorithms>
```

Description

Defines the set of SSH algorithms that are enabled, either by prompting for each algorithm or by specifying a complete list of disabled algorithms. For example "MACs:hmac-sha2-256,hmac-sha1;Ciphers:aes128-gcm@openssh.com;" disables 2 MACs and one cipher and leaves all other algorithms enabled. Available algorithm types are 'MACs', 'Ciphers', 'KEX' and 'HostKey'.

set services smtppassword

Syntax

```
set services smtppassword
```

Description

Sets the SMTP password.

set services testemail

Syntax

```
set services testemail <Email Address> [comment <Comment>]
```

Description

Allows you to validate the SMTP server configuration by proving a test email.

Note: *Telnet and SMTP to port 25 are insecure.*

show services

Syntax

```
show services [viewalgorithms <enable|disable>]
show services smtplog
show services smtplog clear
```

Description

Displays current service settings.

Displays or clears SMTP log.

Site Commands

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

set site add|edit

Syntax

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

Parameters

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

Set the site password and CHAP secret (any extra parameters will be ignored):

```
set site dialoutpassword <Site Name>
set site chapsecret <Site Name>
```

Deletes a site:

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

SLC Network Commands

set slcnetwork

Syntax

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

Parameters

```
add <IP Address>
delete <IP Address>
search <localsubnet|ipaddrlist|both>
```

Description

Detects and displays all SLC 9000 advanced console server or user-defined IP addresses on the local network.

show slcnetwork

Syntax

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

Description

Detects and displays all SLC 9000 advanced console servers 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).

SNMP Commands

set snmp

Syntax

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

Parameters

```
agent <enable|disable>                location <Physical Location>
v1 <enable|disable>                   contact <Admin Contact Info>
v2c <enable|disable>                  rocommunity <Read-Only Community>
v3 <enable|disable>                   rwcommunity <Read-Write Community>
v3tls <enable|disable>                trapcommunity <Trap Community>
tlsport <TLS Port>                    v3security <noauth|auth|authencrypt>
nms1 <IP Address or Name>             v3encrypt <des|aes|aes192|aes256>
nms2 <IP Address or Name>             v3auth <md5|sha|sha2_224|
alarmdelay <1-6000 Seconds>           sha2_256|sha2_384|sha2_512>
traps <enable|disable>                v3user <v3 RO User>
trapversion <1|2|3>                   v3rwuser <v3 RW User>
trapsovertls <enable|disable>         v3trapuser <v3 Trap User>
trapsrcipaddr <none|eth1|eth2|veth1|veth2>
trapsrcipv6addr <none|eth1|eth2|veth1|veth2>

Note: v1 and v2c are insecure.
```

Description

Configure SNMP agent.

set services v3password

Syntax

```
set snmp v3password|v3phrase|v3rwpassword|v3rwphrase|v3trappassword
   |v3trapphrase
```

Description

Set SNMP v3 read-only, read-write and trap password/passphrase.

set snmp trapenable

Syntax

```
set snmp trapenable <prompt|Comma separated list of Trap Numbers>
```

Description

Defines the set of SNMP traps that are sent by the SLC. (See *Enable Traps on page 124* or SNMP web page for supported traps). When specifying a list of trap numbers, specify the last 2 digits of the trap OID, e.g "5.3,0.2,0.24".

set snmp snmpcertificate import

Syntax

```
set snmp certificate import via <sftp|scp> rootfile <Cert Auth File>
     certfile <Agent Certificate File> keyfile <Agent Private Key File>
     clientcert <Client Certificate File> host <IP Address or Name>
     login <User Login> [path <Path to Files>]
set snmp certificate delete
set snmp certificate attributes
         fingerprint <Client Certificate SHA1 or SHA256 Fingerprint>
         mapfield <username|email|fqdn|ipaddr|commonname|any>
         token <Field String>
set snmp certificate show
```

Description

Manage SNMP agent and client (outbound traps) X.509 certificates for TLS connections.

show snmp

Syntax

```
show snmp
```

Description

Displays SNMP agent.

SSH Key Commands

set sshkey import

Syntax

```
set sshkey import <ftp|sftp|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

Import SSH key.

set sshkey export

Syntax

```
set sshkey export <ftp|sftp|scp|copypaste> keyuser <SSH Key User>
            keyname <SSH Key Name> type <rsa|ecdsa>
            [bits <1024|2048|3072|4096|256|384|521>]
            [host <IP Address or Name>] [login <User Login>]
            [path <Path to Copy Key>] [format <openssh|secsh>]
```

Description

Create and export sshkey.

set sshkey allexport

Syntax

```
set sshkey allexport <ftp|sftp|scp|copypaste>
            [pubfile <Public Key File>]
            [host <IP Address or Name>] [login <User Login>]
            [path <Path to Copy Keys>]
```

Description

Exports the public keys all of the previously created SSH keys.

set sshkey delete keyuser

Syntax

```
set sshkey delete keyuser <SSH Key User> keyhost <SSH Key Host>
```

Description

Delete imported SSH key. Specify the `keyuser` and `keyhost` for the imported key.

set sshkey delete keyuser

Syntax

```
set sshkey delete keyuser <SSH Key User> keyname <SSH Key Name>
```

Description

Delete exported SSH key. Specify the `keyuser` and `keyname` to delete exported key.

show sshkey import

Syntax

```
show sshkey import <one or more parameters>]
```

Parameters

```
[keyuser <SSH Key User>]
[keyhost <SSH Key IP Address or Name>]
[viewkey <enable|disable>]
```

Description

Displays all keys that have been imported or keys for a specific user, IP address, or name.

show sshkey export

Syntax

```
show sshkey export <one or more parameters>
```

Parameters

```
[keyname <SSH Key Name>]
[keyuser <SSH Key User>]
[viewkey <enable|disable>]
```

Description

Displays all exported keys or keys for a specific user, IP address, or name.

set sshkey server import type

Syntax

```
set sshkey server import type <rsa|ecdsa|ed25519> via <sftp|scp>
            pubfile <Public Key File> privfile <Private Key File>
            host <IP Address or Name> login <User Login> [path <Path to
              Key File>]
```

Description

Imports an SLC host key.

set sshkey server reset

Syntax

```
set sshkey server reset [type <all|rsa|ecdsa|ed25519>]
```

Description

Resets defaults for all or selected host keys.

set sshkey server remove

Syntax

```
set sshkey server remove
```

Description

Remove all host keys; they will be regenerated after SLC reboot.

show sshkey server

Syntax

```
show sshkey server [type <all|rsa|ecdsa|ed25519>]
```

Description

Displays host keys (public key only).

Status Commands

show connections

Syntax

```
show connections [deviceport <Device Port # or Name>]
                [email <Email Address>]
```

Description

Displays a list of current connections. Optionally emails 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

Provides details, for example, endpoint parameters and trigger, for a specific connection. Optionally emails the displayed information.

Note: *Use the basic* `show connections` *command to obtain the Connection ID.*

show portcounters

Syntax

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

Description

Generates a device port statistics report for one or more ports. Optionally emails the displayed information. Use a comma-separated Device Port list (or “ALL”) to specify a group of device ports (i.e. “1-4,8,10-12”).

show portcounters zerocounters

Syntax

```
show portcounters zerocounters <Device Port List or Name>]
```

Description

Displays zero port counters for one or more device ports.

show portstatus

Syntax

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

Description

Displays device port modes and states for one or more ports. Optionally emails the displayed information. A comma-separated device port list (or “All”) can be used to specify a group of device ports (i.e. “1-4,8,10-12”).

show sysconfig

Syntax

```
show sysconfig [display <basic|auth|devices>] [email <Email Address>]
```

Description

Displays a snapshot of all configurable parameters, or a shorter report with basic system settings, authentication settings, or device settings. Optionally emails the displayed information.

show sysstatus

Syntax

```
show sysstatus [email <Email Address>]
```

Description

To display the overall status of all SLC units. Optionally emails the displayed information.

Switch Commands

set switch port

Syntax

```
set switch port <Port # or Name> <one or more parameters>
```

Parameters

```
name <Switch Port Name>
state <enable|disable>
type <access|trunk>
mode <auto|10mbit-half|100mbit-half|
      10mbit-full|100mbit-full|1000mbit-full>
```

```
Note: by default, all ports are enabled in access mode, and a member of
VLAN #1.Description
```

Configure ports on the Ethernet switch, including membership in up to 5 VLANs.

set switch port (VLAN)

Syntax

```
set switch port <Port # or Name> addtovlan <VLAN ID or List of IDs or
Name>
            [vlanstate <enable|disable>] [pvidstate <enable|disable>]
            [egresspolicy <tag|untag>]
set switch port <Port # or Name> editportvlan <VLAN ID or VLAN Name>
            [vlanstate <enable|disable>] [pvidstate <enable|disable>]
            [egresspolicy <tag|untag>]
set switch port <Port # or Name> deletefromvlan <VLAN ID or VLAN Name>
```

```
Note: by default, when a port is added to a VLAN, the vlanstate and the
pvidstate will be set to disabled, and the egresspolicy will be set to
tag. These parameters can only be configured when the port type is set to
trunk.
```

Description

Configure switch port VLAN membership

show switch port

Syntax

```
show switch port <Port # or List or Name> [display
<status|statistics|vlan|all>]
```

Description

Display configuration and status of all ports or individual ports.

set switch vlan

Syntax

```
set switch vlan <VLAN ID> <one or more parameters>
Parameters: name <VLAN Name>
            membership <Switch Port List>
            newvlanid <2-4094>

Note: The default VLAN for all ports is #1, and VLAN ID #1 cannot be
removed.
To remove a VLAN, set the VLAN Name to a blank string:
set switch vlan <VLAN ID> name ""
```

Description

Configure up to 10 VLANs (a 'Default' VLAN initially contains all switch ports):

show switch vlan

Syntax

```
show switch vlan [vid <VLAN ID>] [name <VLAN Name>]
```

Description

Display status of a single VLAN or all VLANs:

set switch internal

Syntax

```
set switch internal <enable|disable>
Note: to set the switch IP address and netmask, see the 'set dhcp'
command.
```

Description

Enable or disable the internal switch Ethernet port.

show switch ipaddr

Syntax

```
show switch ipaddr [search <dhcpclient|ipneighbor|ping>]
```

Description

Display (scan for) IP addresses accessible via the Ethernet switch:

show switch macaddr

Syntax

```
show switch macaddr
```

Description

Display the MAC address table:

show switch detail

Syntax

```
show switch detail [port <Port # or List or Name>]
```

Description

Display detailed internal status for all ports or individual ports:

System Log Commands

show syslog

Syntax

```
show syslog [<parameters>]
```

Parameters

```
log <all|netlog|servlog|authlog|devlog|diaglog|genlog>
level <error|warning|info|debug>
```

```
display <head|tail> [numlines <Number of Lines>]
starttime <MMDDYYhhmm[ss]>
endtime <MMDDYYhhmm[ss]>
[email <Email Address>]
Defaults: log=all, level=error, numlines=40
```

Description

Displays the system logs containing information and error messages.

Note: *The level, display, and time 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.

Temperature Commands

set temperature

Syntax

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

Parameter

```
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.*

Description

Sets the acceptable range for the internal temperature sensor (an SNMP trap is sent if the temperature is outside of this range). Temperatures can be entered in either Celsius or Fahrenheit; to indicate a temperature is Fahrenheit, append the degrees with an ‘F’, i.e., “75F”.

show temperature

Syntax

```
show temperature
```

Description

Displays the acceptable range and the current reading from the internal temperature sensor.

USB Access Commands

set usb access

Syntax

```
set usb access <enable|disable>
```

Description

Enables or disables access to USB devices.

USB Device Commands

show usb devices

Syntax

```
show usb devices
```

Description

Displays all usb devices with the port each device is connected to.

diag usb

Syntax

```
diag usb [<parameters>]
```

Parameters

```
treedisplay <enable|disable>
mapdevice <enable|disable>
details <enable|disable>
email <Email Address>
```

Defaults: `treedisplay=enable`

Description

Displays information about USB buses and the devices connected to them, including the mapping between a USB device and the SLC port.

Note: *For "mapdevice enable", the port names will displayed at the end of the line in square brackets.*

Note: *To see a list of USB devices with vendor id and product id, use 'treedisplay disable'.*

USB Modem Commands

set usb modem

Syntax

```
set usb modem <u1|u2> <parameters>
```

Parameters

```
accesslist <Access List Name>
auth <pap|chap>
baud <300-115200>
```

9600 is the default.

```
calleridcmd <Modem Command String>
calleridlogging <enable|disable>
cbcpnocallback <enable|disable>
cbcptype <admin|user>
chapauth <chaphost|localusers>
chaphost <CHAP Host or User Name>
checkdialtone <disable|5-600 minutes>
databits <7|8>
dialbackdelay <PPP Dialback Delay>
dialbacknumber <usernumber|Phone Number>
dialbackretries <1-10>
dialinlist <Host List for Dial-in>
dialoutlogin <Remote User Login>
dialoutnumber <Phone Number>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
flowcontrol <none|xon/xoff|rts/cts>
group <Local or Remote Group Name>
initscript <Modem Init Script>
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>
usesites <enable|disable>
```

Description

Configures a currently loaded USB Modem.

Note: *It is recommended that the* `initscript` *be prepended with* `'AT'` *and include* `'E1 V1 x4 Q0'` *so that the SLC may properly control the modem.*

Set the dialout password and CHAP secrets (any extra parameters will be ignored):

```
set usb modem <U1|U2> dialoutpassword
set usb modem <U1|U2> chapsecret
set usb modem <U1|U2> dodchapsecret
```

show usb modem

Syntax

```
show usb modem
```

Description

Display product information and settings for any USB modem:

USB Serial Commands

set usb serial

Syntax

```
set usb serial <U1|U2> <parameters>
```

Parameters

```
baud <300-230400>                          databits <7|8>
parity <none|odd|even>                     stopbits <1|2>
flowcontrol <none|xon/xoff|rts/cts>      service <none|telnet|ssh|tcp>
telnetport <TCP Port>                      telnetauth <enable|disable>
sshport <TCP Port>                         sshauth <enable|disable>
tcpport <TCP Port>                         tcpauth <enable|disable>
Note: the maximum number of simultaneous connections to a USB device is
3.
```

Description

Configures a serial device connected to a USB port.

show usb serial

Syntax

```
show usb serial
```

Description

Display product information and settings for any USB serial device:

USB Storage Commands

set usb storage copy

Description

Copies a file on a thumb drive.

Syntax

```
set usb storage copy <U1|U2> file <Filename> newfile <New Filename>
```

set usb storage delete

Description

Removes a file on a thumb drive.

Syntax

```
set usb storage delete <U1|U2> file <Current Filename>
```

set usb storage dir

Syntax

```
set usb storage dir <U1|U2> [subdir <Directory Path>]
```

Description

Views a directory listing of a USB flash drive.

set usb storage fsck

Syntax

```
set usb storage fsck <U1|U2>
```

Description

Runs a file system check on a thumb drive (recommended if it does not mount).

set usb storage format

Syntax

```
set usb storage format <U1|U2> [filesystem <ext2|ext3|ext4|fat16|fat32>]
```

Description

Formats a USB flash drive.

set usb storage mount

Syntax

```
set usb storage mount <U1|U2>
```

Description

Mounts a USB flash drive in the SLC 9000 advanced console server for use as a storage device. The USB flash drive must be formatted with a file system before you mount it.

set usb storage rename

Description

Renames a file on a thumb drive.

Syntax

```
set usb storage rename <U1|U2> file <Filename> newfile <New Filename>
```

set usb storage unmount

Syntax

```
set usb storage unmount <U1|U2>
```

Description

Unmounts a USB flash drive. Enter this command before removing the USB device.

show usb storage

Description

Display product information and settings for any USB thumb drive.

Syntax

```
show usb storage
```

show usb

Syntax

```
show usb
```

Description

Display currently attached USB devices with product information and settings.

Virtual Interface Commands

set virtual

Syntax

```
set virtual port <1|2> <parameters>
```

Parameters

```
state <enable|disable>
ipaddr <IP Address> mask <Mask>
ipv6addr <IPv6 Address/Prefix>
```

Note: *It is highly recommended that an IP address/subnet for VEth1 and VEth2 be different than the IP address/subnet for Eth1 and Eth2. Configuring VEth1 or VEth2 with the same IP address/subnet as Eth1 or Eth2 may cause the console manager to become unreachable.*

Description

Configure Virtual Interface Port 1 or 2:

show virtual [port <1|2>]

Syntax

```
show virtual [port <1|2>]
```

Description

Display virtual interface Port 1 or 2

VPN Commands

set vpn

Syntax

```
set vpn <parameters>
```

Description

Configures setting for an IPSec VPN tunnel.

Parameters

```
tunnel <enable|disable>
name <VPN Tunnel Name>
auth <rsa|psk|x509>
remotehost <Remote Host IP Address or Name>
remoteid <Authentication Name>
remotehop <IP Address>
remotesubnet <one or more subnets in CIDR notation>
remotesourceip <config|<CIDR>|IP Address Range|poolname>
localip <IP Address>
localid <Authentication name>
localhop <IP Address>
localsubnet <one or more subnets in CIDR notation>
localsourceip <config4|config6|IP Address>
ikenegotation <main|aggressive>
ikeenc <any|3des|aes|aes192|aes256>
ikeauth <any|sha1|md5|sha2_256|sha2_384|sha2_512>
ikedhgroup <any|dh2|dh5|dh14|dh15|dh16|dh17|dh18|dh19>
ikever <any|ikev1|ikev2>
espenc <any|3des|aes|aes192|aes256>
espauth <any|sha1|md5|sha2_256|sha2_384|sha2_512|sha2_256_96>
espdhgroup <any|dh2|dh5|dh14|dh15|dh16|dh17|dh18|dh19>
lifetime <SA Lifetime in Seconds (3600) or Bytes with 'b' suffix (3600b)>
xauthclient <enable|disable>
xauthlogin <User Login>
ciscounity <enable|disable>
modeconfig <push|pull>
forceencaps <enable|disable>
deadpeerdelay <disable|1-300 seconds>
deadpeertimeout <5-1200 seconds>
deadpeeraction <restart|hold|clear>
tunnelrestart <enable|disable>
email <Email Address>
startvpnfailoveronly <enable|disable>
```

Enter RSA public key or Pre-Shared Key of remote host:

```
set vpn key
```

Enter XAUTH password (any extra parameters will be ignored):

```
set vpn xauthpassword
```

Configure X.509 certificate for remote peer or local peer:

```
set vpn certificate local via <sftp|scp> rootfile <Cert Authority File>
        certfile <Certificate File> keyfile <Private Key File>
        host <IP Address or Name> login <User Login> [path <Path to
             Files>]
set vpn certificate remote via <sftp|scp> [rootfile <Cert Authority
             File>]
        certfile <Certificate File> host <IP Address or Name>
        login <User Login> [path <Path to Files>]
```

Delete X.509 certificate for local and/or remote peer:

```
set vpn certificate delete
```

Generate RSA Key for the SLC (any extra parameters will be ignored):

```
set vpn genrsakey
```

Upload or delete RSA Key for remote VPN peer:

```
set vpn peerrsaaction upload via <sftp|scp> host <IP address or Name>
        login <User Login> rsafile <RSA Key File> [path <Path to key
file>]
```

set vpn peerrsaaction delete

Download IPSec conf file (VPN tunnel must be enabled to generate ipsec.conf for download; can be customized and uploaded to access more strongSwan options):

```
set vpn confaction download via <sftp|scp> host <IP address or Name>
        login <User Login> [path <Directory for Download>]
```

Upload IPSec conf file to the SLC:

```
set vpn confaction upload via <sftp|scp> host <IP address or Name>
        login <User Login> conffile <Conf File> [path <Path to Conf
              File>]
```

Delete uploaded IPSec conf file:

```
set vpn confaction delete
```

show vpn

Syntax

```
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 X.509 certificate for local peer (SLC) and remote peer:

```
show vpn certificate
```

Display RSA public key of the local peer (SLC) and remote peer:

```
show vpn rsakey
```

Display the uploaded or auto-generated IPSec conf file:

```
show vpn vpnconf
```

Description

Shows the settings for the IPsec VPN tunnel.

Xmodem Commands

`set xmodem repo`

Syntax

```
set xmodem repo import <Xmodem File> via <ftp|sftp|scp>
                host <IP Address or Name> login <User Login>
                [path <Path to Xmodem File>]
set xmodem repo rename <Xmodem File> newfile <New Filename>
set xmodem repo delete <Xmodem File>
```

Description

Manages a repository of files that can be sent to or received from a device port with Xmodem, Ymodem, or Zmodem. The maximum file size is 20 MB, and the maximum total repository size is 25 MB.

`set xmodem send/receive`

Syntax

```
set xmodem send <Device Port # or Name> file <Xmodem File>
           protocol <xmodem|ymodem|zmodem> xfer <binary|ascii>
set xmodem receive <Device Port # or Name> [file <Xmodem File>]
           protocol <xmodem|ymodem|zmodem> xfer <binary|ascii>
           [overwrite <enable|disable>]
```

Description

Send or receive files with Xmodem, Ymodem or Zmodem (by default receive will not overwrite a file in the repository with the same name).

`show xmodem`

Syntax

```
show xmodem
```

Description

Shows the Xmodem repository files.

Appendix A: Security Considerations

The SLC advanced console server provides data path security by means of SSH or Web/SSL. Even with the use of SSH/SSL, however, do not assume you have complete security. Securing the data path is only one measure needed to ensure security. This appendix briefly discusses some important security considerations.

Security Practice

Develop and document a Security Practice. The Security Practice should state:

- The dos and don'ts of maintaining security. For example, the power of SSH and SSL is compromised if users leave sessions open or advertise their password.
- The assumptions that users can make about the facility and network infrastructure, for example, how vulnerable the CAT 5 wiring is to tapping.

Factors Affecting Security

External factors affect the security provided by the SLC unit, 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 may be secure, but the path from the SLC 9000 advanced console server to the end device may not be secure.
- With the right tools, a person with physical access to open the SLC unit may be able to read the encryption keys.
- There is no true test for a denial-of-service attack. There is always a legitimate scenario for a request storm. A denial-of-service filter locks out some high-performance automated/scripted requests. The SLC 9000 advanced console server will attempt to service all requests and will not filter out potential denial-of-service attacks.

Security Best Practices

The following practices are suggested for configuring the SLC 9000 with the most secure configuration for encryption protocols (both incoming and outgoing network traffic), as well as access to external components. By default, the console manager is configured with the web UI enabled via HTTPS port 443, SSH enabled via port 22, and the Discovery Server enabled (supports the Lantronix Discovery Protocol for discovering other Lantronix devices on the local subnet on UDP port 30718).

- **SSH** - use the following SSH settings: enable SHA2 and Higher ciphers, disable NIST Algorithms, disable RSA Host Key Algorithms, configure a SSH Timeout, and require SSH users logging into the SLC 9000 to use MFA via SSH public key plus a password. See *SSH/ Telnet/Logging*.

- **TLS/SSL** - use only TLSv1.3 and the Highest ciphers and a trusted certificate, or disable the web server if only CLI access is needed. See *Web Server*.
- **VPN** - use the following VPN settings: use IKEv2 (avoid IKEv1 with Aggressive Mode), configure both the IKE Encryption and ESP Encryption algorithms (use AES256, SHA2_256 or higher, Diffie-Hellman group 18 or higher), and a trusted certificate for Authentication. See *VPN Settings*.
- **SNMP** - disable SNMP v1, SNMP v2 and use only SNMP v3 over TLS with a trusted certificate. See *SNMP*.
- **SMTP** - use TLS with SMTP authentication. See *SSH/Telnet/Logging*.
- **LDAP** - encrypt traffic with SSL and a trusted certificate. See *LDAP*.
- **Device Port**s - if direct network access to a Device Port is enabled, it should be only via SSH with Authentication; in addition, SSH Timeouts, Group Access, New User Message, and Max Direct Connects can be configured for each device port to control which users have access to a port, how many users can simultaneously access a port, and notifications when another user connects to a port. See *Device Ports - Settings*.
- **External USB Port(s)** - if the external USB ports are not used for firmware updates, saving configurations, serial connections, external analog modems or port logging, the ports can be disabled. See *USB Storage*.
- **External Modems** - in addition to disabling the external USB ports (see above), Access Lists can be used to control phone numbers that will be granted dial-in access. See *Access Lists*.
- **LDP (Lantronix Discovery Protocol)** - this protocol (and open UDP port 30718) can be disabled with the Discovery Server setting. See *SSH/Telnet/Logging*.
- **Saving Device Configurations** - configurations saved via the Maintenance web page (tarball format) are not encrypted, and if used, should be securely stored as configurations contain credentials that should be protected. See *Firmware & Configurations*.
- **Local Users** - configure the following Local User settings: enable Complex Passwords, disable reuse of passwords, enable Failed Login Attempts before Account is Locked, and limit sysadmin access to the console port only. Enable Password Expiration for each user.
- **User Permissions** - for Local Users, Remote Users, Groups and any remote authentication protocols, configure the minimum permissions needed for each user or group. For LDAP and RADIUS, user permissions can be pulled from the authentication server instead of configuring permissions on the console manager.

Appendix B: Safety Information

Safety Precautions

Please follow the safety precautions described below when installing and operating the SLC advanced console server.

Caution: ***EQUIPMENT IS FOR INDOOR USE ONLY!***

Caution: ***Equipment is intended for installation in a Restricted Access Area.***

Fuse Caution Statement

For protection against fire, replace the power-input-module fuse with the same type and rating.

Pour préserver la protection contre l'incendie, remplacez toujours le fusible du module d'alimentation électrique par un modèle du même type et de la même capacité.

Ersetzen Sie die Netzteilsicherung nur durch eine Sicherung desselben Typs und derselben Nennstromstärke um die Gefahr eines Brandes zu vermeiden.

Para proteger la unidad contra el fuego, sustituya el fusible del módulo de entrada de alimentación por otro del mismo tipo y capacidad.

주의 – 전원 입력 모듈 퓨즈를 교환할 때는 화재 예방을 위해 형식과 정격 전압 전류가 동일한 퓨즈를 사용하십시오 .

Предупреждение : Для защиты от пожара заменяйте предохранитель блока питания на предохранитель такого же типа и с такой же характеристикой.

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. The exception is access to the internal modem and RTC battery. For these you don't have to remove the chassis cover, but just the battery/modem door.
- Refer all servicing to Lantronix.
- All interior installation and servicing is to be performed by qualified skilled personnel only

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 SLC unit.
- The SLC 9000 unit must be connected to a branch circuit provided with 15A or 20A, single pole circuit breaker.
- Install the SLC 9000 advanced console server 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

Caution: ***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

1. Maintain reliable grounding of this product.
2. Pay particular attention to supply connections when connecting to power strips, rather than directly to the branch circuit.

Rack

If rack mounted SLC 9000 advanced console servers 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 SLC 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 9000 advanced console server in an environment with an ambient temperature less than the maximum operating temperature of the SLC unit. See *Technical Specifications (on page 30)*.
- 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.
- Mount the equipment in the rack so that a hazardous condition is not achieved due to uneven mechanical loading.
- 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).
- Before operating the SLC 9000 advanced console server, make sure the SLC unit is secured to the rack.

Port Connections

Caution: ***Only Laser Class 1 optical transceivers shall be used.***

- Only connect the network port to an Ethernet network that supports 10/100/1000 Base-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).

- Only connect a telephone line to the MODEM port.

Caution: ***To reduce the risk of fire, use only number 26 AWG or larger (e.g., 24 AWG) UL-listed or CSA-certified telecommunication line cord.***

Caution: ***Risk of fire or explosion if the battery is replaced by an incorrect type. Dispose of Used Batteries According to the instructions.***

Appendix C: 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 9000 advanced console server 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.

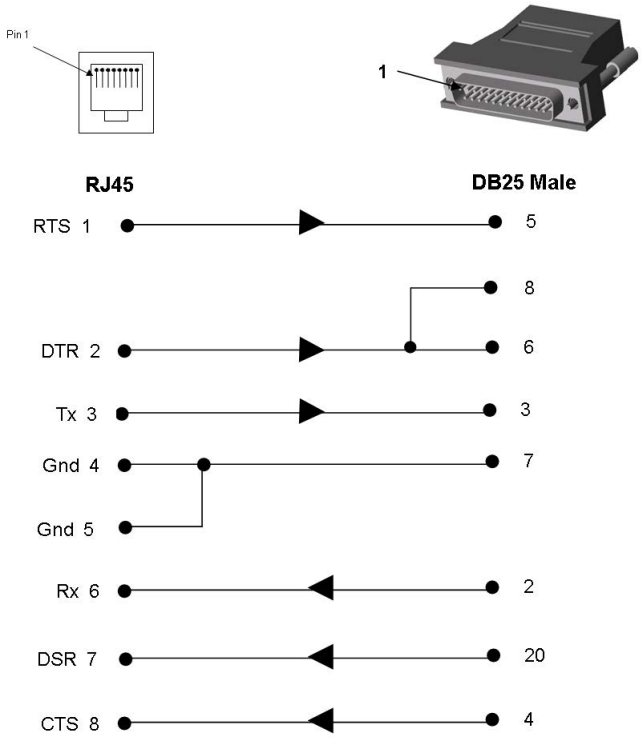
In most cases, you will need an adapter for your serial devices. Lantronix offers a variety of RJ45-to-serial connector adapters for many devices. These adapters convert the RJ45 connection on the SLC unit to a 9-pin or 25-pin serial connector found on other manufacturers' serial devices or re-route the serial signals for connections to other devices that use RJ45 serial connectors.

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 Devices > Console Port page, or the command line interface* `show console port` *and* `set consoleport` *commands.*

The adapters illustrated below are compatible with the Lantronix SLC models.

Figure C-1 RJ45. Receptacle to DB25M DCE Adapter for the SLC unit (PN 200.2066A)



Use PN 200.2066A adapter with a dumb terminal.

Figure C-2 RJ45 Receptacle to DB25F DCE Adapter for the SLC unit (PN 200.2067A)

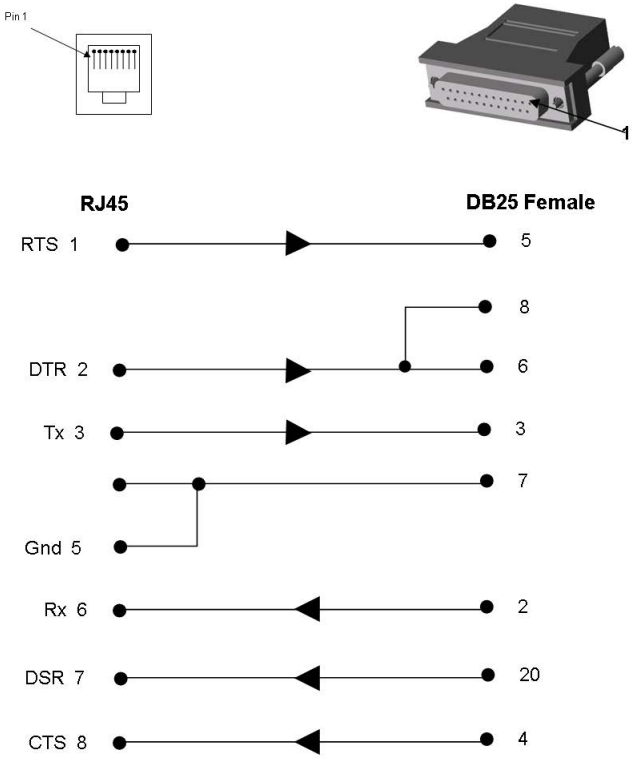


Figure C-3 RJ45 Receptacle to DB9M DCE Adapter for the SLC unit (PN 200.2069A)

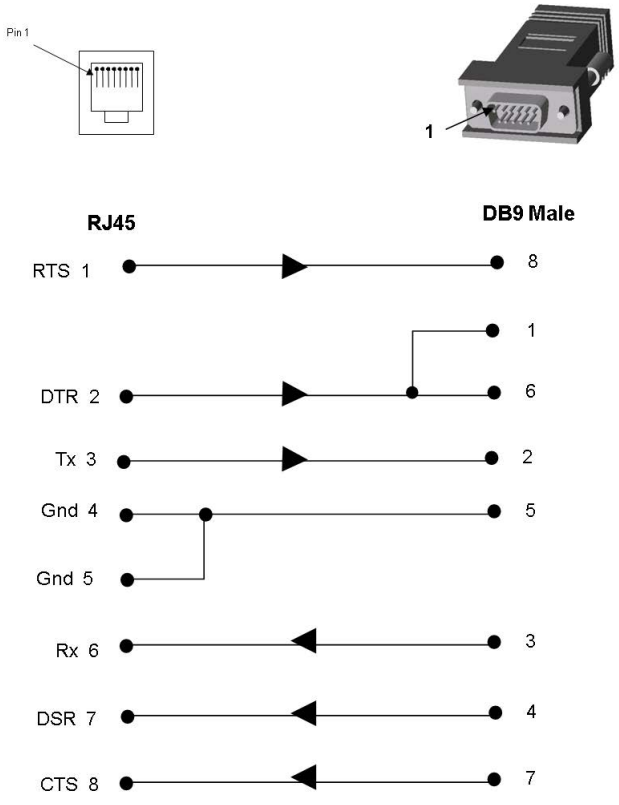
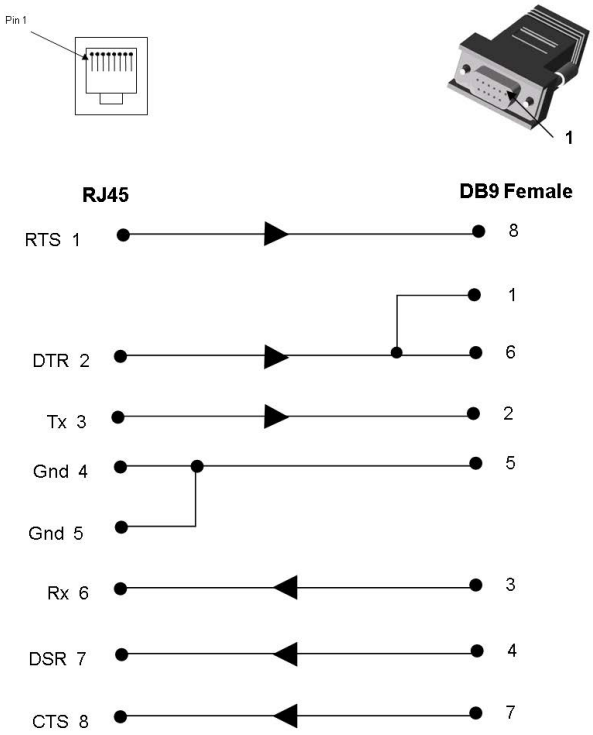
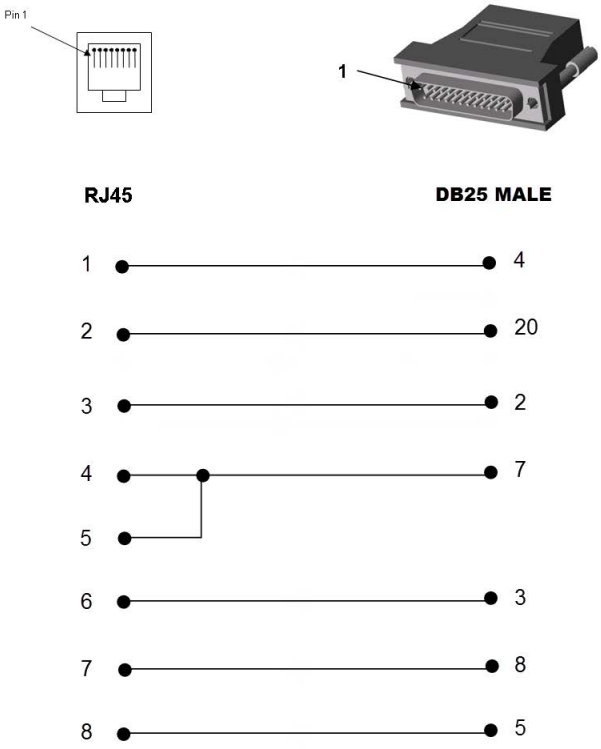


Figure C-4 RJ45 Receptacle to DB9F DCE Adapter for the SLC unit (PN 200.2070A)



Use PN 200.2070A adapter with a PC's serial port.

Figure C-5 RJ45 Receptacle to DB25M DTE Adapter (PN 200.2073)



Appendix D: 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 nameserver to translate text host names into numeric IP addresses.

IPSec

A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

LDAP (Lightweight Directory Access Protocol)

A protocol for accessing directory information.

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.

NMS (Network Management System)

NMS acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP.

NTP (Network Time Protocol)

A protocol used to synchronize time on networked computers and equipment.

PAP (Password Authentication Protocol)

A method of user authentication in which the username and password are transmitted over a network and compared to a table of name-password pairs.

PPP (Point-to-Point Protocol)

A protocol for creating and running IP and other network protocols over a serial link.

RADIUS (Remote Authentication Dial-In User Service)

An authentication and accounting protocol. Enables remote access servers to communicate with a central server to authenticate dial-in users and their access permissions. A company stores user profiles in a central database that all remote servers can share.

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.

TLS

A security protocol that provides privacy and data security for communications over internet.

Appendix E: Compliance Information

Manufacturer's Name & Address

Lantronix Inc., 48 Discovery, Suite 250, Irvine, CA 92618 USA

Declares that the following product:

Product Name(s): SLC™ 9000 Advanced Console Server

Conforms to the following standards or other normative documents:

Safety

- IEC 60950-1:2005 (2nd Edition); Am 1:2009 + A2:2013
- EN 60950-1:2006 + A11:2009 + A1:2010 + + A12:2011 + A2:2013
- UL 60950-1, 2nd Edition, 2014-10-14 (Information Technology Equipment - Safety - Part 1: General Requirements)
- CAN/CSA C22.2 No. 60950-1-07, 2nd Edition, 2014-10 (Information Technology Equipment - Safety - Part 1: General Requirements)
- GB4943.1: 2011 China Product Safety Compliance for ITE

Electromagnetic Emissions

- FCC Part 15, Subpart B, Class A EN 55022: 2011 (IEC/CISPR 22: 2009), class A
- EN 55032: 2012 + AC: 2013 (IEC/CISPR 32: 2015), class A
- KN 22: 2008 and KN 32: 2015 Korea Radio Disturbance Characteristics Compliance for ITE
- GB9254: 2008 China Radio Disturbance Characteristics Compliance for ITE

Electromagnetic Immunity

- EN 55024: 2010 Information Technology Equipment-Immunity Characteristics
- EN 61000-4-2: 2008, KN 61000-4-2 Electro-Static Discharge Test
- EN 61000-4-3: 2010, KN 61000-4-3 Radiated Immunity Field Test
- EN 61000-4-4: 2012, KN 61000-4-4 Electrical Fast Transient Test
- EN 61000-4-5: 2014, KN 61000-4-5 Power Supply Surge Test
- EN 61000-4-6: 2013, KN 61000-4-6 Conducted Immunity Test
- EN 61000-4-8: 2009, KN 61000-4-8 Magnetic Field Test
- EN 61000-4-11: 2004, KN 61000-4-11 Voltage Dips & Interrupts
- KN 24:2008 and KN 35: 2015 Korea Immunity Characteristics Compliance for ITE

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: 2008 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
- UL/CUL
- RCM
- CB Scheme
- NIST-certified implementation of AES as specified by FIPS 197
- CCC*
- KC*

Note: **Not available in some hardware configurations.*

This product carries the CE mark since it has been tested and found compliant with the following standards:

- Safety: EN 60950-1
- Emissions: EN 55022, EN 55032 Class A
- Immunity: EN 55024

RoHS, REACH and WEEE Compliance Statement

Please visit http://www.lantronix.com/legal/rohs/ for Lantronix's statement about RoHS, REACH and WEEE compliance.

Appendix F: Ansible Interoperability

Ansible is a tool that can be used to automate IT tasks. This page shows an example of an Ansible playbook that queries and configures an EMG console manager. For more information on Ansible see the Ansible documentation suite.

Ansible Installation

The Ansible control node (the host that runs Ansible) can be nearly any Unix/Linux host or Windows host running Windows Subsystem for Linux (WSL) with Python installed. The sample playbook shown here was run on Ubuntu 20.04.03 with Python3 3.10.4 and Ansible 2.17.7 with pyenv (Python version management, example setup here). The Ansible documentation link above contains detailed instructions for installing Ansible.

In addition to Python3 and Ansible, the following modules or packages are required:

- ansible.netcommon.network_cli plugin
- ansible-pylibssh Python bindings
- Python3 paramiko SSHv2 module

Sample ansible version after installation:

```
(ansible_test) sh-5.0$ ansible --version
ansible [core 2.17.7]
  config file = /home/ansy/ansible_test/ansible.cfg
  configured module search path = ['/home/ansy/.ansible/plugins/
modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /home/ansy/.local/share/virtualenvs/
ansible_test-5QOcfLIY/lib/python3.10/site-packages/ansible
  ansible collection location = /home/ansy/.ansible/collections:/usr/
share/ansible/collections
  executable location = /home/ansy/.local/share/virtualenvs/
ansible_test-5QOcfLIY/bin/ansible
  python version = 3.10.4 (main, Dec  5 2024, 15:01:48) [GCC 9.4.0] (/
home/ansy/.local/share/virtualenvs/ansible_test-5QOcfLIY/bin/python)
  jinja version = 3.1.4
  libyaml = True
```

```
(ansible_test) sh-5.0$ pip freeze
ansible==10.7.0
ansible-core==2.17.7
ansible-pylibssh==1.2.2
cffi==1.17.1
cryptography==44.0.0
Jinja2==3.1.4
MarkupSafe==3.0.2
packaging==24.2
pycparser==2.22
PyYAML==6.0.2
resolvelib==1.0.1
```

Ansible Setup

Create a subdirectory to hold the Ansible config and playbook files: a configuration file, a public/private SSH key, an inventory (target hosts) file, and a sample YAML playbook:

```
(ansible_test) sh-5.0$ ls -l
total 60
-rw-rw-r-- 1 ansy ansy    89 Dec  5 15:34 ansible.cfg
-rw------- 1 ansy ansy  1675 Dec  5 15:33 id_rsa
-rw-r--r-- 1 ansy ansy   396 Dec  5 15:33 id_rsa.pub
-rw-rw-r-- 1 ansy ansy   217 Dec  5 15:38 inventory.ini
-rw-rw-r-- 1 ansy ansy   956 Dec  5 17:42 slc_example.yml

(ansible_test) sh-5.0$ cat ansible.cfg
[defaults]
inventory = inventory.ini
host_key_checking = false
host_key_auto_add = false
private_key_file = id_rsa

(ansible_test) sh-5.0$ cat inventory.ini
[all:vars]
ansible_connection=ansible.netcommon.network_cli
ansible_user=christi
ansible_become=no
ansible_network_os=cisco.ios.ios

[allhosts]
10.0.1.91
10.0.1.156


(ansible_test) sh-5.0$ cat slc_example.yml
---
- name: Query version info, run set and show commands, print to terminal
window
  hosts: allhosts
  gather_facts: false

  tasks:
    - name: Ping all hosts
      ansible.builtin.ping:

    - name: Run 'admin version' command
      ansible.netcommon.cli_command:
        command: admin version
      register: command_output
    - debug: var=command_output.stdout_lines

    - name: Run 'show network dns' command
      ansible.netcommon.cli_command:
        command: show network dns
      register: command_output
```

```
    - debug: var=command_output.stdout_lines

    - name: Run 'set network dns' command
      ansible.netcommon.cli_command:
        command: set network dns 1 ipadd 192.168.10.254
      register: command_output
    - debug: var=command_output.stdout_lines

    - name: Run 'show network dns' command
      ansible.netcommon.cli_command:
        command: show network dns
      register: command_output
    - debug: var=command_output.stdout_lines
```

This setup contains the IP addresses of 2 hosts - a SLC and EMG, each running different firmware versions. Ansible authenticates to the SLC and EMG using a local user named **christi** with a SSH public key that has been imported into the SLC and EMG. The local user that Ansible is configured with should have the appropriate console manager permissions and rights to run the CLI commands in the playbook.

```
[emg0c80]> show localu
___Current Local Users
Settings_____________________________________________________
State: enabled
Order: 1
Complex Passwords: disabled
Allow Reuse of Passwords: enabled
Reuse History: 4
Password Lifetime: 90 days
Warning Period: 7 days
Max Failed Login Attempts before Account is Locked: disabled
Lockout Period: disabled
Multiple Sysadmin Web Logins: disabled
Sysadmin Access Limited to Console Port: disabled

Login        Lock Grp Data     Listen   Clear    Esc   Break Menu
Dialback
============ ==== === ======== ======== ======== ===== ===== ======
sysadmin     no   Adm 1-8,U1   1-8,U1   1-8,U1   \x1bA \x1bB  N/
christi      no   Adm 1-8,U1   1-8,U1   1-8,U1   \x1bA \x1bB  N/
2 user(s).  For complete information, use 'show localusers user '.

[emg0c80]> show sshkey import keyuser christi
Imported SSH Keys:
User----------------------Host--------------------------Type----------
christi                   thurmond                      RSA, 2048 bits
```

Pinging Hosts and Running Playbooks

The hosts can be checked for reachability using either SSH (the default) or paramiko:

```
(ansible_test) sh-5.0$ ansible allhosts -m ping -i inventory.ini -c ssh
10.0.1.156 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.0.1.91 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
(ansible_test) sh-5.0$ ansible allhosts -m ping -i inventory.ini -c
paramiko
10.0.1.91 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
10.0.1.156 | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

The **slc_example.yml** playbook queries version information **(admin version)**, queries the current DNS servers, sets a static DNS server, then queries the DNS servers again.

```
$ ansible-playbook -i inventory.ini slc_example.yml

PLAY [Run some set and show commands, and print to terminal window] **

TASK [Ping all hosts] *********************************************
ok: [10.0.1.156]
ok: [10.0.1.91]

TASK [Run 'admin version' command] ********************************
ok: [10.0.1.156]
ok: [10.0.1.91]

TASK [debug] ******************************************************
ok: [10.0.1.91] => {
    "command_output.stdout_lines": [
        "___Current
Version_____________________________________________________________",
        "Model: SLC8016",
        "Firmware Version: 9.5.0.0R15",
        "Firmware Updated: Tue Oct 29 19:37:57 2024",
        "OS Version: IT Management Gateway OS 7.0",
        "Bootloader Version: 2.0.0.0R10",
        "S/N: 0080A38BFC31",
        "Device ID: 00204AVBN213EQJOXUEA1S73KTVQM9YU",
        "Memory: 512 MB",
```

```
        "Flash Size: 512 MB",
        "Power Supply: AC, 2 power supplies",
        "Number of External USB Ports: 2",
        "Ethernet Switch: Installed",
        "Internal Modem: Installed",
        "Eth1 HW Address: 00:80:a3:8b:fc:31",
        "Eth2 HW Address: 00:80:a3:8b:fc:32",
        "Ethernet Switch HW Address: 00:80:a3:8b:fe:f3",
        "Main Board Revision: unknown",
        "NIC Board Type: SFP",
        "NIC Board Revision: 02FPA",
        "NIC Board Eth1 SFP: 1000BASE-T (Vendor: FiberStore PN: SFP-GB-
GE-T Rev: B)",
        "NIC Board Eth2 SFP: [none]",
        "I/O Module Type(s): RJ45-16, ETH-16, ",
        "I/O Module Revision(s): 16SPB, 16ESA,  ",
        "Admin Password Unique to Device: Disabled",
        "Uptime: 9 days, 6 hours, 40 minutes",
        "Software Revisions:",
        "  Kernel: 3.6.5",
        "  Web/TLS: OpenSSL 1.1.1w  11 Sep 2023",
        "  SSH/TLS: OpenSSH_9.8p1, OpenSSL 1.1.1w  11 Sep 2023",
        "  Telnet: netkit-telnet-0.17",
        "  NTP: ntpd 4.2.6p5",
        "  SMB/CIFS: Version 3.6.14",
        "  RIP: 1.2.4",
        "  Web Server: mini_httpd/1.30",
        "  PAM/NIS: 1.3.1",
        "  LDAP: 153",
        "  RADIUS: 2.0.0",
        "  Kerberos: 2.4.8",
        "  TACACS+: 1.6.0",
        "  ShellInABox: 2.19",
        "  VPN: Linux strongSwan U5.9.0/K3.6.5",
        "  Expect: 5.45.4",
        "  Tcl: 8.6",
        "  Python: 3.6.7",
        "  Dnsmasq: 2.84",
        "  Syslog: 2.4.4",
        "",
        "Bootloader Configuration:",
        "  Number of Ports: 16",
        "  Model Number: 103",
        "  Product Name: SLC",
        "  Options: 00000000000000000000000000ffff02",
        "  Features: 0xffff"
    ]
}
ok: [10.0.1.156] => {
    "command_output.stdout_lines": [
        "___Current
Version_____________________________________________________________",
        "Model: EMG851121",
        "Firmware Version: 9.4.0.0R5",
```

```
"Firmware Updated: Thu Apr 18 19:55:34 2024",
"OS Version: IT Management Gateway OS 7.0",
"Bootloader Version: 2.0.0.0R10",
"S/N: 0080A3FA0C80",
"Device ID: 00204ACSKMXENQH72KVF4VYK5X5E426F",
"Memory: 1024 MB",
"Flash Size: 1024 MB",
"Power Supply: external DC",
"Number of External USB Ports: 1",
"Cellular Modem: Installed",
"Cellular Firmware Version: 02.24.05.06",
"Cellular Carrier: VERIZON",
"Cellular USBNet Driver Version: 2020-08-17/SWI_2.64",
"Cellular Serial Driver Version: 2020-08-17/SWI_2.42",
"WiFi: Installed",
"WiFi Radio FW Version: 5.4.46.5",
"WiFi Driver Version: 10.4.0.10",
"Ethernet Switch: Not Installed",
"Internal Modem: Not Installed",
"Eth1 HW Address: 00:80:a3:fa:0c:80",
"Eth2 HW Address: 00:80:a3:fa:0c:81",
"Cellular Modem HW Address: fa:42:6e:a3:4e:08",
"Main Board Revision: 080-0696-00(G)/330-0372-01 (Rev 1)",
"NIC Board Eth1 SFP: [none]",
"NIC Board Eth2 SFP: [none]",
"I/O Module Type(s): RJ45-04, RJ45-04",
"I/O Module Revision(s): 04SPC, 04SPB ",
"Connectivity Module Type(s): WIFI-01, LTE-01",
"Connectivity Module Revision(s): 01WFA, 01LTA",
"Admin Password Unique to Device: Enabled",
"Uptime: 10 days, 6 hours, 31 minutes",
"Software Revisions:",
"  Kernel: 3.6.5",
"  Web/TLS: OpenSSL 1.1.1w  11 Sep 2023",
"  SSH/TLS: OpenSSH_9.6p1, OpenSSL 1.1.1w  11 Sep 2023",
"  Telnet: netkit-telnet-0.17",
"  NTP: ntpd 4.2.6p5",
"  SMB/CIFS: Version 3.6.14",
"  RIP: 1.2.4",
"  Web Server: mini_httpd/1.30",
"  PAM/NIS: 1.3.1",
"  LDAP: 153",
"  RADIUS: 2.0.0",
"  Kerberos: 2.4.8",
"  TACACS+: 1.6.0",
"  ShellInABox: 2.19",
"  VPN: Linux strongSwan U5.9.0/K3.6.5",
"  Expect: 5.45.4",
"  Tcl: 8.6",
"  Python: 3.6.7",
"  Dnsmasq: 2.84",
"  Syslog: 2.4.4",
"",
"Bootloader Configuration:",
```

```
        "  Number of Ports: 8",
        "  Model Number: 120",
        "  Product Name: EMG",
        "  Options: 00000000000000000000000000ffff01",
        "  Features: 0xffff"
    ]
}

TASK [Run 'show network dns' command] ********************************
ok: [10.0.1.156]
ok: [10.0.1.91]

TASK [debug] *********************************************************
ok: [10.0.1.91] => {
    "command_output.stdout_lines": [
        "___Current DNS
Settings_____________________________________________________________",
        "10 of the listed DNS servers are used.",
        "Static DNS Server #1: 11.80.103.7",
        "                  #2: <none>",
        "                  #3: <none>",
        "                  #4: <none>",
        "                  #5: <none>",
        "                  #6: <none>",
        "                  #7: <none>",
        "                  #8: <none>",
        "                  #9: <none>",
        "                 #10: <none>",
        "Eth1 DHCP-Acquired DNS Server #1: 10.0.1.12",
        "Prefer IPv4 DNS Records: enabled",
        "Source IPv4 Address: None",
        "Source IPv6 Address: None"
    ]
}
ok: [10.0.1.156] => {
    "command_output.stdout_lines": [
        "___Current DNS
Settings_____________________________________________________________",
        "3 of the listed DNS servers are used (active).",
        "Static DNS Server #1: 11.80.103.7 (Active)",
        "Static DNS Server #2: <none>",
        "Static DNS Server #3: <none>",
        "Eth1 DHCP-Acquired DNS Server #1: 10.0.1.12 (Active)",
        "Prefer IPv4 DNS Records: enabled",
        "Source IPv4 Address: None",
        "Source IPv6 Address: None"
    ]
}

TASK [Run 'set network dns' command] *********************************
ok: [10.0.1.156]
ok: [10.0.1.91]

TASK [debug] *********************************************************
```

```
ok: [10.0.1.91] => {
    "command_output.stdout_lines": [
        "DNS settings successfully updated."
    ]
}
ok: [10.0.1.156] => {
    "command_output.stdout_lines": [
        "DNS settings successfully updated."
    ]
}

TASK [Run 'show network dns' command] ********************************
ok: [10.0.1.156]
ok: [10.0.1.91]

TASK [debug] *********************************************************
ok: [10.0.1.91] => {
    "command_output.stdout_lines": [
        "___Current DNS
Settings_____________________________________________________________",
        "10 of the listed DNS servers are used.",
        "Static DNS Server #1: 192.168.10.254",
        "                      #2: <none>",
        "                      #3: <none>",
        "                      #4: <none>",
        "                      #5: <none>",
        "                      #6: <none>",
        "                      #7: <none>",
        "                      #8: <none>",
        "                      #9: <none>",
        "                     #10: <none>",
        "Eth1 DHCP-Acquired DNS Server #1: 10.0.1.12",
        "Prefer IPv4 DNS Records: enabled",
        "Source IPv4 Address: None",
        "Source IPv6 Address: None"
    ]
}
ok: [10.0.1.156] => {
    "command_output.stdout_lines": [
        "___Current DNS
Settings_____________________________________________________________",
        "3 of the listed DNS servers are used (active).",
        "Static DNS Server #1: 192.168.10.254 (Active)",
        "Static DNS Server #2: <none>",
        "Static DNS Server #3: <none>",
        "Eth1 DHCP-Acquired DNS Server #1: 10.0.1.12 (Active)",
        "Prefer IPv4 DNS Records: enabled",
        "Source IPv4 Address: None",
        "Source IPv6 Address: None"
    ]
}

PLAY RECAP ***********************************************************
```

```
10.0.1.156              : ok=9    changed=0    unreachable=0    failed=0
skipped=0    rescued=0    ignored=0
10.0.1.91               : ok=9    changed=0    unreachable=0    failed=0
skipped=0    rescued=0    ignored=0
```