

LANTRONIX



vSLM™ 2
Secure Management Software
User Guide

Part Number 900-737-R
Revision C September 2015

Intellectual Property

© 2015 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, *WiBox*, *XPort*, *PremierWave*, and *EDS-MD* are registered trademarks of Lantronix, Inc. in the U.S. and other countries. *SLM*, *vSLM*, *SLC*, *SLB*, *SLP*, *SLK*, *SDS*, *UDS*, *DeviceInstaller*, *Spider*, and *Spider Duo* are trademarks of Lantronix, Inc.

Patented: patents.lantronix.com; Additional patents pending.

Windows and *Internet Explorer* are registered trademarks of Microsoft Corporation. *Firefox* is a registered trademark of the Mozilla Foundation. *Opera* is a trademark of Opera Software ASA. All other trademarks and trade names are the property of their respective holders.

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.

The BSD license is available at <http://opensource.org/licenses>. The GNU General Public License is available at <http://www.gnu.org/licenses/>. Your use of each Open Source component or software is subject to the terms of the applicable license.

Warranty

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

Contacts

Lantronix, Inc.

7535 Irvine Center Drive
Suite 100
Irvine, CA 92618, USA

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

Technical Support

Online: www.lantronix.com/support

Sales Offices

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

Disclaimer

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 or her own expense.*

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user’s authority to operate this equipment.

Changes or modifications to this device not explicitly approved by Lantronix will void the user’s authority to operate this device.

Revision History

Date	Rev.	Comments
December 2014	A	Initial release.
April 2015	B	Updated firmware information.
September 2015	C	Updated document to firmware release 4.1.0.0. to include support for Server Technology PDU/CDU Sentry 3 MIB and 4 MIB for PRO2 models (under “RPM/SLP” in the left navigation menu), the ability to view routing information, the ability to set port viewing for Lantronix devices, and updated CLI commands.

Table of Contents

Intellectual Property	2
Open Source Software	2
Warranty	2
Contacts	2
Disclaimer	3
Revision History	3
List of Figures	12
List of Tables	17
1: About This Guide	21
Purpose and Audience	21
Chapter Summaries	21
Additional Documentation	22
Terminology	23
2: Introduction	25
Benefits	25
IT Management Application	26
Firmware	27
Protocols Supported	27
3: Quick Setup Utility	28
Quick Network Setup	28
Required Information	28
Using Quick Setup on the Command Line Interface	28
Quick Setup Command	31
Syntax	31
Description	31
Using the Web Interface	31
Next Steps	36
4: vSLM 2 Deployment	37
Minimum Hardware Requirements	37
Deployment Instructions	37
30-Day Trial License	39
5: Web and Command Line Interfaces	40
Web Interface	40
Logging in	40

Typical vSLM 2 Web Page	41
Notes	42
Web Page Help	43
Logging Out of the Web Interface	44
Command Line Interface (CLI)	44
Logging into the CLI	44
Commands	45
Command Help	46
Tips	46
Logging Out of the CLI	46
CLI Commands	47
Session Commands	48
Syntax	48

6: Configuration and Operation Overview 49

Step 1: Configure Network Settings	49
Step 2: Define Authentication Methods	49
Step 3: Set Up User Account Groups and Accounts	49
Step 4: Auto-Detect Devices	50
Step 5: Associate Account Groups with Ethernet and Managed Devices	50
Step 6: Manage Devices	50
Step 7: Maintain the vSLM 2 Software	51

7: Network and Modem Settings 52

IP Address and Other Required Information	52
Using the Web Interface	53
Network Port(s)	54
Network Gateways	57
Keep Alive	59
Viewing Network Statistics	59
Routing	60
Changing the Current User's Password	61
Network Commands	61
IPv4 Filters	64
Viewing a List of IPv4 Filters	64
Adding an IPv4 Filter	64
Updating or Deleting an IPv4 Filter	66
Viewing the System IPv4 Filter Sets	68
Setting Properties of an IPv4 Filter	70
IPv4 Filter Commands	71
IPsec Management	73
Internet Key Exchange (IKE) Policies	73
Viewing a List of IKE Policies	73

Adding an IKE Policy: _____	74
Updating or Deleting an IKE Policy _____	77
VPN Connections _____	78
Viewing a List of VPNs _____	78
Adding a VPN _____	79
Updating or Deleting a VPN _____	80
Connecting a VPN _____	81
Modem Management _____	81
Viewing a List of Modems _____	81
Configuring a Modem _____	82
Enabling or Disabling Dial-in Connections _____	83
Viewing a List of Profiles _____	84
Adding a Profile _____	85
Updating and Deleting a Profile _____	88
Discovering a USB Modem _____	89
Modem Commands _____	89
Dial Account Commands _____	91

8: User Management 95

User Authentication Methods _____	95
NIS _____	97
LDAP _____	99
RADIUS _____	101
Kerberos _____	103
TACACS+ _____	104
SSH Keys _____	105
Copy Keys _____	109
Authentication Commands _____	109
Account Groups _____	115
Account Group Types _____	115
Viewing Account Groups _____	116
Adding an Account Group _____	117
Updating or Deleting an Account Group _____	117
Setting Password Requirements for User Accounts _____	118
Assigning Account Group Device Rights _____	119
Viewing Currently Logged-In Accounts _____	123
Account Group Commands _____	124
Accounts _____	125
Viewing Accounts _____	125
Adding an Account to the Administrators Account Group _____	128
Adding an Account to an Ethernet or Managed Device Account Group _____	130
Updating or Deleting an Account _____	132
Account Commands _____	133

9: Ethernet Device Management 136

Auto-Detecting Devices	136
Auto-Detect Commands	138
Ethernet Devices	140
Listing Devices	140
Adding a Device Manually	142
Updating or Deleting Ethernet Device Settings	148
Device Locator	150
Configuring Device Racks	150
Assigning Devices to Racks	151
Viewing Ethernet Device and Rack Locations	152
Persistent Connections	154
Polling	158
SLC/SLB Local Connections	160
Device Modem	161
Viewing Session & Audit Log Files, Ping and SNMP Walk	163
Traps	164
Properties (Ethernet Device Menu Tree)	166
Port Access	167
Updating Passwords in Bulk	172
Changing SNMP Settings for SLC, SLB and RPM/SLP Devices in Bulk	174
SLM Proxy	175
Ethernet Device Commands	176
Persistent Connection Commands	181
Trap Commands	183
Ports	184
Viewing a List of Ports	185
Adding a Port	186
Updating or Deleting a Port	189
Connecting Directly to the Port of an SLC or SLB Device	191
Statistics	193
Applying Power to RPM/SLP Ports on a Single Device	194
Viewing Port Logs	195
Port Commands	196

10: Managed Devices 198

Managed Device Groups	199
Viewing All Managed Devices	199
Viewing Managed Device Groups	200
Adding a Managed Device Group	201
Updating or Deleting a Managed Device Group	202
Configuring Polling Settings	202

Managed Device Group Commands _____	203
Connecting to a Managed Device _____	205
Creating Individual Managed Devices _____	207
From a Port _____	207
From a Ports List _____	208
From an Ethernet Device _____	210
Fusing Managed Devices _____	211
Methods of Fusing _____	211
Guidelines _____	211
Fusing a Port with an Existing Managed Device _____	211
Fusing an Ethernet Device with an Existing Managed Device _____	213
Continuing the One-at-a-Time Fusion Process _____	214
Fusing Managed Devices on the Managed Device Group Page _____	215
Configuring a Modem Connection to a Managed Device _____	218
Configuring a Managed Device _____	220
Updating or Deleting a Managed Device _____	221
Managed Device Commands _____	222
Administrators, Ethernet Account Users and Menu Only Users _____	222
Managed Device Users _____	226

11: Operation and Maintenance 228

Searching for Ethernet Devices, Ports, Persistent Connections, Managed Devices, and Users _____	228
Search for an Ethernet Device _____	229
Search for Ports _____	231
Search for Persistent Connections _____	232
Search for Managed Devices _____	233
Search for Users _____	234
Using Wildcards _____	235
Search Commands _____	236
Connecting to Ethernet and Managed Devices _____	237
Connections Overview _____	237
Ethernet Devices - Connection Methods _____	237
Managed Devices - Connection Methods _____	238
Browsing to an Ethernet or Managed Device's Web Page _____	238
Making a Secure Channel Connection to an SLC, SLM, or SLB Device _____	239
Making an SSH Connection to an Ethernet or Managed Device _____	240
Making a Web Channel Connection to an SLC Console Manager _____	241
Making a Telnet Connection to an Ethernet device _____	242
Connection Commands _____	243
Administrators, Ethernet Users and Menu Only Users _____	243
Managed Device Users _____	245
Services _____	246

Banners	248
SSL	249
Status	250
Services Commands	254
Maintenance	256
Maintenance Commands	258
Date and Time	261
Date and Time Commands	262
SNMP & Syslog	263
Device Firmware Updates	265
SLM Firmware	265
SLC/SLB Firmware	267
RPM/SLP Firmware	269
Spider Firmware	271
WiBox Firmware	272
UDS/SDS Firmware Updates	273
Managing Alternate SLM Devices	274
Managing Devices Through the Actions Tab	275
Using the Actions Tab	275
Rebooting or Shutting Down	276
Getting a Log File	276
Getting or Restoring a Configuration File	277
Getting a Sysconfig File	277
Getting or Pushing SSH Keys	277
Reading Information	278
Add Applet	279
Issuing a CLI Command	279
Getting or Pushing Groups	280
Setting the Location and Sub-Location	281
Viewing Progress of Update FW and CLI Commands	281
Events	282
Event Management	282
Updating and Deleting Events	286
Viewing the Event Log	287
Clearing the Event Log	288
Files	288
File Types	288
File Format	290
Viewing, Deleting, and Renaming Files	290
Exporting, Uploading, and Downloading Files	292
Copying Files	294
Setting up NFS	295
Setting up CIFS	296

Setting up Log Properties _____	298
Logging Commands _____	300
12: Using vSLM 2 Software on a Mobile Browser	307
Requirements _____	307
Using the SLM Mobile Browser _____	307
Logging in to the vSLM 2 Software _____	307
Using Links to Select Options _____	308
Using the Keypad to Select Options _____	308
Obtaining More Data _____	308
Logging Out _____	309
Main Menu _____	310
Status Menu _____	311
System Information _____	311
Connections _____	312
Route Information _____	313
Device Menu _____	313
Ethernet Devices _____	314
Ethernet Unreachable Devices _____	315
Managed Devices _____	316
Log Menu _____	317
Filtering Logs _____	317
View Logs _____	318
Appendix A: Command Reference	320
Introduction to Commands _____	320
Command Syntax _____	320
Command Help _____	321
Tips _____	321
Authentication Commands _____	322
Syntax _____	324
Parameters _____	324
Description _____	324
Account Commands _____	326
Account Group Commands _____	328
Administrative Commands _____	330
All Devices Commands _____	335
Auto-Detect Commands _____	335
CLI Commands _____	337
Connection Commands _____	338
Administrators, Ethernet Users and Menu Only Users _____	338
Managed Device Users _____	340

Date and Time Commands	342
Diagnostic Commands	342
Dial Account Commands	344
Ethernet Device Commands	347
IPv4 Filter Commands	352
Logging Commands	354
Audit Log	354
Event Log	356
Port Log	356
Session Log	359
System Log	360
Trap Log	362
Maintenance Commands	364
Managed Devices	366
Administrators, Ethernet Account Users and Menu Only Users	366
Managed Device Users	371
Menu Commands	373
Modem Commands	374
Network Commands	376
Persistent Connection Commands	378
Port Commands	380
Search Commands	382
Services Commands	383
Session Commands	384
SSH Key Commands	385
Task Progress Command	386

Appendix B: Security Considerations **387**

Security Practice	387
Factors Affecting Security	387
Available Services and Port Numbers	387

Appendix C: Protocol Glossary **389**

List of Figures

Figure 1-1 Rights of Ethernet Device Group and Managed Device Group to Devices	24
Figure 2-1 vSLM 2 Overview	26
Figure 3-1 Beginning of Quick Setup Script	29
Figure 3-3 Completed Quick Setup	30
Figure 3-4 SLM Home Page	31
Figure 3-5 Network - Settings Page	32
Figure 3-7 Network Settings - Gateways Tab	33
Figure 3-9 Network Settings - Routing Tab	34
Figure 3-10 Date & Time Page	34
Figure 3-12 Account Page for Sysadmin	35
Figure 5-1 Web Page Layout	41
Figure 5-2 Menu/Tree	41
Figure 5-3 Note for an Account Group	42
Figure 5-4 Example of a Help Page	43
Figure 5-5 Logout on the Page Header	44
Figure 7-1 SLM Configuration Page	53
Figure 7-2 Network Settings Page	54
Figure 7-6 Network Settings - Gateways Tab	57
Figure 7-9 Network Settings - Statistics Tab	59
Figure 7-11 Network Settings - Routing Tab	60
Figure 7-12 Configuration Page - Password Tab	61
Figure 7-13 IPv4 Filter Definitions - List Tab	64
Figure 7-14 New IPv4 Filter Definition - Configure Tab	65
Figure 7-16 IPv4 Filter - Configure Tab	67
Figure 7-17 IPv4 Filter Definitions - Show Tab	68
Figure 7-18 IPv4 Filter - Show Tab	69
Figure 7-19 IPv4 Filter Definitions - Properties Tab	70
Figure 7-21 Internet Key Exchange Policies Page	73
Figure 7-23 Add Internet Key Exchange Policy Page	75
Figure 7-25 Internet Key Exchange Policy - Configure Tab	77
Figure 7-26 VPN Connections Page	78
Figure 7-29 VPN Connection - Configure Tab	80
Figure 7-30 Modems Page	81
Figure 7-32 Modem Page - Configure Tab	82
Figure 7-34 Modem - Dial in Tab	83
Figure 7-36 Modem Profiles - List Tab	84

Figure 7-38 New Profile-Configure Tab	86
Figure 7-42 Modem Profile Page - Configure Tab	88
Figure 8-1 User Authentication - Configure Tab	96
Figure 8-3 NIS Authentication Page - Configure Tab	98
Figure 8-5 LDAP Authentication Page - Configure Tab	100
Figure 8-7 RADIUS Authentication Page - Configure Tab	102
Figure 8-9 Kerberos Authentication Page - Configure Tab	103
Figure 8-11 TACACS+ Authentication Page - Configure Tab	104
Figure 8-13 Manage SSH Keys - SLM Keys Tab	106
Figure 8-17 Manage SSH Keys - SLC/SLB Keys Tab	108
Figure 8-19 Manage SSH Keys - Copy Keys Tab	109
Figure 8-20 Account Groups Page - Accounts Tab	116
Figure 8-21 Account Groups Page - Members Tab	117
Figure 8-22 Account Group Page - Group Tab	117
Figure 8-24 Account Groups - Group Tab	118
Figure 8-25 Account Groups Page - Passwords Tab	118
Figure 8-27 Ethernet Device Account Group - Accounts Tab	120
Figure 8-28 Ethernet Device Account Group - Assign Tab	121
Figure 8-29 Managed Device Account Group - Accounts Tab	122
Figure 8-30 Managed Device Account Group - Assign Tab	122
Figure 8-31 Account Groups - Connections Tab	123
Figure 8-34 Account Groups - Accounts Tab	126
Figure 8-36 Account Page - Configure Tab	127
Figure 8-37 Administrator Account Group - Accounts Tab	128
Figure 8-38 Add New Account to Group "Administrators"- Configure Tab	128
Figure 8-41 Add New Accounts to Group (Nonadministrative) - Configure Tab	130
Figure 8-43 Manage Account - Configure Tab	132
Figure 9-1 Automatic Device Detection Page - Configure Tab	136
Figure 9-3 All Ethernet Devices Page - List Tab	141
Figure 9-4 Manage "SLC" Group Page - List Tab	142
Figure 9-5 Add SLM Device Page - Configure Tab	143
Figure 9-6 Add SLC Device Page - Configure Tab	143
Figure 9-7 Add SLK Device Page - Configure Tab	144
Figure 9-8 Add RPM/SLP Device Page - Configure Tab	144
Figure 9-9 Add Spider Device Page - Configure Tab	145
Figure 9-10 Add Other Lantronix Device Page - Configure Tab	145
Figure 9-11 Add Non Lantronix Device Page - Configure Tab	146
Figure 9-13 Update SLC Device Page - Configure Tab	149

Figure 9-14 Device Locator - Configure Tab _____	151
Figure 9-15 Device Locator - Assign Tab _____	152
Figure 9-16 Device Locator - View Tab _____	152
Figure 9-17 Device Page - PerCons Search _____	154
Figure 9-18 Device Page - Persistent Connection _____	155
Figure 9-19 Add Persistent Connection _____	155
Figure 9-21 Edit Persistent Connection _____	157
Figure 9-22 All Ethernet Devices - Polling Tab _____	158
Figure 9-24 Device Page - LocalCons Tab _____	160
Figure 9-25 Device Page - Modem Tab _____	161
Figure 9-27 Device Page - Utilities Tab _____	163
Figure 9-29 Selected Ethernet Device - Traps Tab _____	165
Figure 9-32 All Ethernet Devices Page - Properties Tab _____	166
Figure 9-34 Manage SLC Group - SLC Tab _____	168
Figure 9-35 Manage SLB Group - Port Access Tab _____	169
Figure 9-36 Manage RPM/SLP Group - Port Access Tab _____	170
Figure 9-37 Manage Spider Group - Port Access Tab _____	171
Figure 9-38 Manage UDS/SDS Group - Port Access Tab _____	172
Figure 9-39 All Ethernet Devices Page - Passwords Tab _____	173
Figure 9-41 All Ethernet Devices Page - SNMP Tab _____	174
Figure 9-43 All Ethernet Devices - vSLM 2 Proxy Tab _____	175
Figure 9-44 Device - Ports Tab _____	185
Figure 9-46 New SLC Port Page - Configure Tab _____	187
Figure 9-51 Port Page - Configure Tab _____	190
Figure 9-53 Manage SLC Group Page - Port Access Page _____	191
Figure 9-54 Connection to Selected SLC Port _____	192
Figure 9-55 Port Page - Statistics Tab _____	193
Figure 9-56 RPM/SLP Power Manager's Device Page - Ports Tab _____	194
Figure 9-57 Port Page - Logs Tab _____	195
Figure 10-1 Virtual Managed Device _____	198
Figure 10-2 Managed Device Groups Page - Devices Tab _____	199
Figure 10-4 Managed Device Groups Page - List Tab _____	200
Figure 10-5 Managed Device Group Page - List Tab _____	201
Figure 10-6 New Managed Device Group Page - Configure Tab _____	201
Figure 10-7 Managed Device Group Page - Configure Tab _____	202
Figure 10-8 Managed Device Groups - Polling Tab _____	203
Figure 10-10 Managed Device Page - Connect Tab _____	205
Figure 10-12 Port Page - Configure Tab _____	207

Figure 10-13 Link to a Managed Device Page - Configure Tab _____	208
Figure 10-14 Managed Device Page - Connect Tab _____	208
Figure 10-15 Device Page - Ports Tab _____	209
Figure 10-16 Device Page for an SLC Device _____	210
Figure 10-17 Fusing on a Port Page - Configure Tab _____	212
Figure 10-18 Virtual Managed Device Page with Two Connections _____	213
Figure 10-19 Fusing a Managed Device on the Device Page _____	213
Figure 10-20 Virtual Managed Device on Managed Device Page - Connect Tab _____	214
Figure 10-21 Managed Device Group - List Tab _____	215
Figure 10-22 Managed Device Group Page - List Tab (After Fusion) _____	216
Figure 10-23 Virtual Managed Device after Fusion _____	217
Figure 10-24 Managed Device Page - Configure Tab _____	218
Figure 10-25 Managed Device Page - Modem Tab _____	219
Figure 10-27 Managed Device Page - Configure Tab _____	220
Figure 10-30 Managed Device - Configure Tab _____	221
Figure 11-1 Search Fields _____	228
Figure 11-3 Example of a Search by “EDS” Ethernet Device _____	230
Figure 11-6 Example of a Search by Port _____	231
Figure 11-8 Example of a Search by Persistent Connection _____	232
Figure 11-10 Example of a Search by Managed Device _____	233
Figure 11-13 Example of a Search by User _____	234
Figure 11-18 Secure Channel Connection to an SLC Console Manager _____	239
Figure 11-20 SSH Login to SLC Console Manager _____	241
Figure 11-21 Web Channel Connection to an SLC Device _____	242
Figure 11-22 Telnet Connection _____	242
Figure 11-23 SLM Services Page _____	246
Figure 11-25 Services Page - Banners Tab _____	248
Figure 11-27 Services - SSL Tab _____	249
Figure 11-29 Services Page - Status Tab _____	250
Figure 11-30 SLM Maintenance Page _____	256
Figure 11-35 Date & Time Page _____	261
Figure 11-38 SNMP & Syslog Page _____	263
Figure 11-40 Device Firmware Update Page - SLM Tab _____	265
Figure 11-43 Device Firmware Update Page - SLC/SLB Tab _____	267
Figure 11-46 Device Firmware Update - RPM/SLP Tab _____	269
Figure 11-49 Device Firmware Update Page - Spider Tab _____	271
Figure 11-51 Device Firmware Update Page - WiBox Tab _____	272
Figure 11-53 Device Firmware Update Page - UDS/SDS Tab _____	273

Figure 11-55 Auto Saving a Configuration _____	274
Figure 11-57 Manage "SLC" Group Actions Tab _____	275
Figure 11-58 Issuing a CLI Command _____	280
Figure 11-59 Viewing Progress of Update FW and CLI Commands _____	281
Figure 11-61 Background Task Progress - Dev Status Tab _____	282
Figure 11-62 Event Management Page - Events Tab _____	283
Figure 11-65 SNMP Trap Configuration (from Lantronix Tech Support FAQ) _____	286
Figure 11-66 Manage Event Page -Event Tab _____	287
Figure 11-67 Event Management Page - Log Tab _____	288
Figure 11-69 SLM Syslog Files Page - Files Tab _____	291
Figure 11-70 SLM Syslog Files Page - Display Tab _____	291
Figure 11-71 Files Page _____	293
Figure 11-72 File Management Page - Copy Tab _____	294
Figure 11-75 File Management Page - NFS Tab _____	295
Figure 11-78 File Management - CIFS Tab _____	296
Figure 11-81 File Management Page - Logging Tab _____	298

List of Tables

Table 3-2 Quick Setup Script	29
Table 3-6 Network Port Settings	32
Table 3-8 Network Gateway Settings	33
Table 3-11 Date & Time	35
Table 5-6 CLI Commands	45
Table 5-7 Actions and Category Options	45
Table 7-3 Network Port Settings	54
Table 7-4 DNS Servers	56
Table 7-5 Hostname	57
Table 7-7 Network Gateway	57
Table 7-8 Keep Alive Settings	59
Table 7-10 Counters for Rx and Tx Transmissions	60
Table 7-15 IPv4 Filter Definition - Configuration Tab	65
Table 7-20 IPv4 Filter Definitions - Properties Tab	70
Table 7-22 Ike Policy Exchange Information	74
Table 7-24 Add Internet Key Exchange Policy - Configure Tab	75
Table 7-27 VPN Connection Settings	78
Table 7-28 Add VPN Connection Settings	79
Table 7-31 Modem - List Tab	82
Table 7-33 Modem - Configure Tab	83
Table 7-35 Modem - Dial-In Tab	84
Table 7-37 Modem Profile - List Tab	84
Table 7-39 New Profile - Configure Tab - Profile	86
Table 7-40 New Profile - Configure Tab - Text Mode	87
Table 7-41 New Profile - Configure Tab - PPP Mode	87
Table 8-2 User Authentication - Configure Tab	96
Table 8-4 NIS Authentication - Configure Tab	98
Table 8-6 LDAP Authentication Settings	100
Table 8-8 RADIUS Authentication Settings	102
Table 8-10 Kerberos Authentication Settings	103
Table 8-12 TACACS+ Authentication Settings	105
Table 8-14 Host and Login SSH Key Settings	106
Table 8-15 Imported Key Settings	107
Table 8-16 Exported Keys Settings	107
Table 8-18 Manage SSH Keys - SLC Keys Tab	108
Table 8-23 Account Group - Group Tab	117

Table 8-26 Password Requirement Settings _____	119
Table 8-32 Inbound Connections _____	123
Table 8-33 Outbound Connections _____	123
Table 8-35 Account Groups - Accounts Tab _____	126
Table 8-39 Add New Account to an Administrator Group - Configure Tab _____	129
Table 8-40 Add New Account to Group (Administrator) - Configure Tab - Permissions _____	129
Table 8-42 Add New Account to Group - Configure Tab _____	131
Table 9-2 Automatic Device Detection - Configure Tab _____	137
Table 9-12 Manually Added New Device Details _____	146
Table 9-20 Add Persistent Connection - Configure Tab _____	156
Table 9-23 Poll Settings _____	158
Table 9-26 Device - Modem Tab _____	162
Table 9-28 Device Session Log File Name Components _____	163
Table 9-30 Trap Settings _____	165
Table 9-31 Clear or Export Trap Log Settings _____	165
Table 9-33 All Ethernet Devices - Properties Tab _____	167
Table 9-40 Settings to Update Passwords in Bulk _____	173
Table 9-42 Settings to Update SNMPs in Bulk _____	174
Table 9-45 Device - Ports Tab _____	186
Table 9-47 New Port - Configure Tab _____	187
Table 9-48 New Port - Configure Tab - Data Settings _____	188
Table 9-49 New Port - Configure Tab - Hardware Signal Triggers _____	189
Table 9-50 New Port - Configure Tab - IP Settings _____	189
Table 9-52 Port - Configure Tab _____	190
Table 9-58 Port - Logs Tab _____	195
Table 10-3 Managed Device Groups - Devices Tab _____	200
Table 10-9 Managed Device Groups - Polling _____	203
Table 10-11 Connection Icons and Buttons on the Connect Tab _____	205
Table 10-26 Managed Device - Modem Tab _____	219
Table 10-28 Managed Device - Configure Tab _____	220
Table 10-29 Managed Device - Configure Tab (View Only) _____	221
Table 11-2 Available Search Fields _____	229
Table 11-4 Device Search Results _____	230
Table 11-5 Search by Port _____	231
Table 11-7 Search Results - Ports _____	231
Table 11-9 Search by Persistent Connection _____	232
Table 11-11 Search by Managed Device _____	233
Table 11-12 Search for Users _____	234

Table 11-14 Search Results - Users	235
Table 11-15 Searching with Wildcards	236
Table 11-16 Methods of Connecting to Ethernet Devices	237
Table 11-17 Methods of Connecting to Managed Devices	238
Table 11-19 Secure Channel Error Codes	240
Table 11-24 SLM Services - Configure Tab	247
Table 11-26 SLM Services - Banners	248
Table 11-28 SLM Services - SSL Tab	249
Table 11-31 SLM Maintenance - General Maintenance	256
Table 11-32 SLM Maintenance - Password Synchronization	257
Table 11-33 SLM Maintenance - Boot Banks	257
Table 11-34 SLM Maintenance - Configuration Management	257
Table 11-36 Date & Time - Configure Tab	261
Table 11-37 Date & Time - Configure NTP	262
Table 11-39 SNMP & Syslog - Configure	263
Table 11-41 Device Firmware Update - SLM Tab	265
Table 11-42 Device Firmware Update - SLM Tab - FTP/SFTP Server	266
Table 11-44 Device Firmware Update - SLC/SLB Tab	267
Table 11-45 Device Firmware Update - SLC/SLB Tab - FTP/SFTP Server	268
Table 11-47 Device Firmware Update - RPM/SLP Tab	269
Table 11-48 Device Firmware Update - RPM/SLP Tab - FTP/SFTP Server	270
Table 11-50 Device Firmware Update - Spider	271
Table 11-52 Device Firmware Update - WiBox	272
Table 11-54 Device Firmware Update - UDS/SDS	273
Table 11-56 Manage Alternate SLM Devices - Select Tab	274
Table 11-60 Manage "SLC" Group - Actions Tab	281
Table 11-63 Event Management - Events Tab - Alarm Type	283
Table 11-64 Event Management - Events Tab - Trigger Type	284
Table 11-68 File Format	290
Table 11-73 File Management - Copy Tab	294
Table 11-74 File Management - Copy Tab - FTP/SFTP Server	294
Table 11-76 File Management - NFS Tab - Remote Directory	295
Table 11-77 File Management - NFS Tab - Local Directory	296
Table 11-79 File Management - CFS Tab - Remote Directory	297
Table 11-80 File Management - CFS Tab - Local Directory	297
Table 11-82 File Management - Logging Tab - Port Logs	298
Table 11-83 File Management - Logging Tab - Audit Logs	299
Table 11-84 File Management - Logging Tab - Session Logs	299

Table 11-85 File Management - Logging Tab - System Logs	299
Table 11-86 File Management - Logging Tab - Persistent Connection Logs	299
Table 12-1 Navigation Summary	309
Table 12-2 Log Filter by Last and Date/Time	317
Table A-1 Command Syntax	320
Table A-2 Actions and Category Options	320
Table B-1 Administration	387
Table B-2 Management	388
Table B-3 Device Access	388

1: About This Guide

Purpose and Audience

This guide provides the information needed to install, configure, and use the Lantronix® vSLM™ secure management software. The vSLM 2 software enables IT professionals to remotely and securely configure and administer multiple Lantronix and non-Lantronix devices.

Chapter Summaries

The remaining chapters in this guide include:

Chapter	Description
Chapter 2: Introduction	Describes the vSLM 2 software's main features and the protocols it supports.
Chapter 3: Quick Setup Utility	Provides instructions for getting your unit up and running. Describes connection formats and power supplies and how to configure network, date, and time settings so you can use the vSLM 2 secure management software on the network.
Chapter 4: vSLM 2 Deployment	Provides directions on how to deploy vSLM 2 secure management software.
Chapter 5: Web and Command Line Interfaces	Describes the web and command line interfaces available for configuring the unit. Note: <i>The configuration chapters (6-9) provide detailed instructions for using the web interface and include command line interface commands.</i>
Chapter 6: Configuration and Operation Overview	Outlines the process of setting up and using the vSLM 2 software and explains the responsibilities of administrators and other user groups.
Chapter 7: Network and Modem Settings	Provides instructions on entering network, date, and time information.
Chapter 8: User Management	Provides instructions for configuring user authentication methods and setting up user accounts and account groups.
Chapter 9: Ethernet Device Management	Provides instructions for detecting devices on the network, entering information about the devices and ports, granting read/write permissions for devices and ports, and auto-saving an vSLM 2 configuration to another vSLM 2 secure management software.
Chapter 10: Managed Devices	Explains how to add, update, and delete Managed Device Groups as well as how to create and "fuse" individual managed devices. Provides information about connecting to and configuring managed devices via the vSLM 2 software.

Chapter (continued)	Description
Chapter 11: Operation and Maintenance	Explains how the user can search for devices, access notes and logs about the SLC™ console manager and its ports, and open the RPM/SLP™ power manager, SLK™ remote KVM manager and SLC device interfaces using SSH, secure channel (SLC console manager only), or a browser. Provides instructions for upgrading firmware, viewing system logs and diagnostics, and generating reports. Includes information about web pages and commands used to shut down and reboot the vSLM 2 secure management software.
Chapter 12: Using vSLM 2 Software on a Mobile Browser	Provides instructions for accessing and monitoring the vSLM 2 secure management software using a mobile phone.
Appendix A: Command Reference	Lists and describes all of the commands used on the vSLM 2 software command line interface.
Appendix B: Security Considerations	Provides tips for enhancing vSLM 2 secure management software security.
Appendix C: Protocol Glossary	Briefly describes networking protocols.

Additional Documentation

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

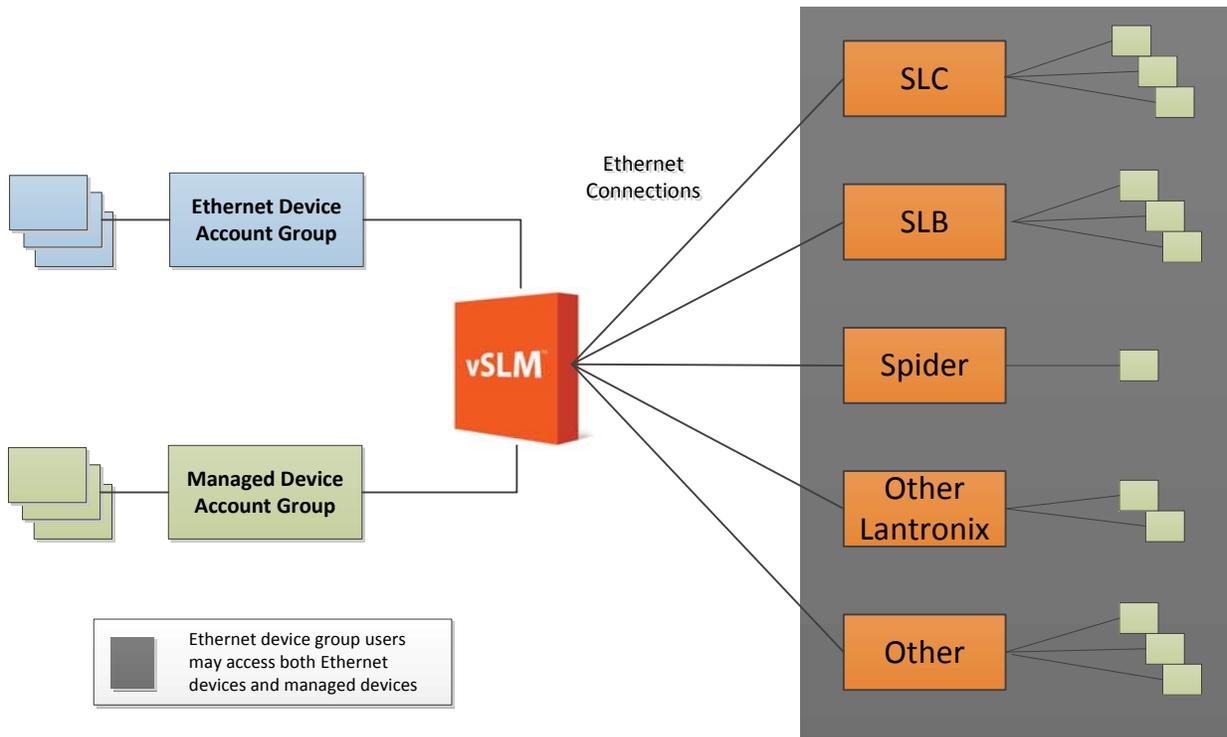
Document	Description
<i>vSLM 2 Secure Management Software Product Brief</i>	Provides basic overview of product information for the vSLM 2 secure management software.
<i>vSLM 2 Secure Management Software - Installation Procedure for ESX, ESXi from vSphere Client</i>	Provides installation procedures for ESX and ESXi from vSphere Client for use with the vSLM 2 software.
<i>vSLM 2 Secure Management Software - Installation Procedure for VMware Workstation</i>	Provides installation procedures for the VMware workstation for use with the vSLM 2 software.
<i>SLM Management Appliance Online Help for the Command Line Interface</i>	Provides online Help for configuring and operating the vSLM 2 software using commands.
<i>SLM Management Appliance Online Help for the Web Interface</i>	Provides online Help for configuring and operating the vSLM 2 software using the web interface.

Terminology

In this User Guide, we use the following terms:

Term	Definition
Ethernet Device	<p>A Lantronix or non-Lantronix device that the vSLM 2 secure management software discovers on the network. Ethernet devices include:</p> <ul style="list-style-type: none"> ◆ Secure IT Management Devices: Members of the secure IT management family of products include the SLC console manager, remote power manager (RPM), SLP power manager, SLK KVM manager, WiBox® device, SLB™ branch office manager, and Spider™ device. These devices enable you to remotely and securely access and manage networking equipment. <p><i>Note: "RPM/SLP" in the document refer to remote power managers (PDU.)</i></p> <ul style="list-style-type: none"> ◆ Management Devices: Lantronix devices that enable you to manage networking equipment. The SCS™05/20 secure console server is an example. ◆ Lantronix Devices: Other Lantronix products that network-enable serial devices so you can remotely control, monitor, diagnose, and troubleshoot your equipment over a network or the Internet. ◆ Other Devices: Non-Lantronix Ethernet devices.
Port	A connector (e.g., serial, power, or KVM) on a management device (e.g., SLC, RPM/SLP, SLK, SCS devices) that allows for control of another device.
Managed Device	A device (such as a Unix server) that has one or more of its connections (e.g., serial, power, or KVM) exposed to allow control and configuration changes by Managed Device Users. A managed device belongs to a Managed Device Group.
Managed Device Group	A group created to allow logical clustering of managed devices (e.g., devices of the same type or devices in the same physical location). A managed device may not be created until at least one Managed Device Group has been defined.
Account	Individual users; must belong to an account group, from which they inherit permissions.
Account Group	<p>A group of accounts (users) with the same privileges. The four types of account groups include:</p> <p>Administrators Group: The sysadmin account, which has all privileges and others with specified configuration privileges.</p> <p><i>Note: Throughout this user guide, the term "administrator" means the person using the sysadmin user name and those members of the Administrators Group permitted to perform the task.</i></p> <p>Ethernet Device Account Groups: Have access to specified Ethernet devices and the managed devices connected to them.</p> <p>Managed Device Account Groups: Have access to devices attached to specified Ethernet device ports.</p> <p>Menu Only Account Groups: May only access the command line interface and use a limited menu of options.</p>

Figure 1-1 Rights of Ethernet Device Group and Managed Device Group to Devices



2: Introduction

The vSLM 2 secure management software is a member of the secure IT management family of products. There are three models of SLM: the vSLM 2 model which is the virtual, software-only version of the vSLM 2 secure management software as well as the SLM-01 and SLM-02 models which include both the hardware and software. This user guide provides information on only the vSLM 2 software. Other products in the Lantronix secure IT management family include, but are not limited to: the SLC 8000 Console Managers, the SLB Branch Office Managers, and Spiders. These products offer systems administrators and other IT professionals a variety of tools for remotely and securely accessing and managing their networking equipment.

Note: For more information about the vSLM 2 software, please see the Lantronix website at www.lantronix.com/vslm.

The vSLM 2 software manages Lantronix and non-Lantronix devices. It "auto-detects" and then displays them in a single, concise view through a web or a command line interface (CLI). A user can search the web view for a desired device or device port (in the case of an SLC console manager or SLK KVM manager) and then connect to a found device or port without using a separate interface. With an SLC device, the user logs in only once, to the vSLM 2 software, and then any subsequent device logins are automatic. The SLM management device can also use LDAP, RADIUS, NIS, Kerberos, TACACS+, and SSH public key to authenticate users connecting remotely to the command line interface.

Benefits

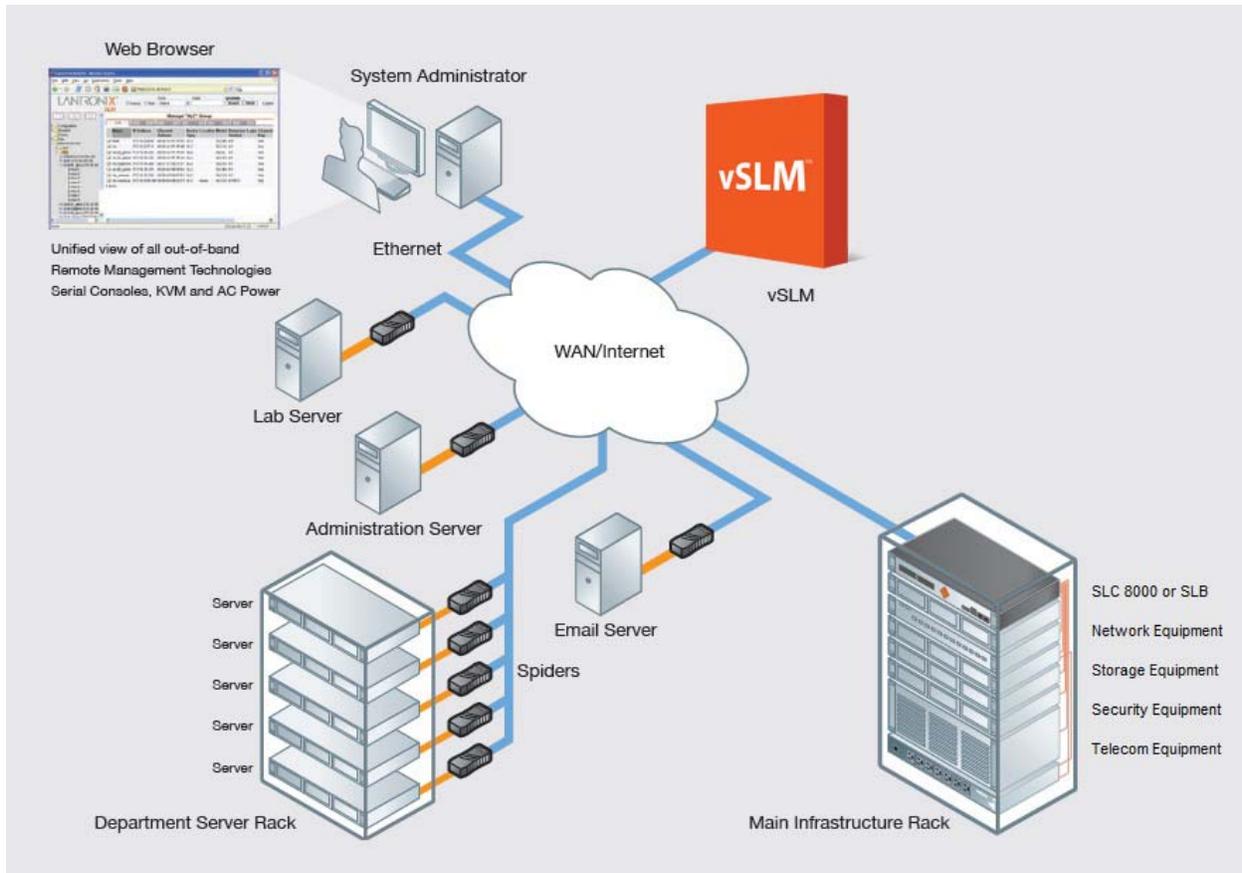
With the vSLM 2 software, you can:

- ◆ Consolidate management of IT infrastructure through a simple browser interface.
- ◆ Maintain a secure, central point of access to all equipment with centralized console logging.
- ◆ Reduce equipment diagnosis and repair time while minimizing the cost of ownership and administrative resources.
- ◆ Maintain more network up time.

IT Management Application

The following diagram shows how a user can perform management activities through the vSLM 2 secure management software.

Figure 2-1 vSLM 2 Overview



Firmware

The SLM firmware has the following features:

- ◆ User and events logging
- ◆ Email notification of trap events, log file events, and Ethernet down
- ◆ ID/Password security, configurable access rights
- ◆ SSH and SSL security
- ◆ External authentication through RADIUS, LDAP, NIS, Kerberos, and TACACS+
- ◆ Shared authentication among SLM and SLC devices
- ◆ SLC firmware version storage and updates
- ◆ Local access through a console port
- ◆ Web presentation of SLC device and ports in a user-configured view
- ◆ Web administration (using most browsers)
- ◆ Direct SSH access to SLC devices or SLC ports from the web view
- ◆ Auto-discovery of devices and other Lantronix and non-Lantronix Ethernet devices
- ◆ Support for an internal PCI or external USB modem
- ◆ SNMP MIB2 and private MIB
- ◆ SNMP trap target
- ◆ Mobile phone WAP browser access

Protocols Supported

In addition to supporting the TCP/IP network protocol, the vSLM 2 secure management software supports:

- ◆ SSH for connections in and out of the SLM
- ◆ SMTP for mail transfer
- ◆ SNMP for remote monitoring and management
- ◆ SFTP and FTP for file transfers and firmware upgrades
- ◆ DHCP and BOOTP for IP address assignment
- ◆ HTTPS (SSL) for secure browser-based configuration
- ◆ NTP for time synchronization
- ◆ LDAP, NIS, RADIUS, Kerberos, and TACACS+, and SSH public key encryption for remote user authentication
- ◆ WAP for mobile phone access

For brief descriptions of these protocols, see [Appendix C: Protocol Glossary](#).

3: Quick Setup Utility

This chapter provides instructions for entering basic network settings so you can configure and use the SLM on a network. For instructions on setting up the vSLM 2 secure management software, go to [Chapter 4: vSLM 2 Deployment](#).

Quick Network Setup

This section helps get the IP network port up and running quickly, so you can administer the vSLM 2 secure management software using your network. Your vSLM 2 software must have a unique IP address on your network. The vSLM 2 secure management software receives an IP address in one of three ways:

Automatically: The first time you power up the vSLM 2 software, Network Port 1 tries to obtain its IP address via DHCP. If you have connected Network Port 1 to a network with a DHCP server, it acquires an IP address. Smaller networks may use BOOTP.

Using DeviceInstaller™ Utility: This software allows you to quickly assign a static IP address to a unit that has an automatically assigned IP address. This utility can be downloaded from the Lantronix website, by selecting the Management Platform product from the Firmware/Downloads page: www.lantronix.com/support/downloads.

Manually: If the vSLM 2 secure management software cannot obtain an IP address by means of DHCP, you must manually enter one using the vSLM 2 console port window, which is the window display by the virtualization software.

The administrator generally provides the IP address and corresponding subnet mask and gateway. If you assign an IP address manually, **it must be within a valid range and unique to your network.**

Required Information

To set up the vSLM 2 software quickly so you can use it on your network, you must first enter some basic information about one network port and the network.

IP address (if not already assigned): _____ . _____ . _____ . _____

Subnet mask (if not already assigned): _____ . _____ . _____ . _____

Gateway: _____ . _____ . _____ . _____

Using Quick Setup on the Command Line Interface

If the vSLM 2 secure management software does not have an IP address, you can use the vSLM 2 console port window to access the command line interface. If the unit already has an IP address, you can use SSH to connect to the command line interface and add or change the IP address or other network-related information.

To complete the command line interface Quick Setup script:

Note: [Chapter 5: Web and Command Line Interfaces](#) describes the command line interface in detail.

1. Do one of the following:
 - ◆ With a serial terminal connection, power up, and when the command line displays, press

Enter.

- ◆ With a network connection, use an SSH program to connect to xx.xx.xx.xx (the IP address in dot quad notation) and press **Enter**. The login prompt displays.
2. Type `sysadmin` (case sensitive) as the user name and press **Enter**.
 3. Type `PASS` (case sensitive) as the password and press **Enter**.

Figure 3-1 Beginning of Quick Setup Script

```
Firmware revision: 4.1.0.0 (FW update success - 08/20 15:58)
Login name: sysadmin
Group name: Administrators
Authentication type: Local User
```

```
vSLM License: 28 days remaining
```

```
Login time: Thu Aug 20 16:34:18 2015
For a list of commands, type 'help'.
```

```
Do you want to do quick setup? [no] yes
```

4. In response to the prompt asking whether you want to do the quick setup, type `yes` and press **Enter**.

Note: The prompt displays the first time you log in only. If you want to run the script again, type `admin quicksetup`.

5. Enter the following information at the prompts:

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

Table 3-2 Quick Setup Script

Script	Description
Configure Port 1 or 2	<p>Select one of the following:</p> <p><1> obtain IP Address from DHCP: The unit will acquire the IP address and gateway from the DHCP server. (The DHCP server may provide the gateway, depending on its setup.) This is the default setting.</p> <p><2> obtain IP Address from BOOTP: Permits a network node to request configuration information from a BOOTP "server" node.</p> <p><3> static IP Address: Requires you to assign a static IP address manually. The administrator generally provides the IP address.</p> <p>Note: For SLM-01, Network Port 1 is 10/100/1000Base-T, while Network Port 2 is 10/100Base-T. For SLM-02, both Network Ports 1 and 2 are 10/100/1000Base-T.</p>
IP Address (if specifying)	<p>An IP address that will be unique and valid on your network and in the same subnet as your PC. There is no default.</p> <p>If you selected DHCP or BOOTP, this prompt does not display.</p> <p>Note: Enter all IP addresses in dot quad notation.</p>

Script	Description
Subnet Mask	The subnet mask specifies the network segment on which the SLM console manager resides. There is no default. If you selected DHCP or BOOTP , this prompt does not display.
Gateway IP Address	IP address of the router for this network.
Hostname	The default host name is vSLM 2 secure management software. The host name can be a short host name or a fully qualified domain name. For example, we might add lantronix.com to the factory default name of vSLM 2 software to get SLM.lantronix.com. There is a 64-character limit (contiguous characters).
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 password for the sysadmin account. It can be up to 128 characters and is case sensitive.

Figure 3-3 Completed Quick Setup

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

The current settings are shown in brackets ('[]').

You can accept the current setting for each question by pressing <return>.

```

____ Ethernet Port and Default Gateway _____
The SLM has two ethernet ports, Port 1 and Port 2.
Current settings are:
Port State      IP address      Subnet mask Mode                IPv4 filter
-----
1    DHCP        172.19.100.216 255.255.0.0 Auto-negotiate (None)
2    Disabled    0.0.0.0         0.0.0.0      Auto-negotiate (None)

Port Static IPv6 address Link IPv6 address
-----
1                                fe80::20c:29ff:fe98:ed25/64
2

Configure Port 1 or 2: [1]
Configure Port 1:  (1) obtain IP Address from DHCP(172.19.100.216)
                  (2) obtain IP Address from BOOTP
                  (3) static IP Address

Enter 1-3: [1]
Specify a hostname: [SLM1F4F]

____ Time Zone _____
The current time zone is 'US/Pacific'.
Enter time zone: [US/Pacific]

____ Date/Time _____

```

```
The current time is Thu Aug 20 16:34:33 2015
Change the current time? [n]
```

```
____Sysadmin Password_____
The default sysadmin (administrator user) password is 'PASS'.
New password: [PASS]
Network settings will be updated, the current terminal may not work.
Please re-connect to SLM with new settings as needed.

[sysadmin@SLM1F4F]>
```

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

Quick Setup Command

admin quicksetup

Syntax

```
admin quicksetup
```

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command.

Using the Web Interface

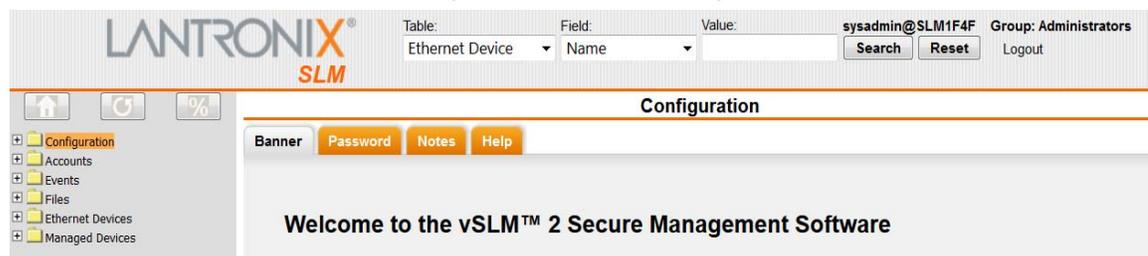
Note: [Chapter 5: Web and Command Line Interfaces](#) describes the web interface in detail.

Once the vSLM 2 secure management software has an IP address, you can use the web interface to configure required network parameters that determine how the vSLM 2 software interacts with the attached network. The unit might have a DHCP-assigned IP address or one assigned manually using Detector software or a serial connection to the command line interface.

To log in to the web interface:

1. Open a web browser (Internet Explorer® 6.0. and later, or Firefox® 1.5 and later, with JavaScript enabled).
2. In the URL field, type `https://` followed by the IP address of your vSLM 2 secure management software.
3. Log in using `sysadmin` as the user name and `PASS` as the password. The SLM Configuration page opens.

Figure 3-4 SLM Home Page



To enter settings for one network port:

1. On the menu (in the pane on the left), click **Configuration > Network Settings**. The following page opens:

Figure 3-5 Network - Settings Page

The screenshot shows the LANTRONIX SLM Network Settings page. The left sidebar contains a navigation menu with 'Configuration' expanded to 'Network Settings'. The main content area has tabs for 'Settings', 'Gateways', 'Keep Alive', 'Statistics', 'Routing', 'Notes', and 'Help'. The 'Settings' tab is active, showing configuration for two network ports. Network Port 1 is configured with IP Address 172.19.100.216, Subnet Mask 255.255.0.0, and Default Gateway 172.19.0.1. Network Port 2 is currently disabled. The page also includes fields for DNS Servers, Hostname (SLM1F4F), and an Update button.

2. Enter the following information for one network port:

Table 3-6 Network Port Settings

Setting	Description
Network Port Settings	<ul style="list-style-type: none"> ◆ Disabled: This is the default setting for Network Port 2. ◆ Obtain from DHCP: Acquires IP address, subnet mask, and gateway from the DHCP server. (The DHCP server may provide the gateway, depending on its setup.) This is the default setting for Network Port 1. If you select this option, skip to step 3. ◆ Obtain from BOOTP: Lets a network node request configuration information from a BOOTP "server" node. Skip to step 3. ◆ Specify: Requires you to assign a static IP address manually. The administrator generally provides the IP address.
IP Address	<p>If specifying an IP address, enter an IP address that will be within a valid range, unique to your network, and in the same subnet mask as your workstation. There is no default.</p> <p>Note: Enter all IP addresses in dot quad notation.</p>
Subnet Mask	<p>If specifying an IP address, enter the network segment on which the vSLM 2 secure management software resides. There is no default.</p>

- To save your entries, click **Apply**. Clicking Apply commits these changes immediately. Next, enter network gateway information.

To enter gateway information:

- On the Network - Settings page, click the **Gateways** tab. The following page opens:

Figure 3-7 Network Settings - Gateways Tab

- Enter the following:

Table 3-8 Network Gateway Settings

Setting	Description
Default	<p>IP address of the router for this network.</p> <p>If this has not been set manually, any gateway assigned by DHCP for Network Port 1 or Network Port 2 displays.</p> <p>All network traffic that matches the Network Port 1 IP address and subnet mask goes out Network Port 1. All network traffic that matches the Network Port 2 IP address and subnet mask goes out Network Port 2.</p> <p>If you set a default gateway, the vSLM 2 software sends any network traffic that does not match Network Port 1 or Network Port 2 to the default gateway for routing.</p>
DHCP Acquired (view only)	Gateway assigned by DHCP for Network Port 1 or Network Port 2. The default setting is None .
Precedence	Indicates whether the gateway assigned by DHCP or the default gateway takes precedence. The default setting is Default . If you select DHCP, and both network ports are configured for DHCP , the vSLM 2 secure management software gives precedence to the Network Port 1 gateway.

Note: You have configured only the settings required to get the vSLM 2 software up and running. To complete the network configuration, see [Chapter 7: Network and Modem Settings](#).

To view the current IPv4 and IPv6 routing information:

- On the Network - Settings page, click the **Routing** tab. The following page opens:

Figure 3-9 Network Settings - Routing Tab

Contents of route.txt

```

Kernel IP routing table
Destination      Gateway         Genmask         Flags         MSS Window  irtt Iface
172.19.39.247   172.19.0.1     255.255.255.255 UGH          0 0        0 eth0
172.19.0.0     0.0.0.0        255.255.0.0    U           0 0        0 eth0
0.0.0.0        172.19.0.1     0.0.0.0        UG          0 0        0 eth0

Kernel IPv6 routing table
Destination      Next Hop        Flags Metric Ref  Use Iface
::1/128         ::              U      0   23  1 lo
2001:db80:ac13:d91e:20c:29ff:fe98:ed25/128 ::              U      0   0   1 lo
2001:db80:ac13:d91e::/64      ::              UA     256 5281 0 eth0
fe80::20c:29ff:fe98:ed25/128 ::              U      0   0   1 lo
fe80::/64        ::              U     256 0   0 eth0
ff02::1/128     ff02::1        UC     0   158 0 eth0
ff00::/8        ::              U     256 0   0 eth0
::/0            fe80::20c:29ff:fee9:bc25 UCDA 1024 1   0 eth0

```

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

You can specify the current date, time, and time zone at the vSLM 2 secure management software's location (default), or the vSLM 2 software can use NTP to synchronize with an NTP server on your network.

1. On the menu, click **Configuration > Services > Date & Time**. The following page opens:

Figure 3-10 Date & Time Page

Change Date/Time:

Date: August 20 2015

Time: 18 : 25 : 32

Time Zone: US/Pacific

SLM Up Time: 0 days, 2 hours, 12 minutes

Enable NTP: The SLM can synchronize its clock with a remote time server using NTP.

Synchronize via: Broadcast from NTP Server

Poll NTP Server:

Public: US/San Jose: clock.sjc.he.net (216.218.254.202)

Local:

2. Enter the following information:

Table 3-11 Date & Time

Date and Time Setting	Description
Change Date/Time	Select the check box to manually enter the date and time at the vSLM 2 secure management software'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.
SLM Up Time	Indicates how long the vSLM 2 software has been up and running.

3. To save, click **Update**.

To change the administrator password:

The default sysadmin password is **PASS**.

1. On the menu, click **Accounts > Administrators > sysadmin**. The following page opens:

Figure 3-12 Account Page for Sysadmin

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main content area is titled 'Manage Account "sysadmin"'. On the left, there is a navigation tree with 'Accounts' expanded to 'Administrators', where 'sysadmin' is selected. The main configuration area has tabs for 'Configure', 'Move', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following fields and options:

- Name: sysadmin
- Password: [masked]
- Retype: [masked]
- Email: [empty]
- Allow Password Change:
- Password Never Expires:
- Change Password on Next Login:
- Synchronize Password:
- Enable Dial-Back: Dial Back Number: [empty]
- Authentication: Local Only
- Account Group: Administrators
- Allow Network Modifications:
- Allow Authentication Modifications:
- Allow Service Modifications:
- Allow Device Management:
- Allow Account Modification:
- Allow Event Modification:
- Allow Log File Management:

At the bottom of the configuration area, there are 'Update' and 'Reset' buttons.

2. Enter the new administrator password in **Password** and (Retype). The password can be up to 128 characters and is case sensitive.

3. Click the **Update** button. When the update is complete, a confirmation message displays.

Next Steps

After quickly getting the vSLM 2 secure management software up and running, you can complete the configuration on the web pages.

- ◆ To learn more about the interfaces, go to [Chapter 5: Web and Command Line Interfaces](#).
- ◆ To continue configuring the vSLM 2 software for your needs, start with [Chapter 7: Network and Modem Settings](#).

4: vSLM 2 Deployment

The vSLM 2 secure management software is a virtual appliance that runs under a variety of virtual machine managers, including VMware. vSLM 2 software can be downloaded from the Lantronix website and launched on a desktop or server, and used to administer secure IT management products. This chapter describes the differences between the SLM and vSLM 2 software.

vSLM 2 software is available as a 32-bit VMware version or a OVF (Open Virtualization Format) version. The VMware version can be launched on VMware Player or VMware Workstation; it can also be converted for use on VMware ESX and ESXi (see <http://kb.vmware.com/kb/900> for more information on converting the VMware version to a format used by ESX or ESXi). The OVF version can be launched on VMware ESX and ESXi, both virtual machine managers that support importing the OVF format.

Minimum Hardware Requirements

- ◆ 3.0 Ghz or faster single core speed
- ◆ RAM: 2GB
- ◆ Disk Space: 60 GB
- ◆ Ethernet: 1 Bridged

Deployment Instructions

Below is an example of instructions for deploying a vSLM VM from the VMware or OVF distribution. The names of the deployment files will update to show the latest firmware revision with each software release. Refer to the documentation for your virtualization manager for specific instructions on opening or launching a VM.

To deploy the VMware version:

1. Download the `SLM-<firmware version>.vmware.zip` distribution from the Lantronix website.
2. Unpack `vslm-4.0.0.0-5.vmware.zip` for distribution:
 - ◆ `SLM-4.0.0.0-5.vmwarevm/`
 - ◆ `SLM-4.0.0.0-5.vmwarevm/SLM-4.0.0.0-5.vmdk`
 - ◆ `SLM-4.0.0.0-5.vmwarevm/SLM-4.0.0.0-5.vmx`
 - ◆ `SLM-4.0.0.0-5.vmwarevm/SLM-VMware-README.txt`
3. Launch your virtualization manager and open the unpacked VM. Do not upgrade the virtual machine if the virtualization manager asks if the virtual machine should be upgraded.
4. Before starting the VM, configure the following settings:
 - ◆ A minimum of 2GB of RAM
 - ◆ USB enabled
 - ◆ MAC addresses assigned to both network interfaces BEFORE the first boot of the vSLM
 - ◆ Sound, floppy disk, and printer support removed

5. Start the VM.

To deploy the OVF version:

1. Download the SLM-<firmware version>.OVF.zip distribution from the Lantronix website.
2. Unpack SLM-4.0.0.0-5.OVF.zip for distribution:
 - ◆ SLM-4.0.0.0-5.OVF/
 - ◆ SLM-4.0.0.0-5.OVF/SLM-4.0.0.0-5-disk1.vmdk
 - ◆ SLM-4.0.0.0-5.OVF/SLM-4.0.0.0-5.mf
 - ◆ SLM-4.0.0.0-5.OVF/SLM-4.0.0.0-5.ovf
 - ◆ SLM-4.0.0.0-5.OVF/SLM-OVF-README.txt
3. Launch your virtualization manager and open or import the unpacked .zip files (see SLM-OVF-README.txt for instructions for using VMware ovftool). Do not upgrade the virtual machine if the virtualization manager asks if the virtual machine should be upgraded.
4. Before starting the VM, configure the following settings:
 - ◆ A minimum of 2GB of RAM
 - ◆ USB enabled
 - ◆ MAC addresses assigned to both network interfaces BEFORE the first boot of the vSLM 2 software
 - ◆ Sound, floppy disk and printer support removed

5. Start the VM

After the VM boots (this may take a few minutes while it is performing its initial setup), the login prompt will be displayed on the console. The initial credentials are username "**sysadmin**" and password "**PASS**". After logging in, the settings for the first network interface can be displayed with the command "show network port 1". The web interface can be accessed with the URL:

`https://<IP Address of the first network interface>`

At this point you can follow the instructions from [Chapter 3: Quick Setup Utility](#) for Quick Setup starting with [Quick Setup Utility on page 28](#).

It is recommended that the vSLM 2 software be shutdown or restarted using its "admin shutdown" and "admin reboot" commands, rather than using the virtualization manager to shutdown or restart the vSLM 2 secure management software.

30-Day Trial License

The vSLM 2 software has a 30-day trial period during which all features are available. At the end of the 30 day trial period, most features will be disabled, and a license will be required to reenable the features. The current license options can be viewed at the CLI with the "admin showoptions" command:

```
[sysadmin@SLM1F4F]> admin showoptions
Physical device location:      Disabled
Auto firmware update expiration: aug2017
Virtual Machine:              Disabled    (27 days remaining in trial
period)
Maximum concurrent users:      25
[sysadmin@SLM1F4F]>
```

To obtain a perpetual vSLM 2 license, contact your regional Lantronix Sales Representative or go to the Lantronix Online Store at store.lantronix.com and search for **vSLM** in the search bar or under **IT/Data Center Management -> Management Platform** to make the purchase. Once purchased, you will need to provide the unique signature of your vSLM 2 software to your Lantronix Sales Representative to receive the perpetual license activation key.

```
[sysadmin@SLMB1DC]> admin signature show
Signature: 6f32deb993d767081dada4ff9a2b27c2
```

5: Web and Command Line Interfaces

The vSLM 2 secure management software offers two interfaces for configuring the vSLM 2 software: a web interface and a command line interface (CLI). This chapter introduces you to both.

Web Interface

A web interface allows the administrator to configure and manage the vSLM 2 secure management software using most web browsers (Internet Explorer 6.0. and later or Firefox 1.5 and later with JavaScript enabled).

Note: *Certain features, for example Browse http and Browse https access to some non-Lantronix devices, require IE 7.*

Logging in

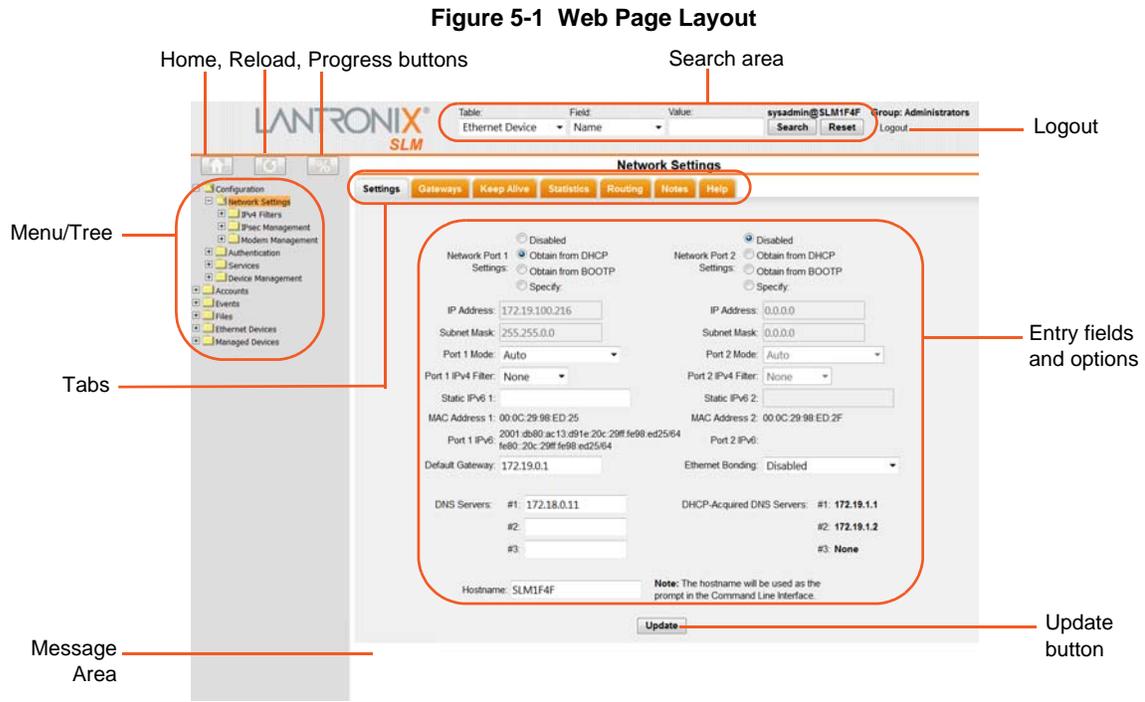
To log in to the vSLM 2 web interface:

1. Open a web browser (Internet Explorer 6.0. and later or Firefox 1.5 and later with JavaScript enabled).
2. In the URL field, type `https://` followed by the IP address of your vSLM 2 software.
3. To configure the vSLM 2 secure management software, use `sysadmin` as the user name and `PASS` as the password. (These are the default values.)

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

Typical vSLM 2 Web Page

The following figure shows a typical web page:



The web page has the following components:

Search Fields: Enable you to search for devices (e.g., SLC, RPM/SLP, and SLK devices), ports, managed devices, users and persistent connections in the vSLM 2 database.

Menu/Tree: Enables you to display a page to configure settings or to perform a function.

- ◆ Clicking the expand (plus sign) or contract (minus sign) icon causes the tree structure to toggle between expanded and contracted views but does not populate the page.
- ◆ Clicking the folder or document icon causes the tree structure to toggle between expanded and contracted views (for folders) and populates the page.
- ◆ Clicking the text only populates the page; the tree structure remains unchanged.

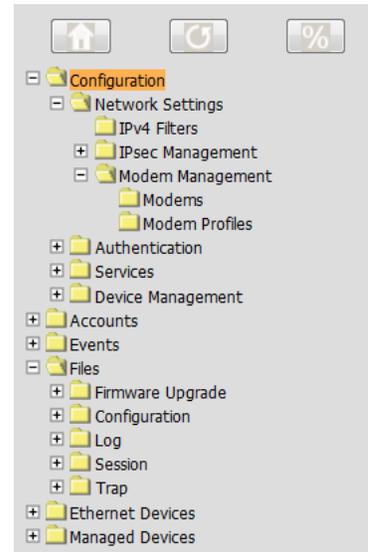
Tabs: Display a series of pages related to a particular entity (e.g., account group, network settings, and Ethernet devices).

Home Button: Displays the Lantronix web site home page.

Reload Button: Use to refresh the tree structure after auto-detect, or if some other process (another logged-in user) makes changes that affect the database.

Progress Button: Indicates status of background processes such as bulk updates and automatic detection for SLC, SLM, SLK, RPM/SLP, and SCS devices.

Figure 5-2 Menu/Tree



Entry Fields and Options: Enable you to enter data and select configuration options.

Update Button: Makes and saves the changes immediately.

Reset Button: Sets field contents to their original values.

Message area: Displays messages such as update confirmations or error messages.

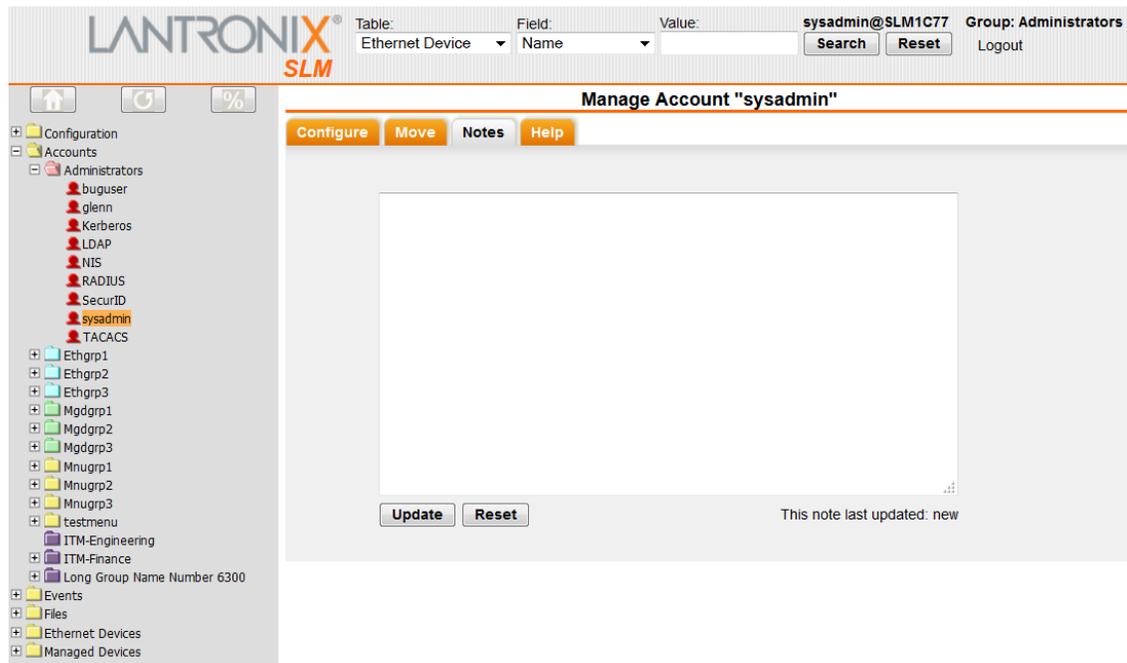
Notes

Administrators and authorized users can add, update, and delete information about any of the entities in the system (e.g., account, account group, device, and event) in the form of a note. All users with permission to view the entity can view notes about it. In this example, we add a note to an account group.

To view, add, update, and delete a note:

1. On the page for the entity to which you want to add a note (e.g., Account Group page), click the Notes tab. The following page opens.

Figure 5-3 Note for an Account Group



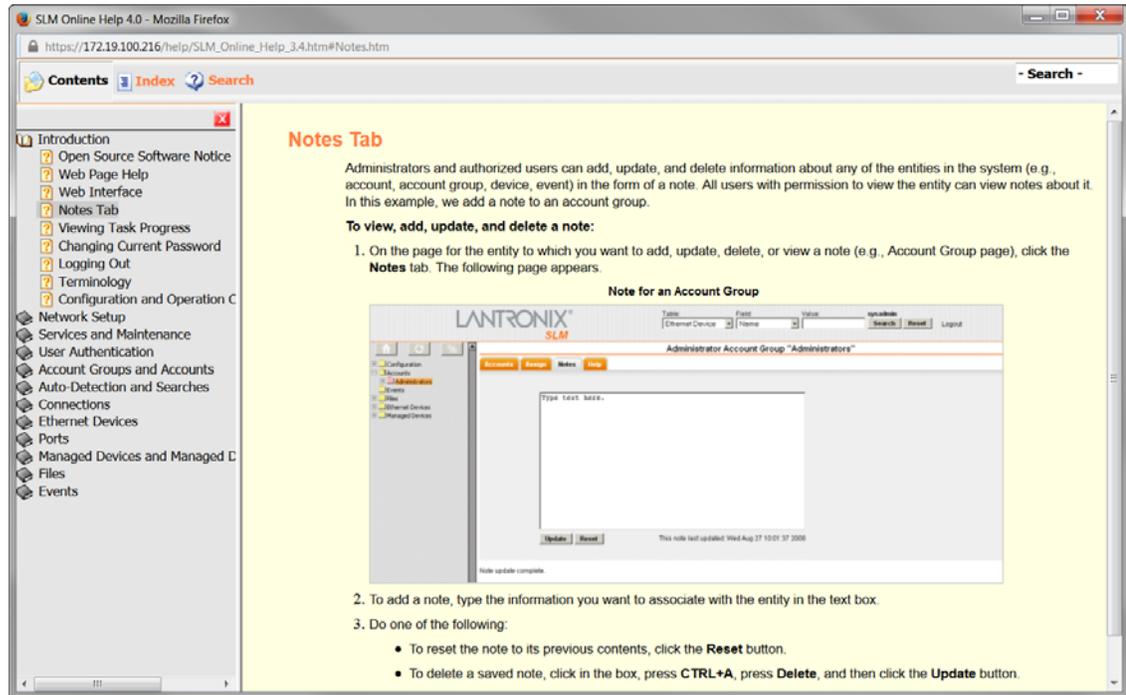
2. In the text box, type the information you want to associate with the entity.
3. Do one of the following:
 - ◆ To reset the note to its previous contents, click the **Reset** button.
 - ◆ To delete a saved note, click in the box, press **CTRL+A** (or your browser's key sequence to "select all text"), press **Delete**, and then click the **Update** button.
 - ◆ To save a new note, click the **Update** button. A confirmation message displays. The next time you open the page, it displays the note and the date and time of the update.

Web Page Help

To view context sensitive information about any vSLM 2 web page:

1. Click the **Help** tab. A Help page opens for the tab you are viewing. The **Contents** and **Search** buttons are above the pane on the left.

Figure 5-4 Example of a Help Page



To search for information:

1. Click the **Search** button. A search field displays.
2. Enter the word(s) you want to search for and press **Enter**.

Note: You can also enter the word in the search field to the left of the Lantronix logo and press **Enter**.

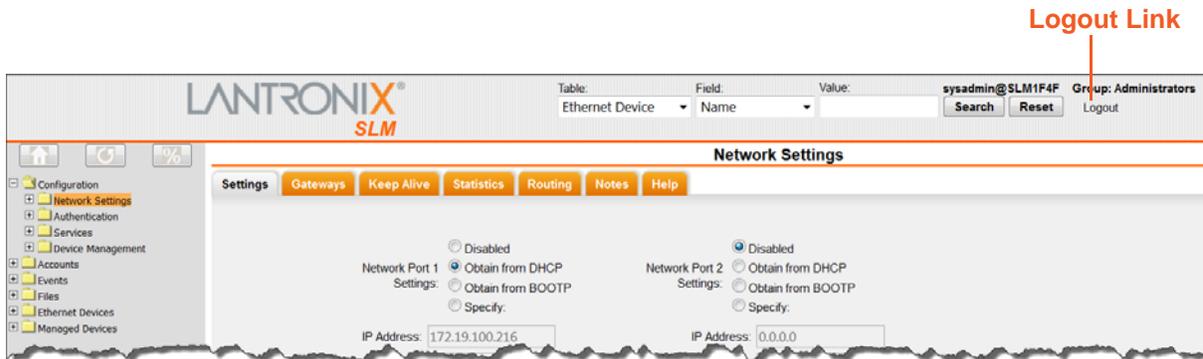
Logging Out of the Web Interface

A **Logout** link is available in the upper right corner of every page.

To log out of the vSLM 2 web interface:

1. Click **Logout** to the right of the search buttons on the vSLM 2 page banner.

Figure 5-5 Logout on the Page Header



Command Line Interface (CLI)

A command line interface is available for entering the commands for the vSLM 2 software. You can access the CLI using SSH or the virtualization manager console window.

In this User Guide, after each section of instructions for using the web interface, you will find related CLI commands. Not all web page entries have corresponding commands, and vice versa. The sysadmin user has access to the complete command set, while all other users have access to a reduced command set.

Logging into the CLI

To log in to the vSLM 2 command line interface:

1. Do one of the following:
 - ◆ With the console window of the virtualization manager, power up, and when the command line displays, press **Enter**.
 - ◆ If the vSLM 2 secure management software already has an IP address (manually assigned previously or assigned by DHCP), 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 administrator for setup and configuration:
 - a. Type **sysadmin** as the user name and press **Enter**.
 - b. Type **PASS** as the password and press **Enter**.

Note: The administrator may have changed the password using the methods described in the previous chapter.

3. To log in as any other user:
 - a. Enter your vSLM 2 user name and press **Enter**.
 - b. Enter your vSLM 2 password and press **Enter**.

Commands

Commands have the following format:

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

where

<action> is set, show, connect, diag, admin, or logout.

<category> is a group of related parameters you want to configure or view. Examples are devicegroup, account, and network.

<parameter(s)> is one or more name-value pairs in one of the following formats:

Table 5-6 CLI Commands

Command	Description
<parameter name> <aa bb>	Specify one of the values (aa or bb) separated by a vertical line (). The values are all lowercase and must be entered exactly as shown. Bold indicates a default value.
<parameter name> <Value>	Specify an appropriate value, for example, a device group name. This User Guide shows parameter values in mixed case to indicate they are case sensitive. For example, if you saved a device group name in mixed case, you must enter it in mixed case; if you saved it in lowercase, you must enter it in lowercase.
Square brackets []	Indicate optional parameters.

Table 5-7 Actions and Category Options

Action	Category
set	network service ipfilter account accountgroup auth nis ldap radius kerberos tacacs+ ethernetdevice manageddevice mgroup datetime cli menu sshkey history modem dialaccount persistent ipmi ilo
show	network service ipfilter iptables account accountgroup auth nis ldap radius Kerberos tacacs+ device port ethernetdevice manageddevice auditlog syslog portlog traplog eventlog sessionlog datetime cli menu sshkey history connection progress sysconfig sysinfo modem dialaccount routing persistent ipmi ilo user
connect	device remote index ssh telnet tn3270 terminate persistent wakeonlan
diag	ping ping6 arp traceroute netstat nettrace internals

Action	Category
admin	autodetect locallog version option showoptions config quicksetup securechannel signature banner reboot shutdown showbootbank switchbank copybank web
logout	Terminates CLI session.

Command Help

For general command help, type: help

For more information about a specific command, type help followed by the command, for example:

```
help set network
```

OR

type ? after the command:

```
set network ?
```

Tips

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


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

 can be shortened 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 to complete the name if only one is possible, or to display the possible names if more than one is possible.
- ◆ Should you make a mistake while typing, backspace by pressing the Backspace key 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.
- ◆ When the number of lines displayed by a command exceeds the size of the window (the default is 20), the "Type more to see the next page" message displays. To display the next page, type more and press **Enter**. You can override the number of lines (or disable the feature altogether) with the set cli command.
- ◆ To clear an IP address, type 0.0.0.0.

Logging Out of the CLI

To log out of the vSLM 2 command line interface:

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

CLI Commands

The following commands relate to the CLI itself.

set cli terminallines

Syntax

```
set cli terminallines <disable|1-1000>
```

Description

Sets the number of lines that display in a page for the auditlog, syslog, portlog, traplog, and device list. Default is 20.

set history clear

Syntax

```
set history clear
```

Description

Clears the CLI command history.

show cli

Syntax

```
show cli
```

Description

Displays the terminal lines settings. Shows the number of lines "more" will allow to be displayed in a page, for the auditlog, syslog and device list.

show history

Syntax

```
show history
```

Description

Displays the 100 most recent CLI commands.

Session Commands

connect terminate

Syntax

```
connect terminate <connect ID> <one or more parameters>
```

Parameters

```
outbound <outbound ID>
```

You must specify connection ID (inbound ID) to terminate an outbound connection.

Use `show connection` to view the current connections and their ID.

Examples

```
connect terminate 3  
connect terminate 3 outbound 1
```

Description

Terminates a user connection to the vSLM 2 session. Use `show connection` to view the current connections and IDs.

show connection

Syntax

```
show connection
```

Description

Displays active user connections and connection IDs.

6: Configuration and Operation Overview

To best use the vSLM 2 secure management software, review the setup and configuration process outlined below before undertaking the tasks detailed in Chapters 6-10.

Note: Throughout this user guide, the term "administrator" means the person using the **sysadmin** user name and those members of the Administrators Account Group permitted to perform the task.

Following is an overview of the tasks the administrator and other users perform to configure and use the vSLM 2 secure management software, in roughly the order performed.

The typical user employs vSLM 2 software as follows:

- ◆ Searches for Lantronix Devices and other Ethernet devices.
- ◆ Connects by browser, SSH, or Telnet to Lantronix Devices and other Ethernet devices, and additionally, by secure channel to SLC devices and other vSLM 2 secure management software.
- ◆ Accesses notes and logs about the management devices and their ports.

The administrator performs the following configuration and maintenance activities:

- ◆ Updates vSLM 2 firmware and configurations.
- ◆ Configures properties of the log files.
- ◆ Manages syslog, portlog, auditlog, upgrade, configuration, session, and trap files.
- ◆ Configures an SNMP agent.
- ◆ Configures and views events.
- ◆ Updates firmware on Lantronix Ethernet devices (including SLM, WiBox, UDS™, Spider, RPM/SLP, and SLC devices).

Step 1: Configure Network Settings

The administrator enters the network settings that enable the vSLM 2 secure management software to access the network, manages modems, and sets up IPv4 filter sets

Step 2: Define Authentication Methods

The vSLM 2 software supports LDAP, RADIUS, NIS, Kerberos, TACACS+, and SSH public key authentication. Remote authentication is optional. The administrator can opt to use only local authentication.

Step 3: Set Up User Account Groups and Accounts

The vSLM 2 secure management software comes with four types of account groups: Administrators, Ethernet Device, Managed Device, and Menu Only users. Administrators create

account groups of each type (except Administrators) and create and assign accounts to the account groups.

The administrator can create additional administrator accounts that have the following rights enabled or disabled:

- ◆ Network Settings
- ◆ Authentication
- ◆ Services (e.g., SNMP and syslog, Date and Time, and Maintenance)
- ◆ Device Management
- ◆ Accounts
- ◆ Events
- ◆ File Management

Step 4: Auto-Detect Devices

The administrator uses auto-detection methods to find Lantronix devices and other devices on the network and to add them to the vSLM 2 database for the vSLM 2 secure management software to manage. There is no need to add a device manually, although that option is available. Currently, auto-detect supports Lantronix Discovery Protocol (LDP) for SLC console managers and other Lantronix devices, the Lantronix SCS05/20 device discovery protocol, and SNMP for RPM/SLP, SLK, and all other Ethernet devices.

Step 5: Associate Account Groups with Ethernet and Managed Devices

Once the vSLM 2 administrator adds account groups and Ethernet devices, the next step is to associate the account groups with the Ethernet devices and managed devices (devices attached to Ethernet device's ports) to which they will have access. In the case of SLC console manager or SCS console servers, permissions also allow specific account groups listen-only access or full bidirectional control.

Step 6: Manage Devices

The user selects Ethernet devices from the menu's tree structure or enters search criteria to search for Ethernet devices, ports, and managed devices. The user then views port settings (if the device has ports) and can connect to an attached device through a web browser or the CLI.

For ease of communication and management, managed devices that link together device ports (e.g., SLC, SCS, SLK, and RPM/SLP device) may be created or "fused" together. Users may then manage all of these ports through the managed device on a single web page. In the case of an SLC or another vSLM 2 software, the user can make a secure channel connection through which the vSLM 2 secure management software forwards user permission information so a secondary login is not required. For SLC devices, once a secure channel has been set up, the user can make a web channel connection.

Step 7: Maintain the vSLM 2 Software

The vSLM 2 secure management software enables the following maintenance tasks:

SLM Firmware Updates: The SLM administrator updates the SLM firmware.

Auto-Save: The administrator saves the configuration of one vSLM 2 software on another SLM. If there is a need, the second vSLM 2 secure management software can "become" the first vSLM 2 software.

Configuration Save and Restore: The administrator saves and restores system configurations, providing rapid recovery of inadvertent configuration changes.

User Log (Audit Trail): Every successful login, logout, and command on the command line interface and web is logged into a database table. The administrator reads this information from the CLI or web and creates an audit report for one or multiple users.

Events: The administrator defines alarms and triggers that constitute an event. Events are sent to specific users or recorded on the syslog or on another device through an SNMP trap.

Files: The administrator manages (imports, exports, deletes, and renames) and views upgrade, configuration, syslog, audit log, port log, sysconfig, device session, and trap files.

7: Network and Modem Settings

This chapter is primarily for the administrator. It explains how to enter the network configuration, IPv4 filters, and modem settings for the vSLM 2 secure management software using the vSLM 2 web interface or the CLI. If you used a procedure in [Chapter 3: Quick Setup Utility](#) to get your unit up and running on the network, you can add or update settings here.

IP Address and Other Required Information

Note: The vSLM 2 secure management software supports two bridged network adapters.

To configure the unit for use on the network, you need the following information:

Network Port 1:

IP address (if not already assigned): _____ . _____ . _____ . _____

Subnet mask: _____ . _____ . _____ . _____

Network Port 2: (optional)

IP address (if not already assigned): _____ . _____ . _____ . _____

Subnet mask: _____ . _____ . _____ . _____

Default Gateway: _____ . _____ . _____ . _____

DNS Server: _____ . _____ . _____ . _____

Your vSLM 2 software must have a unique IP address on your network. If you assign an IP address manually, it must be within a valid range and unique to your network. The administrator generally provides this information.

The vSLM 2 secure management software receives an IP address in one of the following ways:

Automatically: The first time you power up the vSLM 2 software, Network Port 1 tries to obtain its IP address automatically through DHCP. If you have connected the network port to a network with a DHCP server, the network port acquires an IP address. Smaller networks may use BOOTP.

Using Detector Utility: This software allows you to quickly assign a static IP address to a unit that has an automatically assigned IP address. This utility can be downloaded from the Lantronix website, by selecting the vSLM 2 product from the Firmware/Downloads page: www.lantronix.com/support/downloads.

Manually: If the vSLM 2 secure management software cannot obtain an IP address by means of DHCP, you can use the vSLM 2 console port window, which is the window displayed by the virtualization software.

Once the vSLM 2 software has an IP address, you can configure the remaining settings (and change the IP address, if desired) using the CLI or the web interface.

Using the Web Interface

After the unit has an IP address, you can configure network parameters that determine how the vSLM 2 secure management software interacts with the attached network and enter the date, time, and timezone.

Note: *Chapter 5: Web and Command Line Interfaces* describes the web interface in detail.

To log in:

1. Open a web browser (Internet Explorer 7.0. and later or Firefox 15.0 and later with JavaScript enabled).
2. In the URL field, type `https://` followed by the IP address of your vSLM 2 software.
3. Log in using `sysadmin` as the user name and `PASS` as the password. The SLM Configuration page opens.

Figure 7-1 SLM Configuration Page



Network Port(s)

Notes:

- ◆ 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.
- ◆ Both Ethernet ports should not be on the same subnet.

To enter settings for one or both network ports:

1. On the menu, click **Configuration > Network Settings**. The following page opens:

Figure 7-2 Network Settings Page

The screenshot shows the LANTRONIX SLM Network Settings page. The page is titled "Network Settings" and has a navigation menu with options: Settings, Gateways, Keep Alive, Statistics, Routing, Notes, and Help. The "Settings" tab is selected. The page is divided into two columns for Network Port 1 and Network Port 2. Network Port 1 is configured with IP Address 172.19.100.216, Subnet Mask 255.255.0.0, and Port 1 Mode set to Auto. Network Port 2 is configured with IP Address 0.0.0.0, Subnet Mask 0.0.0.0, and Port 2 Mode set to Auto. The page also includes fields for MAC addresses, IPv6 addresses, Default Gateway, DNS Servers, and Hostname (SLM1F4F). A note states: "Note: The hostname will be used as the prompt in the Command Line Interface." An "Update" button is located at the bottom right of the form.

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

Table 7-3 Network Port Settings

Network Port Setting	Description
Network Port Settings	<p>Disabled: This is the default setting for Network Port 2.</p> <p>Obtain from DHCP: Acquires IP address, subnet mask, and gateway from the DHCP server. (The DHCP server may provide the gateway, depending on its setup.) This is the default setting for Network Port 1. If you select this option, skip to step 3.</p> <p>Obtain from BOOTP: Lets a network node request configuration information from a BOOTP "server" node. Skip to step 3.</p> <p>Specify: Requires you to assign a static IP address manually. The administrator generally provides the IP address.</p>

Network Port Setting	Description
IP Address	<p>If specifying an IP address, enter an IP address that is within a valid range, unique to your network, and in the same subnet mask as your workstation. There is no default.</p> <p>Note: Enter all IP addresses in dot quad notation.</p>
Subnet Mask	<p>If specifying an IP address, enter the network segment on which the vSLM 2 secure management software resides. There is no default.</p>
Port Mode	<p>The method of data transmission (Auto, Half-Duplex, or Full-Duplex).</p>
Port 1 and Port 2 IPv4 Filter	<p>If you have added filter sets on the IPv4 Filter Definitions page, select the desired one. (See IPv4 Filters.)</p>
Static IPv6	<p>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.</p> <p>Note: The vSLM 2 software stores all IP addresses internally using IPv6 format. When rendering these addresses for display, the vSLM 2 software uses IPv4 unless the address cannot be displayed in that format, in which case it uses shortened IPv6.</p>
MAC Address (display only)	<p>Also referred to as the Hardware or Ethernet address.</p>
Port IPv6 (display only)	<p>IPv6 addresses active on this network port.</p>
Default Gateway	<p>IP address of the router for this network.</p> <p>If this has not been set manually, any gateway acquired by DHCP for Network Port 1 or Network Port 2 displays.</p> <p>All network traffic that matches the Network Port 1 IP address and subnet mask goes out Network Port 1. All network traffic that matches the Network Port 2 IP address and subnet mask goes out Network Port 2.</p> <p>If you set a default gateway, the vSLM 2 secure management software sends any network traffic that does not match Network Port 1 or Network Port 2 to the default gateway for routing.</p>

Network Port Setting	Description
Ethernet Bonding	<p>Ethernet bonding is a way of joining two Ethernet interfaces into a single virtual interface for redundancy and/or load balancing. The vSLM 2 software supports four types of Ethernet bonding in addition to the default state of disabled.</p> <p>Note: With bonding enabled, the IP/netmask settings for network port 1 are applied to the virtual bonding interface.</p> <p>Select one of the following:</p> <p>Active Backup: Only one of the two Ethernet interfaces will be active (involved in transmitting and receiving data) at any one time. If the vSLM 2 secure management software detects that the Ethernet interface has lost network connectivity, the system makes the secondary interface the new active one after a few seconds (~3.5 - 4) of delay. (This delay length is also used with the other bonding settings.)</p> <p>802.3ad Layer 2: IEEE 802.3ad-compliant dynamic link aggregation. This is a load-balancing strategy that uses the destination MAC address as the criterion for determining which interface to send each data frame out of.</p> <p>802.3ad Layer 3+4: Much like 802.3ad Layer 2, but uses the destination IP and TCP/UDP port number to determine which interface to send data from.</p> <p>Note: Both 802.3ad bonding modes require that both network interfaces share the same speed/duplex modes. This rule is currently enforced by the web interface, but not by the CLI.</p> <p>Adaptive Load Balancing: This mode determines which interface to send data from by looking at the current load on each interface. It also controls which interface will receive a response by modifying the vSLM 2 secure management software's ARP replies before they are sent out. If a link failure occurs on one of the network ports, the system will fail over to the other interface.</p> <p>Note: In theory, the active-backup and adaptive load balancing modes do not require any special network switch configuration, while the two 802.3ad modes do. The active-backup mode is recommended for most situations, as redundancy tends to be a more important goal than the relatively small increase in bandwidth (note that bonding two interfaces for load balancing does not double the available bandwidth because of protocol overhead issues).</p>

- Configure up to three name servers, either by entering the IP addresses or by accepting the IP addresses assigned by DHCP:

Table 7-4 DNS Servers

IP Address Setting	Description
#1	IP address of the primary name server. This entry is required if you choose to configure DNS (Domain Name Server) servers. Note: Assigning DNS servers allows FQDNs to be used in place of most IP addresses throughout the system.
#2 (optional)	IP address of the secondary DNS name server.
#3 (optional)	IP address of the tertiary DNS name server.
DHCP-Acquired DNS Servers (view only)	DNS servers automatically assigned by DHCP. The default setting for up to three servers is None .

- Enter the following:

Table 7-5 Hostname

Hostname Setting	Description
Hostname	The default hostname is "SLM". You can specify a fully qualified domain name (for example, SLM.lantronix.com). There is a 64-character limit (contiguous characters, no spaces). <i>Note:</i> The hostname becomes the prompt in the command line interface.

- To save your entries, click the **Update** button.

Network Gateways

You can enter network gateway information.

To enter gateway information:

- On the Network - Settings page, click the **Gateways** tab. The following page opens:

Figure 7-6 Network Settings - Gateways Tab

- Enter the following:

Table 7-7 Network Gateway

Network Gateway Setting	Description
Default	IP address of the router for this network. If this has not been set manually, any gateway assigned by DHCP for Network Port 1 or Network Port 2 displays. All network traffic that matches the Network Port 1 IP address and subnet mask goes out Network Port 1. All network traffic that matches the Network Port 2 IP address and subnet mask goes out Network Port 2. If you set a default gateway, the vSLM 2 secure management software sends any network traffic that does not match Network Port 1 or Network Port 2 to the default gateway for routing.
DHCP Acquired (view only)	Gateway assigned by DHCP for Network Port 1 or Network Port 2. The default setting is None .

Network Gateway Setting	Description
Precedence	Indicates whether the gateway assigned by DHCP or the default gateway takes precedence. The default setting is Default. If you select DHCP, and both network ports are configured for DHCP, the vSLM 2 software gives precedence to the Network Port 1 gateway.
Alternate	An alternate IP address of the router for this network, to be used if an IP address usually accessible through the default gateway fails to return one or more pings.
IP Address to Ping	IP address to ping to determine whether to use the alternate gateway.
Ethernet Port to Ping	Ethernet port to use for the ping.
Delay between Pings	Number of seconds between pings
Number of Failed Pings	Number of pings that fail before the vSLM 2 secure management software uses the alternate gateway.

3. To save your entries, click the **Update** button.

Keep Alive

Keep Alive settings keep TCP connections active and monitor for connections that are no longer active.

To enter Keep Alive settings:

1. Click the **Keep Alive** tab.
2. Enter the following information:

Table 7-8 Keep Alive Settings

Keep Alive Setting	Description
Start Probes	Number of seconds the vSLM 2 software 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 vSLM 2 secure management software sends before closing a session. The default is 5.
Interval	The number of seconds the vSLM 2 software waits between probes. The default is 60 seconds.

3. To save your entries, click the **Submit** button.

Viewing Network Statistics

You can check Ethernet counters for the network port(s).

To view network statistics:

1. On the Network - Settings page, click the **Statistics** tab. The following page opens:

Figure 7-9 Network Settings - Statistics Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device' and 'Field: Name'. Below the search bar, there is a navigation menu with tabs for Settings, Gateways, Keep Alive, Statistics (selected), Routing, Notes, and Help. The main content area displays 'Ethernet Counters' with a table showing Rx and Tx statistics for Eth1 and Eth2. A Refresh button is located below the table.

Ethernet Counters							
	Rx				Tx		
	Bytes	Packets	Errors	Multicast	Bytes	Packets	Errors
Eth1	53800540	598973	0	0	24079551	309892	0
Eth2	0	0	0	0	0	0	0

Statistics include the following:

Table 7-10 Counters for Rx and Tx Transmissions

Network Statistic Setting	Description
Bytes	Number of bytes received or transmitted through this Ethernet interface.
Packets	Number of Ethernet packets received or transmitted through the interface.
Errors	Number of received or transmitted packets with physical layer errors.
Multicast (Tx only)	Number of received or transmitted packets with the destination address equivalent to a multicast address.

Routing

To view the current IPv4 and IPv6 routing information:

1. On the Network - Settings page, click the Routing tab. The following page opens:

Figure 7-11 Network Settings - Routing Tab

The screenshot shows the LANTRONIX SLM Network Settings interface. The 'Routing' tab is active, displaying the 'Contents of route.txt' for both Kernel IP and Kernel IPv6 routing tables.

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
172.19.39.247	172.19.0.1	255.255.255.255	UGH	0	0	0	eth0
172.19.0.0	0.0.0.0	255.255.0.0	U	0	0	0	eth0
0.0.0.0	172.19.0.1	0.0.0.0	UG	0	0	0	eth0

Kernel IPv6 routing table

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
::1/128	::	U	0	23	1	lo
2001:db80:ac13:d91e:20c:29ff:fe98:ed25/128	::	U	0	0	1	lo
2001:db80:ac13:d91e::/64	::	UA	256	5281	0	eth0
fe80::20c:29ff:fe98:ed25/128	::	U	0	0	1	lo
fe80::/64	::	U	256	0	0	eth0
ff02::1/128	ff02::1	UC	0	158	0	eth0
ff00::/8	::	U	256	0	0	eth0
::/0	fe80::20c:29ff:fee9:bc25	UGDA	1024	1	0	eth0

Changing the Current User's Password

Users logged in locally (not using remote authentication) may change passwords at any time, unless the administrator has disabled this option.

To change your password:

1. On the menu, click **Configuration**. The Configuration Home page opens.
2. Click the **Password** tab. The following page opens:

Figure 7-12 Configuration Page - Password Tab

The screenshot shows the LANTRONIX SLM Configuration Page. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user 'sysadmin@SLM1C77' and group 'Administrators' are logged in. The main navigation menu on the left includes 'Configuration', 'Network Settings', 'Authentication', 'Services', 'Device Management', 'Accounts', 'Events', 'Files', 'Ethernet Devices', and 'Managed Devices'. The 'Configuration' tab is selected, and the 'Password' sub-tab is active. The 'Change Current User Password' form contains two input fields: 'New Password' and 'Retype', both with masked characters (dots). An 'Update' button is located below the 'Retype' field.

3. Enter the **New Password** and **Retype** fields.
4. Click the **Update** button.

Network Commands

admin quicksetup

Syntax

```
admin quicksetup
```

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command.

set network dns

Syntax

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

Description

Configures up to three DNS servers.

set network gateway

Syntax

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

Parameters

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

Description

Sets the default gateway.

set network host**Syntax**

```
set network host <Hostname>
```

Description

Sets the vSLM 2 secure management software hostname.

set network bonding**Syntax**

```
set network bonding <disabled|active-backup|802.3ad-2|802.3ad-34|adaptive-balancing>
```

Description

Configures Ethernet bonding.

set network port**Syntax**

```
set network port <1|2> <parameters>
```

Parameters

```
state <dhcp|bootp|static|disable>
[ipaddr <IP Address> mask <Mask>]
ipv6addr <IPv6 Address|CLEAR>
mode <auto|10mbit-half|100mbit-half|10mbit-full|100mbit-full>
[ipfilter <IPv4 Filter Name | CLEAR>]
CLEAR removes the IP filter assignment.
```

Description

Configures Network Port 1 or 2.

show network all

Syntax

```
show network all
```

Description

Displays all network settings.

show network bonding

Syntax

```
show network bonding
```

Description

Shows all network bonding settings.

show network port

Syntax

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

Description

Displays Network Port 1 and Network Port 2 connection information.

show network settings

Syntax

```
show network settings
```

Description

Displays all network settings.

show routing

Syntax

```
show routing
```

Description

Display the kernel IP routing tables:.

IPv4 Filters

Warning: *IPv4 filters configuration is a feature for advanced users. Adding and enabling IPv4 filter sets incorrectly can disable your vSLM 2 secure management software.*

IPv4 Filters act as a firewall to allow or deny individual or a range of IP addresses, ports, and protocols. On the IPv4 Filter Definitions pages, the administrator defines and edits IPv4 filter sets and displays the current system-recognized filters.

Viewing a List of IPv4 Filters

Each IPv4 filter set is composed of one or more filter rules.

To view a list of available IPv4 filters sets:

1. On the menu, click **Configuration > Network Settings > IPv4 Filters**. The following page displays a list of existing filters.

Figure 7-13 IPv4 Filter Definitions - List Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main content area is titled 'IPv4 Filter Definitions' and has tabs for 'List', 'Show', 'Properties', 'Notes', and 'Help'. The 'List' tab is active, showing a table with two columns: 'Name' and 'Comment'. The table contains two entries: 'HTTP_SSH' and 'SSH'. Below the table, it says '2 items' and there is an 'Add New Filter' button. On the left, a navigation tree shows 'Configuration' > 'Network Settings' > 'IPv4 Filters' selected.

2. View the list of filters and the associated comments.

Adding an IPv4 Filter

Note: *User-created IPv4 filter sets display on the menu tree and are composed of one or more filter rules. When a network connection or modem is configured to use an IPv4 filter set, all network traffic through that connection is compared, in order, to the rules of that filter set. 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 set.*

To add an IPv4 filter:

1. On the List tab, click the **Add New Filter** button. The Configure tab displays.

Figure 7-14 New IPv4 Filter Definition - Configure Tab

Note: A new filter set is initialized with a rule to allow all established TCP connections. You may remove this rule from your filter set, but do so with caution as loss of connectivity may result.

2. Enter the following for each filter in the set:

Table 7-15 IPv4 Filter Definition - Configuration Tab

IPv4 Filter Setting	Description
IP[/mask] or IP1-IP2 (optional)	Specify any IP address, IP prefix with mask, or IP range. Examples: 172.19.220.64 - this specific IP address only 172.19.0.0/16 - IP addresses 172.19.0.0 - 172.19.255.255 172.19.0.128 - 172.19.64.0 - IP addresses in this range
Protocol	From the drop-down list, select the type of protocol (if any) through which the filter will operate. The default setting is All.
Port Range	Enter a range of destination 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

IPv4 Filter Setting	Description
Action	Select whether to drop, reject, or allow communications from IPv4 addresses within the specified 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.
Filter Name	Name that identifies a filter. The name may be composed of letters, numbers and hyphens only. (The name cannot start with a hyphen.) Example: FILTER-2
Save as new filter definition	Select to make small changes to an existing filter set and then save it as a new filter set. If you select this option, you must supply a Filter Name that does not already exist.
Comment (optional)	Enter information related to the filter. It displays next to the filter name on the List tab.
Generate filter to allow the specified protocol or 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 Filter 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 list box on the right, or click the **Add Filter** button to add a predefined rule to the bottom of the list box.
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 **Update** button. A confirmation message displays, and the new filter displays in the menu tree.

Note: To add another new filter, return to the List tab (step 1).

Updating or Deleting an IPv4 Filter

The administrator can update or delete IPv4 filters.

To update or delete an IPv4 filter:

1. On the **List** tab, click the **Edit**  icon to the left of the filter. The Configure tab displays.

Figure 7-16 IPv4 Filter - Configure Tab

The screenshot displays the LANTRONIX SLM web interface for configuring a new IPv4 filter. The top navigation bar shows the user is logged in as 'sysadmin@SLM1F4F' with the role of 'Administrators'. The main content area is titled 'New IPv4 Filter Definition' and contains the following fields and options:

- Table:** Ethernet Device
- Field:** Name
- Value:** (empty)
- Buttons:** Search, Reset, Logout
- Navigation:** Home, Refresh, Percentage icons
- Menu Tree:** Configuration, Network Settings, IPv4 Filters, IPsec Management, Modem Management, Authentication, Services, Device Management, Accounts, Events, Files, Ethernet Devices, Managed Devices
- Configure Tab:** Configure, Show, Notes, Help
- IP[mask] or IP1-IP2:** (text input)
- Protocol:** All (dropdown)
- Port Range:** (text input)
- Action:** Drop (selected), Reject, Allow (radio buttons)
- Clear:** (button)
- Filter List:** 0.0.0.0/0;TCP Established;Allow, 0.0.0.0/0;All;Drop (list with up/down arrows)
- Filter Name:** (text input)
- Comment:** (text input)
- Save as new filter definition:** (checked checkbox)
- Generate filter to allow the specified protocol or service:**
 - LDP
 - NFS
 - FTP
 - TACACS+
 - SLC/SLB Logging
 - SMTP
 - Syslog
 - Kerberos
 - SSH
 - SNMP
 - BOOTP/DHCP
 - LDAP
 - Telnet
 - HTTPS
 - NTP
 - RADIUS
 - Samba
 - HTTP
 - NIS
 - DNS
- Buttons:** Add Filter, Update, Delete

2. To delete a filter:

Note: You may not delete a filter set currently referenced by a network interface or a modem.

- a. Click the **Delete** button.
 - b. In response to the request for confirmation, click **OK**.
 - c. Click **IPv4 Filters** on the menu tree. The deleted filter is no longer on the menu tree or listed on the List tab.
3. To update an IPv4 filter:
- a. Edit the information as desired.
 - b. Click the **Update** button. A confirmation message displays.

Viewing the System IPv4 Filter Sets

The administrator may view a list of all IPv4 filter sets (user and system) or an individual IPv4 filter set.

To view all filter sets:

1. On the menu, click **IPv4 Filters**. The List tab displays.
2. Click the **Show** tab. The following page opens:

Figure 7-17 IPv4 Filter Definitions - Show Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with fields for 'Table' (set to 'Ethernet Device'), 'Field' (set to 'Name'), and 'Value'. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main content area is titled 'IPv4 Filter Definitions' and has tabs for 'List', 'Show', 'Properties', 'Notes', and 'Help'. The 'Show' tab is active, displaying the contents of the 'slm_ipfilter.txt' file. The file content shows several chains: INPUT, FORWARD, OUTPUT, HTTP_SSH, and SSH, each with a policy and a list of rules. A 'Refresh' button is located at the bottom of the content area.

```

Contents of slm_ipfilter.txt

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out    source         destination
1500K 161M ACCEPT    all  --  *      *        0.0.0.0/0      0.0.0.0/0
0      0 ACCEPT    all  --  lo     *        0.0.0.0/0      0.0.0.0/0

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

Chain OUTPUT (policy ACCEPT 995K packets, 86M bytes)
pkts bytes target      prot opt in     out    source         destination
343K  38M ACCEPT    all  --  *      lo     0.0.0.0/0      0.0.0.0/0

Chain HTTP_SSH (0 references)
pkts bytes target      prot opt in     out    source         destination
0      0 ACCEPT    tcp  --  *      *        0.0.0.0/0      0.0.0.0/0      tcp dpt:22
0      0 ACCEPT    tcp  --  *      *        0.0.0.0/0      0.0.0.0/0      tcp dpt:80
0      0 ACCEPT    tcp  --  *      *        0.0.0.0/0      0.0.0.0/0      tcp flags:10
0      0 REJECT    all  --  *      *        0.0.0.0/0      0.0.0.0/0      reject-with :

Chain SSH (0 references)
pkts bytes target      prot opt in     out    source         destination
0      0 ACCEPT    tcp  --  *      *        0.0.0.0/0      0.0.0.0/0      tcp dpt:22
0      0 ACCEPT    tcp  --  *      *        0.0.0.0/0      0.0.0.0/0      tcp flags:10
0      0 DROP     all  --  *      *        0.0.0.0/0      0.0.0.0/0

IP Filter Mode: Not in Test Mode

Refresh

```

To view an individual IPv4 filter set:

1. On the menu, click the individual filter set name. The IPv4 Filter page for the filter set displays.
2. Click the **Show** tab.

Figure 7-18 IPv4 Filter - Show Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1C77' with the group 'Administrators'. The main content area is titled 'IPv4 Filter "Judy"' and has tabs for 'Configure', 'Show', 'Notes', and 'Help'. The 'Show' tab is active, displaying the contents of 'sim_ipfilter.txt'.

Contents of sim_ipfilter.txt

```
Chain INPUT (policy ACCEPT 10 packets, 1890 bytes)
pkts bytes target prot opt in out source destination
773K 193M ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT all -- lo * 0.0.0.0/0 0.0.0.0/0

Chain judy (0 references)
pkts bytes target prot opt in out source destination tcp flags
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp flags:!0x17/0x02
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

IP Filter Mode: Not in Test Mode

Refresh

Setting Properties of an IPv4 Filter

For IPv4 filters to be in effect, the **Enable IPv4 Filters** check box must be selected on the Properties tab.

To enable and test the IPv4 filter:

1. On the menu, click **IPv4 Filters**. The IPv4 Filter Definitions page displays.
2. Click the **Properties** tab.

Figure 7-19 IPv4 Filter Definitions - Properties Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with fields for 'Table:' (set to 'Ethernet Device'), 'Field:' (set to 'Name'), and 'Value:'. To the right, the user is identified as 'sysadmin@SLM1C77' with the group 'Administrators' and a 'Logout' link. Below the search bar, there are navigation icons (home, refresh, percentage) and a breadcrumb trail: 'IPv4 Filter Definitions'. The main content area has tabs for 'List', 'Show', 'Properties' (selected), 'Notes', and 'Help'. Under the 'Properties' tab, there is a form with the following elements:

- 'Enable IPv4 Filters: ' (checkbox is unchecked)
- 'Filter Test Period (minutes): ' (input field contains '0')
- 'Submit' button

On the left side, there is a navigation menu with the following items:

- Configuration
 - Network Settings
 - IPv4 Filters (highlighted)
 - Judy
 - IPsec Management
 - Modem Management
 - Authentication
 - Services
 - Device Management
- Accounts
- Events
- Files
- Ethernet Devices
- Managed Devices

3. Enter the following:

Table 7-20 IPv4 Filter Definitions - Properties Tab

IPv4 Filter Setting	Description
Enable IPv4 Filters	To enable the filters, select the check box. Disabled by default.

IPv4 Filter Setting	Description
Filter Test Period (minutes)	<p>Note: There may be times when a complex IPv4 filter set may accidentally lock all users out of the vSLM 2 secure management software. To allow testing of new filter sets, the administrator can enable and test the filter sets for a specified period.</p> <p>Before enabling an untested complex filter, enter the number of minutes you would like filters to be active before being automatically disabled.</p> <ul style="list-style-type: none"> ◆ A zero (0) in this field indicates that filtering will not be automatically disabled, and the Enable IPv4 Filters state you specified will take place immediately. ◆ A non-zero value is the number of minutes until IPv4 filters are disabled, whether or not a lockout condition occurs. <p>➤ Example: You set this value to 5 and enable IPv4 filters. If your system locks up because of a bad filter set definition, then in five minutes, filtering will automatically be disabled. Note that even if there are no problems with the filter set, IPv4 filtering will still be disabled in 5 minutes. Once you are satisfied with the IPv4 filter definitions, return to this page and set the Filter Test Period to 0 and resubmit to enable IPv4 filtering permanently.</p> <p>Note: If you submit a new Filter Test Period (larger than 0) when the IP filter is already in test mode, the test timer resets to the new test period and starts test mode again. If you submit a zero Filter Test Period when the IP filter is in test mode, the test mode stops, and the specified Enable IPv4 Filters state takes effect immediately. If you have physical access to the vSLM 2 software, you can always disable IPv4 from the console using the CLI.</p>

4. To save, click the **Submit** button.
5. In response to the confirmation request, click **OK**. A confirmation message displays in the message area.

Note: To determine whether the IPv4 filter is still in test mode, when the test mode was started, and how long until the test mode ends, click the **Show** tab on the IPv4 Filters page or on an individual IPv4 Filter Set page.

IPv4 Filter Commands

```
set ipfilter delete
```

Syntax

```
set ipfilter delete <Name> [rule <rule number>]
```

Example:

```
set ipfilter delete MyFilter
```

Description

Deletes IPv4 filter set by specified name.

set ipfilter delete all**Syntax**

```
set ipfilter delete all
```

Description

Deletes all references to filters.

set ipfilter delete interactive**Syntax**

```
set ipfilter delete interactive
```

Description

Deletes IPv4 filters by interactive mode.

Example

```
set ipfilter delete MyFilter rule 3
```

Description

Deletes IPv4 filter rule by specified name and rule number.

set ip filter state**Syntax**

```
set ipfilter state <enable|disable>
```

Description

Enables or disables IPv4 filters.

set ipfilter test**Syntax**

```
set ipfilter test <number of minutes>
```

Description

Enables or disables IPv4 filter test mode.

show ipfilter

Note: Type *show ipfilter* to display index.

Syntax

```
show ipfilter <parameters>
```

Parameters

```
[name <Filter Name>]  
[index <number>]
```

Examples

```
show ipfilter
show ipfilter name MyFilter
show ipfilter index 2
```

Description

Displays IPv4 filter information.

show iptables

Syntax

```
show iptables
```

Description

Displays all IP filtering rules for all chains.

IPsec Management

Internet Protocol Security (IPsec) for the vSLM 2 secure management software includes IKE certificates and policies for internet key exchanges and Virtual Private Network connections.

Internet Key Exchange (IKE) Policies

The administrator can view, add, and update one or more IKE policies.

Viewing a List of IKE Policies

The administrator can view IKE Policies.

To view a list of available IKE policies:

1. On the menu, click **IPsec Management > IKE Policies**. The following page displays, listing current IKE policies.

Figure 7-21 Internet Key Exchange Policies Page

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with fields for 'Table' (set to 'Ethernet Device'), 'Field' (set to 'Name'), and 'Value'. There are 'Search' and 'Reset' buttons, and a 'Logout' link for 'sysadmin@SLM1C77' in the 'Group: Administrators'.

The left sidebar contains a navigation menu with the following items: Configuration, Network Settings, IPv4 Filters, IPsec Management (highlighted), IKE Certificates, IKE Policies (highlighted), VPN Connections, Modem Management, Authentication, Services, Device Management, Accounts, Events, Files, Ethernet Devices, and Managed Devices.

The main content area is titled 'Internet Key Exchange Policies'. It has tabs for 'List', 'Notes', and 'Help'. Below the tabs is a table with the following columns: Name, Gateway Type, Authentication, Exchange Type, Local Peer ID Type, Remote Peer ID Type, Certificate, PFS, DH Group, Auth Algorithm, Encrypt Algorithm, Lifetime, and XAUTH. The table currently displays '0 items' and an 'Add New Policy' button.

2. View the list of policies and associated information:

Table 7-22 IKE Policy Exchange Information

Ike Policy Setting	Description
Name	Name identifying the IKE policy.
Gateway Type	IPv4 or IPv6 type of address.
Authentication	Method of verifying data integrity: PSK: Pre-Shared Key uses a password exchange and matching process.
Exchange Type	Mode during the security association phase of the key exchange. <i>Note:</i> Aggressive mode will be available in a future release.
Local Peer ID Type	Local SLM identification type: IPv4: Internet Protocol version 4 IPv6: Internet Protocol version 6 FQDN: Fully Qualified Domain Name User Email: Email address of the local user
Remote Peer ID Type	Remote host or gateway identification type.
Certificate	<i>Note:</i> This feature will be available in a future release.
PFS	Perfect Forward Secrecy (PFS) ensures that a given IPsec SA key was not derived from any other secret, such as another key. Enabled by default.
DH Group	Diffie-Hellman key group (DHx) used for an encryption key.
Authentication Algorithm	From the drop-down list, select an algorithm for verifying data integrity: SHA1: Secure Hash Algorithm 1 MD5: Message Digest SHA2-256: 256-bit Secure Hash Algorithm
Encryption Algorithm	Method of encrypting data, in order of security level provided: 3DES: Data Encryption Standard AES: Advanced Encryption Standard AES-192: 192-bit key with AES encryption AES-256: 256-bit key with AES encryption
Lifetime	Duration in seconds before a key expires.
XAUTH	XAUTH in use.

Adding an IKE Policy:

The administrator can add an IKE policy.

To add a new IKE policy:

1. On the **List** tab, click the **Add New Policy** button. The **Configure** tab displays.

Figure 7-23 Add Internet Key Exchange Policy Page

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1C77' with the role of 'Administrators'. The main heading is 'Add Internet Key Exchange Policy'. The configuration area includes the following fields and options:

- Policy Name: [Text Input]
- Gateway Address Type: IPv4 (dropdown)
- Remote Gateway Address: [Text Input]
- Authentication Method: PSK (dropdown)
- Exchange Type: Main Mode (radio selected), Aggressive Mode (radio)
- Local Peer ID Type: IPv4 (dropdown)
- Local Peer ID Value: [Text Input]
- Remote Peer ID Type: IPv4 (dropdown)
- Remote Peer ID Value: [Text Input]
- Certificate File: [Text Input]
- PSK Value: [Text Input]
- PFS: (checked)
- DH Group: MODP1024 (dropdown)
- Authentication Algorithm: SHA1 (dropdown)
- Encryption Algorithm: 3DES (dropdown)
- XAUTH: (client only)
- Lifetime: 3600
- Login: [Text Input]
- Password: [Text Input with masked characters]

Buttons for 'Submit' and 'Delete' are located at the bottom of the configuration area.

2. Enter the following information:

Table 7-24 Add Internet Key Exchange Policy - Configure Tab

Ike Policy Setting	Description
Policy Name	Enter a name to identify the IKE policy. Must be 1-63 characters, including digits, letters, hyphens, and underscores.
Gateway Address Type	From the drop-down list, select the version of the Internet Protocol used for the address: IPv4: Internet Protocol version 4 (default) IPv6: Internet Protocol version 6
Remote Gateway Address	Enter the IP address of the remote end of the gateway.
Authentication Method	From the drop-down list, select the method of verifying data integrity: PSK: Pre-Shared Key uses a password exchange and matching process. (default) RSA Signature: Uses a private and public key that together comprise a digital signature. <i>Note: This feature will be available in a future vSLM 2 release.</i>
Exchange Type	Select the mode during the security association phase of the key exchange: Main Mode: (default) <i>Note: Aggressive mode will be supported in a future release.</i>
Local Peer ID Type	From the drop-down list, select the method of filtering incoming data. IPv4: Internet Protocol version 4 IPv6: Internet Protocol version 6 FQDN: Fully Qualified Domain Name User Email: Email address of the local user
Local Peer ID Value	Enter the local vSLM 2 identification value. This value depends on the Local Peer ID Type setting.

Ike Policy Setting	Description
Remote Peer ID Type	Select the method of filtering outgoing data: IPv4: Internet Protocol version 4 (default) IPv6: Internet Protocol version 6 FQDN: Fully Qualified Domain Name User Email: Email address of the remote user
Remote Peer ID Value	Enter the identification value of the remote host or gateway.
Certificate File	Note: This feature will be available in a future release.
PSK Value	Enter the value of a pre-shared key.
PFS	Select the checkbox to enable PFS (Perfect Forward Secrecy). PFS ensures that a given IPsec SA key was not derived from any other secret, such as another key. Enabled by default.
DH Group	Initial Diffie-Hellman value. MODP1024 MODP1536 MODP2048
Authentication Algorithm	From the drop-down list, select an algorithm for verifying data integrity: SHA1: Secure Hash Algorithm 1. MD5: Message Digest 5. SHA2-256: 256-bit Secure Hash Algorithm
Encryption Algorithm	From the drop-down list, select the method of encrypting data (listed below in order of security level provided): 3DES: Data Encryption Standard AES: Advanced Encryption Standard AES-192: 192-bit key with AES encryption AES-256: 256-bit key with AES encryption
XAUTH	Select to use a "group" shared secret rather than digital certificates for authentication. Disabled by default. Note: This feature will be available in a future vSLM 2 release.
Lifetime	Enter the duration in seconds before a key expires. Default is 3600.
Login	Enter the username for XAUTH.
Password	Enter the password for XAUTH.

- To save your entries, click the **Submit** button.

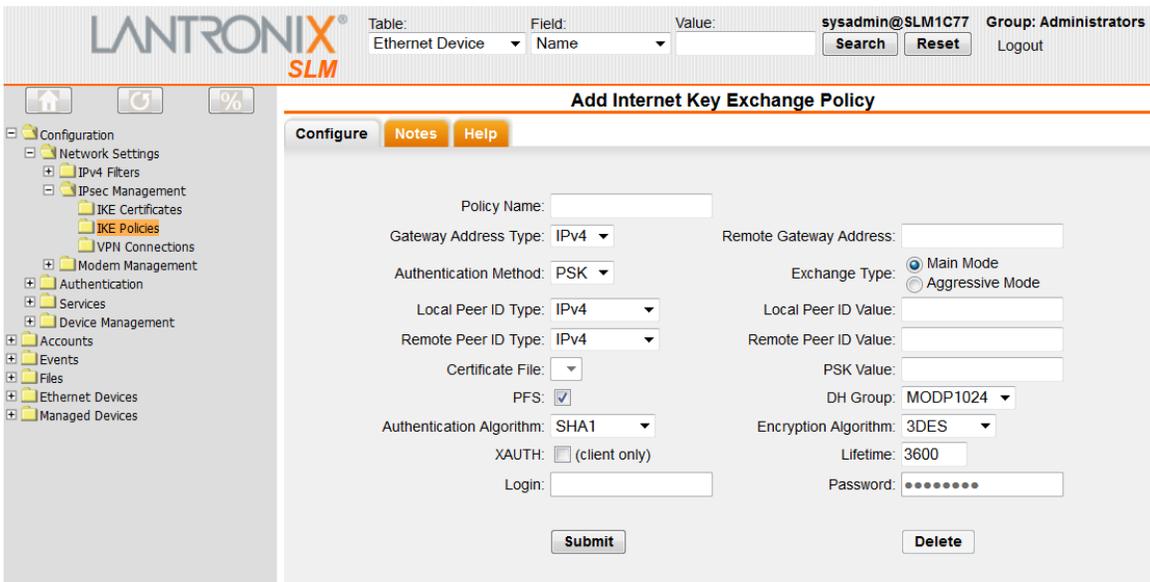
Updating or Deleting an IKE Policy

The administrator can update or delete IKE policies.

To update or delete a policy:

1. On the **List** tab, click the **Edit**  icon to the left of the policy. The **Configure** tab displays.

Figure 7-25 Internet Key Exchange Policy - Configure Tab



The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1C77' with the group 'Administrators'. The main content area is titled 'Add Internet Key Exchange Policy' and has three tabs: 'Configure', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following fields:

- Policy Name:
- Gateway Address Type: IPv4 (dropdown)
- Remote Gateway Address:
- Authentication Method: PSK (dropdown)
- Exchange Type: Main Mode, Aggressive Mode
- Local Peer ID Type: IPv4 (dropdown)
- Local Peer ID Value:
- Remote Peer ID Type: IPv4 (dropdown)
- Remote Peer ID Value:
- Certificate File:
- PSK Value:
- PFS:
- DH Group: MODP1024 (dropdown)
- Authentication Algorithm: SHA1 (dropdown)
- Encryption Algorithm: 3DES (dropdown)
- XAUTH: (client only)
- Lifetime: 3600
- Login:
- Password:

At the bottom of the configuration area, there are 'Submit' and 'Delete' buttons.

2. To delete a policy:

Note: You may not delete a policy currently referenced by a VPN.

- a. Click the **Delete** button.
 - b. In response to the request for confirmation, click **OK**.
 - c. Click **IKE Policies** on the menu bar.
3. To update a policy:
 - a. Edit the information as desired.
 - b. Click the **Update** button. A confirmation message displays.
 4. To save your entries, click the **Save** button.

VPN Connections

The administrator can view, add, or update one or more Virtual Private Networks (VPNs). Each VPN must reference an IKE Policy. You can only delete an IKE Policy that is not referenced by a VPN.

Viewing a List of VPNs

The administrator can view a list of VPNs.

To view a list of VPNs:

1. On the menu, click **Configuration > Network Settings > IPsec Management > VPN Connections**. The following page displays:

Figure 7-26 VPN Connections Page

2. View the following information about each VPN:

Table 7-27 VPN Connection Settings

VPN Connection Setting	Description
Name	Name that identifies VPN.
IKE Policy	IKE policy that references this VPN.
Encapsulation Mode	Tunnel mode: Used when the remote peer is an IPsec gateway. Host mode: Used when the remote peer is an IPsec host.
Remote Address Type	Subnet type: The subnet that is the destination of the IPsec traffic. Single: The single host that is the destination of the IPsec traffic.
Network Port	Network port on the vSLM 2 secure management software that connects to the VPN.
Local Protocol	IP protocol selected to protect data traffic.
Local Port	Method selected to protect data traffic on the TCP port of the vSLM 2 software.
Subnet Prefix	Subnet prefix length for Subnet type clients.
Auth Algorithm	Algorithm for verifying data integrity.

VPN Connection Setting	Description
Encrypt Algorithm	Method of encrypting data, in ascending order of security level provided: <ul style="list-style-type: none"> ◆ 3DES (Data Encryption Standard) ◆ Advanced Encryption Standard (AES) ◆ AES-192: 192-bit key with AES encryption ◆ AES-256: 256-bit key with AES encryption
Lifetime	Duration in seconds before a key expires.
Active	Indicates whether the VPN is ready to be connected.
Status	Indicates whether the VPN is connected or disconnected.

Adding a VPN

Administrators may add VPNs.

1. On the List tab, click the **New VPN Connection** button. The Configure tab displays.

Table 7-28 Add VPN Connection Settings

VPN Connection Setting	Description
VPN Name	Enter a name to identify the VPN.
Encapsulation Mode	Tunnel mode: Used when the remote peer is an IPSec gateway. Host mode: Used when the remote peer is an IPsec host.
Network Port	Select the network port connecting to the VPN.
Protocols	Select the protocol used in the VPN connection: <ul style="list-style-type: none"> ◆ ALL: All of the listed protocols are used. ◆ TCP: Transmission Control Protocol ◆ UDP: User Datagram Protocol ◆ ICMP: Internet Control Message Protocol ◆ ICMPv6: Internet Control Message Protocol version 6 ◆ IGMP: Internet Group Management Protocol
Port	Select the type of security used on the port: <ul style="list-style-type: none"> ◆ All ◆ SSH ◆ Telnet ◆ FTP Data ◆ FTP Control ◆ HTTP ◆ RLOGIN ◆ TFTP
IKEPolicy	IKE Policy that references this VPN.
Remote Peer Address Type	Subnet type: The subnet that is the destination of the IPsec traffic. Single: The single host that is the destination of the IPsec traffic.
Remote Peer IP Start	Starting IP address in a range of remote IP addresses.
Subnet Prefix	Prefix of the subnet for Subnet Type peers.

VPN Connection Setting	Description
Authentication Algorithm	From the drop-down list, select the algorithm for verifying data integrity: None SHA1: MD5: SHA2-256:
Encryption Algorithm	From the drop-down list, select the method of encrypting data: 3DES (Data Encryption Standard) AES AES-192 AES-256
SA Lifetime	Duration in seconds before an IPsec Security Association (SA) expires. The default is 28800.
Active	Select to activate the VPN.

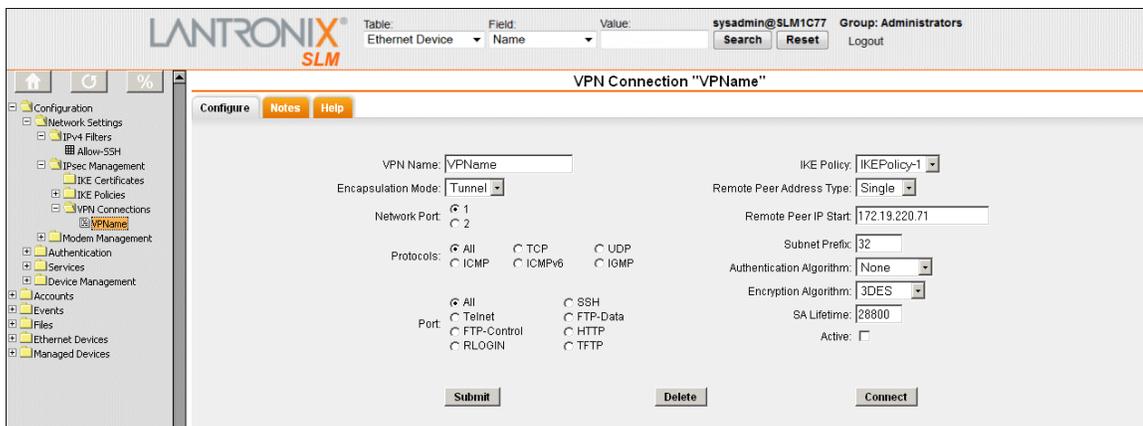
- To save, click the **Submit** button.

Updating or Deleting a VPN

To update or delete a VPN:

- On the List tab, click the **Edit**  icon to the left of the policy. The Configure tab displays.

Figure 7-29 VPN Connection - Configure Tab



The screenshot shows the LANTRONIX SLM web interface. The top navigation bar includes a search function with fields for Table (Ethernet Device), Field (Name), and Value. The user is logged in as sysadmin@SLM1C77. The main content area is titled 'VPN Connection "VPNName"' and has tabs for 'Configure', 'Notes', and 'Help'. The 'Configure' tab is active, showing various settings for the VPN connection. On the left, a sidebar menu shows the current location: Configuration > Network Settings > IPsec Management > VPN Connections > VPNName. The configuration form includes:

- VPN Name: VPNName
- Encapsulation Mode: Tunnel
- Network Port: Radio buttons for 1 and 2.
- Protocols: Radio buttons for All, TCP, UDP, ICMP, ICMPv6, and IGMP.
- IKE Policy: IKEPolicy-1
- Remote Peer Address Type: Single
- Remote Peer IP Start: 172.19.220.71
- Subnet Prefix: 32
- Authentication Algorithm: None
- Encryption Algorithm: 3DES
- SA Lifetime: 28800
- Active:

Buttons for 'Submit', 'Delete', and 'Connect' are located at the bottom of the form.

- To delete a VPN:
 - Click the **Delete** button.
 - In response to the request for confirmation, click **OK**.
 - Click **VPN Connections** on the menu bar.
- To update a policy:
 - Edit the information as desired.
 - Click the **Update** button. A confirmation message displays.
- To save your entries, click the **Save** button.

Connecting a VPN

To connect a VPN:

1. On the **List** tab, click the **Edit**  icon to the left of the VPN. The VPN Connection page displays.
2. Make sure you have updated the connection.
3. Select the **Active** checkbox (if not already selected).
4. Click the **Connect** button. It will take a couple of seconds before the connection is established.

Modem Management

Dial-up modem support ensures access when the network is not available. vSLM 2 secure management software supports dial-in (text mode and PPP mode) and dial-out (PPP mode) as follows:

- ◆ The administrator can configure dial-in and dial-out from either the web interface or the CLI.
- ◆ A user dialing in from a remote computer in text mode can access the CLI on the SLM module.
- ◆ A user dialing in from a remote computer in PPP mode can access the CLI and the web interface on the vSLM 2 secure management software. Depending on the PPP settings, the user may access all devices that the vSLM 2 software has access to as well.
- ◆ A user can dial out from the CLI and the web interface in PPP mode.

Viewing a List of Modems

The administrator can view a list of the vSLM 2 secure management software's internal and external modems.

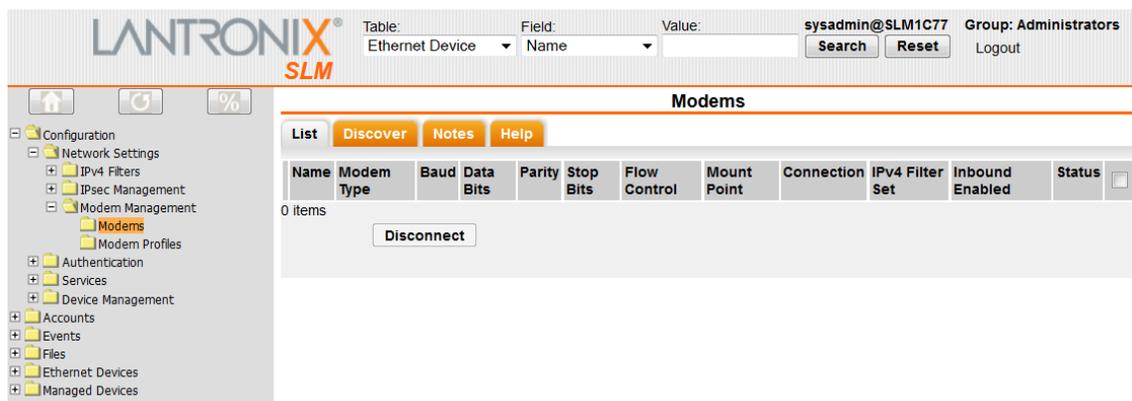
Note: The vSLM 2 software supports USB modems only. See [Discovering a USB Modem](#). vSLM 2 secure management software does not support plug-and-play.

To view a list of available modems:

1. On the menu, click **Configuration > Network Settings > Modem Management > Modems**.

The following page displays.

Figure 7-30 Modems Page



The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with fields for 'Table:' (set to 'Ethernet Device'), 'Field:' (set to 'Name'), and 'Value:'. There are 'Search' and 'Reset' buttons, and a 'Logout' link. The user is identified as 'sysadmin@SLM1C77' with the group 'Administrators'. The main content area is titled 'Modems' and has tabs for 'List', 'Discover', 'Notes', and 'Help'. Below the tabs is a table with the following columns: Name, Modem Type, Baud, Data Bits, Parity, Stop Bits, Flow Control, Mount Point, Connection, IPv4 Filter Set, Inbound Enabled, and Status. The table is currently empty, showing '0 items'. There is a 'Disconnect' button below the table. On the left side, there is a navigation menu with a tree view showing 'Configuration' > 'Network Settings' > 'Modem Management' > 'Modems' selected.

- View the following information about each modem:

Table 7-31 Modem - List Tab

Modem Setting	Description
Name	Name that identifies the modem.
Modem Type	Identifies the type of modem (e.g., PCI or USB).
Baud	Communication speed between the vSLM 2 secure management software and a modem.
Data Bits	Number of data bits used to transmit a character.
Parity	Type of parity checking. Parity checking detects simple, single-bit errors.
Stop Bits	Number of stop bit(s) used to indicate that a byte of data has been transmitted.
Flow Control	Method of preventing buffer overflow and loss of data.
Mount Point	Name of the serial interface device to which the modem is assigned.
Connection	Name of connection assigned for dial-in. See Enabling or Disabling Dial-in Connections on page 83 .
IPv4 Filter Set	IPv4 filter being used.
Inbound Enabled	Indicates whether the modem is enabled to receive dial-in calls.
Status	Indicates whether the modem is currently connected.

- To disconnect a connection, select its check box and click the **Disconnect** button.

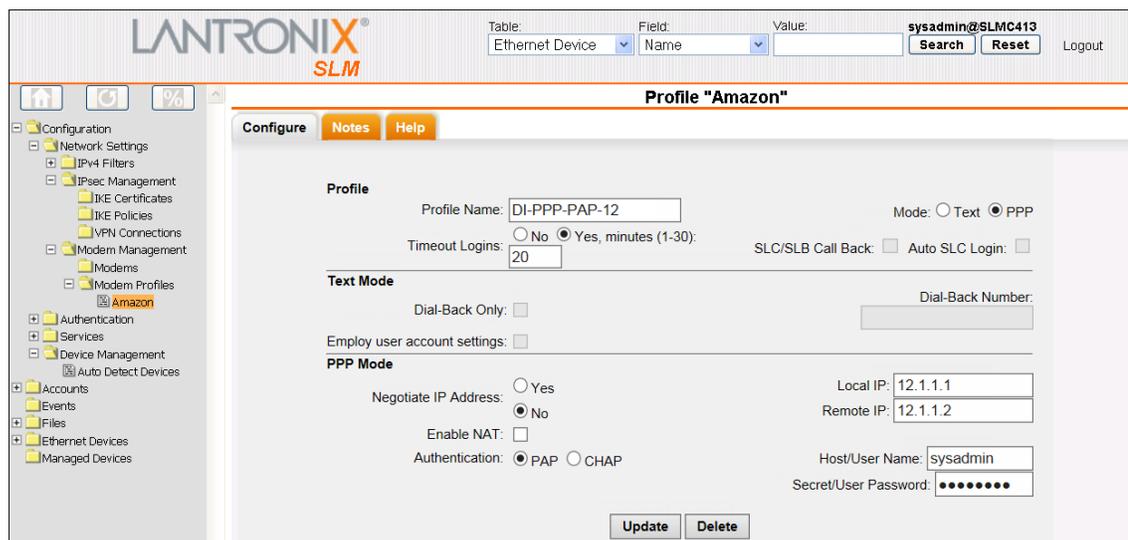
Configuring a Modem

The administrator can configure the modem for an incoming connection from a remote device or computer.

To configure a modem:

- Select the modem and click the **Configure** tab. The following page opens:

Figure 7-32 Modem Page - Configure Tab



The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLMC413'. The main content area is titled 'Profile "Amazon"' and has three tabs: 'Configure', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following settings:

- Profile:** Profile Name: DI-PPP-PAP-12; Mode: Text PPP
- Text Mode:** Timeout Logins: No Yes, minutes (1-30): 20; SLC/SLB Call Back: ; Auto SLC Login: ; Dial-Back Only: ; Dial-Back Number: [empty field]; Employ user account settings:
- PPP Mode:** Negotiate IP Address: Yes No; Local IP: 12.1.1.1; Remote IP: 12.1.1.2; Enable NAT: ; Authentication: PAP CHAP; Host/User Name: sysadmin; Secret/User Password: [masked]

At the bottom of the form, there are 'Update' and 'Delete' buttons. On the left side, there is a navigation tree with categories like Configuration, Network Settings, IPsec Management, Modem Management, and Modem Profiles.

2. Enter the following information:

Note: In most cases, you do not need to change these settings.

Table 7-33 Modem - Configure Tab

Modem Setting	Description
Modem Name	You may change the modem name assigned by the vSLM 2 software.
Modem Type (view only)	Displays PCI or USB .
Model (view only)	Manufacturer's name for the modem.
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 vSLM 2 secure management software uses a default initialization string of <code>AT S7=45 S0=0 V1 X4 &D2 &C1 E1 Q0</code> . Note: We recommend that the modem initialization script always be preceded with <code>AT</code> and include <code>E1 V1 x4 Q0</code> so that the vSLM 2 software can properly control the modem.
Baud	Communication speed between the SLM appliance and the modem. From the drop-down list, select the baud rate. The default setting is 115200 .
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 detects simple, single-bit errors. From the drop-down list, select the parity. The default is none.
Stop Bits	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	Method of preventing buffer overflow and loss of data. The available methods include none, XON/XOFF (software), and RTS/CTS (hardware). The default is RTS/CTS .
Current Status (view only)	Status of the connection.

3. To save, click the **Update** button. A confirmation message displays.

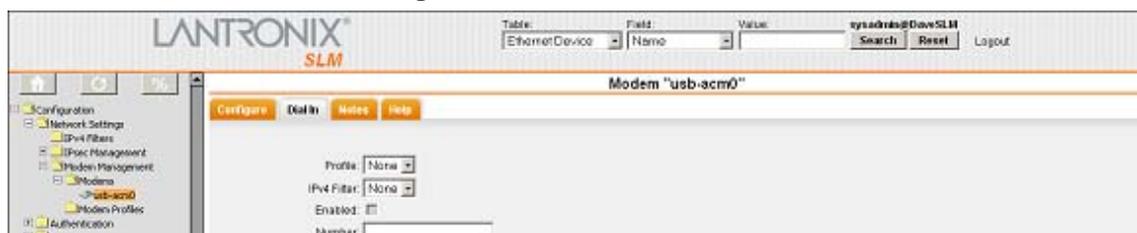
Enabling or Disabling Dial-in Connections

The system administrator can enable the modem to answer incoming calls and can set the mode to use when establishing these connections.

To enable or disable dial-in connections to a modem:

1. Click the **Dial in** tab. The following page opens:

Figure 7-34 Modem - Dial in Tab



2. Enter the following information:

Table 7-35 Modem - Dial-In Tab

Modem Setting	Description
Profile	From the drop-down list, select the desired profile. The default is none .
IPv4 Filter	From the drop-down list, select an IPv4 filter for the connection. The default is none .
Enabled	Select this check box to allow incoming connections on this modem. Disabled until a connection is selected.

3. To save, click the **Submit** button. A confirmation message displays.

Viewing a List of Profiles

The administrator can view a list of modem connections.

1. On the menu, click **Configuration > Network Settings > Modem Management > Modem Profiles**. The following page opens:

Figure 7-36 Modem Profiles - List Tab

Name	Modem Mode	Timeout	Negotiate	Local IP	Remote IP	Modem Authentication	Host/User Name	NAT
DI-PPPAPNAT172	PPP	20	No	172.19.39.17	172.19.39.23	PAP	sysadmin	Yes
DI-PPP-CHAP-12	PPP	20	No	12.1.1.1	12.1.1.2	CHAP	test	No
DI-PPP-CHAP172	PPP	20	No	172.19.39.17	172.19.39.23	CHAP	test	No
DI-PPPCHAPNAT12	PPP	20	No	12.1.1.1	12.1.1.2	CHAP	test	Yes
DI-PPPCHNAT172	PPP	20	No	172.19.39.17	172.19.39.23	CHAP	test	Yes
DI-PPP-PAP-12	PPP	20	No	12.1.1.1	12.1.1.2	PAP	sysadmin	No
DI-PPP-PAP172	PPP	20	No	172.19.39.17	172.19.39.23	PAP	sysadmin	No
DI-PPP-PAPNAT12	PPP	20	No	12.1.1.1	12.1.1.2	PAP	sysadmin	Yes
DI-Text-T0	Text	20	Yes	0.0.0.0	0.0.0.0	PAP		No
DI-Text-T1	Text	1	Yes	0.0.0.0	0.0.0.0	PAP		No
DO-PPPAPNAT172	PPP	20	No	172.19.39.17	172.19.39.23	PAP	sysadmin	Yes
DO-PPP-CHAP-12	PPP	20	No	12.1.1.1	12.1.1.2	CHAP	test	No
DO-PPP-CHAP172	PPP	20	No	172.19.39.17	172.19.39.23	CHAP	test	No
DO-PPPCHAPNAT12	PPP	20	No	12.1.1.1	12.1.1.2	CHAP	test	Yes
DO-PPPCHNAT172	PPP	20	No	172.19.39.17	172.19.39.23	CHAP	test	Yes
DO-PPP-PAP-12	PPP	20	No	12.1.1.1	12.1.1.2	PAP	sysadmin	No
DO-PPP-PAP172	PPP	20	No	172.19.39.17	172.19.39.23	PAP	sysadmin	No
DO-PPP-PAPNAT12	PPP	20	No	12.1.1.1	12.1.1.2	PAP	sysadmin	Yes
test	Text	20	Yes	0.0.0.0	0.0.0.0	PAP		No

2. View the following information about each connection:

Table 7-37 Modem Profile - List Tab

Modem Profiles Setting	Description
Name	A name identifying the specific connection.

Modem Profiles Setting	Description
Modem Mode	The format in which the data flows back and forth: Text: In this mode, the vSLM 2 secure management software assumes that the modem is for remotely logging into the CLI. Text mode is only for dialing in. PPP: This mode establishes an IP-based link over the modem. Dial-out mode uses PPP connections (e.g., the vSLM 2 software connects to an external network). You can dial out from both the CLI and the web interface.
Timeout	Indicates whether the connection times out logins after the connection is inactive for a specified number of minutes (1-30).
Negotiate	If Yes , the remote device or PC specifies the local (vSLM 2 secure management software) IP and remote addresses. If No , the vSLM 2 software assigns the local (vSLM 2 secure management software) IP and remote IP addresses.
Local IP	IP address of the vSLM 2 software.
Remote IP	IP address of the remote device or remote PC.
Modem Authentication	Indicates whether the vSLM 2 secure management software uses PAP or CHAP to authenticate modem logins.
Host/User Name	Username for dial-ins or dial-outs between the vSLM 2 software and a remote system.
NAT	If Yes , the vSLM 2 secure management software uses Network Address Translation (NAT) for dial-in PPP connections. Users dialing into the vSLM 2 software access the network connected to Eth1 and/or Eth2. <i>Note: This does not apply to dial-out PPP.</i>

Adding a Profile

The administrator can define a Text or PPP profile for use by an appropriate modem in the system.

To add a profile:

1. On the menu, click **Configuration > Network Settings > Modem Management > Modem Profiles**, and then click the **Add New Profile** button. The following page opens:

Figure 7-38 New Profile-Configure Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1C77' with the group 'Administrators'. The main content area is titled 'New Profile' and has three tabs: 'Configure', 'Notes', and 'Help'. The 'Configure' tab is active and contains the following settings:

- Profile:** Profile Name (text input), Mode (radio buttons for Text and PPP), Timeout Logins (radio buttons for No and Yes, minutes (1-30)), SLC/SLB Call Back (checkbox), Auto SLC (checkbox), and Login (checkbox).
- Text Mode:** Dial-Back Only (checkbox), Dial-Back Number (text input), and Employ user account settings (checkbox).
- PPP Mode:** Negotiate IP Address (radio buttons for Yes and No), Enable NAT (checkbox), Authentication (radio buttons for PAP and CHAP), Local IP (text input), Remote IP (text input), Host/User Name (text input), and Secret/User Password (password input).

At the bottom of the configuration area are 'Update' and 'Delete' buttons.

2. Enter the following information:

Table 7-39 New Profile - Configure Tab - Profile

New Profile Setting	Description
Profile Name	A name identifying the specific profile.
Mode	The format in which the data flows back and forth: Text: In this mode, the vSLM 2 secure management software assumes that the modem is for remotely logging into the CLI. Text mode is only for dialing in. Enabled by default. PPP: This mode establishes an IP-based link over the modem. Dial-out mode uses PPP connections (e.g., the vSLM 2 software connects to an external network). You can dial out from both the CLI and the web interface.
Timeout Logins	For both Text and PPP modes, you can enable logins to time out after the connection is inactive for a specified number of minutes (1-30).
Call Back	Select to enable this security feature. When the vSLM 2 secure management software user calls an SLC console manager and logs in, the SLC device hangs up and calls the user back. The vSLM 2 software then logs in again. This feature is currently available in text mode only.
Auto Login	If you select the check box, when the vSLM 2 software attempts to connect to an SLC console manager via a text mode connection, it automatically uses the Login and Password specified on the SLC Device page. If you do not select it, the user will have to enter the password and login manually.

Table 7-40 New Profile - Configure Tab - Text Mode

Text Mode Setting	Description
Dial-Back Only	<p>Select to grant a local user dial-back access. Users with dial-back access can dial into the vSLM 2 secure management software and enter their login and password. Once the vSLM 2 software authenticates them, the modem hangs up and dials them back. Disabled by default.</p> <p>Following are the rules the vSLM 2 software follows concerning Dial-Back Only in Text mode.</p> <p>If both Dial-Back Only and Use User Profile are not selected, users can dial in text mode. (Regular usage).</p> <p>If Dial-Back Only is not selected and Use User Profile is selected:</p> <ul style="list-style-type: none"> ◆ If Enable Dial-back is selected on the Manage Account page, the user can only dial in using dial-back with the number defined on the Manage Account page. ◆ If Enable Dial-back is not selected, the user can dial in using text mode. <p>If Dial-Back Only is selected and Use User Profile is not selected, users can only dial in using dial-back. vSLM 2 secure management software dials back to the number defined on the Modem Connection.</p> <p>If Dial-Back Only is selected and Use User Profile is selected</p> <ul style="list-style-type: none"> ◆ If Enable Dial-back on the Manage account page is selected, the user can only dial in using dial-back with the number defined on the Manage account page. ◆ If Enable Dial-back on the Manage account page is not selected, the user can only dial in using dial-back. vSLM 2 software dials back to the number defined on the Modem connection page.
Dial-Back Number	Enter the phone number the modem dials back on. It can be a fixed number or a number associated with the user's login. If you select Fixed Number , enter the number in the format 2123456789.
Employ User Account Settings	Select to indicate that the vSLM 2 secure management software takes dial-back rules from the local user account on the Manage Account page (see Accounts on page 125).

Table 7-41 New Profile - Configure Tab - PPP Mode

PPP Mode Setting	Description
Negotiate IP Address	<p>For the remote device or PC to specify the local (vSLM 2 software) IP and remote addresses, select Yes. Defaults to Yes.</p> <p>For the vSLM 2 secure management software to assign the local (vSLM 2 software) IP and remote IP addresses, select No, and enter the local IP (IP address of the vSLM 2 software) and remote IP (IP address of the remote device or PC).</p>
Local IP	IP address of the vSLM 2 secure management software.
Remote IP	IP address of the remote device or remote PC.
Enable NAT	<p>Select to enable Network Address Translation (NAT) for dial-in PPP connections. Users dialing into the vSLM 2 software access the network connected to Eth1 and/or Eth2.</p> <p>Note: This does not apply to dial-out PPP.</p>
Authentication	<p>Enables PAP or CHAP authentication for modem logins. PAP is the default.</p> <ul style="list-style-type: none"> ◆ With PAP, if you do not specify username and password, 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. You must specify the username and password.

PPP Mode Setting	Description
Host/User Name	User name for dial-ins or dial-outs between the vSLM 2 software and a remote system for PAP or CHAP authentication.
Secret/User Password	Password for dial-ins or dial-outs between the vSLM 2 secure management software and a remote system for PAP or CHAP authentication.

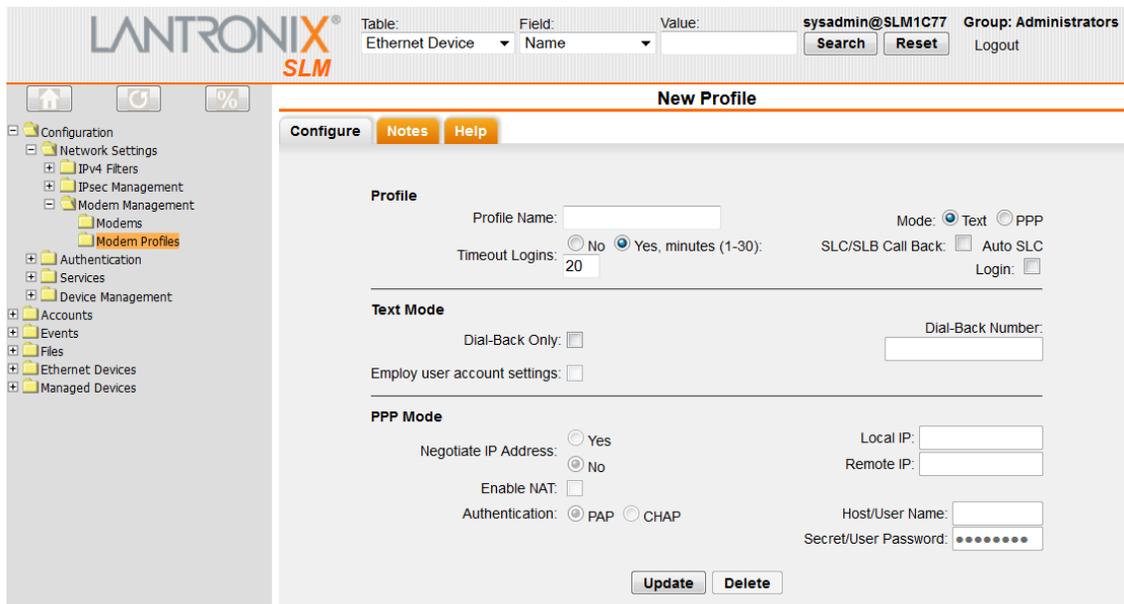
Updating and Deleting a Profile

The administrator can update or delete profiles.

To update or delete a modem profile:

1. On the menu, click **Configuration > Network Settings > Modem Management > Modem Profiles**, and then click the **Edit**  icon to the left of the modem profile you want to update or delete. The Configure tab displays.

Figure 7-42 Modem Profile Page - Configure Tab



The screenshot shows the LANTRONIX SLM web interface. At the top, there's a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1C77' with the group 'Administrators'. The left sidebar shows a tree view with 'Modem Profiles' selected. The main area is titled 'New Profile' and has three tabs: 'Configure', 'Notes', and 'Help'. The 'Configure' tab is active and contains the following fields:

- Profile Name:** [Text input]
- Mode:** Text PPP
- Timeout Logins:** No Yes, minutes (1-30): [20]
- SLC/SLB Call Back:** Auto SLC
- Login:**
- Dial-Back Only:**
- Dial-Back Number:** [Text input]
- Employ user account settings:**
- Negotiate IP Address:** Yes No
- Local IP:** [Text input]
- Remote IP:** [Text input]
- Enable NAT:**
- Authentication:** PAP CHAP
- Host/User Name:** [Text input]
- Secret/User Password:** [Password input]

At the bottom of the form are 'Update' and 'Delete' buttons.

2. To delete a profile:
 - a. Click the **Delete** button.
 - b. In response to the request for confirmation, click **OK**.
 - c. Click **Modem Profiles** on the menu tree. The deleted connection is no longer on the menu tree or listed on the List tab.
3. To update a profile:
 - a. Edit the information as desired.
 - b. Click the **Update** button. A confirmation message displays.

Note: For information about configuring a dial-out profile, see [Configuring a Modem Connection to a Managed Device on page 218](#).

Discovering a USB Modem

The system administrator can attach a USB modem to an vSLM 2 secure management software and configure it into the system without rebooting the vSLM 2 software. For the vSLM 2 software, a USB modem must first be connected to the vSLM VM prior to discovery of the modem; refer to the documentation for your virtualization manager for instructions on connecting a USB device to a VM.

To "discover" a USB Modem:

1. On the menu, click **Configuration > Network Settings > Modem Management > Modems** and then click the **Discover** tab. The Discover tab displays.
2. Click the **Discover** button. A message displays indicating that the task (discovering USB modems) has started.
3. After a few moments, refresh the tree structure. Any new USB modems display in the tree.

Modem Commands

set modem reset

Note: You may only use this command when the modem is completely stuck. Wait for minimum timeout period (3 minutes) before you use this command when:

- ◆ You dial out via PPP and encounter no dial tone.
- ◆ You dial out via PPP and encounter a busy signal.

Syntax

```
set modem reset
```

Description

Resets a modem connection.

set modem disconnect

Note: Type `show modem` to view the current modem connections.

Syntax

```
set modem disconnect <Name>
```

Example

```
set modem disconnect MyPCIModem
```

Description

Terminates modem dial-out connection.

set modem edit

Syntax

```
set modem edit <Modem Name> <parameters>
```

Parameters

name <New Name>
baud <300-115200>
flowcontrol <none|xon/xoff|rts/cts>
speaker <enable|disable>
initscript <Modem Initialization Script>
defaultinitscript <Modem Default Initialization Script>
dialin <Dial Account Name|CLEAR|disable|enable>

dialin CLEAR removes the dial account assignment.

dialin disable disables dial-in.
dialin enable enables dial-in
ipfilter <IPv4 Filter Name|CLEAR>

ipfilter CLEAR removes the ipfilter assignment.

number <modem telephone number|CLEAR>

Description

Configures a currently loaded modem.

show modem**Syntax**

show modem

Description

Displays all modems.

show modem connection**Syntax**

show modem connection <parameters>

Parameters

[index <number>]

Description

Displays active (established) modem connections.

show modem settings**Syntax**

show modem <parameters>

Parameters

[name <Modem Name>]
[index <number>]

Description

Displays modem settings.

show modem status**Syntax**

```
show modem status
```

Description

Displays the status of the modem.

Dial Account Commands

set dialaccount add**Syntax**

```
set dialaccount add <Dial Account Name> <parameters>
```

Parameters

```
modemmode <text|ppp>  
localipaddr <negotiate|IP Address>  
remoteipaddr <negotiate|IP Address>  
auth <pap|chap>  
username <User Name>  
password <Password>  
nat <enable|disable>  
callback <disable|enable> (text mode for SLC dialback)  
dialbacknumber <dial-back number|CLEAR> (apply only text mode)  
useraccount <disable|enable> (text mode dialback)  
timeout <disable|1-30 minutes>
```

Default is 20.

The parameter "dialbacknumber CLEAR" remove the dial-back number.

The parameter "useraccount enable" use local user defined dial-back configuration.

Use "set modem" command to assign dial account to modem dialin.

Use "set manageddevice" command to assign dial account to modem dialout.

Description

Creates a new dial account.

set dialaccount delete**Syntax**

```
set dialaccount delete <Dial Account Name>
```

Description

Delete a dial account.

set dialaccount edit**Syntax**

```
set dialaccount edit <Dial Account Name> <parameters>
```

Parameters

```
modemmode <text|ppp>
localipaddr <negotiate|IP Address>
remoteipaddr <negotiate|IP Address>
auth <pap|chap>
username <User Name>
password <Password>
nat <enable|disable>

callback <disable|enable> (text mode for SLC dialback)
dialbacknumber <dial-back number|CLEAR> (apply only text mode)
CLEAR removes the dial-back number.
useraccount <disable|enable> (apply only text mode)
Uses local user-defined dial-back configuration.
timeout <disable|1-30 minutes>
```

Description

Modifies a dial account's settings.

set manageddevice config**Syntax**

```
set manageddevice config <Device Name> [dialout <Dial Account
Name|enable|disable> modem <Modem Name> phonenumber
<phonenumber>]application <ssh|telnet|http|none>]
```

Description

Configures modem and dial account settings for a managed device. Find managed device by device name and modify device parameters.

set manageddevice index**Syntax**

```
Type show manageddevice all to display index.

set manageddevice index <number> fuse
    ethernetdevice <EthernetDeviceName|IP>
    [port <Port Name|Port Number>]
set manageddevice index <number> defuse
[device|serial|kvm|power1|power2]
```

Examples

```
set ma add MD-1 group 'MD Group A' eth slc16
set ma fuse MD-1 eth slb-04 port 9
set ma defuse MD-1 serial
```

```
set ma index 2 fuse eth 172.19.220.64 port 8
```

Find managed device by device name and modify device parameters:

```
set manageddevice config <Device Name>
    <one or more parameters>
```

Find managed device by index and modify device parameters:

Type 'show manageddevice all' to get index.

```
set manageddevice index <number>
    <one or more parameters>
```

Parameters

```
[name <New Name>]
    [powerport <1|2> state <on|off|cyclepower>]
    [delete]
    [dialout <Dial Account Name|enable|disable>
        modem <Modem Name>
        phonenumber <phone number>]
    application <ssh|telnet|http|none>]
```

To set modem parameters, you must specify dialout option. Other modem options follow.

Examples

```
set ma config port-1 name waimea-port-1
set ma config slp-sunset-port1 powerport 1 state off
set ma index 1 delete
set ma index 1 dialout myaccount modem pci-s4 phone 3334444
```

Find managed device by device name and disconnect modem:

```
set manageddevice config <Device Name> disconnect modem
```

Find managed device by index and disconnect modem:

Type 'show manageddevice all' to get index.

```
set manageddevice index <number> disconnect modem
set ma index 2 disconnect modem
```

Assign or remove permissions for a managed device by name:

```
set manageddevice assign <managedDeviceName>
    group <managedDeviceGroup>
    [write|remove]
```

Assign or remove permissions for a managed device by index:

```
set manageddevice index <number> assign
    group <managedDeviceGroup>
    [write|remove]
set ma assign MD-device group MD-group
set ma assign MD-device group MD-group remove
set ma index 1 assign group MD-group write
```

Description

Finds managed device by index and modifies or defuses an Ethernet device or port.

To set modem parameters, you must specify a dial-out option.

show dialaccount

Note: Type *show dialaccount* to display index.

Syntax

```
show dialaccount <parameters>
```

Parameters

```
[name <Dial Account Name>]  
[index <number>]
```

Examples

```
show dialaccount  
show dialaccount name ppp-pap  
show dialaccount index 2
```

Description

Displays dial account settings.

show dialaccount mapping

Syntax

```
show dialaccount mapping
```

Description

Shows dial account used by dial-in and dial-out.

8: User Management

This chapter is primarily for administrators, who configure authentication methods, add, update, and delete accounts and account groups, and grant account and account group permissions.

By default, local authentication is enabled and is the first method the vSLM 2 secure management software uses to authenticate users. The administrator can select additional authentication methods, such as NIS, LDAP, RADIUS, and SSH public key or CLI login. The ability to assign different degrees of access to individual users or user groups provides another level of security.

The vSLM 2 software supports management of a variety of remote power managers (RPMs), including the Lantronix SLP and the ServerTech Sentry3 and Sentry4/PRO2 devices. A main unit and up to 3 expansion units are supported, with each unit having up to 96 outlets.

User Authentication Methods

On this page you may enable, disable and order methods for authenticating users attempting to log in to the vSLM 2 software. The methods include NIS, LDAP, RADIUS, Kerberos, TACACS+, and Local. The authentication method selection on the vSLM 2 software does not affect devices or vSLM 2 software interaction with devices.

By default, local authentication is enabled and is the first method the vSLM 2 secure management software uses to authenticate users. The ability to assign different degrees of access to individual users or user groups provides another level of security.

The authentication method selection on the vSLM 2 software does not affect devices or vSLM 2 software interaction with devices.

Note: For a user to be authenticated using one of the remote methods, the user's account must be configured for remote access (*Remote Only* or *Local & Remote*), or there must be an account defined whose login name is the same as the protocol (e.g., "NIS" for NIS).

If you enable multiple authentication methods, the vSLM 2 secure management software attempts login authentication in the order specified. When Attempt next method on authentication rejection is enabled, login authentication continues until a configured method reports success or all configured methods have been exhausted. When Attempt next method on authentication rejection is disabled, login authentication continues until a configured method reports success or failure, skipping non-responding methods.

Note: Adding an NIS user with the same user name as a local user may result in undefined behavior. For this reason, the vSLM 2 software prevents the addition of such accounts when NIS is configured and enabled, but it is unable to stop the creation of such accounts when NIS is disabled. The other remote authentication types are not affected by this issue.

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

1. On the menu, click **Configuration > Authentication**. The following page opens:

Figure 8-1 User Authentication - Configure Tab

2. To enable a method currently in the Disabled methods list, select the method and click the left arrow.

Table 8-2 User Authentication - Configure Tab

User Authentication Setting	Description
Local	The vSLM 2 secure management software authenticates users in the local database by user name and password. If this method is enabled, it always responds.
NIS (Network Information System)	A network naming and administration system developed by Sun Microsystems for smaller networks. Each host client or server computer in the system has knowledge about the entire system. A user at any host can access files or applications on any host in the network with a single user name and password. NIS uses the client/server model and the Remote Procedure Call (RPC) interface for communication between hosts. NIS consists of a server, a library of client programs, and some administrative tools. NIS is often used with the Network File System (NFS).
LDAP (Lightweight Directory Access Protocol)	A set of protocols for accessing information directories, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection-oriented transfer services.
RADIUS (Remote Authentication Dial-In User Service)	An authentication and accounting system used by many Internet Service Providers (ISPs). This client/server protocol 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.

User Authentication Setting	Description
Kerberos	Kerberos is a network authentication protocol that enables two parties to exchange private information across an unprotected network. It works by assigning a unique electronic credential, called a ticket, to each user who logs on to the network. The ticket is embedded in messages to identify the sender.
TACACS+ (Terminal Access Controller Access Control System)	TACACS+ allows a remote access server to communicate with an authentication server to determine whether the user has access to the network. TACACS+ is a completely new protocol and is not compatible with TACACS or XTACACS. The vSLM 2 software supports TACACS+ only.

- To disable a method currently in the Enabled methods list, select the method and click the right arrow between the lists.
- To set the order in which the vSLM 2 software will authenticate users, click the up and down arrows to the left of the Enabled methods list.
- To instruct the vSLM 2 secure management software to attempt authentication using the next configured method in the list when an authentication method responds to, and fails, a login, select the Attempt next method on authentication rejection check box.
- Check the box to Limit sysadmin account logins to the system console.
- Click the **Apply** button.

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

NIS

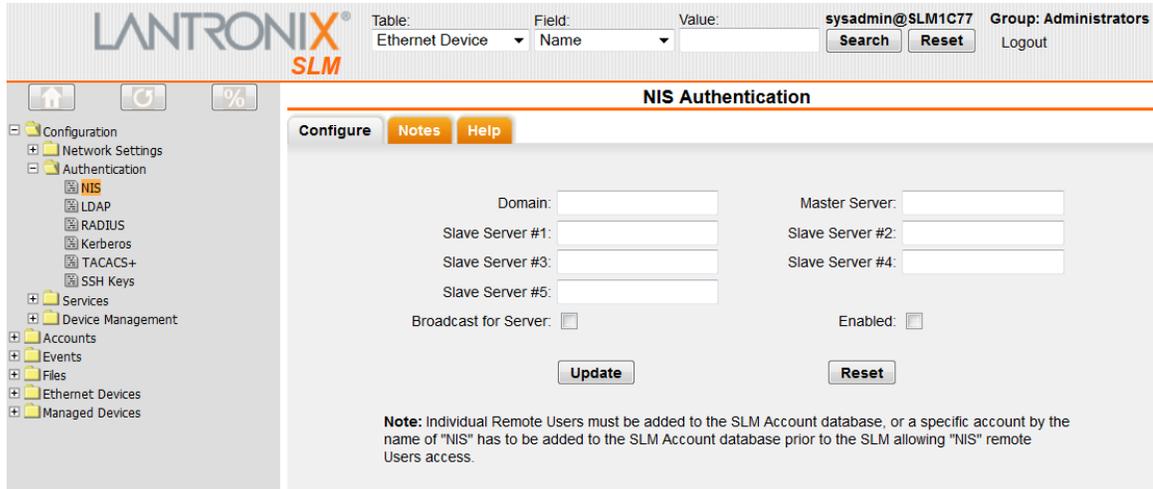
The administrator can configure the vSLM 2 software to use NIS to authenticate users attempting to log in to the vSLM 2 software through the web interface, SSH, Telnet, or the console port.

Note: For a user to log in remotely using NIS, the user's account must have remote access (*Remote Only* or *Local & Remote*), or there must be an account defined whose login name is NIS. See [Accounts on page 125](#) for information on setting up accounts.

To configure the vSLM 2 software to use NIS to authenticate users:

1. On the menu, click **Configuration > Authentication > NIS**. The following page opens.

Figure 8-3 NIS Authentication Page - Configure Tab



2. Enter the following:

Table 8-4 NIS Authentication - Configure Tab

NIS Authentication Page Setting	Description
Domain	The NIS domain of the vSLM 2 secure management software must be the same as the NIS domain of the NIS server.
Master Server (required)	The IP address or hostname of the master server.
Slave Server #1 - 5	The IP addresses or hostnames of up to five slave servers.
Broadcast for Server	Select the check box for the vSLM 2 software to send a broadcast datagram to find the NIS Server on the local network.
Enabled	Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box. <i>Note:</i> You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.

3. To save, click the **Update** button. A confirmation message displays.

LDAP

The administrator can configure the vSLM 2 secure management software to use LDAP to authenticate users attempting to log in to the vSLM 2 software through the web interface, SSH public key, Telnet, or the console port.

LDAP allows vSLM 2 software 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.

Note: For a user to log in remotely using LDAP, the user's account must have remote access (**Remote Only** or **Local & Remote**), or there must be an account defined whose login name is **LDAP**. See [Accounts on page 125](#) for information on setting up accounts.

Users that are authenticated via an LDAP server may automatically be created and assigned to SLM account groups. There are two methods for this: one using any type of group name of the LDAP server, and one using groups prefixed with "SLM_" (for backward compatibility).

For the method using any type of group name, if an LDAP account is a member of a group AND an account group exists on the SLM with the same name, then a user logging into the SLM using LDAP authentication will have an account automatically created for them in the matching account group, and the user will inherit all permissions assigned to that group. If a user is a member of more than one group, the SLM will try each group (in the order they were received from the LDAP server) until it finds one that matches.

For the method using groups prefixed with "SLM_", if an LDAP account is a member of a group and the name has the format "SLM_xxxxx" AND an account group exists on the SLM named "xxxxx" (without the "SLM_" prefix), then a user logging into the SLM using LDAP authentication will have an account automatically created for them in the matching account group, and the user will inherit all permissions assigned to that group. Example: user "dsmith" has an account on the LDAP server and is a member of group "SLM_musers". The account group "musers" has been defined on the SLM. When user dsmith logs into the SLM, a "dsmith" account will be created in the "musers" account group and user dsmith will log into the SLM using that account. If the dsmith LDAP account is a member of more than one group starting with "SLM_", the first one received from the LDAP server will be used; any other "SLM_xxxxx" groups will be ignored.

If later, the LDAP account dsmith is assigned to a different group, then at the next login, the dsmith account on the SLM will be moved to the new account group.

If a user is a member of both groups prefixed with "SLM_xxxxx" and groups that are not, the groups that are prefixed with "SLM_xxxxx" will be used to assign group membership.

For some LDAP servers, such as Microsoft Active Directory LDAP servers, the User Login Attribute, Group Filter Objectclass and Group Member Attribute/Group Member Value may need to be specified for the group assignment features. See these fields below for their use and suggested values.

To configure the vSLM 2 secure management software to use LDAP to authenticate users:

1. On the menu, click **Configuration > Authentication > LDAP**. The following page opens.

Figure 8-5 LDAP Authentication Page - Configure Tab

LANTRONIX[®] SLM

Table: Ethernet Device Field: Name Value: sysadmin@SLM1C77 Group: Administrators
 Search Reset Logout

LDAP Authentication

Configure Notes Help

Server: 172.19.211.15 Port: 636

Base: dc=patdomain,dc=local Active Directory Support:

Bind Name: cn=ldapbind,cn=Users,dc=patdomain Disabled

Bind Password: •••••••• Encrypt: Start TLS SSL

Retype Password: •••••••• Enabled:

User Login Attribute: sAMAccountName

Group Filter Objectclass: Group

Group Member Attribute: member

Group Member Value: DN Name

Update Reset

Note: Individual Remote Users must be added to the SLM Account database, or a specific account by the name of "LDAP" has to be added to the SLM Account database prior to the SLM allowing "LDAP" remote Users access.

2. Enter the following:

Table 8-6 LDAP Authentication Settings

LDAP Authentication Setting	Description
Server	The IP address or host name of the LDAP server.
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 and 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.
User Login Attribute	The attribute used by the LDAP server for user logins. If nothing is specified for the user filter, the SLM 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 SLM will use "posixGroup". For AD LDAP servers, the objectclass for groups is typically "Group".

LDAP Authentication Setting	Description
Group Member Attribute	The attribute used by the LDAP server for group membership. This attribute may be used in two ways to search for a user's group membership:
Group Member Value	<p>1. When the user's login record is retrieved (see User Login Attribute), the SLM will search for an attribute that matches the Group Member Attribute in the user's record. If nothing is specified for the group member attribute, the SLM will use "memberUID". For AD LDAP servers, the value used for this is typically "memberOf".</p> <p>2. To search through group records for group membership by a name (ie, "msmith") or a Distinguished Name (ie, "uid=msmith,ou=People,dc=ltx,dc=com"). Select either Name or DN as appropriate for the LDAP server. If nothing is specified for the group member attribute, the SLM will use "memberUID" for name and "uniqueMember" for DN. For AD LDAP servers, the Group Member Value is typically DN, with the Group Member Attribute of "member".</p>
Port	Number of the TCP port on the LDAP server to which the vSLM 2 secure management software talks. The default setting is 389 .
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 stores information about network resources within a domain. It is LDAP- and Kerberos- compliant. Disabled by default.
Encrypt	<p>Select Start TLS or SSL to encrypt messages between the SLM and the LDAP server. Disabled by default.</p> <ul style="list-style-type: none"> ◆ 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.
Enabled	<p>Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box.</p> <p>Note: You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.</p>

3. To save, click the **Update** button. A confirmation message displays.

RADIUS

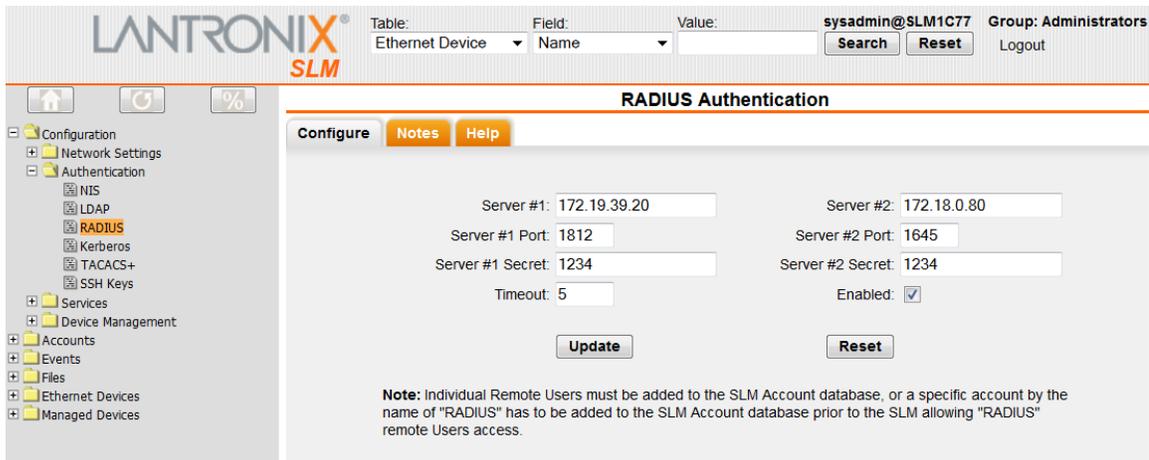
The administrator can configure the vSLM 2 secure management software to use RADIUS to authenticate users attempting to log in to the vSLM 2 software through the web interface, SSH public key, Telnet, or the console port.

Note: For a user to log in remotely using RADIUS, the user's account must have remote access (*Remote Only* or *Local & Remote*), or there must be an account defined whose login name is RADIUS. See [Accounts on page 125](#) for information on setting up accounts.

To configure the vSLM 2 software to use RADIUS to authenticate users:

1. On the menu, click **Configuration > User Authentication > RADIUS**. The following page opens.

Figure 8-7 RADIUS Authentication Page - Configure Tab



LANTRONIX[®] SLM

Table: Ethernet Device Field: Name Value: sysadmin@SLM1C77 Group: Administrators
 Search Reset Logout

RADIUS Authentication

Configure Notes Help

Server #1: 172.19.39.20 Server #2: 172.18.0.80
 Server #1 Port: 1812 Server #2 Port: 1645
 Server #1 Secret: 1234 Server #2 Secret: 1234
 Timeout: 5 Enabled:

Update Reset

Note: Individual Remote Users must be added to the SLM Account database, or a specific account by the name of "RADIUS" has to be added to the SLM Account database prior to the SLM allowing "RADIUS" remote Users access.

2. Enter the following:

Table 8-8 RADIUS Authentication Settings

RADIUS Authentication Setting	Description
Server #1	IP address or hostname of the primary RADIUS server.
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 vSLM 2 secure management software uses the default RADIUS port (1812). <i>Note:</i> Older RADIUS servers may use 1645 as the default port. Check your RADIUS server configuration.
Server #1 Secret	Text that serves as a shared secret between a RADIUS client and the server (vSLM 2 software). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.
Server #2	IP address or hostname of the secondary RADIUS server.
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 vSLM 2 software uses the default RADIUS port (1812). <i>Note:</i> Older RADIUS servers may use 1645 as the default port. Check your RADIUS server configuration.
Server #2 Secret	Text that serves as a shared secret between a RADIUS client and the server (vSLM 2 software). 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 after which the connection attempt times out. The default setting is 30.
Enabled	Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box. <i>Note:</i> You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.

3. To save, click the **Update** button. When the update is complete, a confirmation message displays.

Kerberos

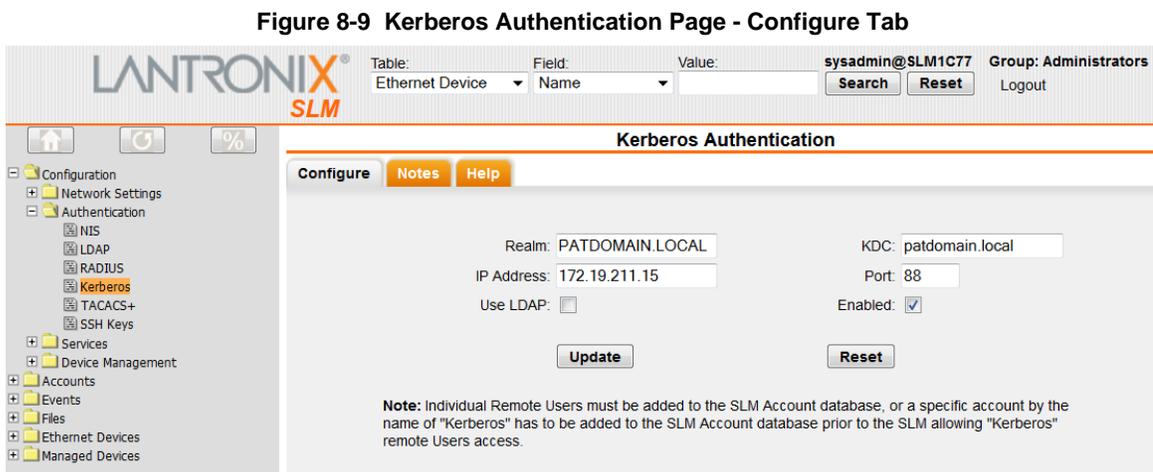
Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

The administrator can configure the vSLM 2 secure management software to use Kerberos to authenticate users attempting to log in to the vSLM 2 software through the web interface, SSH, Telnet, or the console port.

Note: For a user to log in remotely using Kerberos, the user's account must have remote access (Remote Only or Local & Remote), or there must be an account defined whose login name is Kerberos. See [Accounts on page 125](#) for information on setting up accounts.

To configure the vSLM 2 software to use Kerberos to authenticate users:

1. On the menu, select **Configuration > Authentication > Kerberos**. The following page opens.



2. Enter the following:

Table 8-10 Kerberos Authentication Settings

Kerberos Authentication Setting	Description
Realm	Enter the name of the logical network served by a single Kerberos database and a set of Key Distribution Centers. Usually, realm names are all uppercase letters to differentiate the realm from the Internet domain. Realm is similar in concept to an NT domain.
KDC	A key distribution center (KDC) is a server that issues Kerberos tickets. A ticket is a temporary set of electronic credentials that verify the identity of a client for a particular service. Enter the KDC in the fully qualified domain name format (FQDN). An example is SLC.local.
IP Address	Enter the IP address of the Key Distribution Center (KDC).
Port	Port on the KDC listening for requests. Enter an integer with a maximum value of 65535. The default setting is 88 .

Kerberos Authentication Setting	Description
Use LDAP	Indicate whether Kerberos should rely on LDAP to look up user IDs and Group IDs. This setting is disabled by default. <i>Note: Make sure to configure LDAP if you select this option.</i>
Enabled	Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box. <i>Note: You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.</i>

3. To save, click the **Update** button. A confirmation message displays.

TACACS+

Similar to RADIUS, the main function of TACACS+ is to perform authentication for remote access. The vSLM 2 software supports the TACACS+ protocol (not the older TACACS or XTACACS protocols).

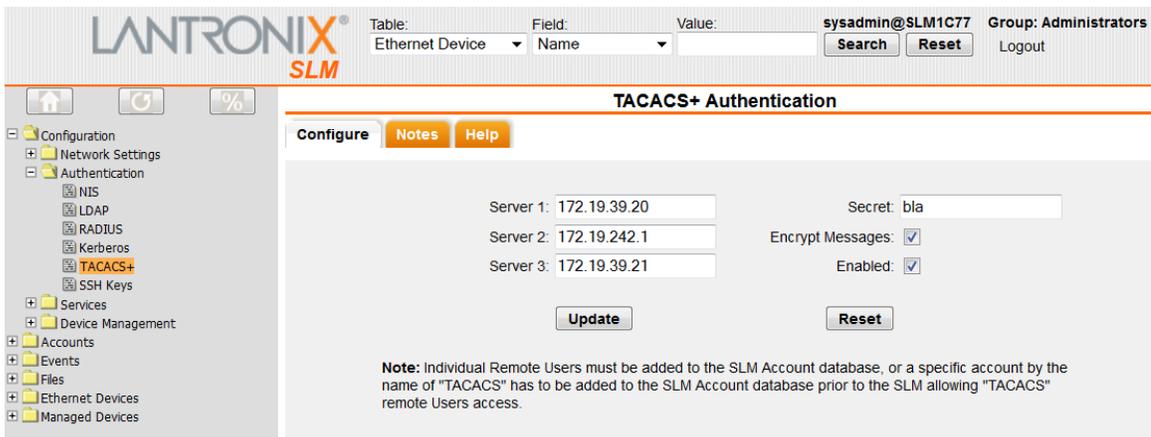
The administrator can configure the vSLM 2 secure management software to use TACACS+ to authenticate users attempting to log in to the vSLM 2 software through the web interface, SSH, Telnet, or the console port.

Note: For a user to log in remotely using TACACS+, the user's account must have remote access (Remote Only or Local & Remote), or there must be an account defined whose login name is TACACS.

To configure the vSLM 2 software to use TACACS+ to authenticate users:

1. On the menu, select **Configuration > Authentication > TACACS**. The following page opens.

Figure 8-11 TACACS+ Authentication Page - Configure Tab



The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with fields for Table (Ethernet Device), Field (Name), and Value, along with Search and Reset buttons. The user is logged in as sysadmin@SLM1C77 with the group Administrators. The main content area is titled "TACACS+ Authentication" and has tabs for Configure, Notes, and Help. The Configure tab is active, showing three server configuration rows:

Server	IP Address	Secret	Encrypt Messages	Enabled
Server 1	172.19.39.20	bla	<input type="checkbox"/>	<input type="checkbox"/>
Server 2	172.19.242.1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Server 3	172.19.39.21		<input type="checkbox"/>	<input checked="" type="checkbox"/>

At the bottom of the configuration area, there are Update and Reset buttons. A note at the bottom of the page reads: "Note: Individual Remote Users must be added to the SLM Account database, or a specific account by the name of 'TACACS' has to be added to the SLM Account database prior to the SLM allowing 'TACACS' remote Users access."

2. Enter the following:

Table 8-12 TACACS+ Authentication Settings

TACACS+ Authentication Setting	Description
Servers 1-3	IP address or host name of up to three TACACS+ servers.
Secret	Shared secret for message encryption between the vSLM 2 software and the TACACS+ server. Enter an alphanumeric secret of up to 127 characters.
Encrypt Messages	Select the check box to encrypt messages between the vSLM 2 software and the TACACS+ server. Selected by default.
Enabled	Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box. <i>Note:</i> You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.

3. To save, click the **Update** button. A confirmation message displays.

SSH Keys

The vSLM 2 secure management software 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.

For imported and exported SSH keys, the vSLM 2 software supports both RSA and DSA keys and can import and export keys in OpenSSH and SECSH formats. Both imported and exported keys must be associated with a local vSLM 2 software user.

Imported Keys

Imported SSH keys must be associated with an vSLM 2 software local user. The key can be generated on host "MyHost" for user "MyUser," and when the key is imported into the vSLM 2 software, it must be associated with either "MyUser" (if "MyUser" is an existing vSLM 2 software local user) or an alternate vSLM 2 software local user. The public key file can be imported through SCP or FTP; once the file is imported, you can view or delete the public key. Any SSH connection into the vSLM 2 secure management software from the designated host/user combination uses the SSH key for authentication.

Exported Keys

The vSLM 2 software can generate SSH keys for SSH connections out of the vSLM 2 software for any vSLM 2 software user. The vSLM 2 secure management software retains both the private and public key on the vSLM 2 software, and makes the public key available for export through SCP, FTP, or copy and paste. The name of the key is used to generate the name of the public key file that is exported (for example, <keyname>.pub), and the exported keys are organized by user and key name. Once a key is generated and exported, any SSH connection out of the vSLM 2 software for the designated host/user combination uses the SSH key for authentication.

To configure the vSLM 2 secure management software to use SSH keys to authenticate users:

1. On the menu, select **Configuration > Authentication > SSH Keys**. The following page opens.

Figure 8-13 Manage SSH Keys - SLM Keys Tab

2. To the right of the **Submit** button, click **Import** or **Export** to indicate the type of keys you are setting.
3. Enter the following:

Table 8-14 Host and Login SSH Key Settings

SSH Key Setting	Description
Host	IP address of the remote server from which to SCP or FTP the public key file.
Path	Optional pathname to the public key file.
Login	User ID to use to SCP or FTP the file.
Password/Retype	Password to use to SCP or FTP the file.

Imported Keys (SSH In)

These entries (the Host, User, Import via, and Filename fields are always required for importing keys) are required in the following cases:

- ◆ The imported key file does not contain the host from which the user will be making an SSH connection.
- ◆ The vSLM 2 software local user login for the connection is different from the user name from which the key was generated or is not included in the imported key file.

If either of these conditions is true, or the imported file is in SECSH format, you must specify the host and user. The following is an example of a public key file that includes the host and user:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAEEApUHCX9EWsHt+jmUGXa1YC3us
ABYxIXUhSU1N+NU9HNaUADUff8LYz8/gUnUSH4Ksm8GRT7/8/Sn9jCVfGPh
UQ== asallaway@winserver
```

Table 8-15 Imported Key Settings

Imported Key Setting	Description
Host	Host name or IP address from which the SSH connections to the vSLM 2 software will be made.
User	User ID of the person given secure access to the remote server.
Import via	Select SCP or FTP as the method for importing the SSH keys. The default is SCP .
Filename	Name of the public key file (for example, mykey.pub).

Exported Keys (SSH Out)

Table 8-16 Exported Keys Settings

Exported Key Setting	Description
User	User ID of the person given secure access to the remote server.
Key Type	Select either the RSA or the DSA encryption standard followed by the number of bits (512 or 1024) in the key. DSA 512 is the default. All export fields are disabled during import and vice versa.
Key Name	Name of the key. This will generate the public key filename (e.g., <keyname>.pub).
Passphrase/Retype	Optionally, enter a passphrase associated with the key. The passphrase may have up to 50 characters. The passphrase is an optional password that can be associated with an SSH key. It is unique to each user and to each key.
SECSH Format	Indicate whether the keys will be exported in SECSH format. The default is OpenSSH.
Export via	Select the method (SCP, FTP, or Cut and Paste) of exporting the key to the remote server. Cut and Paste, the default, requires no other parameters for export.

4. Click the **Submit** button. The keys display in the list below.
5. To view a user's key, select the user and click the **View** button.
6. To delete a user's key, select the user and click the **Delete** button.

To add or view export SLC keys:

You can enable the vSLM 2 secure management software to retrieve all the public keys (each with a specific user and host name) from a particular SLC console manager and store them in the vSLM 2 software database. Then you can push those public keys to other SLC devices, allowing those particular users to access the other SLC devices from those particular hosts.

Note: For information about importing and exporting keys, see [Using the Actions Tab on page 275](#).

1. On the menu, select **Configuration > Authentication > SSH Keys**, and click the **SLC/SLB Keys** tab. The following page opens:

Figure 8-17 Manage SSH Keys - SLC/SLB Keys Tab

2. Enter the following information:

Table 8-18 Manage SSH Keys - SLC Keys Tab

SLC Key Setting	Description
User	User login of the person given secure access to the SLC console manager.
Host	Host name or IP address from which the SSH connections to the SLC device will be made.
Type	Select either the RSA or the DSA encryption standard followed by the number of bits (512 , 1024 or 2048) in the key. DSA 512 is the default. All export fields are disabled during import and vice versa.
Key	Enter the SSH key content.

3. Click the **Add Key** button. The key information (except the key itself) displays in the table on the top of the page.
4. To view the key, select the check box for the user, and click the **View** button in the top right of the page. The SLC key displays.

Example of an SLC key:

SLC key for sysadmin@SLM_tpham17

```

RSA 1024:
AAAAB3NzaC1yc2EAAAABIwAAAQEAy7zXy+l1YDbaXalMYVRKGPBue+HdR+ihmdZZqGcN8xc
O2Lqdw61yJO4QN4PcQ6n88VwLM0/UEJgW1PF3vp/Z+kKw4v48NHJUOZSKRfTejMssgp1S6
Ttf+YWzHCr1mX/+yRUyA+I9VXb9cI2r9uqIlMk/GVTgpI/8YERnAsQ9Aerfy/20MXOSGg895
tdBW6piLKWoJ5P6NRcXsFJScmowGXNU4snUpk2cvVNyGiVMe9jb454fb080+/lphmMrJMUPY
X3uG22Qsm0KZGosnLFFktYzimDaOoRQ2QI9my19i/baFX9RiH2yda+vLmBsTchaEx30Dp7Pw
baHi7gf8Rb9Q==

```

5. To delete one or more keys:
 - a. Select the check box for each key to be deleted and click the **Delete** button.
 - b. In response to the request for confirmation, click **OK**.

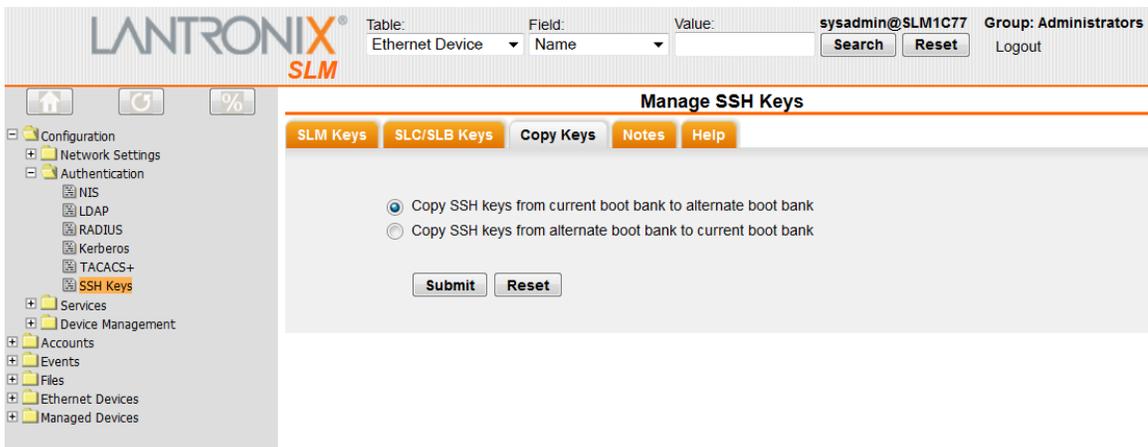
Copy Keys

If your vSLM 2 secure management software is set up with dual booting, you can move SSH keys from one boot partition to another.

To copy a key:

1. On the menu, select **Configuration > Authentication > SSH Keys**, and then click the **Copy Keys** tab.

Figure 8-19 Manage SSH Keys - Copy Keys Tab



2. Select one of the following:
 - ◆ Copy SSH keys from current boot bank to alternate boot bank.
 - ◆ Copy SSH keys from alternate boot bank to current boot bank.
3. Click the **Submit** button.
4. To return to the original settings, click the **Reset** button.

Authentication Commands

set auth

Syntax

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

Parameters

```
local <1-6>
nis <1-6>
ldap <1-6>
radius <1-6>
kerberos <1-6>
tacacs+ <1-6>
authusenextmethod <enable|disable>
limitsysadmin <enable|disable>
```

Description

Sets ordering of authentication methods and how authentication methods are used.

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

Any methods omitted from the `set auth` command will be disabled if at least one method is selected.

set kerberos**Syntax**

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

Parameters

```
state <enable|disable>
realm <Kerberos Realm>
kdc <Key Distribution Center>
ipaddr <Key Distribution Center IP Address>
port <Key Distribution Center TCP Port>
useldap <enable|disable>
```

Description

Configure the vSLM device to use Kerberos to authenticate users who login to the vSLM via SSH, Telnet, the Web or the Console Port.

set ldap**Syntax**

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

Parameters

```
state <enable|disable>
server <IP Address or Name>
port <TCP Port>
base <LDAP Base>
bindname <Bind Name>
bindpassword <Bind Password>
adsupport <enable|disable>
encrypt <starttls|ssl|disable>
filteruser <User Login Attribute|CLEAR>
filtergroup <Group Filter Objectclass|CLEAR>
grmemberattr <Group Member Attribute|CLEAR>
grmembervalue <dn|name>
```

Description

Configures the vSLM 2 software to use LDAP to authenticate users who log in to the vSLM 2 software via SSH, Telnet, the web, or the console port.

set nis

Syntax

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

Parameters

```
state <enable|disable>  
domain <NIS Domain Name>  
broadcast <enable|disable>  
master <IP Address or Name>  
slave1 <IP Address or Name>  
slave2 <IP Address or Name>  
slave3 <IP Address or Name>  
slave4 <IP Address or Name>  
slave5 <IP Address or Name>
```

Description

Configures the vSLM 2 software to use NIS to authenticate users who log in to the vSLM 2 secure management software via SSH, Telnet, the web, or the console port.

set radius

Syntax

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

Parameters

```
state <enable|disable>  
timeout <1-30 seconds>  
server1 <IP Address or Name>  
port1 <TCP Port>  
secret1 <Secret>  
server2 <IP Address or Name>  
port2 <TCP Port>  
secret2 <Secret>
```

Description

Configures the vSLM 2 software to use RADIUS to authenticate users who login to the vSLM 2 software via SSH, Telnet, the web, or the console port.

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>
```

```
secret <TACACS+ Secret>  
encrypt <enable|disable>
```

Description

Configure the SLM to use TACACS+ to authenticate users who login to the SLM via SSH, Telnet, the Web or the Console Port.

set sshkey import

Syntax

```
set sshkey import <copypaste>
```

Note: RSA keys must be 1024 bits.

Description

Imports an SSH key.

set sshkey copybank dest

Syntax

```
set sshkey copybank dest <alt|cur>
```

Description

Copy ssh keys between boot banks.

set sshkey delete keyuser

Syntax

```
set sshkey delete keyuser <SSH Key User> keyhost <SSH Key Host>
```

Description

Delete imported SSH key.

show auth

Syntax

```
show auth
```

Description

Displays all authentication methods. Set ordering of authentication methods and how authentication methods are used. Authentication can occur using all methods, in the order of their precedence, until a successful authentication is obtained, or using only the first authentication method that responds (in the event that a server is down). Any methods omitted from 'set auth' command will be disabled if at least one method is selected.

Parameters

```
local <1-6>
```

```
nis <1-6>
ldap <1-6>
radius <1-6>
kerberos <1-6>
tacacs+ <1-6>
authusenextmethod <enable|disable>
limitsysadmin <enable|disable>
```

show kerberos

Syntax

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

Parameters

```
state <enable|disable>
realm <Kerberos Realm>
kdc <Key Distribution Center>
ipaddr <Key Distribution Center IP Address>
port <Key Distribution Center TCP Port>
uselldap <enable|disable>
```

Description

Configure the SLM to use Kerberos to authenticate users who login to the SLM via SSH, Telnet, the Web or the Console Port.

show ldap

Syntax

```
show ldap
```

Description

Displays all LDAP information. Configure the SLM to use LDAP to authenticate users who login to the SLM via SSH, Telnet, the Web or the Console Port.

Parameters

```
state <enable|disable>
server <IP Address or Name>
port <TCP Port>
base <LDAP Base>
bindname <Bind Name>
bindpassword <Bind Password>
adssupport <enable|disable>
encrypt <starttls|ssl|disable>
filteruser <User Login Attribute|CLEAR>
filtergroup <Group Filter Objectclass|CLEAR>
grmemberattr <Group Member Attribute|CLEAR>
grmembervalue <dn|name>
```

show nis**Syntax**

```
show nis
```

Description

Displays all NIS information. Configure the SLM to NIS to authenticate users who login to the SLM via SSH, Telnet, the Web or the Console Port.

Parameters

```
state <enable|disable>
domain <NIS Domain Name>
broadcast <enable|disable>
master <IP Address or Name>
slave1 <IP Address or Name>
slave2 <IP Address or Name>
slave3 <IP Address or Name>
slave4 <IP Address or Name>
slave5 <IP Address or Name>
```

show radius**Syntax**

```
show radius
```

Description

Displays all RADIUS information. Configure the SLM to NIS to authenticate users who login to the SLM via SSH, Telnet, the Web or the Console Port.

Parameters

```
state <enable|disable>
domain <NIS Domain Name>
broadcast <enable|disable>
master <IP Address or Name>
slave1 <IP Address or Name>
slave2 <IP Address or Name>
slave3 <IP Address or Name>
slave4 <IP Address or Name>
slave5 <IP Address or Name>
```

show tacacs+**Syntax**

```
show tacacs+ <one or more parameters>
```

Parameters

```
state <enable|disable>
server1 <IP Address or Name>
```

```
server2 <IP Address or Name>  
server3 <IP Address or Name>  
secret <TACACS+ Secret>  
encrypt <enable|disable>
```

Description

Configure the SLM to use TACACS+ to authenticate users who login to the SLM via SSH, Telnet, the Web or the Console Port.

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 imported SSH keys.

Account Groups

The administrator organizes accounts into account groups to simplify the task of assigning permissions. Accounts inherit device rights from the account group to which they belong. To assign unique permissions to an individual account, it must be the only member of an account group. The sysadmin account always has all permissions enabled.

Note: Only functions and devices for which the user has rights display in that user's menu on the web interface or on the CLI.

Account Group Types

There are four types of account groups: Administrators, Ethernet Device, Managed Device, and Menu Only.

Administrators Account Group: Has rights and permissions to configure the vSLM 2 secure management software and to add, edit, and delete account groups within the Ethernet Device, Managed Device, and Menu Only categories. Administrators cannot delete or rename the Administrators Group, although they can add additional accounts to it. Administrators have access to configuration, events, logs, and files, can create groups of managed devices, and interact with Ethernet and managed devices. Administrators can log into both the web interface and the CLI.

Ethernet Device Account Groups: Can interact with SLC, SLK, RPM/SLP, and other vSLM 2 software, other Lantronix devices, some non-Lantronix device, the ports of the devices, and the managed devices created from these ports to which the group has rights. Ethernet Device Account groups can log into both the web interface and the CLI. Ethernet Device Account groups may also create, update, and delete Managed Device Groups and assign managed devices to which they have rights (by having rights to their parent Ethernet device) to those groups.

Managed Device Account Groups: Have access to the managed devices (e.g., servers and switches) connected to Ethernet device ports to which the group has rights. Managed Device Account Groups can log into both the web interface and the CLI.

Device Permissions Account Groups: These groups are similar in function to the Ethernet Device groups, but have an additional set of permissions for SLC and SLB devices. These groups can be pulled from SLC and SLB devices (creating or overwriting Device Permission groups on the SLM software) or pushed to SLC and SLB devices (creating or overwriting groups on the SLC and SLB).

Menu Only Account Groups: These groups can log into the CLI but not the web interface. They can interact with managed devices only. The administrator assigns a restricted menu of numbered options that these users can select.

Viewing Account Groups

Administrators can view account groups.

To view account groups:

1. On the menu, click **Accounts**.

The following page opens:

Figure 8-20 Account Groups Page - Accounts Tab

Name	Email Address	Config Network	Config Authentication	Config Services	Device Management	Config Accounts	Config Events	Config Log Files	Authentication	Password Change	Password Expire	Next Login	Synchronize	Last Access
buguser	buguser@test.com	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Local Only	Yes	Yes	No	No	2014-12-01 00:40:35
christi		No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-02 10:23:09
eth1_1	eth1_1@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:14
eth1_2	eth1_2@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:19
eth1_3	eth1_3@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:24
eth1_4	eth1_4@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:29

2. Click the **Members** tab. A list of existing account member names displays.

Figure 8-21 Account Groups Page - Members Tab

Name	Account Group Type	Listen Ports	Data Ports	Clear Ports	Outlets	Escape Sequence	Break Sequence	Custom Menu	Auto Menu	Enable Dialback	Dialback Number	Permissions	Assigned Menu
Administrators	Administrator								Yes	No			
Ethgrp1	Ethernet Device								Yes	No			
Ethgrp2	Ethernet Device								Yes	No			
Ethgrp3	Ethernet Device								Yes	No			
Mgdgrp1	Managed Device								Yes	No			
Mgdgrp2	Managed Device								Yes	No			
Mgdgrp3	Managed Device								Yes	No			
testmenu	Menu Only								Yes	No			glenn8
Mnugrp1	Menu Only								Yes	No			glenn1
Mnugrp2	Menu Only								Yes	No			glenn2
Mnugrp3	Menu Only								Yes	No			glenn3
ITM-Finance	Device Permissions	1-3.5	1-3.5	1-3.5	1-3.5	\x1bA	\x1bB		Yes	No		nt.do.dp.po.wb	
ITM-Engineering	Device Permissions	1-3.5	1-3.5	1-3.5	1-3.5	\x1bA	\x1bB		Yes	No		nt.do.dp.po.wb	
Long Group Name Number 6300	Device Permissions	1-3.5	1-3.5	1-3.5	1-3.5	\x1bA	\x1bB		Yes	No		nt.do.dp.po.wb	

Adding an Account Group

1. On the Account Groups page, click the **Group** tab. The following page opens:

Figure 8-22 Account Group Page - Group Tab

2. Enter the following:

Table 8-23 Account Group - Group Tab

Account Group Setting	Description
Account Group Name	The name of the new account group.
Account Group Type	From the drop-down list, select the type of account group. The default setting is Ethernet Device .

3. To save, click the **Add** button. A confirmation message displays and the new group displays in the **Accounts** menu tree.
4. To display the list of account groups, click **Accounts** on the menu. The new group displays.

Updating or Deleting an Account Group

The administrator can update or delete any group except for sysadmin.

To update or delete an account group:

1. On the **Members** tab, click the **Edit**  icon to the left of the group you want to update or delete. The **Group** tab displays.

Figure 8-24 Account Groups - Group Tab



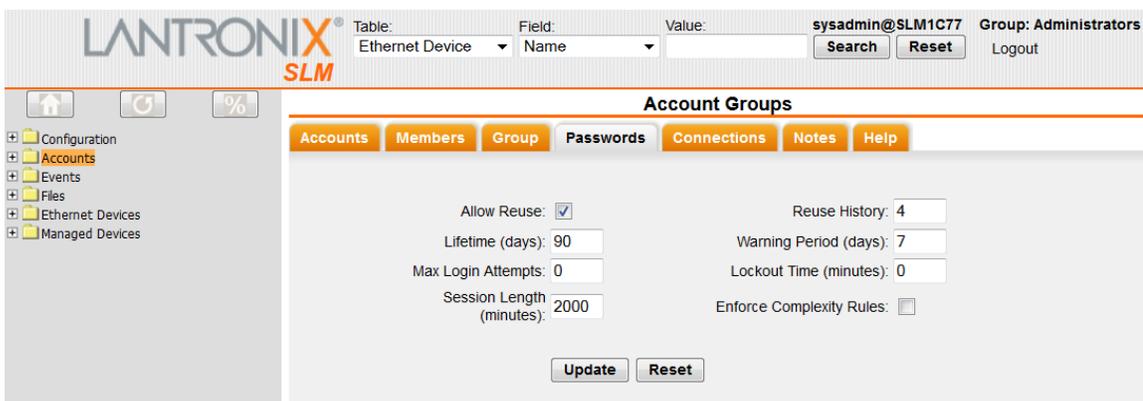
2. To delete an account group:
 - Note:** You can rename an account group but not change its type. You cannot delete an account group if it contains any accounts; delete the accounts first.
 - a. Click the **Delete** button.
 - b. In response to the request for confirmation, click **OK**. A blank **Group** tab opens.
 - c. Click **Accounts** on the menu tree. The deleted group is no longer on the menu tree or listed on the **Members** tab.
3. To update the name of an account group:
 - a. Edit the name as desired.
 - b. Click the **Update** icon. A confirmation message displays.
 - c. Click **Accounts** on the menu tree. The updated group is on the menu tree and listed on the **Members** tab.

Setting Password Requirements for User Accounts

The administrator sets parameters for passwords that apply to all accounts.

1. On the Account Groups page, click the **Passwords** tab.

Figure 8-25 Account Groups Page - Passwords Tab



2. Enter the following information:

Table 8-26 Password Requirement Settings

Password Requirement Setting	Description
Allow Reuse	Select to enable users to continue to reuse old passwords. If you disable the check box, the user 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.
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 the user can attempt to log in unsuccessfully before the system locks the user out. The default setting is 0 (disabled).
Lockout Time (minutes)	The number of minutes the locked-out user must wait before trying to log in to the web interface again. The default setting is 0 (disabled).
Session Length (minutes)	The number of minutes a session can be idle before it times out. The minimum is five minutes. The default setting is 20. This applies to both web and CLI sessions. <i>Note: The vSLM 2 secure management software ships with a default maximum of 25 concurrent user sessions (or "seats"). If you require more than 25 concurrent user sessions, please contact your sales associate to order them. When all seats are in use, the sysadmin can still log in one more time, from the CLI interface only, and terminate other connections.</i>
Enforce Complexity Rules	Select to enable the vSLM 2 secure management software to enforce rules concerning the password structure (e.g., alphanumeric requirements, number of characters, punctuation marks). Disabled by default. Complexity rules: <ul style="list-style-type: none"> ◆ Passwords must be at least eight characters long. ◆ Passwords must contain one upper case letter (A-Z), one lower case letter (a-z), one digit (0-9), and one punctuation character ({}~!@#%&*-+=\ {}[]:;'"<>.,?/_).

- To save, click the **Update** button. When the update is complete, a confirmation message displays.

Assigning Account Group Device Rights

Accounts inherit the device rights of the account group to which they belong. Administrators can add or remove permission to an account group to view, configure, or interact with specific Ethernet devices or specific ports and the managed devices connected to them.

- ◆ **Administrators Account Group:** Can view, configure, and interact with all Ethernet devices and with the managed devices connected to the Ethernet device's ports.
- ◆ **Ethernet Device Account Groups and Device Permissions Account Groups:** Can view, configure, and interact with specific Ethernet devices, their ports, and the managed devices connected to the ports.
- ◆ **Managed Device Account Groups:** Can view, configure, and interact with specific managed devices.
- ◆ **Menu Only Account Groups:** Can view and interact with specific managed devices, according to the menu they have permission to use.

To assign permissions to an Ethernet Device Account Group:

The administrator assigns permissions to an Ethernet Device Account Group to access specific Ethernet devices. All members of the group inherit these permissions.

1. Select the account group from the menu. The following page opens.

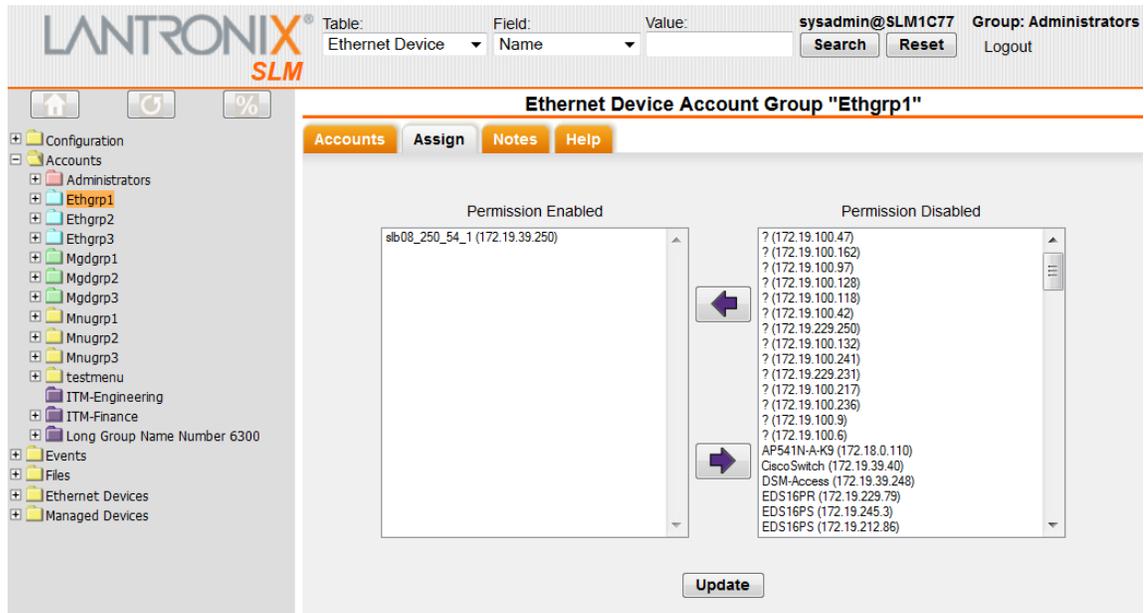
Figure 8-27 Ethernet Device Account Group - Accounts Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value: sysadmin@SLM1077'. Below this, the page title is 'Ethernet Device Account Group "Ethgrp1"'. The main content area is titled 'Accounts' and contains a table with the following columns: Name, Email Address, Config Network, Config Authentication, Config Services, Device Management, Config Accounts, Config Events, Config Log Files, Authentication, Password Change, Password Expire, Next Login, Synchronize, and Last Access. The table lists five accounts: eth1_1, eth1_2, eth1_3, eth1_4, and glenn_ad. Below the table is an 'Add Account' button. On the left side, there is a navigation menu with various categories like Configuration, Accounts, Administrators, and Ethernet Devices.

Name	Email Address	Config Network	Config Authentication	Config Services	Device Management	Config Accounts	Config Events	Config Log Files	Authentication	Password Change	Password Expire	Next Login	Synchronize	Last Access
eth1_1	eth1_1@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:14
eth1_2	eth1_2@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:19
eth1_3	eth1_3@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:24
eth1_4	eth1_4@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:29
glenn_ad	glenn_ad@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:44

2. Click the **Assign** tab. The following page opens:

Figure 8-28 Ethernet Device Account Group - Assign Tab



This tab displays two lists: **Permission Enabled** and **Permission Disabled**.

Note: You can use **Ctrl+click** to select multiple devices from these lists.

3. To enable access to a device listed in Permission Denied, select the device and click the left arrow. The device is now in the Permission Enabled list.
4. To remove access to a device, select the device in the Permission Enabled list and click the right arrow. The device is now in the Permission Disabled list.
5. Click the **Update** button. When the update is complete, a confirmation message displays. When the user logs in, only Ethernet and managed devices for which the user has permission display in the menu tree.

To assign permissions to a Managed Device Account Group:

The administrator assigns permissions that allow a Managed Device Account Group to access specific managed devices. All members of the group inherit these permissions.

1. Select the account group from the menu. The following page opens:

Figure 8-29 Managed Device Account Group - Accounts Tab



2. Click the **Assign** tab.

Figure 8-30 Managed Device Account Group - Assign Tab



3. To enable permission to read from and write to a managed device connected to an Ethernet device port, select it from the **Permission Disabled** list and click the top **left arrow**. The device displays in the **Connect Direct Devices** list.

Note: You can use **Ctrl+Right click** to select multiple devices.

4. To enable permission to listen only to a managed device, select it from the **Permission Disabled** list and click the bottom **left arrow**. The device displays in the **Listen-only Devices** list.
5. To disable permission for a managed device, select it from the **Connect Direct Devices** or **Listen-only Devices** list, and click the corresponding **right arrow**. The device displays in the **Permission Disabled** list.
6. Click the **Update** button. When the update is complete, a confirmation message displays. When the user logs in, only managed devices for which the user has permission display on the menu tree.

Viewing Currently Logged-In Accounts

Administrators can see which users are currently logged into the vSLM 2 secure management software and whether they are connected to any managed devices. The page also displays the maximum number of concurrent users for which this vSLM 2 software is licensed.

To view logged-in accounts:

1. On the menu, click **Accounts**, and then click the **Connections** tab. The following page opens:

Figure 8-31 Account Groups - Connections Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with the text 'sysadmin@SLM1C77' and 'Group: Administrators'. Below the search bar is a navigation menu with tabs for 'Accounts', 'Members', 'Group', 'Passwords', 'Connections', 'Notes', and 'Help'. The 'Connections' tab is selected. The main content area displays two tables: 'Inbound Connections' and 'Outbound Connections'. The 'Inbound Connections' table has columns for 'User Account', 'U.I.', 'Location', 'Last Access', and 'Minutes Idle'. The 'Outbound Connections' table has columns for 'App', 'Destination', 'Managed Device', and 'Start Time'. At the bottom, it shows 'Licensed for 25 concurrent users' and a 'Terminate' button.

2. View the following information:

Table 8-32 Inbound Connections

Inbound Connection Setting	Description
User Account	User name for logging in to the vSLM 2 software.
U.I.	Type of interface (web or command line) the user is logged in to.
Location	IP address of the client.
Last Access	Date and time the user last accessed the vSLM 2 software.
Minutes Idle	Number of minutes since the user last took an action in the session.

Table 8-33 Outbound Connections

Inbound Connection Setting	Description
App	Application used to manage the device.
Destination	IP address of the managed device.
Managed Device	Name of the managed device.
Start Time	Time the vSLM 2 secure management software made the connection.

- To terminate a session, select the check box for the inbound or outbound session(s) and click the **Terminate** button.

Note: *All outbound connections associated with a closed inbound session will also close.*

- To refresh the page only, click the **Terminate** button with no sessions selected.

Account Group Commands

set accountgroup add

Syntax

```
set accountgroup add <Group Name> type <ethernet|managed|menu|device>
<parameters>
```

Parameters

```
[menu <Menu Name>]
[dataports <Port List>]
[listenports <Port List>]
[clearports <Port List>]
[accessoutlets <Outlet List>]
[escapeseq <1-10 Chars>]
[breakseq <1-10 Chars>]
[custommenu <Menu Name>]
[displaymenu <enable|disable>]
[allowdialback <enable|disable>]
[dialbacknumber <Phone Number>]
[permissions <Permission List>]
```

Description

Creates and configures a local account group. Group type includes Ethernet user, managed user, menu user, or device permissions.

set accountgroup edit

Syntax

```
set accountgroup edit <Group Name> <one or more parameters>
```

Parameters

```
[name <new name>]
[menu <Menu Name|CLEAR>]
[dataports <Port List|CLEAR>]
[listenports <Port List|CLEAR>]
[clearports <Port List|CLEAR>]
[accessoutlets <Outlet List|CLEAR>]
[escapeseq <1-10 Chars>]
[breakseq <1-10 Chars>]
[custommenu <Menu Name|CLEAR>]
[displaymenu <enable|disable>]
[allowdialback <enable|disable>]
```

```
[dialbacknumber <Phone Number|CLEAR>]  
[permissions <Permission List|CLEAR>]
```

Description

Configures a local account group. Group type is Ethernet user, managed user, or menu user or device permission.

show accountgroup

Syntax

```
show accountgroup <Group Name>  
show accountgroup name <Group Name>
```

Description

Displays account group information.

show accountgroup all

Syntax

```
show accountgroup all  
show accountgroup
```

Description

Displays information about all account groups.

show accountgroup index

Note: Type `show accountgroup all` to display the index.

Syntax

```
show accountgroup index <number>
```

Description

Displays account groups by index number.

Accounts

The Accounts page is for administrators who add, update, and delete accounts. Accounts inherit device rights from the account group to which they belong. To assign unique permissions to an individual account, create the account as the sole member of an account group. The sysadmin account always has all permissions enabled.

Note: Only functions and devices for which the user has rights display in that user's menu on the web interface or on the CLI.

Viewing Accounts

1. On the menu, click **Accounts**. The Accounts tab on the Account Groups page displays a list of authenticated users with the functions each user has permission to perform.

Figure 8-34 Account Groups - Accounts Tab

Name	Email Address	Config Network	Config Authentication	Config Services	Device Management	Config Accounts	Config Events	Config Log Files	Authentication	Password Change	Password Expire	Next Login	Synchronize	Last Access
buguser	buguser@test.com	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Local Only	Yes	Yes	No	No	2014-12-01 00:40:35
christi		No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-02 10:23:09
eth1_1	eth1_1@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:14
eth1_2	eth1_2@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:19
eth1_3	eth1_3@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:24
eth1_4	eth1_4@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:43:29

- View the following information about each user:

Note: Modification of user access rights can only be performed through Administrator accounts. See [Figure 8-36](#).

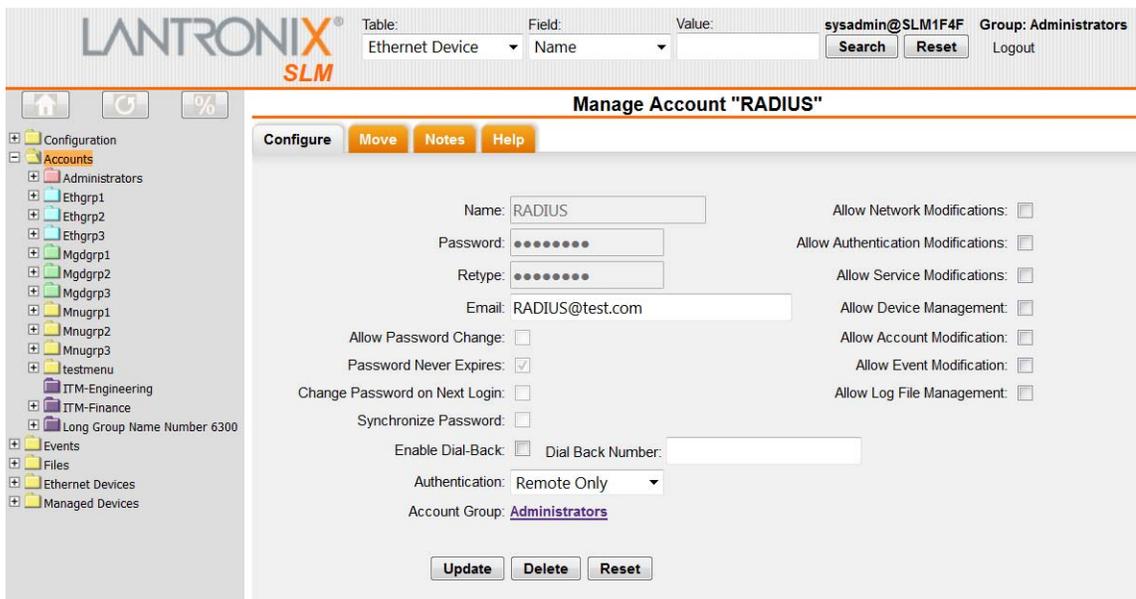
Table 8-35 Account Groups - Accounts Tab

Account Groups Setting	Description
Name	The user name for logging in to the vSLM 2 software.
Email Address	User's email address; may be used for event notification.
Config Network	Indicates whether the user has permission to open the Network Settings page and configure network settings.
Config Authentication	Indicates whether the user has permission to select and prioritize authentication methods and to configure related settings.
Config Services	Indicates whether the user has permission to configure services such as date and time and SNMP Agent & syslog and to update SLC console managers to which the user has access.
Device Management	Indicates whether the user has permission to configure settings for auto-detecting devices and ports and for managing alternate vSLM 2 software.
Config Accounts	Indicates whether the user has permission to add, update, and delete all accounts and to grant account permissions.
Config Events	Indicates whether the user has permission to set alarms and triggers.
Config Log Files	Indicates whether the user has permission to view, copy, and delete various log files.
Authentication	Indicates whether authentication for this user is Local Only , Remote Only , Local & Remote , or Disabled .
Password Change	Indicates whether the user has permission to use the current password indefinitely.
Password Expire	No allows the user to keep a password indefinitely.
Change Password Next Login	Indicates whether the user has permission to change the password the next login.

Account Groups Setting	Description
Synchronize	<p>When the Push Passwords check box on the Maintenance page is selected, the vSLM 2 secure management software uses the password on all accounts with Synchronize Password enabled to update accounts on remote SLM, SLC, SCSxx05/20, and RPM/SLP devices. The accounts must have access rights to and local user accounts on the devices.</p> <p>Note: RPM/SLP password synchronization uses SSH and CLI commands not an SNMP command, so you must provide the sysadmin login and password in the RPM/SLP device page for RPM/SLP password synchronization to work. Rebooting the vSLM 2 software for any reason causes it to ignore user account password changes made but not yet pushed before the reboot.</p>
Last Access	Date and time the account group was last updated.

3. click the **Edit**  icon to the left of a user. The following page opens:

Figure 8-36 Account Page - Configure Tab



The screenshot displays the LANTRONIX SLM web interface. At the top, there is a search bar with the following details: Table: Ethernet Device, Field: Name, Value: (empty), and a user profile for sysadmin@SLM1F4F (Group: Administrators). The main heading is "Manage Account 'RADIUS'". Below this, there are tabs for "Configure", "Move", "Notes", and "Help". The "Configure" tab is active, showing a form for the "RADIUS" account. The form includes the following fields and options:

- Name: RADIUS
- Password: (masked with dots)
- Retype: (masked with dots)
- Email: RADIUS@test.com
- Account Group: Administrators
- Authentication: Remote Only (dropdown menu)
- Update, Delete, and Reset buttons at the bottom.
- Permissions checkboxes on the right:
 - Allow Network Modifications:
 - Allow Authentication Modifications:
 - Allow Service Modifications:
 - Allow Device Management:
 - Allow Account Modification:
 - Allow Event Modification:
 - Allow Log File Management:
- Other checkboxes on the left:
 - Allow Password Change:
 - Password Never Expires:
 - Change Password on Next Login:
 - Synchronize Password:
 - Enable Dial-Back: Dial Back Number: (empty field)

Adding an Account to the Administrators Account Group

The sysadmin account can add other administrators to the Administrators Group, assigning a user name and email address for each user. The name is for logging in over the web interface or the command line interface. The vSLM 2 secure management software uses the email address to send emails to users based on configured alarm settings.

To add a user to the Administrators Group:

1. On the menu, click **Accounts > Administrators**. The following page opens.

Figure 8-37 Administrator Account Group - Accounts Tab

Name	Email Address	Config Network	Config Authentication	Config Services	Device Management	Config Accounts	Config Events	Config Log Files	Authentication	Password Change	Password Expire	Next Login	Synchronize	Last Access
buguser	buguser@test.com	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Local Only	Yes	Yes	No	No	2014-12-01 00:40:35
gienn	gienn@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:40:40
Kerberos	Kerberos@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-02 09:42:17
LDAP	LDAP@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:20
NIS	NIS@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:23
RADIUS	RADIUS@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:14
SecurID	SecurID@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:26
sysadmin		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Local Only	Yes	No	No	No	2014-12-10 22:35:46
TACACS	TACACS@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:29

2. Click the **Add Account** button at the bottom of the table. The following page opens:

Figure 8-38 Add New Account to Group "Administrators"- Configure Tab

Name: sysadmin

Password: ●●●●

Retype:

Email:

Allow Password Change:

Password Never Expires:

Change Password on Next Login:

Synchronize Password:

Enable Dial-Back: Dial Back Number:

Authentication: Local Only

Account Group: Administrators

Allow Network Modifications:

Allow Authentication Modifications:

Allow Service Modifications:

Allow Device Management:

Allow Account Modification:

Allow Event Modification:

Allow Log File Management:

3. Enter the following information:

Table 8-39 Add New Account to an Administrator Group - Configure Tab

Setting	Description
Name	User ID for logging into the vSLM 2 software. Must be alphanumeric, start with an alpha character, and may include an underscore (_).
Password and Retype	User's password for logging in to the vSLM 2 software.
Email	User's email address.
Allow Password Change	Select to allow user to change passwords. Enabled by default.
Password Never Expires	Selected by default. Select to allow the user to use current password indefinitely. Selected by default.
Change Password on Next Login	Select to require the user to change the password the next time the user logs in. (You may change this setting at any time.)
Synchronize Password	When the Push Passwords check box on the Maintenance page is selected, the vSLM 2 secure management software uses the password on all accounts with Synchronize Password enabled to update accounts on remote SLM, SLC, SCSxx05/20, and RPM/SLP devices. The accounts must have access rights to and local user accounts on the devices. <i>Note: RPM/SLP password synchronization uses SSH and CLI commands not an SNMP command, so you must provide the sysadmin login and password on the RPM/SLP device page for RPM/SLP password synchronization to work. Rebooting the vSLM 2 software for any reason causes it to ignore user account password changes made but not yet pushed.</i>
Enable Dial-Back	Users with dial-back access can dial into the vSLM 2 secure management software and enter their login and password. Once the SLC console manager authenticates them, the modem hangs up and dials them back.
Dial Back Number	Select the phone number the modem dials back on. It can be a fixed number or a number associated with their login. If you select Fixed Number , enter the number (in the format 2123456789).
Authentication	From the drop-down list, select how the user will be authenticated (Local Only , Remote Only , or Local & Remote). The default setting is Local Only .
Account Group (link)	Click the link to view the Administrator Account group.

Table 8-40 Add New Account to Group (Administrator) - Configure Tab - Permissions

Permission Setting	Description
Allow Network Modifications	Select to allow the user to configure network settings.
Allow Authentication Modifications	Select to allow the user to configure authentication settings.
Allow Service Modifications	Select to allow the user to configure settings for services.

Permission Setting	Description
Allow Device Management	Select to allow the user to auto-detect and to auto-save a configuration to another vSLM 2 software.
Allow Account Modification	Select to allow the user to set up accounts and account groups.
Allow Event Modification	Select to allow the user to modify event settings.
Allow Log File Management	Select to allow the user to manage log files.

- To save, click the **Add** button. A confirmation message displays, and the account displays in the Administrators Group on the menu tree.
- Click **Administrators** on the menu tree. The Account Group Accounts tab opens. The added user displays in the list.

Adding an Account to an Ethernet or Managed Device Account Group

Administrators assign a user name and email address for each user. The name is for logging in over the web interface or the command line interface. The vSLM 2 software uses the email address to send emails to users based on configured alarm settings.

To add an account to an Ethernet Device, Managed Device, or Menu Only Account Group:

Note: In this section, we use the example of an Ethernet account.

- On the menu, select the account group.
- Click the **Add Account** button at the bottom of the table. The following page opens:

Figure 8-41 Add New Accounts to Group (Nonadministrative) - Configure Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value: sysadmin@SLM1C77'. Below the search bar, there are buttons for 'Search', 'Reset', and 'Logout'. The main content area is titled 'Add New Account to Group "Mgdgrp1"'. On the left, there is a navigation menu with 'Configuration' expanded to show 'Accounts' and 'Administrators'. The 'Mgdgrp1' group is selected. The configuration form on the right has the following fields and options:

- Name: sysadmin
- Password: [masked]
- Retype: [input field]
- Email: [input field]
- Allow Password Change:
- Password Never Expires:
- Change Password on Next Login:
- Synchronize Password:
- Enable Dial-Back: Dial Back Number: [input field]
- Authentication: Local Only
- Account Group: Mgdgrp1

At the bottom of the form, there are 'Add' and 'Reset' buttons.

- Enter the following:

Table 8-42 Add New Account to Group - Configure Tab

Account Setting	Description
Name	User ID for logging into the vSLM 2 secure management software. Must be alphanumeric, start with an alpha, and may include an underscore (_).
Password and Retype	User's password for logging in to the vSLM 2 software.
Email	User's email address.
Allow Password Change	Select to allow the user to change passwords. Selected by default.
Password Never Expires	Select to allow the user to use the current password indefinitely. Disabled by default.
Change Password on Next Login	Select to require the user to change the password the next time the user logs in. (You may change this setting at any time.)
Synchronize Password	<p>When the Push Passwords check box on the Maintenance page is selected, the vSLM 2 software uses the password on all accounts with Synchronize Password enabled to update accounts on remote SLM, SLC, SCSxx05/20, and RPM/SLP devices. The accounts must have access rights to and local user accounts on the devices.</p> <p>Note: RPM/SLP password synchronization uses SSH and CLI commands not an SNMP command, so you must provide the sysadmin login and password in the RPM/SLP device page for RPM/SLP password synchronization to work. Rebooting the vSLM 2 secure management software for any reason causes it to ignore user account password changes made but not yet pushed.</p>
Enable Dial-Back	Once the vSLM 2 software authenticates them, users with dial-back access can dial into the vSLM 2 software and enter their login and password. Once the SLC console manager authenticates them, the modem hangs up and dials them back.
Dial Back Number	Select the phone number the modem dials back on. It can be a fixed number or a number associated with their login. If you select Fixed Number , enter the number (in the format 2123456789).
Authentication	From the drop-down list, select how the user will be authenticated (Local Only , Remote Only , or Local & Remote). The default setting is Local Only .
Account Group (link)	Click the link to view the parent Account Group page.

- To save, click the **Add** button. A confirmation message displays.
- Click the account group name on the menu tree. The account displays in the list of accounts and in the list on the **Accounts** tab.

Updating or Deleting an Account

Administrators can edit the password, email information, and configuration permissions for an account and remove accounts from an account group (except for the sysadmin account from the Administrators Group).

Note: In this section, we use the example of an Ethernet account.

To update an account or remove it from an account group:

1. In the menu tree, click a specific account. The following page opens:

Figure 8-43 Manage Account - Configure Tab

The screenshot displays the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1C77' with the role of 'Group: Administrators'. The main heading is 'Manage Account "buguser"'. Below this, there are tabs for 'Configure', 'Move', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following fields and options:

- Name: buguser
- Password: [masked]
- Retype: [masked]
- Email: buguser@test.com
- Allow Password Change:
- Password Never Expires:
- Change Password on Next Login:
- Synchronize Password:
- Enable Dial-Back: Dial Back Number: [empty field]
- Authentication: Local Only (dropdown)
- Account Group: Administrators
- Allow Network Modifications:
- Allow Authentication Modifications:
- Allow Service Modifications:
- Allow Device Management:
- Allow Account Modification:
- Allow Event Modification:
- Allow Log File Management:

At the bottom of the configuration area, there are three buttons: 'Update', 'Delete', and 'Reset'. The left-hand menu tree includes 'Configuration', 'Accounts', 'Administrators' (with 'buguser' selected), 'Ethgrp1-3', 'Mgdgrp1-3', 'Mnugrp1-3', 'testmenu', 'ITM-Engineering', 'ITM-Finance', 'Long Group Name Number 6300', 'Events', 'Files', 'Ethernet Devices', and 'Managed Devices'.

2. To update the account:
 - a. Make changes as desired.
 - b. Click the **Update** button.
3. To remove the account from the account group:
 - a. Click the **Delete** button.
 - b. In response to the confirmation request, click **OK**. A message confirming the deletion displays.
 - c. To verify the deletion, click the account group in the menu. The user is no longer listed.

Account Commands

Use the following commands to configure local accounts (including sysadmin) to authenticate users who login to the vSLM 2 software by means of SSH, Telnet, the web, or the console port.

set account add

Syntax

```
set account add <User Name> group <Group Name|admin> <parameters>
```

Parameters

```
[email <Email Address>]
[auth <local|remote|localremote|disable>]
[allowdialback <enable|disable>]
[dialbacknumber <dial-back number>]
[allowpwchange <enable|disable>]
[pwneverexpires <enable|disable>]
[changepwnextlogin <enable|disable>]
```

Description

Creates a new user account.

set account delete

Syntax

```
set account delete <User Name>
```

Description

Deletes a user account.

set account edit

Syntax

```
set account edit <User Name> group <Group Name|admin> <parameters>
```

Parameters

```
[email <Email Address|CLEAR>]
[auth <local|remote|localremote|disable>]
[allowdialback <enable|disable>]
[dialbacknumber <dial-back number|CLEAR>]
[allowpwchange <enable|disable>]
[pwneverexpires <enable|disable>]
[changepwnextlogin <enable|disable>]
```

Note: The parameter "email CLEAR" removes the current email.

Description

Modifies a user account.

set account password**Syntax**

```
set account password <User Name>
```

Note: Administrators with permission to change passwords must enter the username. Other users may not enter a username (they are changing their own password).

Description

Configures a user account's password for the vSLM 2 secure management software.

show account**Syntax**

```
show account <User Name>  
show account user <User Name>
```

Description

Displays account information by user name.

show account all**Syntax**

```
show account all  
show account
```

Description

Displays all account names and information.

show account index

Note: Type `show account all` to display the index.

Syntax

```
show account index <number>
```

Description

Displays accounts by index number.

show account search**Syntax**

Note: All searches are case insensitive.

```
show account search name <name>  
show account search email <email address>
```

Examples

```
show account search name sys
```

Description

Searches for accounts by name or email address and displays account information.

9: Ethernet Device Management

The vSLM 2 database contains information about SLC console managers and other secure IT management devices (SLK, RPM/SLP, and other SLM units) connected on the network. It may also contain information about other Lantronix and even non-Lantronix devices on the network, but you may have limited ability to manage them.

Administrators can enter vSLM 2 software one at a time or, preferably, let the vSLM 2 secure management software auto-detect them. The vSLM 2 software uses the Lantronix discovery protocol to auto-detect SLM appliances and other Lantronix devices, Lantronix SCS05/20 discovery protocol to auto-detect Lantronix SCS05/20 devices within a specified IP range, and SNMP to detect all other devices within a specified IP range.

Auto-Detecting Devices

Auto-detect enables the vSLM 2 software to search for and register Ethernet devices automatically. When the vSLM 2 software detects an Ethernet device, it also scans the device for ports and port information. You only need to define search protocols and parameters once; they are saved for use in any future searches. When the vSLM 2 secure management software performs a device search, it uses all defined protocols simultaneously.

After performing an auto-detect search once, you need to run it again only if the search protocols change, or if new (undetected) devices are added to the network.

To add auto-detect devices:

1. On the menu, click **Configuration > Device Management > Auto-Detect Devices**. The following page opens.

Figure 9-1 Automatic Device Detection Page - Configure Tab

The screenshot shows the 'Automatic Device Detection' configuration page. At the top, there is a navigation bar with the LANTRONIX SLM logo, a search bar, and a user profile 'sysadmin@SLMC413'. The main content area is titled 'Automatic Device Detection' and has tabs for 'Configure', 'Notes', and 'Help'. The 'Configure' tab is active, showing three discovery protocols:

- Lantronix discovery protocol:** Fields for IP address, Optional Ending IP, and Timeout (1000).
- SNMP on IP range:** Fields for Starting IP address, Ending IP address, Timeout (100), and Community (public).
- SCS05/20 discovery on IP range:** Fields for Starting IP address, Ending IP address, and Timeout (100).

Below these fields, there is a note: 'Web configuration [https] must be enabled for SCS detection'. It also provides instructions: 'Use 255.255.255.255 for LDP broadcast' and 'Use 239.255.255.251 for LDP multicast'. A note states 'All timeout values are in milliseconds'. On the right side, there is a list of detected devices with a 'Delete' button and a search button at the bottom.

2. Enter the following information:

Notes: The maximum range of IP addresses to enter is 64K entries. We strongly recommend that you break the intended discovery range into several smaller ranges, to speed up the discovery process.

The discovery process may take up to 17 hours (1 second timeout for each entry) to complete for a full range of 64K IP entries; there is no option to cancel during discovery process.

Table 9-2 Automatic Device Detection - Configure Tab

Automatic Device Detection Setting	Description
Lantronix discovery protocol	<p>This protocol discovers SLC console managers and other Lantronix-built devices on the network.</p> <p>Note: To discover RPM/SLP and SLK devices, use SNMP; to discover SCSs, use SCS05/20 discovery. Use IP address 255.255.255.255 to discover all Lantronix-built devices on the local subnet, and use a remote subnet broadcast address if the routers in the network forward subnet broadcast packets.</p> <p>The Lantronix IP multicast address is 239.255.255.251. Any device can join the 239.255.255.251 multicast group by notifying or registering to its subnet router. vSLM 2 software then sends out a single discovery request, which is delivered to all devices in that multicast group by routers on different subnets. Once vSLM 2 software gets a discovery response from members, it queries each individual device for further information.</p> <p>Note: See [RFC1112] for a description of the basic IGMP protocol.</p> <p>IP address: Specify the subnet (e.g., 255.255.255.255) to be searched, or if specifying a range of IP addresses, the IP address at the beginning of the range in which the vSLM 2 secure management software is to detect devices.</p> <p>Optional Ending IP: If specifying a range of addresses, enter the IP address at the end of the range.</p> <p>Timeout: Number of milliseconds the vSLM 2 software will continue to look for a device before moving on. The default is 1000.</p> <p>Note: You may specify more than one protocol search definition before the search.</p>
SNMP on IP range	<p>Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks. Enter the following to discover all devices within one or more ranges of IP addresses on the network.</p> <p>SNMP requires that you specify a range of IP addresses.</p> <p>Starting IP Address: The IP address at the beginning of the range in which the vSLM 2 software is to detect devices.</p> <p>Ending IP Address: The IP address at the end of the range in which the vSLM 2 software may detect devices.</p> <p>Timeout: Number of milliseconds the vSLM 2 secure management software will continue to look for a device before moving on. The default is 100.</p> <p>Community: An SNMP community is the group to which devices and management stations running SNMP belong. The default setting is public.</p>

Automatic Device Detection Setting	Description
SCS05/20 discovery on IP range	<p>To locate Lantronix SCS05/20 products on the network, specify:</p> <p>Starting IP Address: The IP address at the beginning of the range in which the vSLM 2 secure management software is to detect devices.</p> <p>Ending IP Address: The IP address at the end of the range in which the vSLM 2 software is to detect devices.</p> <p>Timeout: Number of milliseconds the vSLM 2 software will continue to look for a device before moving on. The default is 100.</p> <p>Note: Web configuration must be enabled on an SCS device for the vSLM 2 secure management software to discover it.</p>
Attempt secure channel connections	<p>To establish a secure channel connection to discovered SLC and vSLM 2 software, select the check box and one of the following options:</p> <p>Use default password: If you select this option, the vSLM 2 software attempts to set up a secure channel to discovered SLC and vSLM 2 software using the default sysadmin password of PASS. This is the default option.</p> <p>Use password: Enter a password to use for secure channel connections to discovered SLC and vSLM 2 software. If the password has been changed, the user must manually establish secure channels on the device pages (using the appropriate password) later.</p>

3. To add an entry to the current search list, click the **right arrow**.
4. To remove an entry from the current search list, select the entry and click the **Delete** button.
5. After defining all the searches, click the **Search** button.
6. If desired, check the progress of the search by clicking the **Progress** button above the menu. The table shows how far along the search is towards completion.

Note: You can continue working while the auto-detect process takes place in the background.

7. To add the detected devices to the menu tree, click the **Reload** button. When you open the device groups, the devices display in the proper place on the menu tree.

Note: When you first auto-detect devices, all devices that respond are entered into the vSLM 2 software database. You may decide to change the names of these devices (and ports) to something more meaningful than "SLC" or "Port-1." If you then auto-detect again, and auto-detect notices these devices again, the vSLM 2 secure management software retains the names you assigned. If you want to rename a device back to its original name, change the device name to ? before running the auto-detect. If auto-detect finds a device with the name ?, the vSLM 2 updates the name to the value the device returns.

Auto-Detect Commands

admin autodetect filter delete

Syntax

```
admin autodetect filter delete
```

Description

Deletes one of the current auto-detect search filters.

admin autodetect filter ltrx**Syntax**

```
admin autodetect filter ltrx <IP range> [timeout <number of milliseconds>]
```

Example

```
IP range: 192.168.0.1-192.168.0.155 timeout 1500  
timeout: default is 1000ms; range is 1000-60000ms
```

Description

Sets Lantronix discovery protocol search filters. The ending IP address is optional.

admin autodetect filter scs**Syntax**

```
admin autodetect filter scs <IP range> [timeout <number of milliseconds>]
```

Example

```
IP range: 192.168.0.1-192.168.0.155  
timeout: default is 100 msec; range is 100-60000 msec
```

Description

Sets SCS discovery protocol search filters.

admin autodetect filter show**Syntax**

```
admin autodetect filter show
```

Description

Displays the current auto-detect search filters.

admin autodetect filter snmp**Syntax**

```
admin autodetect filter snmp <IP range> [community <name>] [timeout <number of milliseconds>]
```

Example

```
IP range: 192.168.0.1-192.168.0.155  
name: public (default)  
timeout: default is 100 msec; range is 100-60000 msec
```

Description

Sets SNMP protocol search filters.

admin autodetect start**Syntax**

```
admin autodetect start <one or more parameters>
```

Parameters

```
[securechannel <default|password>]
[option <ltrxonly|delnonltrx>]
```

`ltrxonly` detects only Lantronix devices

`delnonltrx` detects only Lantronix devices and removes existing non-Lantronix devices.

Examples

```
admin autodetect start securechannel default
```

Attempts secure channel using the default password

```
admin autodetect start securechannel mypass option delnonltrx
```

Attempts secure channel using password `mypass`. Detects only Lantronix devices and removes existing non-Lantronix devices.

Description

Starts the vSLM 2 auto-detect device process, using the protocol and filters configured.

show progress**Syntax**

```
show progress
```

Description

Shows the progress of background tasks.

Ethernet Devices

The vSLM 2 secure management software enables you to list all devices, groups of devices, and individual devices in the vSLM 2 database. These devices have been auto-detected or added manually. This section shows how the Administrator and Ethernet Device Account groups add devices manually, edit device settings, and delete devices.

Listing Devices

You can view a list of all devices in the vSLM 2 database. The list may include other Lantronix-built devices and even non-Lantronix devices.

To list all devices on the network:

- To view all of detected devices, click **Ethernet Devices** on the menu.
 - The All Ethernet Devices page displays all devices in the database to the right.
 - Product-specific folders are nested beneath the Ethernet Devices folder according to settings under *Properties (Ethernet Device Menu Tree) (on page 166)*, and all discovered Ethernet devices are organized within these folders.

Figure 9-3 All Ethernet Devices Page - List Tab

LINK	Routing	Setup	Procedures	Config	Item Policy	Notes	Help	All Ethernet Devices								
Name	IP Address	Ethernet Address	Device Type	Location	Sub-Location	Model	Firmware	Last FW Update	Login	Channel Key	Port	Reach	Fail Count	SSH	Port	Back
AP641N-A49	172.18.0.110	8A:FB:AB:02:0D:00	Non Lantronix	My Cubicle						No	Yes	0			22	
CloudWatch	172.18.39.40	00:02:83:F4:F0:00	Non Lantronix							No	Yes	0			22	
OS6A-A066	172.18.39.248	00:80:A3:29:3F:07	SLB	Irving, CA 92018 USA		SLB894	5.4		vsadmin	Yes	Yes	0			22	
EDS16PR	172.18.229.79	00:20:4A:9E:83:C4	EDS			EDS16PR	5.0.2		admin	No	Yes	0			22	
EDS16PS	172.18.245.3	00:20:4A:9E:7E:3F	EDS			EDS16PS	5.0.2		admin	No	Yes	0			22	
EDS16PS	172.18.212.86	00:20:4A:9E:06:7A	EDS			EDS16PS	5.0.2		admin	No	Yes	0			22	
EDS2100	172.18.213.11	00:20:4A:8D:12	EDS			EDS2100	5.0.2		admin	No	Yes	3155			22	
EDS2100	172.18.100.223	00:20:4A:8B:8D	EDS			EDS2100	5.0.2		admin	No	Yes	0			22	
EDS32PR	172.18.248.6	00:20:4A:8E:89:87	EDS			EDS32PR	5.0.2		admin	No	Yes	0			22	
EDS32PR	172.18.212.198	00:20:4A:8E:8D:AC	EDS			EDS32PR	5.0.2		admin	No	Yes	0			22	
EDS32PR	172.18.248.7	00:20:4A:8E:8E:28	EDS			EDS32PR	5.0.2		admin	No	Yes	0			22	
EDS32PR	172.18.229.8	00:20:4A:8E:8E:00	EDS			EDS32PR	5.0.2		admin	No	Yes	0			22	
EDS32PR	172.18.212.187	00:20:4A:8E:83:00	EDS			EDS32PR	5.0.2		admin	No	Yes	0			22	
EDS32PR	172.18.248.8	00:20:4A:9E:0E:26	EDS			EDS32PR	5.0.2		admin	No	Yes	0			22	
EDS32PR	172.18.229.72	00:20:4A:9E:5C:7A	EDS			EDS32PR	5.0.2		admin	No	Yes	0			22	
EDS4100	172.18.213.104	00:20:4A:83:84:CC	EDS			EDS4100	5.0.2		admin	No	Yes	155			22	
EDS4100	172.18.21.180	00:20:4A:05:00:77	EDS	Michael's Cubicle		EDS4100	5.0.2		admin	No	Yes	0			22	
EDS4100	172.18.212.207	00:20:4A:83:83:88	EDS			EDS4100	5.0.2		admin	No	Yes	0			22	
EDS4100	172.18.229.86	00:20:4A:8D:01:88	EDS			EDS4100	7.0.2		admin	No	Yes	0			22	
ETB_2899F2	172.18.18.130	00:80:A3:28:83:72	Non Lantronix	Terminal Server						No	Yes	0			22	
Feeder-340-1	172.18.231.39	00:80:A3:9C:01:61	Router			SL3	3.3		vsadmin	Yes	Yes	0			22	
GreenDell-UPAC	172.18.100.229	00:80:A3:9C:47:05	Switch			SL3	3.0		vsadmin	Yes	Yes	0			22	
HP960Cna0524	172.18.21.96	00:01:8B:13:0B:A1	Non Lantronix	Mika's Cubicle						No	Yes	0			22	
Lantronix Tech Support Switch	172.18.0.105	00:22:87:FF:23:50	Non Lantronix	157 Technology Way, Irving, CA 92018						No	Yes	0			22	
linux20	172.18.38.20	11:22:33:44:55:20	Non Lantronix	Japan-Linx	Oakli	Model				No	Yes	0			22	
linux21	172.18.39.21	00:15:F2:0B:24:10	Non Lantronix	ITM Test Lab	North	Model				No	Yes	0			22	
linux22	172.18.38.22	11:22:33:44:55:22	Non Lantronix	Irving-Linx	North	Model				No	Yes	0			22	

- If there are more products than can fit on the screen, scroll forward and backward through the data using the mouse scroll wheel or the scroll bar in your vSLM window on the far right.
- Sort the list of products by specific column header by clicking the column header. The list will be sorted by either alphabetical or numerical values, depending on the column header type.
- Toggle between ascending and descending product order listing by clicking it again. The devices will re-order according to that column header in either ascending or descending order.

To list all Ethernet devices of a specific product type:

- Click **Ethernet Devices** to expand this folder and view all product-specific folders.
- Click the product folder representing the product type you wish to view. All products specific to that folder will appear to the right.
- If there is more data in a table than fits on the screen, scroll forward and backward through the data using the mouse scroll wheel or the scroll bar in your vSLM window on the right.
- Sort the list of products by specific column header by clicking the column header.
- Toggle between ascending and descending product order listing by clicking it again. The devices will re-order according to that column header in either ascending or descending order.

For example:

- To list all SLC console managers managed by the vSLM 2 secure management software, click **Ethernet Devices > SLC** on the menu tree (see [Figure 9-4](#)).
- If you click the **Name** column header, all products will list in ascending alphabetical order by the name of the products.
- Clicking the **Name** column header again will list the products in descending alphabetical order.
- Clicking the **IP Address** column header, all products will list in ascending numerical order by the IP Address of the product.
- Clicking the **IP Address** column header again will list the products in descending numerical order.

Figure 9-4 Manage “SLC” Group Page - List Tab

Name	IP Address	Ethernet Address	Device Type	Location	SubLocation	Model	FW Ver	Last FW Update	Login	Channel Key	Poll	Reach Fail Count	SSH Port	Rack
mslc48	172.18.21.66	00:80:A3:8D:53:29	SLC	location		SLC48-03	6.1.0.0		sysadmin	No	Yes	0	22	
mslc8048	172.18.21.61	00:20:4A:9D:03:64	SLC	location		SLC8048-01	7.1.0.0R11		sysadmin	No	Yes	0	22	
slbdb40	172.19.39.253	00:80:A3:89:07:01	SLC	location		SLC8	6.2.0.0		sysadmin	Yes	Yes	0	22	
slc16_glenn	172.19.39.254	00:80:A3:89:07:03	SLC	Engineering Lab		SLC16	5.4		sysadmin	Yes	Yes	5525	22	
slc4331	172.19.250.119	00:80:A3:96:43:31	SLC			SLC8048	7.2.0.0R20		sysadmin	Yes	Yes	0	22	R01C01P01
slc4657	172.19.213.8	00:80:A3:89:46:58	SLC	location		SLC48	6.1.0.0RC2		sysadmin	Yes	Yes	5524	22	
slc48_glenn_1	172.19.100.90	00:80:A3:8F:80:02	SLC	Engineering Lab		SLC48	6.1.0.0		sysadmin	Yes	Yes	170	22	
slc5e35	172.19.100.116	00:80:A3:8D:5E:35	SLC			SLC16	6.1		sysadmin	No	Yes	2	22	
slca508	172.19.250.120	D4:AE:52:BC:A5:08	SLC	location		SLC8048	7.2.0.0T1		sysadmin	Yes	Yes	5525	22	
slc-md-u	172.19.100.125	00:20:4A:9D:03:7C	SLC			SLC8048	7.2.0.0T1		sysadmin	Yes	Yes	0	22	
slcRef250120	172.19.100.221	00:20:4A:9D:03:36	SLC			SLC8048-01	7.2.0.0R20		sysadmin	Yes	Yes	0	22	R03C01P01
slcRefreshR17_167	172.19.250.167	00:20:4A:9D:03:48	SLC	Irvine, CA 92618 USA		SLC8032	7.1.0.0R17		sysadmin	Yes	Yes	5523	22	
tsslc32	172.18.0.107	00:30:31:FF:FF:54	SLC			SLC32	5.4		sysadmin	Yes	Yes	5523	22	

Adding a Device Manually

If you know there is a new device on the network, or for some reason, the vSLM 2 software does not auto-detect a device, the administrator can manually add it.

To add a device:

Note: Ethernet device pages may differ slightly, depending on the type of device. The procedure below the examples notes these differences.

1. On the menu tree, click **Ethernet Devices** and then the type of device you are adding (e.g., SLC, SLK, Spider, or other Lantronix devices).
2. Click the **Add** tab. Depending on the device type, one of the following pages or a similar page displays.

Note: The connection buttons on the right are inactive until the Ethernet device has been added to the system. See [Connecting to Ethernet and Managed Devices \(on page 237\)](#) for instructions on using the buttons. The **TN3270** button is inactive for all Lantronix devices.

Figure 9-5 Add SLM Device Page - Configure Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main heading is 'Device "slm02_glenn17"'. Below this are tabs for 'Configure', 'Ports', 'PerCons', 'LocalCons', 'Utilities', 'Display', 'Traps', 'Modem', 'Notes', and 'Help'. The 'Configure' tab is active, showing various configuration fields: Name (slm02_glenn17), MAC Address (00:30:48:5B:6A:10), IP Address (172.19.211.17), Model (SLM), Location, Sub-Location, FW Version (3.8), Secure channel (Yes), Link Down - last checked: Status: 09/09/2015 04:18, TCP Port for SSH (22), TCP Port for Telnet (23), Rack Location (Not assigned), Managed Device (New Device), mgroup_1, Read info from device (checkbox), Write info to device (checkbox), Poll (checkbox checked), and a list of services: Browse http, Browse https, Web Channel, Secure Channel, SSH Connection, Telnet, and TN3270, each with a checkbox. At the bottom are 'Update', 'Reset', and 'Delete' buttons.

Figure 9-6 Add SLC Device Page - Configure Tab

The screenshot shows the LANTRONIX SLM web interface for adding a new SLC device. The main heading is 'Add "SLC" Device'. Below this are tabs for 'Configure', 'Ports', 'PerCons', 'LocalCons', 'Utilities', 'Display', 'Traps', 'Modem', 'Notes', and 'Help'. The 'Configure' tab is active, showing various configuration fields: Name, MAC Address, IP Address, Model, Location, Sub-Location, FW Version, Secure channel (No), Login, Link Status (Down - last checked: Never), Password, Retype Password, Rack Location (Not assigned), SNMP Read Community (public), SNMP Write Community, SNMP Trap Community, Synchronized (No), Device Ports (8), Poll (checkbox checked), and a list of services: Browse http, Browse https, Web Channel, Secure Channel, SSH Connection, Telnet, and TN3270, each with a checkbox. At the bottom are 'Add', 'Reset', and 'Delete' buttons.

Figure 9-7 Add SLK Device Page - Configure Tab

LANTRONIX SLM

Table: Ethernet Device Field: Name Value: Search Reset

sysadmin@SLM1F4F Group: Administrators Logout

Add "SLK" Device

Configure Ports PerCons LocalCons Utilities Display Traps Modem Notes Help

Name: _____ MAC Address: _____

IP Address: _____ Model: _____

Location: _____ FW Version: _____

Sub-Location: _____

Secure channel: No Link Status: Down - last checked: Never

Login: _____ Password: ••••••

Retype Password: ••••••

TCP Port for Telnet: 23

Device Ports: 1

Rack Location: Not assigned

Poll:

SLM Proxy

Browse http

Browse https

Web Channel

Secure Channel

SSH Connection

Telnet

TN3270

Add Reset Delete

Figure 9-8 Add RPM/SLP Device Page - Configure Tab

LANTRONIX SLM

Table: Ethernet Device Field: Name Value: Search Reset

sysadmin@SLM1F4F Group: Administrators Logout

Add "RPM/SLP" Device

Configure Ports PerCons LocalCons Utilities Display Traps Modem Notes Help

Name: _____ MAC Address: _____

IP Address: _____ Model: _____

Location: _____ FW Version: _____

Sub-Location: _____

Secure channel: No Link Status: Down - last checked: Never

Login: _____ Password: ••••••

Retype Password: ••••••

TCP Port for SSH: 22

TCP Port for Telnet: 23

SNMP Read Community: public

SNMP Trap Community: public

Main/Master Ports: 0

Expansion/Link #1 Ports: 0

Expansion/Link #2 Ports: 0

Expansion/Link #3 Ports: 0

Rack Location: Not assigned

Current load: -1.00 amps

Poll:

SLM Proxy

Browse http

Browse https

Web Channel

Secure Channel

SSH Connection

Telnet

TN3270

Add Reset Delete

Figure 9-9 Add Spider Device Page - Configure Tab

LANTRONIX[®] SLM

Table: Ethernet Device Field: Name Value: sysadmin@SLM1F4F Group: Administrators

Search Reset Logout

Add "Spider" Device

Configuration Ports PerCons LocalCons Utilities Display Traps Modem Notes Help

Name: _____ MAC Address: _____

IP Address: _____ Model: _____

Location: _____ FW Version: _____

Sub-Location: _____

Secure channel: No Link Status: Down - last checked: Never

Login: _____ Password: ●●●●●●

TCP Port for SSH: 22 Retype Password: ●●●●●●

TCP Port for Telnet: 23 Rack Location: Not assigned

Device Ports: 1 Poll:

Browse http
 Browse https
 Web Channel
 Secure Channel
 SSH Connection
 Telnet
 TN3270

Add Reset Delete

Figure 9-10 Add Other Lantronix Device Page - Configure Tab

LANTRONIX[®] SLM

Table: Ethernet Device Field: Name Value: sysadmin@SLM1F4F Group: Administrators

Search Reset Logout

Add "Other Lantronix" Device

Configuration Ports PerCons LocalCons Utilities Display Traps Modem Notes Help

Name: _____ MAC Address: _____

IP Address: _____ Model: _____

Location: _____ FW Version: _____

Sub-Location: _____

Secure channel: No Link Status: Down - last checked: Never

Login: _____ Password: ●●●●●●

TCP Port for SSH: 22 Retype Password: ●●●●●●

TCP Port for Telnet: 23 Rack Location: Not assigned

Device Ports: 1 Poll:

Browse http
 Browse https
 Web Channel
 Secure Channel
 SSH Connection
 Telnet
 TN3270

Add Reset Delete

Figure 9-11 Add Non Lantronix Device Page - Configure Tab

The screenshot shows the Lantronix SLM web interface. At the top, there is a search bar with fields for 'Table' (set to 'Ethernet Device'), 'Field' (set to 'Name'), and 'Value'. The user is logged in as 'sysadmin@SLM1F4F' with the role of 'Administrators'. The main heading is 'Add "Other Lantronix" Device'. Below this, there are tabs for 'Configure', 'Ports', 'PerCons', 'LocalCons', 'Utilities', 'Display', 'Traps', 'Modem', 'Notes', and 'Help'. The 'Configure' tab is active, showing a form with the following fields and options:

- Name: [text input]
- MAC Address: [text input]
- IP Address: [text input]
- Model: [text input]
- Location: [text input]
- FW Version: [text input]
- Sub-Location: [text input]
- Secure channel: No
- Link Status: Down - last checked: Never
- Login: [text input]
- Password: [password input]
- Retype Password: [password input]
- TCP Port for SSH: 22
- TCP Port for Telnet: 23
- Rack Location: Not assigned
- Poll:

On the right side of the form, there are several checkboxes for connection types:

- Browse http:
- Browse https:
- Web Channel:
- Secure Channel:
- SSH Connection:
- Telnet:
- TN3270:

At the bottom of the form, there are 'Add', 'Reset', and 'Delete' buttons.

3. Enter the following as required by the device type:

Table 9-12 Manually Added New Device Details

New Device Setting	Description
Name (required)	Name that identifies the device.
MAC Address (required)	Network (Ethernet) number of the device (on the device label). Note: Enter all Ethernet addresses in hexadecimal, colon-separated format (e.g., 12:34:56:AB:CD:EF).
IP Address (required)	IP address that uniquely identifies the device on the network. There is no default. Note: Enter all IP addresses in dot quad notation.
Model	Model number of the device. Required for both the RPM/SLP, SCS05/20 and SLB devices.
Location	Place where the device is installed (e.g., city, building, or room).
FW Version	Release number of the firmware.
Sub-Location	Sub region or location where the device is installed.
Secure Channel (view only)	Indicates whether the vSLM 2 software has a Lantronix secure channel connection from the web interface to the command line interface of an SLC console manager and its ports. The default is No .
Link Status (view only)	Indicates whether or when the vSLM 2 software polled the connection from the vSLM 2 secure management software to the device.
Login (not on vSLM 2)	User name for logging into any Ethernet device that can be logged into using http or https.
Password and Retype Password (not on vSLM 2)	Password for logging into any Ethernet device that can be logged into using http or https.
TCP Port for SSH	Number of the port for establishing an SSH connection to the device or its ports. The default setting is 22.

New Device Setting	Description
TCP Port for Telnet	Number of the port for establishing a Telnet connection to the device or its ports. The default setting is 23 for all devices except WiBox and UDS, which use 9999.
TN3270 Logical Unit	Used by devices that support TN3270 connections.
SNMP Read Community (SLC, SLB, RPM/SLP only)	An SNMP community is the group to which devices and management stations running SNMP belong. The default setting is public..
SNMP Write Community (SLC, SLB, RPM/SLP only)	A string that acts like a password for an SNMP manager to modify data where permitted.
SNMP Trap Community (SLC, SLB, RPM/SLP only)	A string that is sent along when a trap is broadcast. Only management devices that are listening for that value process the trap. Management devices that are not listening for that trap community ignore the trap.
Current load (SLB and RPM/SLP - view only)	Displays the total current voltage (Amps) for each tower or unit on the SLB or RPM/SLP devices. A negative value indicates that the current load could not be read from the device.
Managed Device (SLC, SLB, SCS, SLM, and RPM/SLP only)	<p>If desired, create a managed device from the Ethernet device. For more information, see Configuring a Managed Device (on page 220).</p> <p>Note: This field is unavailable if no Managed Device Groups exist in the system.</p> <p>To associate the Ethernet device with a managed device or managed device group, select either a specific managed device or a managed device group and click the Create button. The associated managed device or managed device group will display in a link providing access to the configuration page for the managed device or managed device group.</p> <p>To disassociate the Ethernet device and an associated managed device or managed device group, click the Defuse button.</p>
Read info from device (SLC, SLB, SCS, SLM, and RPM/SLP only)	<p>If selected, the vSLM 2 software will attempt to update its internal database by interrogating the physical device. The vSLM 2 software must have a Secure Channel established to the Ethernet device (or provide the sysadmin login and password of the Ethernet devices) for this function to work.</p> <p>Currently, the vSLM 2 secure management software can read the following information:</p> <ul style="list-style-type: none"> ◆ SLC: SLC host name, firmware version, device port names, device port parameters (e.g. baud, flow control), and the vSLM 2 logging parameters for each port ◆ SCSxx05/20: SCS host name and the port names ◆ vSLM 2: vSLM 2 host name and firmware version ◆ RPM/SLP: RPM/SLP outlet names, wakeup state (if applicable) and outlet IDs ◆ SLB: SLB host name, firmware version, device port names, device port parameters (e.g. baud, flow control), and the vSLM 2 logging parameters for each port

New Device Setting	Description
Write info to device (SLC, SLB, SCS, SLM, and RPM/SLP only)	<p>If selected, the vSLM 2 software will attempt to update the physical device using the values currently in its internal database. The vSLM 2 software must have a Secure Channel established to the Ethernet device (or provide the sysadmin login and password of the device) for this function to work.</p> <p>Currently, the vSLM 2 secure management software can write the following information:</p> <ul style="list-style-type: none"> ◆ SLC: SLC host name, device port names, device port parameters (e.g. baud, flow control), and the vSLM 2 logging parameters for each port ◆ SCSxx05/20: SCS port names ◆ vSLM 2: vSLM 2 software host name ◆ RPM/SLP: RPM/SLP outlet name and wakeup state (if applicable) ◆ SLB: SLB host name, device port names, device port parameters (e.g. baud, flow control), and the vSLM 2 logging parameters for each port.
Synchronized (SLC and SLB only)	If you make a change to an SLC or SLB configuration but only save the change to the local database, this field displays No. It will change to Yes if you push the configuration to the physical device or read or write information to make the database match the physical device.
Poll	If selected, the vSLM 2 software will include this device when performing periodic polling of Ethernet devices. Selected by default.
Device Ports	Select the number of device ports on the Ethernet device.

4. Click the **Add** button.
5. Click **Ethernet Devices** and then the device group (e.g., SLC console manager) to which you added the device. The added device displays at the end of the list and on the menu tree.

Updating or Deleting Ethernet Device Settings

The Administrator and Ethernet Device Account groups can edit settings for secure IT management (including SLC, SLB, SLK, RPM/SLP, SLB, Spider, and other SLM units) and other Ethernet devices. They can also delete a device from the vSLM 2 database so that the vSLM 2 secure management software will no longer manage it.

To update an Ethernet device:

1. On the All Ethernet Devices or the Manage Group page, click the **Edit**  icon to the left of the desired device,

OR

On the menu tree, click the name of the desired device. The Configure tab for the device opens.

Note: An example of the Configure tab for updating an SLC console manager is shown below.

Figure 9-13 Update SLC Device Page - Configure Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1F4F' with the role 'Group: Administrators'. The main content area is titled 'Device "mislc8048"' and has several tabs: 'Configure', 'Ports', 'PerCons', 'LocalCons', 'Utilities', 'Display', 'Traps', 'Modem', 'Notes', and 'Help'. The 'Configure' tab is active, showing various configuration fields:

- Name: mislc8048
- MAC Address: 00:20:4A:9D:03:64
- IP Address: 172.18.21.61
- Model: SLC8048-01
- Location: location
- FW Version: 7.1.0.0R11
- Sub-Location: (empty)
- Secure channel: No
- Link Status: Up - last checked: 08/28/2015 19:48
- Login: sysadmin
- Password: (masked with dots)
- Retype Password: (masked with dots)
- TCP Port for SSH: 22
- TCP Port for Telnet: 23
- Rack Location: Not assigned
- SNMP Read Community: public
- SNMP Write Community: (masked with dots)
- SNMP Trap Community: public
- Managed Device: New Device (dropdown), mgroup_1 (dropdown), Create button
- Read info from device: (checkbox, unchecked)
- Write info to device: (checkbox, unchecked)
- Synchronized: No
- Poll: (checkbox, checked)

On the right side, there are several buttons and checkboxes for connection types:

- Browse http: (checkbox, unchecked)
- Browse https: (checkbox, unchecked)
- Web Channel: (checkbox, checked)
- Secure Channel: (checkbox, checked)
- SSH Connection: (checkbox, checked)
- Telnet: (checkbox, checked)
- TN3270: (checkbox, checked)

At the bottom, there are 'Update', 'Reset', and 'Delete' buttons.

Note: See [Connecting to Ethernet and Managed Devices \(on page 237\)](#) for instructions on how to use the active connect buttons.

2. Add or update information as desired. In addition to the fields described on [Configuring a Managed Device \(on page 220\)](#), enter the following for the SLC, SLB, SCS, SLM, and RPM/SLP devices (see [Table 9-12](#)):
 - ◆ Managed Device
 - ◆ Read info from device
 - ◆ Write info to device
3. Click the **Update** button. When the update is complete, a confirmation message displays.

To delete the device:

1. Click the **Delete** button.
2. In response to the request for confirmation, click **OK**. A blank device page opens.
3. Click **Ethernet Devices** on the menu tree. The deleted device is no longer on the menu tree or listed on the Device Group page.

Device Locator

Note: Use of Device Locator is not included with your vSLM 2 installation. Please contact Lantronix Sales at 800-422-7055 for additional information on enabling Device Locator.

At times it is desirable for the user to know the physical location of Ethernet devices that are being managed by the vSLM 2 secure management software. Device Locator takes advantage of the vSLM 2 software management to assign a specific Row, Cluster and Rack Position to any device in the vSLM 2 database. Once the physical location of the device has been entered into the device record (or determined during the discovery process for an SLC/SLB device), users can:

- ◆ Immediately determine where the device is located on a map representation of the machine room
- ◆ Check the names and types of all devices in a specific rack
- ◆ Access any device using any valid protocol with a single mouse click

To take advantage of this feature, the user must first determine the physical makeup of the machine room to be managed. How many rows of racks are there? How many clusters exist within each row (may be 1)? And, finally, how many racks are there in each cluster? The user should use the actual number of rows, the maximum number of clusters, and the average number of racks, as these can be added to or deleted from later.

Configuring Device Racks

Click on the **Device Locator** icon in the tree pane, directly below Ethernet Devices, then click on the Configure tab. You will be presented with:

Figure 9-14 Device Locator - Configure Tab

The screenshot displays the LANTRONIX SLM web interface. At the top, there is a header with the LANTRONIX SLM logo, a search bar, and user information (sysadmin@SLM1F4F, Group: Administrators). Below the header is a navigation tree on the left side, with 'Device Locator' selected. The main content area is titled 'Rack and Device Locations' and contains three tabs: 'View', 'Configure', 'Assign', 'Notes', and 'Help'. The 'Configure' tab is active, showing three sections:

- Define Room:** Contains input fields for 'Rows: 4', 'Clusters/Row: 3', and 'Racks/Cluster: 4', along with 'Submit' and 'Reset' buttons.
- Add Rack:** Contains input fields for 'Row:', 'Cluster:', and 'Position:', along with 'Submit' and 'Reset' buttons.
- Remove Empty Racks:** Contains a list of rack IDs (R01C01P02, R01C01P03, R01C01P04, R01C02P01, R01C02P02, R01C02P03, R01C02P04, R01C03P01, R01C03P02, R01C03P03) and a 'Submit' button.

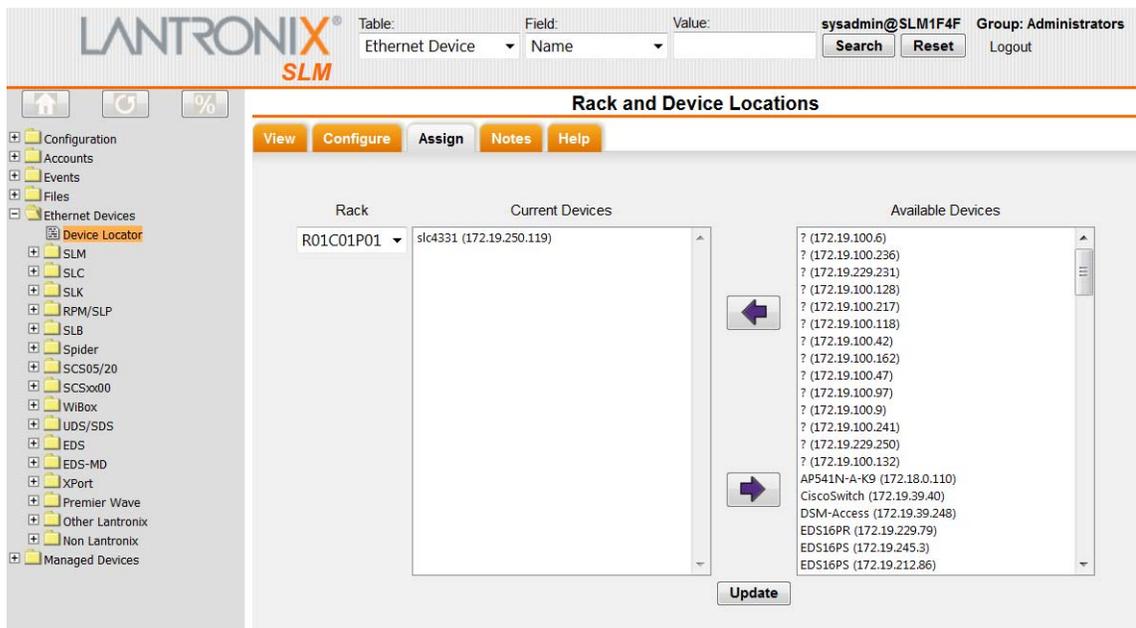
Enter these values in the "Define Room" section and presses "Submit". The racks are all created and assigned names based upon their location. For instance, if the machine room is defined with 3 rows, 2 clusters per row, and 5 racks per cluster, then 30 rack objects will be added to the database. Each rack object will be assigned a name in the format "RrrCccPpp" where "rr" is the row number, "cc" is the cluster and "pp" is the position within the cluster. Additional racks may be added at this time should some clusters contain more racks than typical, and empty racks may also be removed. Note that if a rack is removed from the end of a cluster, then the other racks are "enlarged" to physically fill out the cluster. If a rack is removed from the middle of a cluster, then a "hole" is shown in the cluster to indicate an available space.

Assigning Devices to Racks

Once the racks have been configured, you may now assign the Ethernet devices to their respective racks.

Click on the **Assign** tab. The Ethernet device assignment page shows:

Figure 9-15 Device Locator - Assign Tab

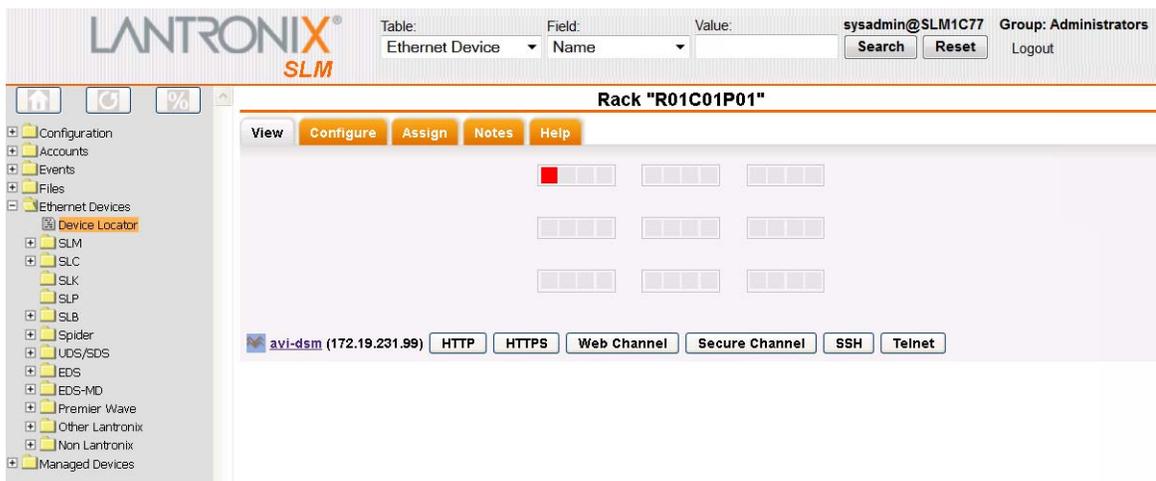


On the left is a drop-down list of all racks in the database. To assign one or more Ethernet devices to a given rack, first select the rack from the drop down (note Row, Cluster and Position number), then select one or more of the Available Devices in the rightmost list and use the left pointing arrow to move them to the Current Devices list. Finally, click on the **Update** button to send these changes to the database. Note that devices may be moved between the Current Devices list and Available Devices list one or more at a time by using Ctrl-click or Shift-click to select multiple devices. Also note that devices may be "removed" from a rack and placed back in the "Available Devices" pool by use of the right pointing arrow. Repeat this action to populate more racks.

Viewing Ethernet Device and Rack Locations

To take advantage of your newly defined machine room, click on the **View** tab:

Figure 9-16 Device Locator - View Tab



Note that racks that are populated are rendered in a pale yellow, rather than the gray of an empty rack. Use the mouse pointer to hover over one of these populated racks and a tool tip appears giving the name of the rack, along with the device type, name and IP address of all Ethernet devices in the rack. Furthermore, by clicking on the rack, that rack is highlighted in red and the bottom of the window is populated with a table containing an entry for each device in the rack. Each entry contains the icon for the device type (hover over the icon to see the device type in a tool tip), the name of the device (along with a link to that device's configuration page), the IP address of the device, and a series of connection buttons, one for each valid connection that the vSLM 2 secure management software can make to that device (note that due to actual configuration settings, some of these connections may not complete.)

One additional note: once a device has been "placed" in a rack, a link appears on that device's configuration page. By clicking on that link, the Device Locator View page is brought up, with its rack highlighted in red and all devices in that rack populated in the table below.

Persistent Connections

Persistent connections are permanent connections made between the vSLM 2 software and an Ethernet device (e.g., an SLC or RPM/SLP device) that include connection capability for up to five simultaneous users.

Note: The number of concurrent users may be increased up to a maximum of 25 users. Please contact Lantronix Sales at 800-422-7055 for additional information.

Some users may have read-only access and may only view all traffic on the connection. Other users may have read/write access and can type into the connection from the vSLM 2 side. Should a persistent connection fail (e.g., inadvertently closed by user or a network problem), the vSLM 2 software will detect this condition and attempt to reestablish the connection. All traffic on the connection may be logged to the vSLM 2 software.

To list existing persistent connections to a device:

1. On a specific device page, click the **PerCons** tab. A list of existing persistent connections display.

Note: You may view all Persistent Connections to which you have rights by performing a search.

Figure 9-17 Device Page - PerCons Search

The screenshot shows the Lantronix SLM web interface. At the top, there is a search bar with fields for 'Table:' (set to 'Ethernet Device'), 'Field:' (set to 'Name'), and 'Value:'. There are 'Search' and 'Reset' buttons, and a user profile 'sysadmin@SLM1F4F Group: Administrators Logout'. Below the search bar, the page title is 'Device "TS"'. A navigation menu includes 'Configure', 'Ports', 'PerCons', 'LocalCons', 'Utilities', 'Display', 'Traps', 'Modem', 'Notes', and 'Help'. The 'PerCons' tab is active, displaying a table with the following data:

Name	Console	Protocol	Time Established	Managed Device Available	Logging Enabled	Connection Enabled	Status
judytest TS		SSH	2015-08-28 23:19:07	Yes	No	Yes	Connecting

Below the table, it says '1 item' and there are buttons for 'Add New Persistent Connection' and 'Refresh'. On the left side, there is a navigation tree with 'Ethernet Devices' expanded, showing a list of devices including 'TS (172.18.0.216)' which is highlighted.

To view a specific persistent connection to a device:

1. On a specific device page, click the **PerCons** tab (see [Figure 9-17](#)).
2. click the **Edit**  icon to the left of the connection. The PerCons page opens.

Figure 9-18 Device Page - Persistent Connection

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1F4F' with the role 'Group: Administrators'. The main heading is 'Persistent Connection "judytest"'. Below this, there are three tabs: 'Configure', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following fields and values:

- Name: judytest
- Parent Ethernet Device: TS
- Protocol: SSH
- Last Established: 08/28/2015 23:19:07
- Logging Enabled:
- Managed Device Available:
- Connection Enabled:
- Use Parent Login:
- Login: [empty]
- Password: [masked with dots]
- Prompt: [empty]
- Application: [empty]
- Escape Sequence: \x1BC
- Reconnect Delay (mins): 1
- Status: Up
- EOL Translation: LF

At the bottom of the configuration area, there are buttons for 'Submit', 'Delete', and 'Connect'. On the left side, there is a navigation tree with categories like Configuration, Accounts, Events, Files, and Ethernet Devices. The 'Ethernet Devices' category is expanded, showing a list of devices including 'TS (172.18.0.216)' which is highlighted.

To add a persistent connection to a device:

1. On the PerCons list page, click the **Add New Persistent Connection** button. The Add Persistent Connection page displays.

Figure 9-19 Add Persistent Connection

The screenshot shows the LANTRONIX SLM web interface for adding a new persistent connection. The top navigation and search bar are identical to Figure 9-18. The main heading is 'Add Persistent Connection'. Below this, there are three tabs: 'Configure', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following fields and values:

- Name: [empty]
- Parent Ethernet Device: TS
- Protocol: SSH
- Last Established: Never
- Logging Enabled:
- Managed Device Available:
- Connection Enabled:
- Use Parent Login:
- Login: [empty]
- Password: [masked with dots]
- Prompt: [empty]
- Application: [empty]
- Escape Sequence: \x1BC
- Reconnect Delay (mins): 1
- Status: Down
- EOL Translation: LF

At the bottom of the configuration area, there are buttons for 'Submit', 'Delete', and 'Connect'. The left navigation tree is also visible, with 'Ethernet Devices' expanded and 'TS (172.18.0.216)' highlighted.

2. Enter the following information:

Table 9-20 Add Persistent Connection - Configure Tab

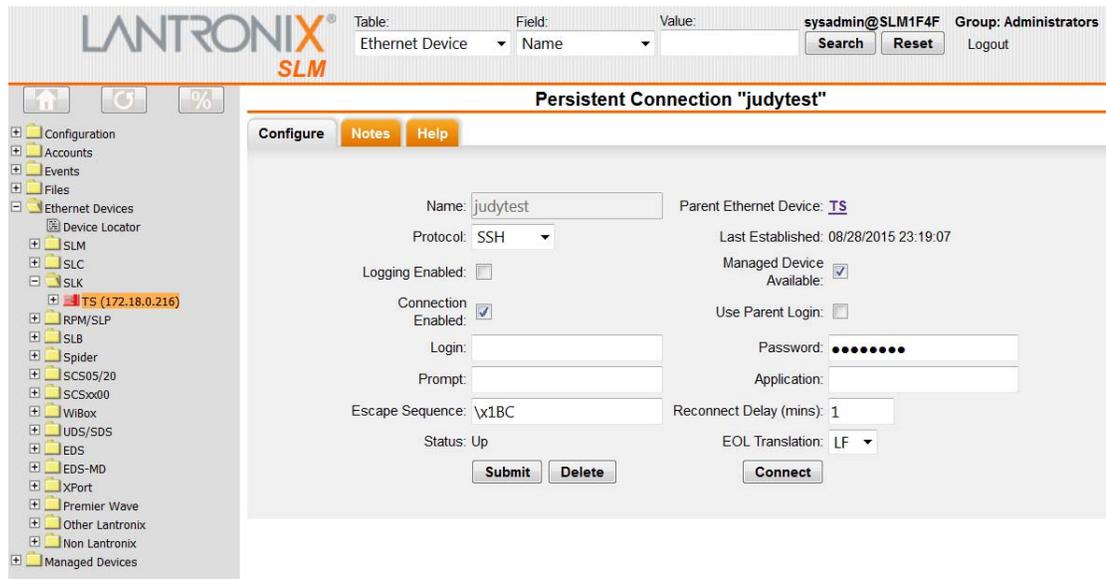
Persistent Connection Setting	Description
Name (required)	Name that identifies the persistent connection.
Protocol	From the drop-down list, select the protocol used to make the persistent connection. The options available depend on the type of Ethernet device. <ul style="list-style-type: none"> ◆ Secure Channel: SLC, SLB, Spider, and SLM units only ◆ SSH ◆ Telnet ◆ TN3270: A special Telnet program that connects to mainframes. It is only available if the Ethernet Device is of type Non-Lantronix. No Lantronix devices use this protocol.
Logging Enabled	Select to enable the vSLM 2 software to log the persistent connection.
Connection Enabled	Clear this box to define the persistent connection, but not to initiate it. Later, when you want to activate the connection, return and select this box.
Login	If specified, this is the account the vSLM 2 secure management software will use for logins when establishing the persistent connection. If you select the Use Parent Login box, this Login field is disabled. If this field is left empty and the Use Parent Login box is not checked, the user will be prompted for the login name when the connection is first established.
Prompt	Prompt that displays on the CLI when you log into the connection.
Escape Sequence	A series of one to ten characters that cause the user to exit the connection. A suggested value is Esc+C (escape key followed by an uppercase "C"), specified as \x1BC (default).
Status (view only)	Indicates whether the connection is active.
Parent Ethernet Device (view only)	Name of the Ethernet device to which the persistent connection is made.
Last Established (view only)	Indicates when the persistent connection was made.
Managed Device Available	If the parent Ethernet device of this persistent connection is being managed as part of a managed device, then users with access to that managed device will also be able to connect into this persistent connection.
Use Parent Login	If selected, you can log in using the userid and password for the Ethernet device. The Login and Password fields become inactive.
Password	Password for logging into the Ethernet device. (Inactive if you select Use Parent Login .)
Application	When the connection is made, the application will start automatically and keep running as long as the connection is active. An example is a program that monitors a system function such as throughput and sends unusual values to the screen. The application is available to anyone who attaches to the persistent connection and can be logged.
Reconnect Delay (min)	If the connection drops by mistake, the number of minutes to wait between attempts to reconnect.
EOL Translation	Specify LF or CR for the end-of-line character

3. Click the **Submit** button. A confirmation message displays, and the persistent connection displays below the list of the Ethernet device's ports on the menu tree.

To update a persistent connection to a device:

1. On the PersCon tab, click the **Edit**  icon to the left of the desired connection,
OR

On the menu tree, click the name of the desired connection (below the list of ports for a device). The PersCon page displays.

Figure 9-21 Edit Persistent Connection


The screenshot shows the Lantronix SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main content area is titled 'Persistent Connection "judytest"' and has three tabs: 'Configure', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following fields and options:

- Name: judytest
- Parent Ethernet Device: TS
- Protocol: SSH
- Last Established: 08/28/2015 23:19:07
- Logging Enabled:
- Managed Device Available:
- Connection Enabled:
- Use Parent Login:
- Login:
- Password:
- Prompt:
- Application:
- Escape Sequence: \x1BC
- Reconnect Delay (mins): 1
- Status: Up
- EOL Translation: LF

At the bottom of the form are 'Submit', 'Delete', and 'Connect' buttons. On the left side, there is a navigation menu tree with categories like Configuration, Accounts, Events, Files, Ethernet Devices, Device Locator, SLM, SLC, SLK, RPM/SLP, SLB, Spider, SCS05/20, SCSxx00, WiBox, UDS/SDS, EDS, EDS-MD, XPort, Premier Wave, Other Lantronix, Non Lantronix, and Managed Devices. The 'SLK' folder is expanded, showing a list of connections, with 'TS (172.18.0.216)' selected.

2. Add or update the information as desired.
3. Click the **Submit** button.

To delete a persistent connection to a device:

1. On the PersCon tab, click the **Edit**  icon the left of the desired connection,
OR

On the menu tree, click the name of the desired connection (at the end of the list of ports for a device). The PersCon page displays.

2. Click the **Delete** button.

Polling

Only administrators with **Allow Device Management** set on their account page can access the global polling page. Any administrator or Ethernet device user with rights to an Ethernet device can change the "poll flag" for the device. This poll flag enables and disables polling on a device-by-device basis. The poll flag of a device is enabled by default, but if not selected, even if polling is turned on, that device will not be polled.

To poll Ethernet devices on the network:

1. On the menu, click **Ethernet Devices**. The All Ethernet Devices page opens.
2. Click the **Polling** tab. The following page opens.

Figure 9-22 All Ethernet Devices - Polling Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1F4F' with the role 'Group: Administrators'. The main navigation menu includes 'List', 'Polling', 'Traps', 'Properties', 'Passwords', 'SNMP', 'SLM Proxy', 'Notes', and 'Help'. The 'Polling' tab is active. The main content area contains the following text: 'Ethernet devices may be tested for network reachability on a periodic basis. Configure the frequency to perform these connection tests.' Below this, there are three settings: 'Periodically poll:

3. Enter the following information:

Table 9-23 Poll Settings

Ethernet Device Setting	Description
Periodically poll	<p>Select to have the vSLM 2 software poll Ethernet devices on the network at regular intervals. Disabled by default.</p> <p>If you select this option, then any Ethernet device that has its "poll" flag set but fails to respond to Auto Connection Fail Count consecutive polling attempts displays with a vertical red stripe in its icon on the menu tree.</p> <p>Note: You can disable polling on a per device basis by clearing the poll flag on an individual device's page.</p>
Poll interval (minutes)	Number of minutes the vSLM 2 software should wait between polls.

Ethernet Device Setting	Description
Auto Connection Fail Count	<p>The following conditions are required for the vSLM 2 secure management software to automatically connect to the SLC console manager through a modem:</p> <ul style="list-style-type: none"> ◆ Ethernet device polling is enabled. ◆ The SLC device has polling enabled for itself. ◆ The SLC console manager has a modem connection and phone number configured. ◆ The SLC module has reached the maximum polling failure count (see below). ◆ There is an available modem on the vSLM 2 software. <p>Enter the number of consecutive times the system must fail to reach the SLC console manager before the vSLM 2 software will connect through a modem. Enter 0 (zero) to disable this feature.</p> <p>Once the connection is established, it will remain connected until after either a successful Ethernet poll or a manual disconnect of the modem by an vSLM 2 user.</p>
Last poll (view only)	Time the last poll was performed.

4. To save, click the **Update** button. A confirmation message displays.

SLC/SLB Local Connections

SLC/SLB serial connections may be monitored and terminated directly from the vSLM 2 secure management software. On the device page for an SLC/SLB module, simply click on the LocalCons tab. That page opens to reveal

Figure 9-24 Device Page - LocalCons Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main content area is titled 'Device "lyonslb"' and has several tabs: Configure, Ports, PerCons, LocalCons (selected), Utilities, Display, Traps, Modem, Notes, and Help. On the left, there is a navigation tree with categories like Configuration, Accounts, Events, Files, Ethernet Devices, Device Locator, SLM, SLC, SLK, RPM/SLP, SLB, Spider, SCS05/20, SCSxx00, WIBox, UDS/SDS, EDS, EDS-MD, XPort, Premier Wave, Other Lantronix, Non Lantronix, and Managed Devices. The SLB category is expanded, showing a list of devices including 'lyonslb (172.18.21.67)'. The main content area displays a table of connections:

Id	Port/Service	Flw	Port/Service	User	Uptime	
3	Console Port	<->	Command Line		393:59:19	<input type="checkbox"/>

Below the table, it says '1 connection' and there is another Refresh button.

This table shows the connection ID, the type of connection (SSH, Console, etc), the flow direction, the Service, the username and how long the connection has been up in hours:minutes:seconds.

To terminate one or more of these connections on the SLC/SLB device, check the connection's box (the **Refresh** button changes to **Terminate selected connections** button) and click on the **Terminate** button.

The window will refresh to show the selected connections no longer active.

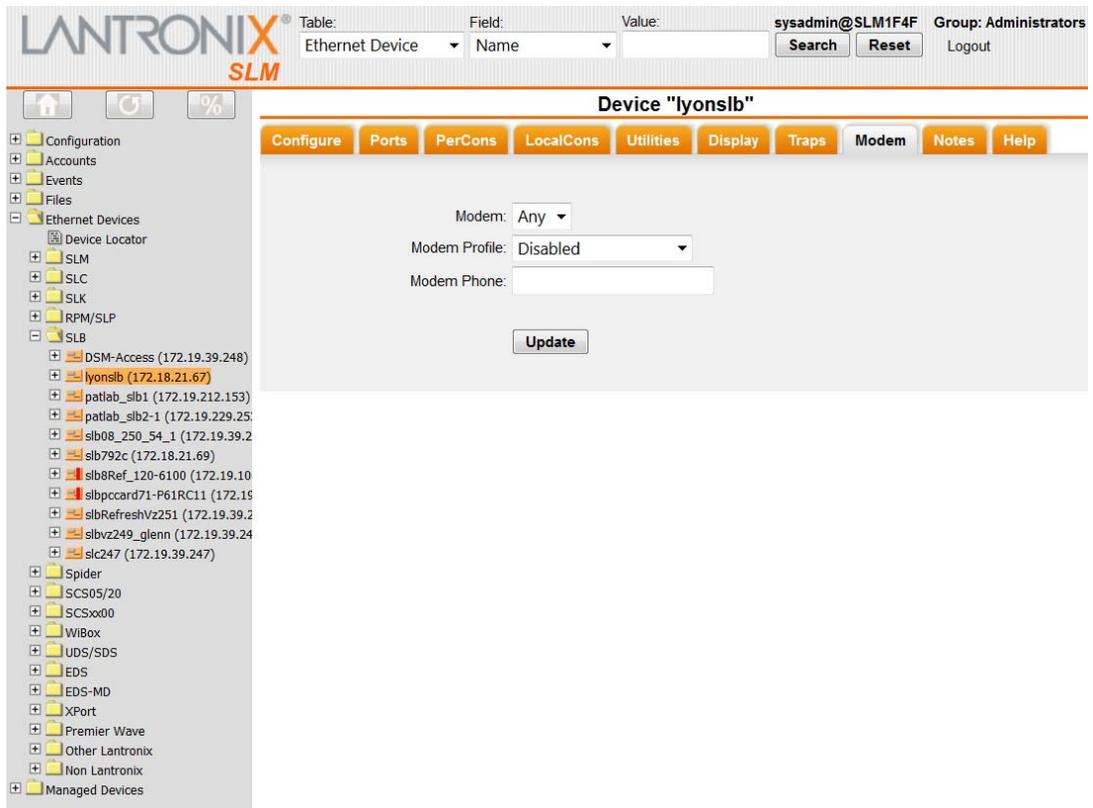
Device Modem

The Modem tab allows you to define modem connectivity between the vSLM 2 secure management software and the Ethernet device. This can include a PPP profile definition for the vSLM 2 software to use to communicate with the device if the Ethernet connection should become severed, or a text profile to be used in call back mode, where the vSLM 2 software calls the SLC/SLB device, the SLC/SLB device hangs up and then calls the vSLM 2 software back (this for security purposes).

Note: The phone number of the modem on the vSLM 2 secure management software and call back mode must be configured on the SLC/SLB device.

1. On the All Ethernet Devices or the Manage Group page, click the **Edit**  icon to the left of the desired device and click the **Modem** tab in the device page which appears.

Figure 9-25 Device Page - Modem Tab



The screenshot displays the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main content area is titled 'Device "lyonslb"' and features a navigation bar with tabs: 'Configure', 'Ports', 'PerCons', 'LocalCons', 'Utilities', 'Display', 'Traps', 'Modem', 'Notes', and 'Help'. The 'Modem' tab is active, showing a form with the following fields: 'Modem:' with a dropdown menu set to 'Any', 'Modem Profile:' with a dropdown menu set to 'Disabled', and 'Modem Phone:' with an empty text input field. An 'Update' button is located below the form. On the left side, a tree view shows the navigation structure, with 'Ethernet Devices' expanded to show a list of devices, including 'lyonslb (172.18.21.67)' which is highlighted.

2. Enter the following information:

Table 9-26 Device - Modem Tab

Device Setting	Description
Modem	<p>From the drop-down list, select a specific modem for the Ethernet device to use. The default is Any.</p> <p>For PPP connections, if you leave Any, the vSLM 2 software will choose any available modem to use.</p> <p>For text connections (call back), specify which modem the SLC console manager is expected to call back on. If you leave Any, the vSLM 2 software will choose the first available modem, and if the SLC device calls back on another modem, the connection will fail. If there is only one modem, then it does not matter whether it is specified or not in text mode.</p>
Modem Profile	From the drop-down list, select profile to be used with the connection. The default setting is Disabled .
Modem Phone	The phone number of the Ethernet device that will be contacted.

3. Click the **Update** button. A Modem Connect or, in the case of an SLC/SLB device, a **Call Back** button may display.
 - ◆ The **Call Back** button allows you to open a window to the SLC/SLB device, view the connection, and type commands.
 - ◆ The **Modem Connect** button establishes a PPP connection between the vSLM 2 secure management software and the remote Ethernet device. It is used when there is a network interruption and the vSLM 2 software needs to contact the Ethernet device. Click this button to establish the connection manually.

Note: The **Modem Connect** button only displays if a modem is present on the system, a PPP profile is configured on the Ethernet device, the Ethernet device references a defined vSLM 2 PPP profile, and a telephone number is defined for the Ethernet device.

Viewing Session & Audit Log Files, Ping and SNMP Walk

On the Device page, you can view all session log files for the device.

To view session log files:

1. On the Device page, click the **Utilities** tab. The following page opens:

Figure 9-27 Device Page - Utilities Tab

Device session log file names have the following format:

```
<hostname>_<host_mac_address>-
<device_port_number>=<username>=<connection_type>-<date_and_time>.log,
where:
```

Table 9-28 Device Session Log File Name Components

Device Setting	Description
<hostname>	Up to the first 8 characters of the hostname of the Ethernet device. If the hostname is shorter than 8 characters, the hostname section is padded with ~ characters to reach this length.
<host_mac_address>	MAC Address of the Ethernet device. This is used by the vSLM 2 software to correlate log files to their corresponding Ethernet devices.
<device_port_number>	Device port number connected to for this session. This field is set to 0 "00" for direct connections to the Ethernet device.

Device Setting	Description
<username>	The vSLM 2 user ID that initiated this session.
<connection_type>	Session connection type: tnt for telnet, ssh for ssh, or scc for secure channel.
<date_and_time>	Date and time string in the format YYMMDD_HHMMSS

2. From the **Device Session** drop-down list, select the log you want to view.
3. Click the **View** button. The contents of the log display on the Display tab.
4. To view an SLC or SLB audit log, select the audit log from the **SLC/SLB** drop-down list and click the **View** button. The contents of the log display on the Display tab.
5. To Ping a device, click on the **Ping-V4** button. A pop-up window will appear to display the results of the ping operation.
6. To perform an SNMP walk of either the private MIB for the device or MIB-2, select the SNMP version. If version 3 is selected, set the v3 Auth, the v3 Encrypt, the v3User, the Auth Passphrase, and lastly, click on the **SNMP Walk** button. The resulting output will appear in the Display tab. Not all devices support this operation or have it enabled. Depending on the type of device, the SNMP OID for the private MIB may be automatically filled in.

Note: For information about a global option for enabling both device session logging and SLC port session logging, see [Logging in to the vSLM 2 Software \(on page 307\)](#).

Traps

Traps are notifications of events sent from one device to another. The traps listed below are those sent by other devices (including SLM, SLC, RPM/SLP, and SLK devices) and received by the vSLM 2 secure management software. This feature is applicable when you select Enable Traps Reception on the SNMP Agent page. Examples of traps the vSLM 2 software can receive include:

- ◆ SNMP Generic Traps:
 - ◆ Cold Start
 - ◆ Warm Start
 - ◆ Ethernet Link Down
 - ◆ Ethernet Link Up
 - ◆ Authentication Failure
 - ◆ EGP Neighbor Loss
- ◆ SLM Custom Traps (specified in vSLM 2 custom MIBs)
- ◆ SLC Custom Traps (specified in SLC custom MIBs)
- ◆ RPM/SLP Custom Traps (specified in RPM/SLP custom MIBs)
- ◆ SLK Custom Traps (specified in SLK custom MIBs)

Note: You can view traps on three levels: All Ethernet devices, Ethernet device group, and individual Ethernet device.

To view traps for devices listed on the All Ethernet Devices page:

1. On the menu, click **All Ethernet Devices**, then select a specific Ethernet device group, select the individual device, and then click the **Traps** tab. The following page opens.

Figure 9-29 Selected Ethernet Device - Traps Tab

2. Review the following information:

Table 9-30 Trap Settings

Ethernet Device Setting	Description
IP Address	IP address of the Ethernet device generating the trap.
Time	Time the Ethernet device generated the trap.
Object ID	Uniquely identifies the trap among all possible traps from all SNMP-capable devices; it is derived from the trap.
Trap Type	Category of trap, for example, device cold/warm start, device Ethernet link up/down, device authentication failure; it is derived from the trap.
Trap Community	Community value.
Device	Name of the device sending the trap; it is derived by associating the sender's IP address to a device name in the vSLM 2 database.
Description	Message text in the trap.
Contents	The entire contents of the SNMP trap.

To clear or export a trap log:

1. On the top part of the page, enter the following:

Table 9-31 Clear or Export Trap Log Settings

Trap Log Setting	Description
Clear Trap Log	Select the check box to clear the trap log.
Export Trap Log	To export a trap log, select the check box and enter the range of dates the log you want to export should cover.

Trap Log Setting	Description
Filename	Enter the name of the log file to export and select one or both of the following options: Overwrite Existing File: Replace an existing log file with the one being exported. Remove Exported Rows: Removes exported rows of Trap data from the database so they will not be perceived as new traps in future viewings.

2. Click the **Update** button.
3. To clear the table, click the **Clear Trap Table** button.

Properties (Ethernet Device Menu Tree)

The system administrator can control the display of Ethernet device folders in the tree menu.

To configure the Ethernet device menu tree:

1. On the menu, click **Ethernet Devices**, then click the **Properties** tab. The following page opens:

Figure 9-32 All Ethernet Devices Page - Properties Tab

LANTRONIX[®] SLM

Table: Ethernet Device Field: Name Value: sysadmin@SLM1F4F Group: Administrators

Search Reset Logout

All Ethernet Devices

List Polling Traps **Properties** Passwords SNMP SLM Proxy Notes Help

Control display of Ethernet device folders in tree frame and Device Type Detection.

SLM: Always	<input type="checkbox"/> Remove existing SLM devices from database
SLC: Always	<input type="checkbox"/> Remove existing SLC devices from database
SLK: Always	<input type="checkbox"/> Remove existing SLK devices from database
RPM/SLP: Always	<input type="checkbox"/> Remove existing RPM/SLP devices from database
SLB: Populated	<input type="checkbox"/> Remove existing SLB devices from database
Spider: Populated	<input type="checkbox"/> Remove existing Spider devices from database
SCS05/20: Populated	<input type="checkbox"/> Remove existing SCS05/20 devices from database
SCSxx00: Populated	<input type="checkbox"/> Remove existing SCSxx00 devices from database
WiBox: Populated	<input type="checkbox"/> Remove existing WiBox devices from database
UDS/SDS: Populated	<input type="checkbox"/> Remove existing UDS/SDS devices from database
EDS: Populated	<input type="checkbox"/> Remove existing EDS devices from database
EDS-MD: Populated	<input type="checkbox"/> Remove existing EDS-MD devices from database
XPort: Populated	<input type="checkbox"/> Remove existing XPort devices from database
Premier Wave: Populated	<input type="checkbox"/> Remove existing Premier Wave devices from database
Other Lantronix: Populated	<input type="checkbox"/> Remove existing Other Lantronix devices from database
Non Lantronix: Populated	<input type="checkbox"/> Remove existing Non Lantronix devices from database

Update Reset

2. Enter the following:

Table 9-33 All Ethernet Devices - Properties Tab

Ethernet Device Setting	Description
Ethernet Device Groups	<p>For each device group, select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ◆ Always: Device folder displays whether populated or not. This is the default setting for the vSLM 2, SLC®, SLK®, and RPM/SLP® device folders. ◆ Always/No Ports: Device folder displays whether populated or not. For each device, the folder will display the main device, but none of the ports or outlets/power ports for the device. ◆ Never: Device folder does not display, even if populated. ◆ Populated: Device folder displays only when populated. This is the default setting for the SCS05/20, SCSxx00, SLB®, Spider®, WiBox®, UDS/SDS™, EDS, EDS-MD®, XPort®, PremierWave®, other Lantronix and non-Lantronix device folders. ◆ Populated/No Ports: Device folder displays only when populated. For each device, the folder will display the main device, but none of the ports or outlets/power ports for the device. ◆ Don't Detect: Prevents devices of this type from being auto detected.

- To remove all devices of a type currently in the vSLM 2 database, select its checkbox.

Note: Check boxes are active only if you change the display mode to **Don't Detect**.

- To save, click the **Submit** button.

Port Access

The Port Access tab is available for SLC, SLB, RPM/SLP, Spider and UDS/SDS devices and provides the following:

- ◆ **SLC devices:** Connection to serial ports.
- ◆ **SLB devices:** Connection to serial ports and access to the port page for power ports.
- ◆ **RPM/SLP devices:** Access to the port page for power ports.
- ◆ **Spider devices:** KVM access to devices connected to a Spider device.
- ◆ **UDS/SDS devices:** Manage connections between UDS/SDS ports.

To connect to an SLC port:

- On the menu, click **Ethernet Devices > SLC**. The Manage SLC Group page opens.
- Click the **Port Access** tab. A list of all SLC console managers displays, along with all of their ports. Numbered squares represent the ports.

Note: Hovering over a port reveals the port name.

Figure 9-34 Manage SLC Group - SLC Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1F4F' with the role 'Group: Administrators'. The main heading is 'Manage "SLC" Group'. Below this, there are tabs for 'List', 'Add', 'Traps', 'Actions', 'Port Access', 'Notes', and 'Help'. The 'Port Access' tab is selected, displaying a table of SLC devices. The table has columns for device name, IP address, and a grid of port status indicators (1-48). The status indicators are green, indicating power load or connection status. The devices listed are:

Device Name	IP Address	Port Status (1-48)
misc48	172.18.21.66	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
misc8048	172.18.21.61	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
slbdb40	172.19.39.253	1 3 5 7 2 4 6 8
slc16_glenn	172.19.39.254	1 3 5 7 9 11 13 15 2 4 6 8 10 12 14 16
slc4331	172.19.250.119	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
slc4657	172.19.213.8	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
slc48_glenn_1	172.19.100.90	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
slc5e35	172.19.100.116	1 3 5 7 9 11 13 15 2 4 6 8 10 12 14 16
slca508	172.19.250.120	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
slc-md-u	172.19.100.125	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
slcRef250120	172.19.100.221	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48
slcRefreshR17_167	172.19.250.167	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32
tssl32	172.18.0.107	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32

At the bottom of the table, there is an 'Auto Refresh' checkbox and a 'Refresh' button.

3. Click the SLC port to open a Secure Channel connection.

To connect to an SLB port or access its port page:

1. On the menu, click **Ethernet Devices > SLB**. The Manage SLB Group page displays:
2. Click the **Port Access** tab. A list of all SLB modules and their IP addresses displays, along with all of their ports and the power load of each port.

Note: *Hovering over a port reveals the port name.*

Figure 9-35 Manage SLB Group - Port Access Tab

The screenshot shows the 'Manage "SLB" Group' page in the LANTRONIX SLM web interface. The page displays a table of SLB devices with their IP addresses and power loads. Each device has a grid of colored squares representing ports (1-8) and their status (Green, Red, Blue, Gray). The table includes columns for Name, IP, Port Access, and Power Load. The interface also shows a navigation menu on the left and search/reset buttons at the top.

Name	IP	Port Access	Power Load
DSM-Access	172.19.39.248	1 3 5 7 P1 P2 P3 P4 2 4 6 8	1.20 amps
lyonslb	172.18.21.67	1 3 5 7 P1 P2 P3 P4 2 4 6 8	0.00 amps
patlab_slb1	172.19.212.153	1 3 5 7 P1 P2 P3 P4 2 4 6 8	0.10 amps
patlab_slb2-1	172.19.229.253	1 3 5 7 P1 P2 P3 P4 2 4 6 8	0.00 amps
slb08_250_54_1	172.19.39.250	1 3 5 7 P1 P2 P3 P4 2 4 6 8	0.00 amps
slb792c	172.18.21.69	1 3 5 7 P1 P2 P3 P4 P5 P6 P7 P8 2 4 6 8	0.00 amps
slb8Ref_120-6100	172.19.100.87	1 3 5 7 P1 P2 P3 P4 P5 P6 P7 P8 2 4 6 8	-1.00 amps
slbpcard71-P61RC11	172.19.250.55	1 3 5 7 P1 P2 P3 P4 2 4 6 8	-1.00 amps
slbRefreshVz251	172.19.39.251	1 3 5 7 P1 P2 P3 P4 P5 P6 P7 P8 2 4 6 8	0.00 amps
slbvz249_glenn	172.19.39.249	1 3 5 7 P1 P2 P3 P4 P5 P6 P7 P8 2 4 6 8	0.00 amps
slc247	172.19.39.247	1 3 5 7 P1 P2 P3 P4 2 4 6 8	0.90 amps

Color-coded numbered squares represent the ports:

- ◆ **Green** = serial ports
- ◆ **Red** = power port on
- ◆ **Blue** = power port off
- ◆ **Gray** = power port state unknown (the device may not be responding)

3. You have the following options:

- ◆ To open a Secure Connection with a serial port, click the corresponding green square.
- ◆ To open an SLB port page, click the corresponding red or blue square.

To access an RPM/SLP port page:

1. On the menu, click **Ethernet Devices > RPM/SLP**. The Manage RPM/SLP Group page displays:
2. Click the **Port Access** tab. A list of all RPM/SLP power managers displays, along with all of their ports and the power load of each port.

Note: *Hovering over a port reveals the port name.*

Figure 9-36 Manage RPM/SLP Group - Port Access Tab

Table: Ethernet Device Field: Name Value: sysadmin@SLM1F4F Group: Administrators Logout

Manage "RPM/SLP" Group

List Add Traps Actions Port Access Notes Help

Red - On, Blue - Off, Grey - Unknown. Hover over port for current load. Total current for each unit displayed on the far right.

SecureLinuxSLP_8b000f	172.18.21.65	1 2 3 4 5 6 7 8	-1.00 amps
SecureLinuxSLP_8b0026	172.19.39.44	1 2 3 4 5 6 7 8	-1.00 amps
SecureLinuxSLP_8b0133	172.18.0.108	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	0.00 amps
SLP_Glenn_237_30	172.19.237.30	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16	2.00 amps
			4.25 amps
			0.50 amps

Auto Refresh Refresh

Color-coded numbered squares represent the ports:

- ◆ **Blue** = power port off
- ◆ **Red** = power port on
- ◆ **Grey** = power state unknown (device may not be responding)

3. Click the port whose port page you want to open.

To gain KVM access to a device connected to a Spider unit:

1. On the menu, click **Ethernet Devices > Spider**. The Manage Spider Group page displays.
2. Click the **Port Access** tab. All Spider devices in the system display as boxes with IP addresses. Some boxes may display the current view of the device the Spider is controlling.

Figure 9-37 Manage Spider Group - Port Access Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@vsm02_glenn250180' with the group 'Administrators'. The main heading is 'Manage "Spider" Group'. Below this, there are tabs for 'List', 'Add', 'Traps', 'Actions', 'Port Access', 'Notes', and 'Help'. The 'Port Access' tab is selected. On the left, a navigation tree shows 'Ethernet Devices' expanded to 'Spider'. The main content area displays four device thumbnails, each with a 'No Signal' status:

- Fedora-242-1 (172.19.231.99): Shows a desktop background.
- GlennDell-XP-PC (172.19.100.229): Shows a Spider KVM device with a USB cable.
- PAT-HostVM (172.19.100.168): Shows a Spider Duo KVM device with multiple cables.
- Rextron-Spider (172.19.38.96): Shows a black screen.

3. Click the screen image to open a Spider KVM session to that device.

To refresh the Port Access tab:

1. You have two options:
 - ◆ To refresh the port information automatically every two minutes, select the **Auto Refresh** check box and click the **Refresh** button.
 - ◆ To refresh the port information once, clear the **Auto Refresh** check box and click the **Refresh** button.

To manage UDS/SDS port connections:

1. On the menu, click **Ethernet Devices > UDS/SDS**. The Manage UDS/SDS Group page opens.
2. Click the **Port Access** tab. A list of all current UDS and SDS port connections displays, along with drop down lists of the unmanaged UDS/SDS ports.

Figure 9-38 Manage UDS/SDS Group - Port Access Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with fields for 'Table' (set to 'Ethernet Device'), 'Field' (set to 'Name'), and 'Value'. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main heading is 'Manage "UDS/SDS" Group'. Below this, there are tabs for 'List', 'Add', 'Traps', 'Actions', 'Port Access' (selected), 'Notes', and 'Help'. The 'Port Access' tab contains two rows of configuration fields: 'Device 1' and 'Device 2', both set to 'UDS2100 (172.19.39.244)'. 'Serial Port' is set to '1' for both. 'Port' is set to '10001' and 'Protocol' is set to 'TCP'. There is a 'Create' button for creating a new connection. Below this is a section for 'UDS to UDS Port Tunnel Configuration' with a table that currently has 0 items. The table has columns for 'Device 1', 'Device 1 Serial Port', 'Device 2', 'Device 2 Serial Port', 'Port', and 'Protocol'. There is a checkbox and a 'Delete' button for deleting checked connections.

To have the vSLM 2 software connect two UDS/SDS ports automatically:

1. Select Device 1 from the drop down list.
2. Select the Serial Port for Device 1.
3. Select Device 2 from the drop down list.
4. Select the Serial Port for Device 2.
5. Choose the port for the connection (defaults to 10001).
6. Select the Protocol (TCP or UDP).
7. Click on the **Create** button.

The vSLM 2 software will attempt to log into both UDS/SDS devices and set up the requested connection. vSLM 2 secure management software will be offered in a future release.

To delete a connection, check the box to the right of the connection to be terminated and click on the **Delete** button.

Updating Passwords in Bulk

The administrator and Ethernet device users can perform bulk password updates on multiple devices in the local database. These changes can also be pushed to remote SLM, SLC, RPM/SLP, and SCS05/20 devices.

- ◆ The user has access to the device.
- ◆ The current user ID on the device matches the Login field.
- ◆ The current password on the device matches the Current Password field.
- ◆ The device type matches one of the types selected on the page described below.

To perform a bulk password update:

1. On the menu, click **Ethernet Devices** and then the **Passwords** tab. The following page opens:

Figure 9-39 All Ethernet Devices Page - Passwords Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1F4F' with the role of 'Administrators'. The main navigation menu on the left includes 'Configuration', 'Accounts', 'Events', 'Files', 'Ethernet Devices', 'Device Locator', and various device types like SLM, SLC, SLK, RPM/SLP, SLB, Spider, SCS05/20, SCSxx00, WiBox, UDS/SDS, EDS, EDS-MD, XPort, Premier Wave, Other Lantronix, Non Lantronix, and Managed Devices. The 'All Ethernet Devices' page has tabs for 'List', 'Polling', 'Traps', 'Properties', 'Passwords', 'SNMP', 'SLM Proxy', 'Notes', and 'Help'. The 'Passwords' tab is active, displaying instructions for bulk password updates and a form with fields for 'Login', 'Current Password', 'New Password', and 'Retype Password'. There are also checkboxes for selecting device types: SLM, SLC, SLK, RPM/SLP, UDS/SDS, XPort, Spider, WiBox, Premier Wave, Other Lantronix, Non Lantronix, SCS05/20, EDS, and SCSxx00. A 'Push Password to Devices' checkbox is also present, with a note that it applies to SLM, SLC, RPM/SLP, SLB, SCS05/20, and Spider devices. 'Update' and 'Reset' buttons are at the bottom of the form.

2. Enter the following:

Table 9-40 Settings to Update Passwords in Bulk

Password Setting	Description
Login	Enter the login currently used by the devices whose password you want to change.
Current Password	Enter the password currently used by the devices whose password you want to change.
New Password and Retype Password	Enter a new password for accessing the devices.
SLM, SLC, SLK, RPM/SLP, SCS05/20, SCSxx00, SLB, Spider, WiBox, UDS/SDS, EDS, EDS-MD, XPort, PremierWave, Other Lantronix, Non Lantronix	Select the check box for each type of device whose password you want to change.
Push Passwords to Devices	Select the checkbox when you want to push the password change to remote SLM, SLC, RPM/SLP, and SCS05/20 devices.

3. Click the **Update** button. A confirmation message displays.

Changing SNMP Settings for SLC, SLB and RPM/SLP Devices in Bulk

For security reasons, some companies change SNMP communities frequently. The administrator can change the SNMP communities for multiple devices at the same time. To change the SNMP communities of an SLC, SLB or RPM/SLP device, the current user must be able to access it.

To perform a bulk SNMP update:

1. On the menu, click **Ethernet Devices** and then the **SNMP** tab. The following page opens:

Figure 9-41 All Ethernet Devices Page - SNMP Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main navigation menu on the left includes 'Configuration', 'Network Settings', 'Authentication', 'Services', 'Maintenance', 'Date & Time', 'SNMP & Syslog', 'Firmware Updates', 'Device Management', 'Auto Detect Devices', 'Accounts', 'Events', 'Files', 'Ethernet Devices', 'Device Locator', 'SLM', 'SLC', 'SLK', 'RPM/SLP', 'SLB', 'Spider', 'SCS05/20', 'SCSxx00', 'WiBox', 'UDS/SDS', 'EDS', 'EDS-MD', 'XPort', 'Premier Wave', 'Other Lantronix', 'Non Lantronix', and 'Managed Devices'. The 'Ethernet Devices' section is expanded, showing 'SLM', 'SLC', 'SLK', 'RPM/SLP', and 'SLB'. The 'SNMP' tab is selected in the top navigation bar. The main content area has a heading 'All Ethernet Devices' and a sub-heading 'Bulk SNMP Community update allows multiple SLC, SLB and RPM/SLP objects to have their read, write and/or trap communities changed with one command. For a device to have its SNMP communities changed it must be reachable by the current user.' Below this, there are three text input fields: 'SNMP Read Community:', 'SNMP Write Community:', and 'SNMP Trap Community:'. There is also a 'Push to all devices:' checkbox. At the bottom of the form are 'Update' and 'Reset' buttons.

2. Enter the following:

Table 9-42 Settings to Update SNMPs in Bulk

SNMP Setting	Description
SNMP Read Community	An SNMP community is the group to which devices and management stations running SNMP belong. The default setting is public. Because SSH-to-RPM/SLP authentication may take a long time, this setting allows the user to choose SNMP support, which is faster.
SNMP Write Community	A string that acts like a password for an SNMP manager to modify data where permitted.
SNMP Trap Community	A string that is sent along when a trap is broadcast. Only management devices that are listening for that value process the trap. Management devices that are not listening for that trap community ignore the trap.
Push to all devices	Select this check box to upload these SNMP settings to all devices of the same type (SLC, RPM/SLP, or SLB device) in the

3. Click the **Update** button. A confirmation message displays.

Note: To clear all values before saving, click the **Reset** button.

SLM Proxy

The vSLM 2 secure management software can act as a proxy server, allowing users outside the internal network to connect to devices securely through the vSLM 2 software. You can set most devices to connect through the vSLM 2 management software. The SLM proxy feature is not limited to connections between the vSLM 2 software's two Ethernet ports; the remote device can even be located on the same subnet as the client browser.

To use the vSLM 2 secure management software as a proxy server:

1. On the menu, click **Ethernet Devices**. The All Ethernet Devices page displays.
2. Click the **SLM Proxy** tab. The tab displays a list of all the Ethernet devices with a column for each method of connection.

Figure 9-43 All Ethernet Devices - vSLM 2 Proxy Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main heading is 'All Ethernet Devices' with tabs for List, Polling, Traps, Properties, Passwords, SNMP, SLM Proxy (selected), Notes, and Help. A sidebar on the left shows a tree view of the configuration menu, with 'Ethernet Devices' expanded. The main table lists various devices with their IP addresses and connection capabilities. At the bottom, there are 'Submit' and 'Reset' buttons.

Name	IP Address	Device Type	HTTP	HTTPS	Web Channel	Secure Channel	SSH	Telnet	TN3270
AP541N-A-K9	172.18.0.110	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
CiscoSwitch	172.19.39.40	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
ETS_2393F2	172.18.18.130	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
HPPProCurve2524	172.18.21.95	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Lantronix Tech Support Switch	172.18.0.106	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
linux20	172.19.39.20	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
linux21	172.19.39.21	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
linux22	172.19.39.22	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
linux242	172.19.242.1	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
NPI2A1A49	172.18.0.104	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
TEST1	172.19.39.23	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
TESTXP1	172.19.39.182	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
TN3270	128.227.128.75	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
tlabel	172.18.0.103	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
TSXPVIRTUAL	172.18.21.16	Non Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
?	172.19.100.6	Other Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
?	172.19.100.9	Other Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
?	172.19.100.42	Other Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
?	172.19.100.47	Other Lantronix	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Premier Wave EN	192.168.0.2	Premier Wave	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Premier Wave XN	172.19.100.12	Premier Wave	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Premier Wave XN	172.19.100.204	Premier Wave	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				

Three types of check boxes display on the page:

- ◆ Active check boxes in the HTTP and HTTPS columns
- ◆ Inactive selected check boxes indicate devices that are automatically set for proxy
- ◆ Inactive unselected check boxes indicate devices that cannot be set for proxy

- To enable a device to use the vSLM 2 software as a proxy in conjunction with HTTP or HTTPS, select the appropriate checkbox.

Note: You may select **Proxy** in conjunction with these protocols and others on the configuration page for an individual device.

Ethernet Device Commands

set ethernetdevice add

Syntax

```
set ethernetdevice add <New Device Name> mac <MAC> ipaddr <IP Address>
  type <slm|slc|slc80xx|slk|rpm|slb|spider|scs0520|scsxx00|
  wibox|uds|eds|edsmd|xport|pwave|other|non>
  [model <Model of Device>]
  [portcount <comma separated # of ports on each unit>] (default 0)
```

Examples

To add a new SLC with 16 ports:

```
set eth add DeviceName mac 11:22:33:44:55:66 ipaddr 172.19.220.64
type slc portcount 16
```

To add a new RPM with 16 ports on master and 8 ports on 3 expansion units:

```
set eth add DeviceName mac 11:22:33:44:55:66 ipaddr 172.19.220.64
type rpm portcount 16,8,8,8 model "Sentry4 STV-6502M"
```

Description

Create a new ethernet device and optional ports.

set ethernetdevice assign

Syntax

```
set ethernetdevice assign <Device Name|IP Address> group
<ethernetDeviceGroup> [remove]
```

Examples

```
set eth assign SLC-19 group Eth-Users-1
set eth assign 172.19.220.64 group Eth-Users-3 remove
```

Description

Assigns or removes permissions for an Ethernet device by name.

set ethernetdevice config**Syntax**

```
set ethernetdevice config <Device Name or IP Address> <one or more
parameters>
```

Parameters

```
[delete]
[dialout <Dial Account Name|enable|disable> phonenumber <phone number>]
[disconnect modem]
[name <Device Name>]
[mac <MAC address>]
[ipaddr <IP Address>]
[location <Location|CLEAR>]
[sublocation <Sub-Location|CLEAR>]
[login <Loginname>]
[model <Model>]
[readinfo]
[sshport <TCP Port for SSH>]
[tnport < TCP Port for Telnet>]
[tn3270lu <Logical Unit>]
[version <Version>]
```

Examples

To refresh SLC database info from device:

```
set eth config slc-device readinfo
```

Description

Finds Ethernet devices by device name or IP address and modifies device parameters.

set ethernetdevice delete**Syntax**

```
set ethernetdevice delete <Device Name or IP Address>
[portnumber <port number or port number range>]
port number range: for example: 1-4
```

Examples

```
set eth delete slc-waimea
set eth delete slc-waimea port 5
set eth delete slc-waimea port 1-5
set eth conf slc-waimea delete
```

Description

Finds a port by ethernet device name or IP address with port number, or just IP address and deletes it.

set ethernetdevice port

Syntax

```
set ethernetdevice port <Device Name or IP Address> portnumber <Port Number> <one or more parameters>
```

Parameters

```
[name <New Port Name>]
```

```
[state <on|off|cyclepower>] (available for RPM/SLP, SLB and Spider Duo® devices only)
```

Powers Ethernet device port on or off.

Examples

To power up an RPM/SLP outlet 2:

```
set eth port slp-sunset po 2 state on
```

You may specify a comma separated outlet list to control multiple outlet at once.

To power up an RPM/SLP outlet port list 1-3,6,8-14:

```
set eth port slp-sunset po 1-3,6,8-14 state on
```

Description

Finds a port by device name or IP address with the port number and modifies port parameters.

set ethernetdevice sync

Syntax

```
set ethernetdevice sync <Device Name or IP Address>
```

Parameters

```
set ethernetdevice sync <Device Name or IP Address> action <read|write>
```

Description

Finds an Ethernet device using device name or IP address and synchronizes device information.

show device

Note: Entries are not case sensitive.

Syntax

```
show device <device name>
```

Description

Searches for and displays Ethernet or managed devices by device name and displays device information.

show device all**Syntax**

```
show device all
show device index <number>
```

Description

Displays all Ethernet and managed devices.

show ethernetdevice account**Syntax**

```
show ethernetdevice account <accountName>
```

Description

Displays all Ethernet devices viewable by the specified user account.

show ethernetdevice accountgroup**Syntax**

```
show ethernetdevice accountgroup <accountGroup>
```

Description

Displays all Ethernet devices viewable by users whose accounts belong to the specified account group.

show ethernetdevice all**Syntax**

```
show ethernetdevice all
```

Description

Displays all Ethernet device information.

show ethernetdevice config**Syntax**

```
show ethernetdevice config <Device Name or IP Address>
```

Description

Finds an Ethernet device using device name or IP address and displays device information.

show ethernetdevice firmware**Syntax**

```
show ethernetdevice firmware
```

Description

Displays firmware versions of all Ethernet devices managed by the vSLM 2 software.

show ethernetdevice group**Syntax**

```
show ethernetdevice group <Group Name> [firmware]
group name: SLM, SLC, SLK, RPM, SCS, SCSX, SLB, SPDR, WiBox, UDS, EDS,
EDSMD, Xport, PWave, other, non
```

Note: Ethernet device group names are not case sensitive.

Description

Displays Ethernet devices by device group.

show ethernetdevice index**Syntax**

```
show ethernetdevice index <number>
```

Description

Displays Ethernet devices by index.

show ethernetdevice port**Syntax**

```
show ethernetdevice port <Device Name or IP Address> all
show ethernetdevice port <Device Name or IP Address> portnumber
<Port Number>
```

Description

Finds an Ethernet device using device name or IP address and displays port information.

show ethernetdevice search device**Syntax**

```
show ethernetdevice search device <one or more parameters>
```

Parameters

```
[name <Device Name>]
[ipaddr <IP Address>]
[location <location>] [firmware <version number>]
```

Note: Search entries are not case sensitive.

Example

```
show ethernetdevice search device name slc firmware 4
```

Description

Displays all devices that match the criteria entered. For example, if you specify `name slc`, the vSLM 2 secure management software searches for all devices whose name starts with `slc`.

Persistent Connection Commands

set persistent add

Syntax

```
set persistent add <persistentConnectionName> ethernetdevice
<ethernetDeviceName|IP>
```

Parameters

```
[protocol <Secure|SSH|Telnet|TN3270>] (default SSH)
[logging <enable|disable>] (default disable)
[managed <enable|disable>] (default enable)
[active <enable|disable>] (default enable)
[parentlogin <enable|disable>] (default disable)
[login <loginAccount>]
[password <loginPassword>]
[prompt <promptString>]
[application <applicationName>]
[escapesequence <escapeString>] (default is '\x1BC')
[reconnectdelay <1-999>] (default is 1)
[eoltranslation <cr | lf>]
```

Description

Creates a new persistent connection.

set persistent edit

Syntax

```
set persistent edit <persistentConnectionName>
```

Parameters

```
[ethernetdevice <ethernetDeviceName|IP>]
[protocol <Secure|SSH|Telnet|TN3270>]
[logging <enable|disable>]
[managed <enable|disable>]
[active <enable|disable>]
[parentlogin <enable|disable>]
[login <loginAccount>]
[password <loginPassword>]
[prompt <promptString>]
[application <applicationName>]
[escapesequence <escapeString>]
[reconnectdelay <1-999>]
[eoltranslation <cr | lf>]
```

Note: For the edit command, the ethernetdevice parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name.

Description

Modifies an existing persistent connection.

set persistent delete

Syntax

```
set persistent delete <persistentConnectionName> [ethernetdevice  
<ethernetDeviceName|IP>]
```

Note: For the delete command, the `ethernetdevice` parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name.

Description

Deletes a persistent connection.

show persistent

Syntax

```
show persistent [[name] <persistentConnectionName>][device  
<devname|IP>][all]
```

Notes:

- ◆ The `device` parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name.
- ◆ The `<devname>` following device may be the name of an Ethernet device or the name of a managed device. Persistent connections automatically belong to managed devices that have an Ethernet device component that has persistent connections defined.

Description

Displays one or more persistent connections.

connect persistent

Syntax

```
connect persistent <persistentConnectionName> [device <devname|IP>]
```

Notes:

- ◆ The `device` parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name.
- ◆ The `<devname>` following device may be the name of an Ethernet device or the name of a managed device. Persistent connections automatically belong to managed devices that have an Ethernet device component that has persistent connections defined.

Description

Connect to an existing persistent connection.

Trap Commands

show traplog index

Syntax

```
show traplog <number> <parameters>
```

Syntax

```
[device <Device Name or IP Address>]
[group <group name>]
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
group name: SLM, SLC, SLK, RPM, SCS, SLB, SPDR, WiBox, LTRX or other.
```

Examples

```
show traplog
```

List of traplog files.

```
show traplog lastminutes 5
```

List traplog files modified in last 5 minutes.

```
show traplog date 0205
```

List traplog files last modified on 0205.

```
show traplog date 0205-0209
```

List traplog files last modified between 0205 and 0209.

```
show traplog index 3
```

Display the specified traplog from top.

```
show traplog index 3 top 10
```

Display the first 10 lines of specified traplog from top.

```
show traplog index 3 tail 15
```

Display the last 15 lines of specified traplog from tail.

```
show traplog index 3 lastminutes 5
```

Display traplog by the index '3'.

To get this index, type 'show traplog lastminutes 5'.

```
show traplog index 3 date 0205
```

Display traplog by the index '3'.

To get this index, type 'show traplog date 0205'.

```
show traplog index 3 date 0205-0209
```

Display traplog by the index '3'.

To get this index, type 'show traplog date 0205-0209'.

```
show traplog index 3 top 10 lastminutes 5
```

Display the first 10 lines of traplog by the index '3'.

To get this index, type 'show traplog lastminutes 5'.

```
show traplog index 3 tail 0 lastminutes 5
```

Display the traplog by the index '3' from tail.

To get this index, type 'show traplog lastminutes 5'.

Description

Displays all current trap log information. The index number displays detailed information about a selected traplog.

show traplog device

Note: Type `show traplog` to display the index.

Syntax

```
show traplog device <Device Name or IP address> [index <number>]
```

Description

Displays the current trap log information for an Ethernet device using device name, IP address, or index number.

show traplog group

Note: Type `show traplog group` to display the index.

Syntax

```
show traplog group <Device Group Name>  
Group name: SLM, SLC, SLK, RPM, SCS, SCSX, SLB, SPDR, WiBox, UDS, EDS,  
EDSMD, Xport, PWave, other, non
```

Description

Displays the current trap log information for an Ethernet device group by index number.

Ports

Administrators and Ethernet device users with rights to an Ethernet device can list, add, update, delete, and interact with its ports. Managed Device users can only interact with managed devices (which may manage one or more ports, and/or a local Ethernet device) that they have permissions on.

Note: Port pages may differ slightly, depending on the type of Ethernet device. The procedures below note these differences.

Viewing a List of Ports

You can view a list of all ports on any Ethernet device that has ports (e.g., SLC, SLK, RPM/SLP, or other devices).

To view port information:

1. On the Device page for the Ethernet device, click the **Ports** tab. The following page opens.

Figure 9-44 Device - Ports Tab

The screenshot displays the LANTRONIX SLM web interface. At the top, the user is logged in as 'sysadmin@SLM1F4F' with the role of 'Administrators'. The main content area is titled 'Device "misc8048"' and features a 'Ports' tab. A table lists 48 ports, each with a 'Name' (e.g., Port-1 to Port-48), 'Port Number', 'Console' (all 'misc8048'), 'Log Enabled' status (all 'No'), 'Log Time Frame' (all '30'), 'Max Log Size (KB)' (all '256'), and 'Byte Threshold' (all '1024'). A sidebar on the left shows a tree view of the device's configuration, with 'misc8048 (172.18.21.61)' selected under 'Ethernet Devices'. At the bottom, there are controls for 'Create Managed Devices' and 'Add Port'.

Name	Port Number	Console	Log Enabled	Log Time Frame	Max Log Size (KB)	Byte Threshold
Port-1	1	misc8048	No	30	256	1024
Port-2	2	misc8048	No	30	256	1024
Port-3	3	misc8048	No	30	256	1024
Port-4	4	misc8048	No	30	256	1024
Port-5	5	misc8048	No	30	256	1024
Port-6	6	misc8048	No	30	256	1024
Port-7	7	misc8048	No	30	256	1024
Port-8	8	misc8048	No	30	256	1024
Port-9	9	misc8048	No	30	256	1024
Port-10	10	misc8048	No	30	256	1024
Port-11	11	misc8048	No	30	256	1024
Port-12	12	misc8048	No	30	256	1024
Port-13	13	misc8048	No	30	256	1024
Port-14	14	misc8048	No	30	256	1024
Port-15	15	misc8048	No	30	256	1024
Port-16	16	misc8048	No	30	256	1024
Port-17	17	misc8048	No	30	256	1024
Port-18	18	misc8048	No	30	256	1024
Port-19	19	misc8048	No	30	256	1024
Port-20	20	misc8048	No	30	256	1024
Port-21	21	misc8048	No	30	256	1024
Port-22	22	misc8048	No	30	256	1024
Port-23	23	misc8048	No	30	256	1024
Port-24	24	misc8048	No	30	256	1024
Port-25	25	misc8048	No	30	256	1024
Port-26	26	misc8048	No	30	256	1024
Port-27	27	misc8048	No	30	256	1024
Port-28	28	misc8048	No	30	256	1024
Port-29	29	misc8048	No	30	256	1024
Port-30	30	misc8048	No	30	256	1024
Port-31	31	misc8048	No	30	256	1024
Port-32	32	misc8048	No	30	256	1024
Port-33	33	misc8048	No	30	256	1024
Port-34	34	misc8048	No	30	256	1024
Port-35	35	misc8048	No	30	256	1024
Port-36	36	misc8048	No	30	256	1024
Port-37	37	misc8048	No	30	256	1024
Port-38	38	misc8048	No	30	256	1024
Port-39	39	misc8048	No	30	256	1024
Port-40	40	misc8048	No	30	256	1024
Port-41	41	misc8048	No	30	256	1024
Port-42	42	misc8048	No	30	256	1024
Port-43	43	misc8048	No	30	256	1024
Port-44	44	misc8048	No	30	256	1024
Port-45	45	misc8048	No	30	256	1024
Port-46	46	misc8048	No	30	256	1024
Port-47	47	misc8048	No	30	256	1024
Port-48	48	misc8048	No	30	256	1024

- View the following information about each port:

Table 9-45 Device - Ports Tab

Port Setting	Description
Name	Name of the Ethernet device port.
Port Number	Number of the Ethernet device port (e.g., a number between 1 and 48 for the SLC 48 device).
Console	Name of the parent Ethernet device.
Log Enabled	Indicates whether logging has been enabled for this port. <i>Note:</i> To enable or disable port logging for one or more ports, select the check box for each affected port, and select Enable Port Logging or Disable Port Logging from the drop-down list at the bottom of the page. Only SLC devices that have established a secure channel connection can have ports with logging enabled.
Log Time Frame	For SLC v3.1 and later v3.x (but not v4.0): The maximum time frame in hours before a new log file is created. The default setting is 1 hour. For SLC v4.0 and later: The maximum time frame in seconds before the SLC console manager sends data to the vSLM 2 software. The default is 30 seconds.
Max Log Size (KB)	Maximum size of each log file in kilobytes. Once it is reached, a new log file is created. The default setting is 256 KB.
Byte Threshold	For SLC v4.0 and later: The number of bytes the SLC device port receives before it forwards them to the vSLM 2 software. For example, a threshold preset at 128 characters means that as soon as the SLC console manager receives 128 bytes of data on this particular device port, it captures log data and sends it to the vSLM 2 secure management software. The minimum byte threshold is 1, and the default is 1024.
Port Status (RPM/SLP and SLB only)	Indicates whether the port's power is on or off.

Adding a Port

Administrators and Ethernet device users with rights to a device may add ports to that device. This is useful when a device does not automatically report port information.

To add a port:

Notes:

- ◆ The example below shows how to add an SLC port. Ports on other devices do not require extra port information such as baud and flow control).
- ◆ During auto detect, if an SLC device does not have SNMP enabled, it will not retrieve these extra SLC port parameters. Then this SLC device is marked with an internal flag to indicate that those port parameters are incorrect. When this flag is set, the user cannot perform a "Write info to device" as this would push incorrect port settings back to the SLC device. This flag is cleared if the user did a "Read info from device" or manually modified one of the SLC device port settings. After this flag is cleared, the user can perform "Write info to device."

- On the **Ports** tab of the Device page, click the **Add Port** button at the bottom. The following page opens:

Figure 9-46 New SLC Port Page - Configure Tab

Note: The connection buttons on the right are inactive until you save the port. See [Connecting to Ethernet and Managed Devices \(on page 237\)](#) for instructions on using the buttons.)

2. Enter the following information:

Table 9-47 New Port - Configure Tab

Port Setting	Description
Port Number	Number of the Ethernet device's port (e.g., a number between 1 and 48 for the SLC 48 device). The system offers all unassigned ports up to 16 above the current highest port number.
Parent Ethernet Device (view only)	Name of the Ethernet device.
Name	Name of the port (e.g., name of the device to which it is attached).
Parent Device Type (view only)	Ethernet device type (e.g., SLC, SLM, SLK devices).

Port Setting	Description
Log Enabled	Indicates whether logging is enabled on the port. Disabled by default. <i>Note:</i> To enable or disable port logging for one or more ports, select the check box for each affected port, and select Enable Port Logging or Disable Port Logging from the drop-down list at the bottom of the page. Only SLC/SLB devices that have established a secure channel connection can have ports with logging enabled.
Log Time Frame	For SLC v3.1 and later v3.x (but not v4.0): The maximum time frame in hours before a new log file is created. The default setting is 1 hour. For SLC v4.0 and later: The maximum time frame in seconds before the SLC console manager sends data to the vSLM 2 software. The default setting is 30 seconds.
Max Log Size (KB)	Maximum size of each log file in kilobytes. Once it is reached, a new log file is created. The default setting is 256 KB .
Byte Threshold	For SLC v4.0 and later: This is the number of bytes the SLC device port receives before it forwards them to the vSLM 2 software. For example, a threshold preset at 128 characters means that as soon as the SLC console manager receives 128 bytes of data on this particular device port, it captures log data and sends the received data regarding this device port to the vSLM 2 secure management software. The minimum byte threshold is 1, and the default is 1024 .
Receiving SLM(s)	An SLC port can log its port data to one, two, or three SLM units at the same time. This field shows the IP address(es) of any SLM management appliance(s) that are receiving log data from this particular SLC port. These IP addresses need not necessarily include the SLM unit you are looking at.
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 .
Managed Device	Not active when you are adding a port.

Table 9-48 New Port - Configure Tab - Data Settings

Data Setting	Description
Baud	The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate.
Data Bits	Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is 8 data bits.
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.

Data Setting	Description
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. Disabled is the default and is the correct setting if the device port is the endpoint for a connection.

Table 9-49 New Port - Configure Tab - Hardware Signal Triggers

Hardware Signal Trigger Setting	Description
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.
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.

Table 9-50 New Port - Configure Tab - IP Settings

IP Setting	Description
Enable Telnet In	Enables access to this port through Telnet. Disabled by default.
Enable SSH In	Enables access to this port through SSH. Disabled by default.
Enable TCP in	Enables access to this port through a raw TCP connection. Disabled by default. <i>Note: When using raw TCP connections to transmit binary data, or where the break command (escape sequence) is not required, clear the Break Sequence of the respective device port.</i>
Port	Automatically assigned Telnet, SSH, and TCP port numbers. You may override this value, if desired.
Authenticate	If selected, the vSLM 2 software requires user authentication before granting access to the port.
Terminal Rows	Value to use when creating a terminal window (by Java applet) to that port.
Terminal Columns	Value to use when creating a terminal window (by Java applet) to that port.

- Click the **Add** button. A confirmation message displays, and the port is now listed below the Ethernet device on the menu tree.

Updating or Deleting a Port

Administrators and permitted Ethernet Device Account groups can update or delete a port.

To delete a port:

- On the device's **Ports** tab, click the **Edit**  icon to the left of the port name,
OR
On the device's menu tree, select the port.

The following page opens:

Figure 9-51 Port Page - Configure Tab

Note: The page below shows an SLC port. Devices other than the SLC console manager do not display as much information.

2. Click the **Delete** button.
3. In response to the request for confirmation, click **OK**. A message confirming the deletion displays.

The deleted port is no longer listed on the Ethernet device's menu tree or on the device's **Ports** tab.

To update a port:

1. Add or update information as desired. In addition to the fields completed when adding a port, complete the following fields:

Table 9-52 Port - Configure Tab

Port Setting	Description
Managed Device	If desired, create a managed device from the port. See Creating Individual Managed Devices (on page 207) . Note: This field is unavailable if no Managed Device Groups exist in the system.

Port Setting	Description
TCP Port for Terminal (SCS and RPM/SLP)	Port number to use when establishing a Telnet connection via that port. A value of zero means use the default port (which is 23); otherwise use the entered value.

2. Click the **Update** button. When the update is complete, a confirmation message displays.

Note: Port configuration fields differ depending on the parent device type.

Connecting Directly to the Port of an SLC or SLB Device

You can get quick secure channel access to any port on any SLC (or SLB) device.

To gain quick secure channel access to an SLC port:

1. On the Manage SLC Group Page, click the **Port Access** tab. The following page displays:

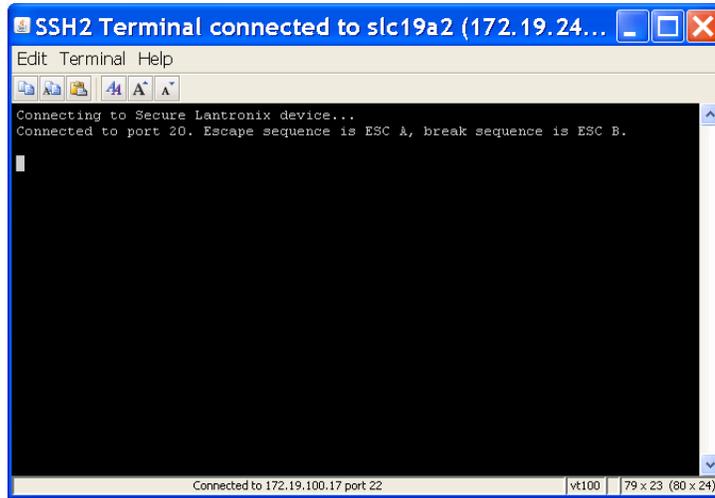
Figure 9-53 Manage SLC Group Page - Port Access Page

The screenshot displays the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1F4F' with the role of 'Administrators'. The main content area is titled 'Manage "SLC" Group' and has several tabs: 'List', 'Add', 'Traps', 'Actions', 'Port Access' (selected), 'Notes', and 'Help'. On the left, a sidebar shows a tree view of the device hierarchy, including 'Ethernet Devices', 'SLM', and 'SLC'. The main table lists SLC devices with their IP addresses and a grid of port access buttons (1-48) for each device. The buttons are color-coded: green for active/available and red for unavailable. At the bottom, there is an 'Auto Refresh' checkbox and a 'Refresh' button.

Device Name	IP Address	Port Access Grid
mllslc48	172.18.21.66	Grid of 48 ports (1-48) in 2 rows of 24.
mllslc8048	172.18.21.61	Grid of 48 ports (1-48) in 2 rows of 24.
slbdb40	172.19.39.253	Grid of 8 ports (1-8) in 2 rows of 4.
slc16_glenn	172.19.39.254	Grid of 16 ports (1-16) in 2 rows of 8.
slc4331	172.19.250.119	Grid of 48 ports (1-48) in 2 rows of 24.
slc4657	172.19.213.8	Grid of 48 ports (1-48) in 2 rows of 24.
slc48_glenn_1	172.19.100.90	Grid of 48 ports (1-48) in 2 rows of 24.
slc5e35	172.19.100.116	Grid of 16 ports (1-16) in 2 rows of 8.
slca508	172.19.250.120	Grid of 48 ports (1-48) in 2 rows of 24.
slc-md-u	172.19.100.125	Grid of 48 ports (1-48) in 2 rows of 24.
slcRef250120	172.19.100.221	Grid of 48 ports (1-48) in 2 rows of 24.
slcRefreshR17_167	172.19.250.167	Grid of 32 ports (1-32) in 2 rows of 16.
tsslsc32	172.18.0.107	Grid of 32 ports (1-32) in 2 rows of 16.

2. Click the desired port on the specific SLC console manager. The following page displays:

Figure 9-54 Connection to Selected SLC Port



Statistics

Users authorized to view or interact with the port may view status and statistics about it.

To view port status and statistics:

1. On the Port page, click the **Statistics** tab. The following page opens:

Figure 9-55 Port Page - Statistics Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1C77' with the group 'Administrators'. The main content area is titled 'Port "SLC-Port-1"' and has tabs for 'Configure', 'Statistics', 'Logs', 'Display', 'Notes', and 'Help'. The 'Statistics' tab is active, showing a table titled 'Port Status and Counters'.

Port Status and Counters			
DSR/CD	No	Bytes input	0
DTR	Yes	Bytes output	3
CTS	No	Framing errors	0
RTS	Yes	Parity errors	0
		Overrun errors	0
Seconds since zeroed	13604623	Flow Control errors	0

Below the table, there is a 'Refresh' button and a 'Clear port counters' checkbox.

The page displays port status and counters.

2. To see the current statistics, click the **Refresh** button.
3. To clear the port counters, select the **Clear** port counters check box and click the **Refresh** button.

Applying Power to RPM/SLP Ports on a Single Device

You can power on, power off, or cycle power on multiple ports on an RPM/SLP power manager.

To manage power on multiple ports of an RPM/SLP module:

1. On the RPM/SLP power manager's Device page, click the **Ports** tab. The following page opens:

Figure 9-56 RPM/SLP Power Manager's Device Page - Ports Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device' and 'Field: Name'. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main content area is titled 'Device "SecureLinuxSLP_8b0133"' and has several tabs: 'Configure', 'Ports', 'PerCons', 'LocalCons', 'Utilities', 'Display', 'Traps', 'Modem', 'Notes', and 'Help'. The 'Ports' tab is active, displaying a table with 16 rows of port information. The table columns are: Name, Port Number, Console, Log Enabled, Log Time Frame, Max Log Size (KB), Byte Threshold, and Port Status. The 'Port Status' column shows 'On/-0.01 amps' for all ports. At the bottom of the table, there is a dropdown menu for 'Create Managed Devices' set to 'mgroup_1', an 'Update' button, and an 'Add Port' button.

Name	Port Number	Console	Log Enabled	Log Time Frame	Max Log Size (KB)	Byte Threshold	Port Status
3ComSuperStack	1	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
SLC32	2	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
SunNetraX1	3	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
SLK16	4	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
TSSLM	5	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
Conservar	6	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
TSFTP	7	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
TSWIN200810	8	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
TSWIN200811	9	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
Update	10	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
Sunfire280R	11	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
DSC	12	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
Outlet13	13	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
Outlet14	14	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
SLBDemo	15	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps
Spider	16	SecureLinuxSLP_8b0133	No	0	0	0	On/-0.01 amps

2. Select the ports whose power you want to power on, power off, or cycle.
3. From the drop-down list at the bottom of the page, select the action you want to take (**Power On, Power Off, or Cycle Power**).
4. Click the **Update** button.

Viewing Port Logs

Depending on the type of device, you can view one or more port and session logs on the Port page.

To view logs:

1. On the Port page, click the **Logs** tab. The following page displays:

Figure 9-57 Port Page - Logs Tab

2. To view a log, select the log from the appropriate drop-down list:

Note: The SLC console manager enables you to view three types of logs, while other devices enable you to view only the current session.

Table 9-58 Port - Logs Tab

Port Log Setting	Description
SLC/SLB Portlog	Select the log of this particular SLC or SLB device port.
SLC/SLB Port Active	Select the log of a currently active vSLM 2 user session to the port.
SLC/SLB Port Saved	Select a session log of a saved vSLM 2 user session to the port.

3. Click the **View** button. The log displays on the **Display** tab.

Port Commands

set ethernetdevice port

Syntax

```
set ethernetdevice port <Device Name or IP Address> portnumber <Port Number> <one or more parameters>
```

Parameters

[name <Port Name>]

[<on|off|cyclepower>] (available for RPM/SLP power manager only)

Powers Ethernet device port on or off.

Example

To power up an RPM/SLP outlet 2:

```
set eth port slp-sunset po 2 state on
```

You may specify a comma separated outlet list to control multiple outlet at once.

To power up an RPM/SLP outlet port list 1-3,6,8-14:

```
set eth port slp-sunset po 1-3,6,8-14 state on
```

Description

Finds a port by device name or IP address with the port number and modifies port parameters.

show ethernetdevice port

Syntax

```
show ethernetdevice port <Device Name or IP Address> all
show ethernetdevice port <Device Name or IP Address> portnumber
<Port Number>
```

Description

Finds an Ethernet device using device name or IP address and displays port information.

show port

Syntax

```
show port <name>
```

Type `show port all` to display index.

Example

`show port slc` displays all Ethernet ports whose name starts with "slc."

Description

Searches Ethernet ports by port name and displays port information.

show port all

Syntax

```
show port all  
show port
```

Displays all Ethernet ports.

show port index

Note: Type `show port all` to display index.

Syntax

```
show port index <number>
```

Description

Displays Ethernet ports by index.

10: Managed Devices

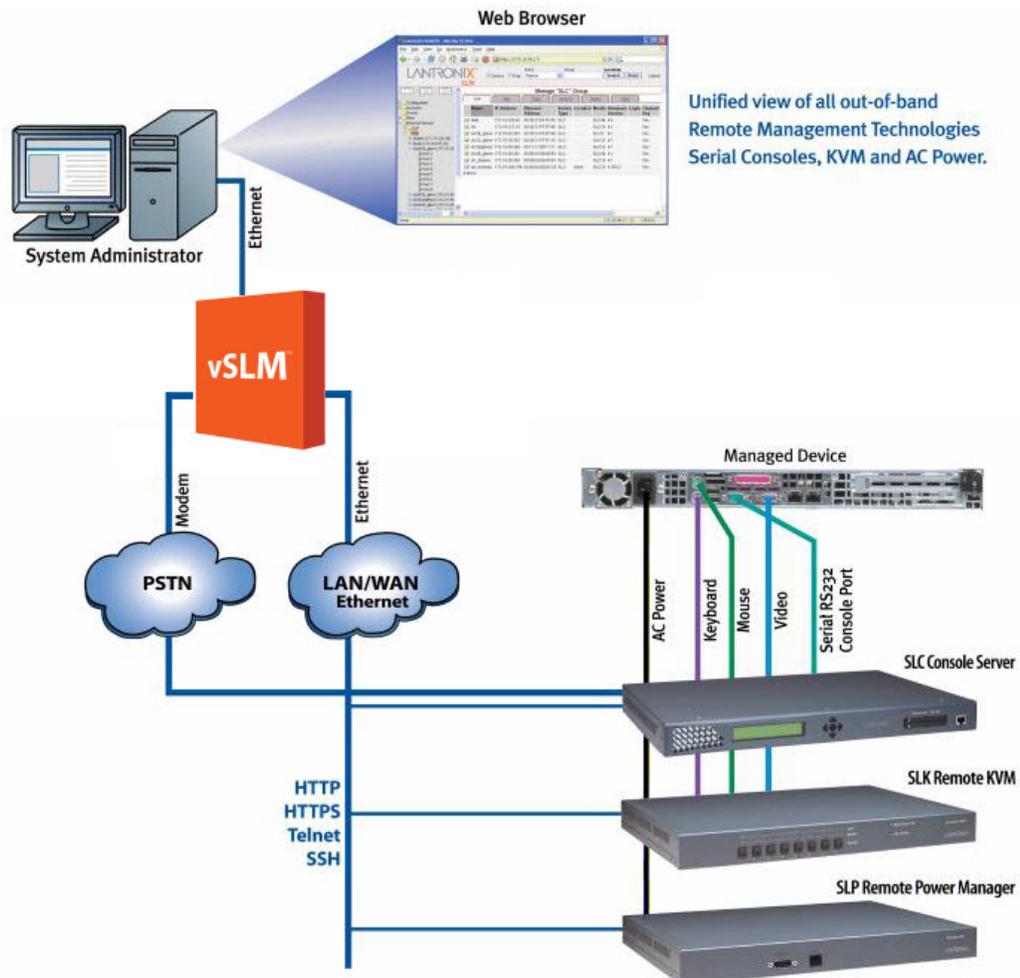
The vSLM 2 secure management software can treat any device connected to a port or connected to the local network as a managed device. Furthermore, multiple managed device objects in the system may be fused into a single managed device to streamline managed device operations and access.

For example, a single device (e.g., a UNIX server) may be connected to an SLC console manager by a serial port, to an RPM/SLP power manager by a power connector, and to an SLK remote KVM manager by a KVM port. You could manage these three individual managed devices separately. However, if you fuse the individual managed devices into one virtual managed device, you can then manage the SLC, RPM/SLP, and SLK connections from a single vSLM 2 web page.

Each virtual managed device in the vSLM 2 system can include a connection to to:

- ◆ 1 SLC or SLB serial port
- ◆ 1 SLK or Spider KVM port
- ◆ 2 RPM/SLP or SLB power ports
- ◆ 1 local Ethernet device

Figure 10-1 Virtual Managed Device



To create individual managed devices and fuse individual devices into a virtual managed device, you have the following options:

- ◆ **On the Port or Device Page:** Create a new managed device or fuse a new managed device into an existing managed device.
- ◆ **On the Ports Page:** Create one or more managed devices at the same time.
- ◆ **On the Managed Device Group Page:** Select two or more individual managed devices and fuse them to create a virtual managed device.

Managed Device Groups

Managed devices are assigned to Managed Device Groups so that users can easily locate them.

Administrators, authorized Ethernet Device Account group users, and authorized Managed Device Account Group users can organize the devices attached to Ethernet ports into groups. For example, an administrator may want to create groups by location, type of device, or user. A Managed Device Group may include devices attached to the ports of several different Ethernet devices.

The administrator creates custom groups of managed devices and then assigns individual devices to the groups. For example, a group called Lab 1 might include all devices attached to the ports of Ethernet devices being tested. The administrator and permitted users can delete a Managed Device Group.

Viewing All Managed Devices

You can view a list all managed devices in the system.

To view all managed devices:

1. On the menu, click **Managed Devices**. The Devices tab on the Managed Device Groups page opens.

Figure 10-2 Managed Device Groups Page - Devices Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. Below the search bar, the page title is 'Managed Device Groups'. The main content area is a table with the following columns: Name, Serial Port, Power Port 1, Power Port 2, KVM Port, Device, Managed Device Type, Managed Group, Modem, Connection, Modem App, Phone, Poll, and Reachable. The table contains 14 rows of device information. At the bottom of the table, it says '14 items' and 'Delete checked managed devices: [Delete]'. The left sidebar shows a navigation menu with 'Managed Device' selected.

Name	Serial Port	Power Port 1	Power Port 2	KVM Port	Device	Managed Device Type	Managed Group	Modem	Connection	Modem App	Phone	Poll	Reachable
CiscoSwitch	Device-1	PowerOutlet-2	PowerOutlet-3		CiscoSwitch	Unknown	mgroup_2			None	No	No	<input type="checkbox"/>
MD-linux20	slcPort-1	PowerOutlet-1	Glenn-PowerOutlet-5	TS-1	linux20	Unknown	mgroup_1			None	No	No	<input type="checkbox"/>
MD-linux21	slcPort-1	PowerOutlet-2	Glenn-PowerOutlet-6	SLS-KVM-1	linux21	Unknown	mgroup_2			None	No	No	<input type="checkbox"/>
MD-linux22	slcPort-1	PowerOutlet-3	Glenn-PowerOutlet-7	SLS-KVM-1	linux22	Unknown	mgroup_3			None	No	No	<input type="checkbox"/>
MD-linux242	slcPort-1	PowerOutlet-4	Glenn-PowerOutlet-8	SLS Duo-KVM-1	linux242	Unknown	mgroup_4			None	No	No	<input type="checkbox"/>
MD-PowerOutlet-1		PowerOutlet-1				Unknown	mgroup_1			None	No	No	<input type="checkbox"/>
MD-PowerOutlet-2		SLC8008PowerOutlet-2				Unknown	mgroup_1			None	No	No	<input type="checkbox"/>
MD-PowerOutlet-3		SLC8024PowerOutlet-3				Unknown	mgroup_1			None	No	No	<input type="checkbox"/>
MD-PowerOutlet-4		PowerOutlet-4				Unknown	mgroup_1			None	No	No	<input type="checkbox"/>
MD-PowerOutlet-5		PowerOutlet-5				Unknown	mgroup_1			None	No	No	<input type="checkbox"/>
MD-PowerOutlet-6		PowerOutlet-6				Unknown	mgroup_1			None	No	No	<input type="checkbox"/>
MD-PowerOutlet-7		PowerOutlet-7				Unknown	mgroup_1			None	No	No	<input type="checkbox"/>
MD-PowerOutlet-8		PowerOutlet-8				Unknown	mgroup_1			None	No	No	<input type="checkbox"/>
TSXPVIRTUAL	Port-6	PowerOutlet-3	PowerOutlet-4		TSXPVIRTUAL	Unknown	mgroup_7			None	No	No	<input type="checkbox"/>

2. View the following information about each managed device:

Table 10-3 Managed Device Groups - Devices Tab

Managed Device Setting	Description
Name	Name of the managed device.
Serial Port	Name of an SLC or SCS serial port that is connected to this managed device.
Power Port 1	Name of an RPM/SLP power port that is connected to this managed device.
Power Port 2	Name of an RPM/SLP power port that is connected to this managed device.
KVM Port	Name of a SLK or Spider KVM port that is connected to this managed device.
Device	Name of a local Ethernet device.
Managed Device Type	Type of managed device (e.g., Solaris Server or Linux Server). <i>Note: If the managed device type is set to Windows, a Remote Desktop option becomes available. If set to Linux Server, the a VNC option becomes available.</i>
Managed Group	Name of the Managed Device Group to which the managed device belongs.
Modem	Name of the modem (if any) to be used when connecting to the managed device.
Connection	Name of the connection to be used with modem access.
Modem App	Application to invoke for the connection (e.g., Secure Channel, SSH, Telnet).
Phone	Telephone number of the modem on the managed device.
Poll	Indicates whether to check the managed device for modem connectivity during modem polling testing.
Reachable	Indicates whether a connection to the modem on this managed device was successful the last time it was tested.

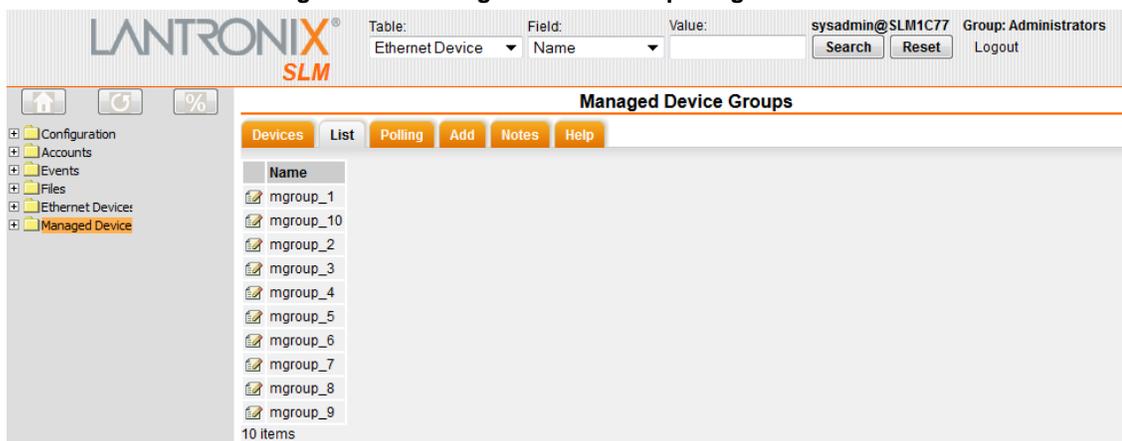
Viewing Managed Device Groups

You can view a list of all the Managed Device Groups and view devices by group.

To view a list of Managed Device Groups:

On the menu, click a device under **Managed Devices**, and then click the **List** tab. The following page opens:

Figure 10-4 Managed Device Groups Page - List Tab



To view a list of devices belonging to a Managed Device Group:

1. On the menu tree, click the name of the device group. The following page opens:

Figure 10-5 Managed Device Group Page - List Tab

2. View the information about each device:

Adding a Managed Device Group

The administrator creates custom groups of managed devices and then assigns individual devices to the groups. For example, a group might include all devices attached to the ports of Ethernet devices being tested.

To add a Managed Device Group:

1. On the menu, click **Managed Devices**, and then click the **Add** tab. The following page opens:

Figure 10-6 New Managed Device Group Page - Configure Tab

2. In the **Name** field, enter the name of the Managed Device Group.
3. Click the **Add** button.
4. Expand **Managed Devices** on the menu tree. The custom group displays as a folder.

Note: A managed device may belong to only one Managed Device Group.

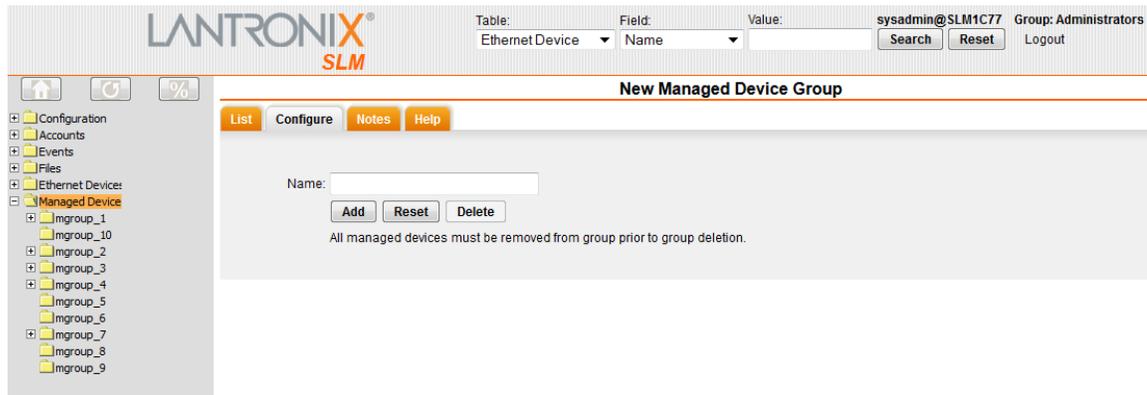
Updating or Deleting a Managed Device Group

The administrator can update or delete a Managed Device Group.

To update or delete a Managed Device Group:

1. On the menu, click the **Managed Device Group** and then the **Configure** tab. The following page opens:

Figure 10-7 Managed Device Group Page - Configure Tab



To update a Managed Device Group:

1. Change the name of the group and click the **Update** button. A confirmation message displays.

To remove the Managed Device Group:

Note: You can only delete a Managed Device Group that has no devices assigned to it

1. Click the **Delete** button.
2. In response to the confirmation request, click **OK**. A message confirming the deletion displays. The menu no longer displays the Managed Device Group.

Configuring Polling Settings

The system administrator or permitted user can specify polling settings for the Managed Device Group. The vSLM 2 software polls the Managed Device Group's connections according to these settings.

To configure polling settings:

1. On the menu, click **Managed Devices**, and then click the **Polling** tab. The following page opens:

Figure 10-8 Managed Device Groups - Polling Tab

2. Enter the following information:

Table 10-9 Managed Device Groups - Polling

Polling Setting	Description
Periodically poll	Select the check box to enable periodic polling of the Managed Device Group's connections. Disabled by default.
Poll interval (days)	From the drop-down list, select the number of days between polls. The range is between 1 and 30. The default is 7.
Poll day	
(if interval a multiple of 7)	If the poll interval is a multiple of 7, from the drop-down list, select the day of the week on which the vSLM 2 software should poll the connections. Default is Sunday.
Poll Hour	Enter the time of day at which the vSLM 2 secure management software should poll the connections. Default is 11:00p.

3. To save the settings, click the **Update** button.

Managed Device Group Commands

```
show manageddevice all
```

Syntax

```
show manageddevice all
show manageddevice
```

Description

Displays information about all managed devices.

```
show manageddevice group
```

Syntax

```
show manageddevice group <Group Name>
```

Description

Displays all managed devices by managed device group.

show manageddevice accountgroup**Syntax**

```
show manageddevice accountgroup <accountGroupName>
```

Parameters

Display all managed devices:

```
show manageddevice
show manageddevice all
```

Displays all managed devices in short form:

```
show manageddevice list
```

Display managed devices by index:

Type 'show manageddevice all' to get index.

```
show manageddevice index <number>
```

Find managed device by device name and display device information:

```
show manageddevice config <Device Name>
```

Display all managed devices grouped by managed device group:

```
show manageddevice group <Group Name>
    group name: managed device group name.
```

Display all managed devices group names:

```
show manageddevice groupnames
```

Display all managed devices viewable by an account group:

```
show manageddevice accountgroup <accountGroupName>
```

Display all managed devices viewable by a user account:

```
show manageddevice account <accountName>
```

Display all ports matched by the value started with.

```
show manageddevice search <one or more parameters>
Parameters: [name <Port Name>]
```

Examples

```
show manageddevice search name "waimea-port"
show ma all
show ma config waimea-port-1
```

Description

Displays all managed device viewable by an accountgroup.

Connecting to a Managed Device

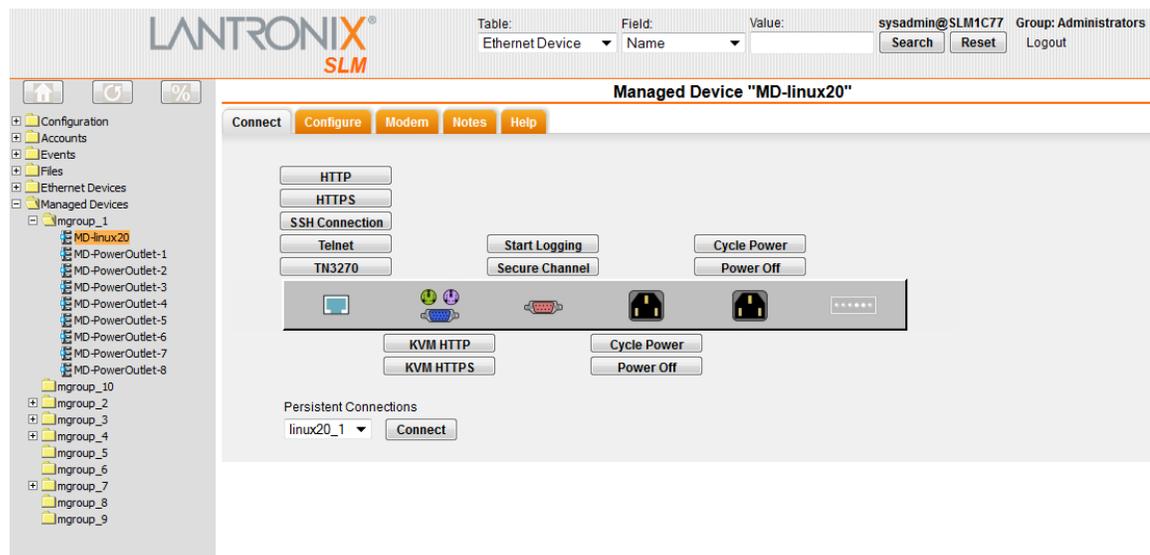
The **Connect** tab on the Managed Device page provides various methods of connecting directly to a managed device. The method depends on the type of Lantronix device server or modem connected to the managed device. The ability to connect also depends on the user's permissions.

To view connection methods to a managed device:

1. On the menu, select the managed device. The following page opens:

Note: This example shows multiple connections being managed.

Figure 10-10 Managed Device Page - Connect Tab



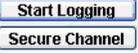
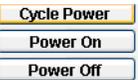
An icon bar contains a series of icons representing the types of connections the vSLM 2 software can make to managed devices. Buttons above or below the icons enable you to connect directly to the managed device. Icons for options not configured into the device are unavailable.

In the example above, the button below the **SLK** icon enables you to connect to the managed device through a KVM port on an SLK remote KVM manager.

Note: For more information about connection methods, see [Connecting to Ethernet and Managed Devices \(on page 237\)](#).

Table 10-11 Connection Icons and Buttons on the Connect Tab

Icon	Connection Buttons	Description
	<p>HTTP</p> <p>HTTPS</p> <p>Web Channel</p> <p>Secure Channel</p> <p>SSH Connection</p> <p>Telnet</p> <p>TN3270</p>	<p>Network connection: Enables the vSLM 2 software to connect to a managed device directly by means of HTTP, HTTPS, Secure Channel, Web Channel, SSH Connection, or Telnet.</p> <p>Note: If the managed device incorporates a local Ethernet device, and that device type is set to Windows, then a Remote Desktop button displays. If the managed device type is set to Linux Server, a VNC button displays.</p>

Icon (continued)	Connection Buttons	Description
		<p>KVM HTTP connection: Enables the vSLM 2 secure management software to connect to the managed device through a port on an SLK or Spider devices using a nonsecure web connection.</p> <p>KVM HTTPS connection: Enables the vSLM 2 software to connect to the managed device through a port on an SLK or Spider devices using a secure web connection.</p>
		<p>SLC Serial Connection: Enables the vSLM 2 secure management software to connect to the managed device through an SLC serial port by secure channel and to cause the managed device to start logging to an SLC console manager.</p> <p>SLC devices display the Secure Channel button. SCSs as well as other Lantronix and Non-Lantronix devices display the SSH Connection button for the serial port.</p> <p>Note: If logging is on, the Stop Logging button displays instead of the Start Logging button, and vice versa.</p>
		<p>Power connection: Enables the vSLM 2 software to control power on the managed device through an RPM/SLP port. Two power connections are available.</p> <p>Note: If the vSLM 2 software detects that the power is on, then only the Power Off and Cycle Power buttons display. If the vSLM 2 detects that the power is off, only the Power On button displays. If the state of the power connection is not known, all buttons display (but you also get a message letting you know that the state was not detectable).</p>
		<p>Modem: Enables the vSLM 2 secure management software to connect to the managed device through the telephone network.</p> <p>The Connect button displays when no session has been established and during session negotiation. Refresh the page after establishing a session, and this button reads “Disconnect”. If you click the Disconnect button, be sure to refresh the page as the session may not have terminated when the new page was rendered.</p> <p>The Call Back button displays under the following conditions:</p> <ul style="list-style-type: none"> ◆ The vSLM 2 software is connected to a modem. ◆ The Managed Device is managing either an SLC or SLB Ethernet device. ◆ The SLC or SLB device is configured for call back operations. This means that on the Modem tab for that Ethernet device, Modem Connection is Text, and there is a modem telephone number. Also, on the Modem Connection page, Call Back is selected.

2. To identify the port or device on the device server to which the managed device is connected, move the pointer over the icon.
3. To go directly to the port or device page, click the icon.

Note: A drop-down list of persistent connections may display below the icon bar. Use the **Connect** button to the right of the list to connect to the managed device through the selected persistent connection.

Creating Individual Managed Devices

The administrator and permitted users can create individual managed devices in the following ways:

- ◆ From a port
- ◆ From a list of ports
- ◆ From a device

From a Port

You can create a managed device from a port on a Lantronix device server such as an SLC, SLK, RPM/SLP, SCS05/20, or SCSxx00 device. The managed device represents the physical device connected to the port.

To create a managed device from a port:

1. On the menu, click **Managed Devices > (specific managed group) > (specific managed device) > Configure tab > Serial Port**. The Port page opens.

Note: In this example, we show a port on an SLC console manager.

Figure 10-12 Port Page - Configure Tab

The screenshot displays the Lantronix SLM web interface for configuring a port. The top navigation bar includes a search function and user information (sysadmin@SLM1C77, Group: Administrators). The left sidebar shows a tree view of managed devices, with 'MD-linux20' selected. The main content area is titled 'Port "slcPort-1"' and features several tabs: 'Configure', 'Statistics', 'Logs', 'Display', 'Notes', and 'Help'. The 'Configure' tab is active, showing various configuration options for the port. The 'Managed Device' dropdown is set to 'MD-linux20'. The 'Parent Ethernet Device' is 'slcRef8008' and the 'Parent Device Type' is 'SLC'. The 'Port Number' is '1' and the 'Name' is 'slcPort-1'. The 'Log Enabled' checkbox is unchecked, and the 'Log Time Frame (seconds)' is '60'. The 'Max Log Size (KB)' is '256' and the 'Byte Threshold' is '100'. The 'Receiving SLM(s)' is empty, and the 'Break Sequence' is '\x1bB'. The 'Data Settings' section includes 'Baud' (9600), 'Data Bits' (8), 'Stop Bits' (1), 'Parity' (None), and 'Flow Control' (RTS/CTS). The 'Hardware Signal Triggers' section includes 'Check DSR on Connect' and 'Disconnect on DSR', both unchecked. The 'IP Settings' section includes 'Enable Telnet In', 'Enable SSH In', and 'Enable TCP In', all unchecked, with ports 5001, 6001, and 7001 respectively. The 'Terminal Rows' is '24' and the 'Terminal Columns' is '80'. The 'Update', 'Reset', and 'Delete' buttons are at the bottom.

2. Leave **New Device** in the **Managed Device** drop-down list, and select the Managed Device Group to which the new device will belong.
3. Click the **Create** button.

The managed device field displays as a link to the managed device's configuration page, and the menu tree lists the new managed device in the assigned Managed Device Group.

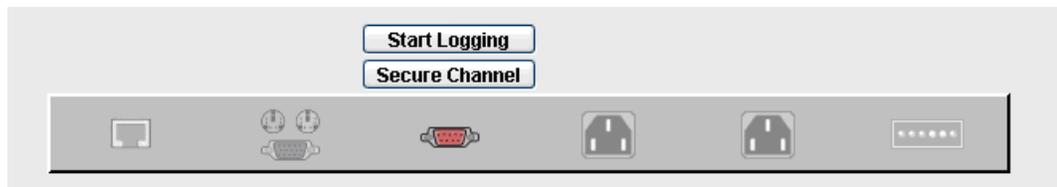
A **Defuse** button displays to the right of the link. Click the button to remove this port from the managed device. If the port was the only component of the managed device, the **Defuse** button removes the managed device itself from the system.

Figure 10-13 Link to a Managed Device Page - Configure Tab



4. On the menu, click the name of the new managed device. The Managed Device page Connect tab displays the available connection buttons for the serial connection.

Figure 10-14 Managed Device Page - Connect Tab



In a similar manner, you can create individual managed devices from RPM/SLP ports and SLK connectors.

From a Ports List

You can create one or more managed devices from an Ethernet device's ports list. In this example, we show ports on an SLC console manager.

To create one or more managed devices on the Ports page:

1. On the Device page, click the **Ports** tab. The following page opens:

Figure 10-15 Device Page - Ports Tab

LANTRONIX[®] SLM

Table: Ethernet Device Field: Name Value: sysadmin@SLM1F4F Group: Administrators
 Search Reset Logout

Device "mlslc8048"

Configure Ports PerCons LocalCons Utilities Display Traps Modem Notes Help

Name	Port Number	Console	Log Enabled	Log Time Frame	Max Log Size (KB)	Byte Threshold
Port-1	1	mlslc8048	No	30	256	1024
Port-2	2	mlslc8048	No	30	256	1024
Port-3	3	mlslc8048	No	30	256	1024
Port-4	4	mlslc8048	No	30	256	1024
Port-5	5	mlslc8048	No	30	256	1024
Port-6	6	mlslc8048	No	30	256	1024
Port-7	7	mlslc8048	No	30	256	1024
Port-8	8	mlslc8048	No	30	256	1024
Port-9	9	mlslc8048	No	30	256	1024
Port-10	10	mlslc8048	No	30	256	1024
Port-11	11	mlslc8048	No	30	256	1024
Port-12	12	mlslc8048	No	30	256	1024
Port-13	13	mlslc8048	No	30	256	1024
Port-14	14	mlslc8048	No	30	256	1024
Port-15	15	mlslc8048	No	30	256	1024
Port-16	16	mlslc8048	No	30	256	1024
Port-17	17	mlslc8048	No	30	256	1024
Port-18	18	mlslc8048	No	30	256	1024
Port-19	19	mlslc8048	No	30	256	1024
Port-20	20	mlslc8048	No	30	256	1024
Port-21	21	mlslc8048	No	30	256	1024
Port-22	22	mlslc8048	No	30	256	1024
Port-23	23	mlslc8048	No	30	256	1024
Port-24	24	mlslc8048	No	30	256	1024
Port-25	25	mlslc8048	No	30	256	1024
Port-26	26	mlslc8048	No	30	256	1024

28 items

Create Managed Devices for checked ports: mgroup_1 Update Add Port

2. Select the check box for one or more ports on the SLC console manager that will be connected to serial devices.
3. From the drop-down list box at the bottom of the page, select **Create Managed Devices**.
4. From the **for checked ports** drop-down list box, select the Managed Device Group to which the selected managed device(s) will belong.
5. Click the **Update** button.
6. In response to the confirmation request, click **OK**. The menu tree displays the new managed device(s) in the assigned Managed Device Group.
7. If desired, repeat [step 2](#) through [step 6](#) above to create managed devices and assign them to other Managed Device Groups.

From an Ethernet Device

Administrators and permitted users can create a managed device from any auto-discovered or manually added Ethernet device, such as a server or a switch, and assign it to a Managed Device Group.

To create a managed device from an Ethernet device:

1. On the menu, click the name of the device (in this example, an SLC console manager). The following page opens:

Figure 10-16 Device Page for an SLC Device

The screenshot displays the LANTRONIX SLM web interface for configuring a device named "slc5e35". The interface includes a top navigation bar with search and user information, and a sidebar with a tree view of device categories. The main configuration area contains the following fields and controls:

- Name:** slc5e35
- IP Address:** 172.19.100.116
- MAC Address:** 00:80:A3:8D:5E:35
- Model:** SLC16
- Location:** (empty)
- Sub-Location:** (empty)
- Secure channel:** No
- Login:** sysadmin
- Password:** (masked with dots)
- Retype Password:** (masked with dots)
- Rack Location:** Not assigned
- SNMP Read Community:** public
- SNMP Write Community:** (masked with dots)
- Managed Device:** New Device
- Group:** mggroup_1
- Read info from device:**
- Write info to device:**
- Synchronized:** No
- Poll:**

On the right side, there is an "SLM Proxy" section with several checkboxes: "Browse http", "Browse https", "Web Channel", "Secure Channel", "SSH Connection", "Telnet", and "TN3270". The "Web Channel", "Secure Channel", "SSH Connection", "Telnet", and "TN3270" options are checked. At the bottom of the configuration area are "Update", "Reset", and "Delete" buttons.

2. In Managed Device, leave New Device and from the Group drop-down list, select the Managed Device Group to which the new managed device will belong.
3. Click the **Create** button. When the page redisplay, the Managed Device field displays as a link to the new managed device, and the assigned Managed Device Group in the menu lists the new managed device. A **Defuse** button displays to the right of the link.
4. Click the **Defuse** button to remove this device from the managed device, as desired. If the device was the only component of the managed device, the **Defuse** button removes the managed device itself from the system.
5. To view the Connect tab for the managed device, click the name of the managed device on the menu. Above the network icon are buttons for connecting to the device through the network.

Note: For more information about connection methods, see [Connecting to Ethernet and Managed Devices \(on page 237\)](#).

Fusing Managed Devices

While the vSLM 2 software can communicate with a device connected to a port of a Lantronix device server (e.g., an SLC, SLK, or SCS05/2 devices) individually, it is often more convenient to communicate from a single web page to a virtual managed device composed of more than one connection to the device. The process of creating the virtual managed device from individual managed devices is called fusing. One convenient application is to fuse the SLC, SLK, and RPM/SLP port connections that manage a single Ethernet device such as a server or a switch.

Methods of Fusing

There are two methods of fusing individual managed devices together:

- ◆ On the Port or Device page, fuse a new managed device with an existing one.
- ◆ On the Managed Device Group page, fuse several existing managed devices at once.

Guidelines

Follow the guidelines below when fusing managed devices:

- ◆ The managed devices must be in the same Managed Device Group.
- ◆ A virtual managed device can consist of only one device (local), one SLC port, one SLK or Spider port, two RPM/SLP ports, and one modem.

Fusing a Port with an Existing Managed Device

The Port Configure tab provides an opportunity to merge a single port with an existing managed device. Previously, we showed an example of creating a managed device from an SLC port.

In the following example, as we configure an SLK port, we fuse it with the SLC port managed device.

To fuse a port with an existing managed device:

1. On the menu tree of an Ethernet device such as an SLC or SLK device, select the port.

The following page opens:

Figure 10-17 Fusing on a Port Page - Configure Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is logged in as 'sysadmin@SLM1C77' with the group 'Administrators'. The main content area is titled 'Port "TS-2"' and has tabs for 'Configure', 'Statistics', 'Logs', 'Display', 'Notes', and 'Help'. The 'Configure' tab is selected. On the left, a navigation tree shows 'Ethernet Devices' expanded to 'TS (172.18.0.216)', with 'TS-2' highlighted. The configuration form includes: 'Port Number: 2', 'Name: TS-2', 'Parent Ethernet Device: TS', 'Parent Device Type: SLK', and 'Managed Device: New Device' (with a dropdown arrow). There are 'Create', 'Update', 'Reset', and 'Delete' buttons. On the right, there are buttons for 'Browse http', 'Browse https', 'Web Channel', 'Secure Channel', 'SSH Connection', and 'Telnet'.

2. From the Managed Device drop-down list, select the existing managed device.
3. Click the **Fuse** button (changed from the **Create** button).

The Managed Device field now displays as a link to the virtual managed device, which has the name of the original managed device.

A **Defuse** button displays to the right of the link. Click the button to remove this port from the managed device. If the port was the only component of the managed device, the **Defuse** button removes the managed device itself from the system.

4. To view the **Connect** tab, click the name of the virtual managed device in the menu.

Figure 10-18 Virtual Managed Device Page with Two Connections



There are four connection buttons above the Ethernet icon and one below the KVM icon, enabling you to connect to the physical managed device through the network and the SLK connection.

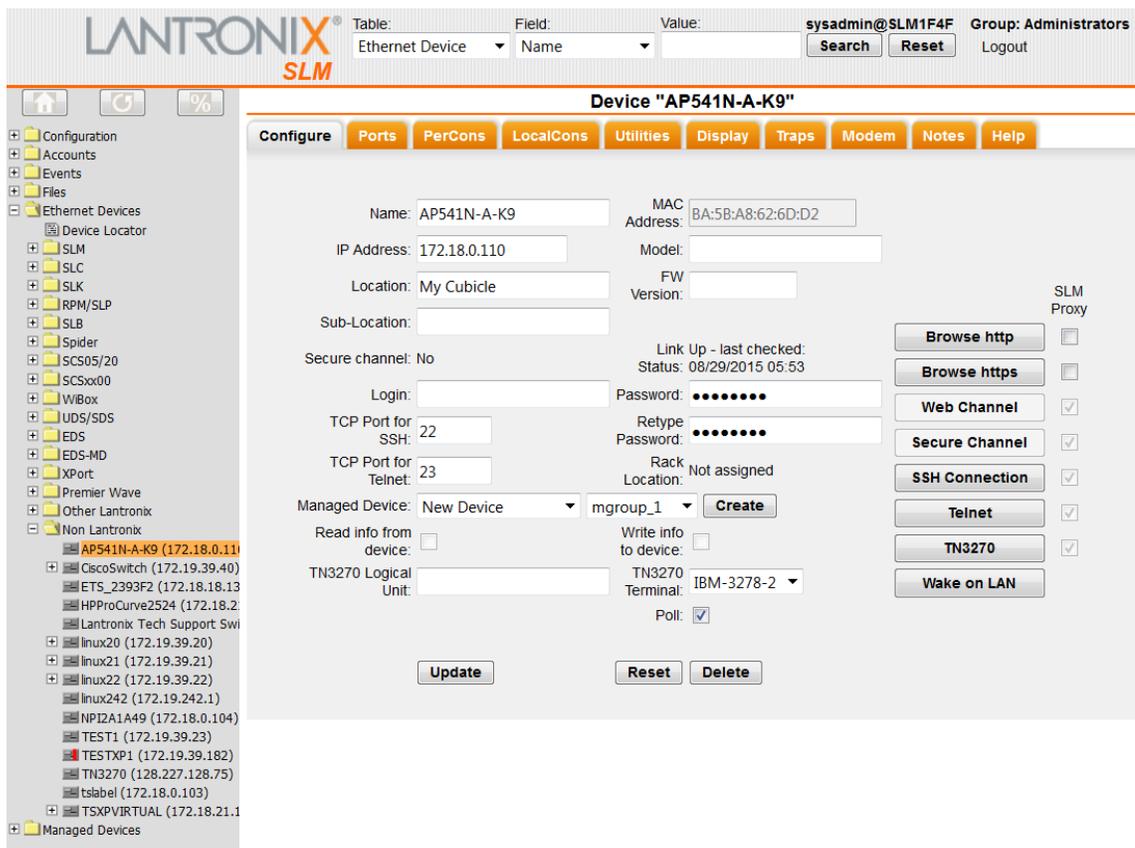
Fusing an Ethernet Device with an Existing Managed Device

The physical device to which a Lantronix device server or a modem is connected may be fused with an existing managed device.

To fuse a device with an existing managed device:

1. On the menu, click the name of the Ethernet device. In this example, we use a switch.

Figure 10-19 Fusing a Managed Device on the Device Page



2. From the Managed Device drop-down list, select the existing managed device.

3. Click the **Fuse** button (changed from the **Create** button).

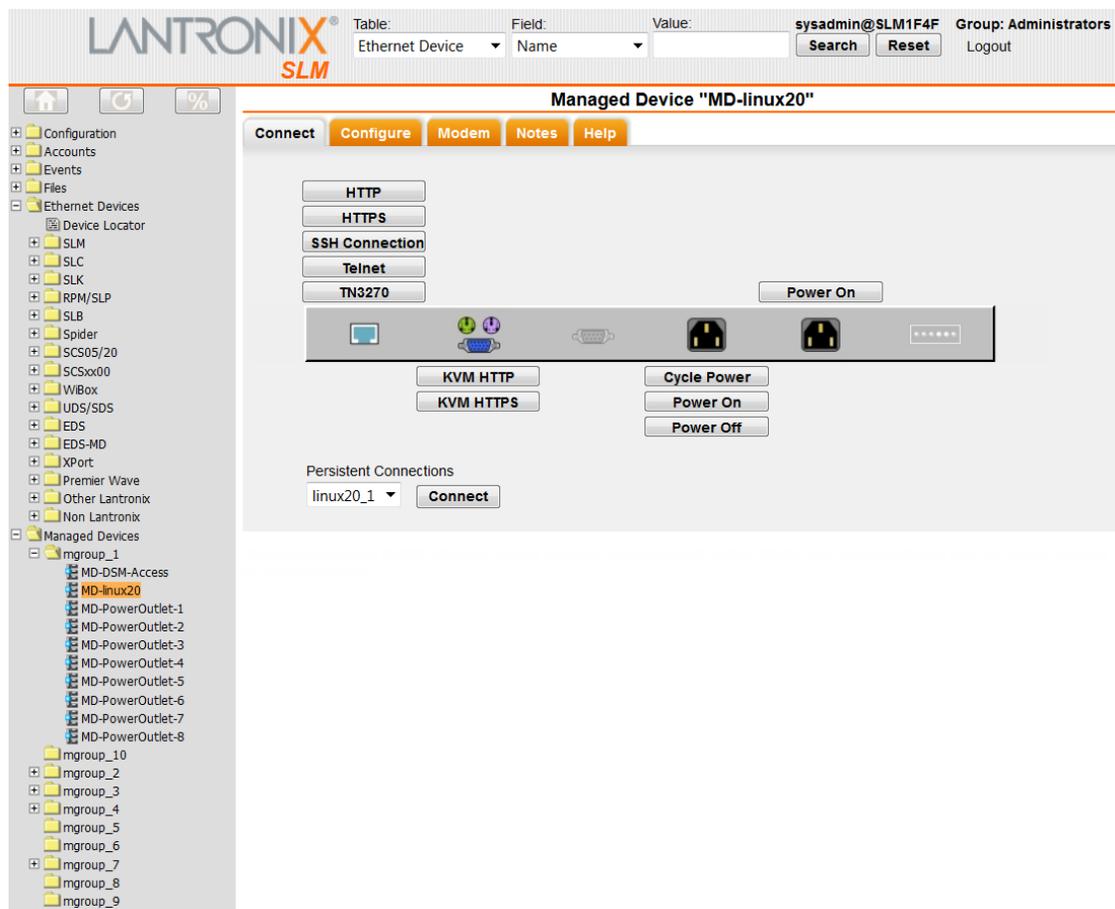
The Managed Device field now displays as a link to the virtual managed device, which has the name of the original managed device. The virtual managed device has taken the name of the existing managed device and still displays in the Managed Device Group.

A **Defuse** button displays to the right of the link. Click the button to remove this device from the managed device. If the device was the only component of the managed device, the **Defuse** button removes the managed device itself from the system.

Continuing the One-at-a-Time Fusion Process

If you continue in this manner, fusing a new serial port managed device and then a new power managed device into the original managed device in the examples above, the Connect tab would look like this:

Figure 10-20 Virtual Managed Device on Managed Device Page - Connect Tab



Fusing Managed Devices on the Managed Device Group Page

Another place to fuse individual managed devices is on the Managed Device Group page. Here you use a single web page to fuse multiple managed devices at the same time.

To use the Managed Device Group page to fuse managed devices:

1. On the menu, click the name of the Managed Device Group that includes the managed devices you want to fuse. This page that opens displays a table listing all the managed devices within the group.

Figure 10-21 Managed Device Group - List Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1F4F' with the group 'Administrators'. The main heading is 'Managed Device Group "mgroup_1"'. Below this, there are tabs for 'List', 'Configure', 'Notes', and 'Help'. The 'List' tab is active, displaying a table of 10 items. The table has columns for Name, Serial Port, Power Port 1, Power Port 2, KVM Port, Device, Managed Device Type, Managed Group, Modem, Connection, Modem App, Phone, Poll, and Reachable. At the bottom of the table, there are buttons for 'Fuse' and 'Delete'.

Name	Serial Port	Power Port 1	Power Port 2	KVM Port	Device	Managed Device Type	Managed Group	Modem	Connection	Modem App	Phone	Poll	Reachable	
MD-DSM-Access					DSM-Access	Unknown	mgroup_1			None	No	No		<input type="checkbox"/>
MD-linux20		PowerOutlet-1	Glenn-PowerOutlet-5	TS-1	linux20	Unknown	mgroup_1			None	No	No		<input type="checkbox"/>
MD-PowerOutlet-1		PowerOutlet-1				Unknown	mgroup_1			None	No	No		<input type="checkbox"/>
MD-PowerOutlet-2		SLC8008PowerOutlet-2				Unknown	mgroup_1			None	No	No		<input type="checkbox"/>
MD-PowerOutlet-3		SLC8024PowerOutlet-3				Unknown	mgroup_1			None	No	No		<input type="checkbox"/>
MD-PowerOutlet-4		PowerOutlet-4				Unknown	mgroup_1			None	No	No		<input type="checkbox"/>
MD-PowerOutlet-5		PowerOutlet-5				Unknown	mgroup_1			None	No	No		<input type="checkbox"/>
MD-PowerOutlet-6		PowerOutlet-6				Unknown	mgroup_1			None	No	No		<input type="checkbox"/>
MD-PowerOutlet-7		PowerOutlet-7				Unknown	mgroup_1			None	No	No		<input type="checkbox"/>
MD-PowerOutlet-8		PowerOutlet-8				Unknown	mgroup_1			None	No	No		<input type="checkbox"/>

10 items

Fuse checked Managed Devices: Delete checked Managed Devices:

2. Select the check box for each managed device you want to fuse.
3. Click the **Fuse** button.
4. In response to the confirmation request, click **OK**. The page redisplay:

Figure 10-22 Managed Device Group Page - List Tab (After Fusion)

The screenshot displays the LANTRONIX SLM interface for the Managed Device Group "mgroup_1". The interface includes a search bar at the top with fields for "Table" (set to "Ethernet Device"), "Field" (set to "Name"), and "Value". The user is logged in as "sysadmin@SLM1F4F" with the group "Administrators".

The main content area shows a table of managed devices. The table has the following columns: Name, Serial Port, Power Port 1, Power Port 2, KVM Port, Device, Managed Device Type, Managed Group, Modem, Connection, Modem App, Phone, Poll, and Reachable. The table lists 10 items, including MD-DSM-Access, MD-linux20, and various MD-PowerOutlet devices. Below the table, there are buttons for "Fuse" and "Delete".

Name	Serial Port	Power Port 1	Power Port 2	KVM Port	Device	Managed Device Type	Managed Group	Modem	Connection	Modem App	Phone	Poll	Reachable
MD-DSM-Access				TS-1	DSM-Access	Unknown	mgroup_1			None		No	No
MD-linux20		PowerOutlet-1	Glenn-PowerOutlet-5		linux20	Unknown	mgroup_1			None		No	No
MD-PowerOutlet-1		PowerOutlet-1				Unknown	mgroup_1			None		No	No
MD-PowerOutlet-2		SLC8008PowerOutlet-2				Unknown	mgroup_1			None		No	No
MD-PowerOutlet-3		SLC8024PowerOutlet-3				Unknown	mgroup_1			None		No	No
MD-PowerOutlet-4		PowerOutlet-4				Unknown	mgroup_1			None		No	No
MD-PowerOutlet-5		PowerOutlet-5				Unknown	mgroup_1			None		No	No
MD-PowerOutlet-6		PowerOutlet-6				Unknown	mgroup_1			None		No	No
MD-PowerOutlet-7		PowerOutlet-7				Unknown	mgroup_1			None		No	No
MD-PowerOutlet-8		PowerOutlet-8				Unknown	mgroup_1			None		No	No

10 items

Fuse checked Managed Devices: Delete checked Managed Devices:

The components of the virtual managed device now display on the same row, and a message in the message area confirms the fusion. The virtual managed device takes the name of the individual managed device that was in the highest row. In the Managed Device Group on the menu, that name remains, but the other fused components do not.

5. On the menu, click the virtual managed device. The Connect tab displays the components of the virtual managed device, each with the button(s) for connecting directly to each component.

Figure 10-23 Virtual Managed Device after Fusion

The screenshot displays the LANTRONIX SLM web interface. At the top, there is a search bar with the following fields: Table: Ethernet Device, Field: Name, Value: (empty), and buttons for Search, Reset, and Logout. The user is logged in as sysadmin@SLM1C77, and the group is Administrators. The main content area is titled "Managed Device 'MD-PowerOutlet-1'" and features a navigation bar with tabs: Connect, Configure, Modem, Notes, and Help. The "Configure" tab is active. Below the navigation bar, there are two sets of controls. The top set includes "Cycle Power" and "Power Off" buttons. Below this is a horizontal bar containing icons for a computer, a modem, a power outlet, and two Ethernet ports. The bottom set of controls also includes "Cycle Power" and "Power Off" buttons. On the left side, a tree view shows the device hierarchy, with "MD-PowerOutlet-1" highlighted under the "Managed Devices" section.

6. Click the **Configure** tab to see the list of managed devices that make up the virtual managed device.

Figure 10-24 Managed Device Page - Configure Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields. The user is logged in as 'sysadmin@SLM1C77' with the group 'Administrators'. The main heading is 'Managed Device "MD-PowerOutlet-1"'. Below this, there are tabs for 'Connect', 'Configure', 'Modem', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following configuration fields:

- Name: MD-PowerOutlet-1
- Serial Port: None
- Local Device: None
- KVM Port: None
- Device Type: Unknown
- Power Port 1: PowerOutlet-1
- Managed Device Group: mgroup_1
- Power Port 2: SLC8008PowerOutlet-2

At the bottom of the configuration area are 'Update' and 'Reset' buttons. On the left side, there is a navigation tree with categories like Configuration, Accounts, Events, Files, Ethernet Devices, and Managed Devices. Under Managed Devices, there are several mgroup folders and individual MD-PowerOutlet devices.

Note: You can change the name of the virtual managed device, identify the device type if a local device is a component of the virtual device, and change the Managed Device Group to which the virtual managed device belongs.

Configuring a Modem Connection to a Managed Device

It is useful to enable the vSLM 2 software to connect over the telephone should a network connection fail. This is possible if, for example, the vSLM 2 software has an internal or a physically connected modem, and a managed device such as a UNIX server on the network is connected to a modem. You can connect to an SLC console manager through a modem if you configure the SLC device as a managed device. Then the vSLM 2 secure management software can connect to the SLC device's attached devices through the modem.

To configure a managed device to use a modem:

1. On a Managed Device page, click the **Modem** tab: The following page opens:

Figure 10-25 Managed Device Page - Modem Tab

The screenshot shows the LANTRONIX SLM interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:' fields, along with 'Search' and 'Reset' buttons. The user is identified as 'sysadmin@SLM1C77' with the group 'Administrators'. The main content area is titled 'Managed Device "MD-PowerOutlet-1"' and has tabs for 'Connect', 'Configure', 'Modem', 'Notes', and 'Help'. The 'Modem' tab is active, showing the following settings:

- Modem: Any (dropdown)
- Profile: Disabled (dropdown)
- Application: None (dropdown)
- Telephone Number: (text input)
- Poll:
- Link Status: Down - last checked: Never

At the bottom of the settings area are 'Submit' and 'Reset' buttons. On the left side, there is a navigation tree with categories like Configuration, Accounts, Events, Files, Ethernet Devices, and Managed Devices. Under Managed Devices, there are several 'MD-PowerOutlet' entries and 'mgroup' folders.

2. Enter the following information:

Table 10-26 Managed Device - Modem Tab

Modem Connection Setting	Description
Modem	From the drop-down list, select the modem, or set to Any to allow the vSLM 2 software to choose the modem.
Connection	From the drop-down list, select the type of modem connection. Disabled by default. For information about types of modem connections, see on Chapter 7: Network and Modem Settings .
Application	From the drop-down list, select the application for connecting to the managed device. The default setting is None. For example, if you select Telnet, the Telnet program launches to connect to the remote system after a PPP connection is established. If you select None, a set of buttons (Secure Channel, SSH, Telnet, HTTP, and HTTPS) displays, enabling you to select a connection method.
Telephone Number	Telephone number of the modem on the managed device
Poll	Select the check box to enable polling of the modem connection Disabled by default. See Configuring Polling Settings (on page 202) .
Link Status (display only)	Indicates whether the modem connection is active.

3. Click the **Submit** button. A message in the message area indicates that the managed device has been updated.

Configuring a Managed Device

The administrator and permitted users can configure a managed device.

To configure a managed device:

1. On the menu, click the name of the managed device, and then click the **Configure** tab. The following page opens:

Figure 10-27 Managed Device Page - Configure Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1C77' with the role of 'Administrators'. The main heading is 'Managed Device "MD-PowerOutlet-1"'. Below this, there are tabs for 'Connect', 'Configure', 'Modem', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following settings:

- Name: MD-PowerOutlet-1
- Serial Port: None
- Local Device: None
- KVM Port: None
- Device Type: Unknown (dropdown menu)
- Power Port 1: PowerOutlet-1
- Managed Device Group: mgroup_1 (dropdown menu)
- Power Port 2: SLC8008PowerOutlet-2

Buttons for 'Update' and 'Reset' are located at the bottom of the configuration area. On the left side, there is a navigation tree with folders for 'Configuration', 'Accounts', 'Events', 'Files', 'Ethernet Devices', and 'Managed Devices'. Under 'Managed Devices', there are sub-folders for 'mgroup_1' through 'mgroup_9'. The 'MD-PowerOutlet-1' device is highlighted in the tree.

2. Edit the following information as desired:

Table 10-28 Managed Device - Configure Tab

Managed Device Setting	Description
Name	A name to identify the managed device.
Local Device	Name of an optional local Ethernet device that is being managed.
Device Type	From the drop-down list, select the type of device. Examples are Cisco IOS , EMS , Firewall , Solaris Server , and Switch . Unknown is the default. <i>Note: If you set the type to Windows, the Remote Desktop button displays on the Connect Tab. If the type is set to Linux Server, then a VNC button is offered.</i>
Managed Device Group	To change the group to which the managed device belongs, select the group from the drop-down list.

3. View the connection information in the column on the right:

Table 10-29 Managed Device - Configure Tab (View Only)

Connection Setting	Description
Serial Port	Indicates whether the managed device is connected to a serial port on an SLC, SLB or SCS device.
KVM Port	Indicates whether the keyboard, video, mouse connector of the managed device is connected to a port on an SLK or Spider module.
Power Point 1 and 2	Indicates whether the managed device is connected to a power port on an RPM/SLP or SLB device.

- To save any changes, click the **Update** button.

Updating or Deleting a Managed Device

The administrator and permitted users can update or delete a managed device.

To update a managed device:

- On the menu, click on a specific managed device and the **Configure** tab. The following page opens:

Figure 10-30 Managed Device - Configure Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: Ethernet Device', 'Field: Name', and 'Value:'. The user is logged in as 'sysadmin@SLM1C77' with the group 'Administrators'. The main heading is 'Managed Device "MD-PowerOutlet-5"'. Below this are tabs for 'Connect', 'Configure', 'Modem', 'Notes', and 'Help'. The 'Configure' tab is active, showing the following configuration details:

- Name: MD-PowerOutlet-5
- Serial Port: None
- Local Device: None
- KVM Port: None
- Device Type: Unknown
- Power Port 1: [PowerOutlet-5](#)
- Managed Device Group: mgroup_1
- Power Port 2: None

At the bottom of the configuration area, there are 'Update' and 'Reset' buttons. On the left side, a navigation tree shows the following structure:

- Configuration
- Accounts
- Events
- Files
- Ethernet Devices
- Managed Devices
 - mgroup_1
 - MD-linux20
 - MD-PowerOutlet-1
 - MD-PowerOutlet-3
 - MD-PowerOutlet-4
 - MD-PowerOutlet-5**
 - MD-PowerOutlet-6
 - MD-PowerOutlet-7
 - MD-PowerOutlet-8
 - mgroup_10
 - mgroup_2
 - mgroup_3
 - mgroup_4
 - mgroup_5
 - mgroup_6
 - mgroup_7
 - mgroup_8
 - mgroup_9

- Add or change the entries and click the **Update** button.

To delete a managed device:

- On the menu, click **Managed Devices**. The **Managed Devices - List** tab displays.
- Check the managed devices that you wish to delete, and click **Delete** button at the bottom of the page.

Managed Device Commands

Administrators, Ethernet Account Users and Menu Only Users

set manageddevice add

Syntax

```
set manageddevice add <Device Name> group <Managed Device Group Name>
```

Parameters

```
ethernetdevice <EthernetDeviceName|IP>  
[port <portName|portNumber>]
```

Description

Create a new managed device from the specified Ethernet device or port.

set manageddevice assign

Syntax

```
set manageddevice assign <managedDeviceName> group <managedDeviceGroup>  
[write|remove]
```

Description

Assigns or removes permissions for a managed device.

set manageddevice config

Syntax

```
set manageddevice config <Device Name> <one or more parameters>
```

Parameters

```
[name <New Name>]  
powerport <1|2> state <on|off|cyclepower>]  
[delete]  
[dialout <Dial Account Name|enable|disable>  
modem <Modem Name>  
phonenumber <phone number>  
application <ssh|telnet|http|none>]
```

To set modem parameters, you must specify the dial-out option.

Examples

```
set ma config port-1 name waimea-port-1
```

Specifies a managed device name (port-1) and renames it to waimea-port-1.

```
set ma config slp-sunset-port1 powerport 1 state off
```

Specifies a managed device name (slp-sunset-port1) and turns the power off.

```
set ma index 1 delete
```

```
set ma index 1 dialout myaccount modem pci-s4 phone 3334444
```

Description

Finds a managed device-by-device name and modifies device parameters.

set manageddevice defuse**Syntax**

```
set manageddevice defuse <DeviceName> device|serial|kvm|power1|power2
```

Description

Defuses an Ethernet device or port from an existing managed device.

set manageddevice fuse**Syntax**

```
set manageddevice fuse <DeviceName> ethernetdevice
<EthernetDeviceName|IP> [port <portName|portNumber>]
```

Description

Fuses an Ethernet device or port to an existing managed device.

set manageddevice index

Note: Type `show manageddevice all` to display index.

Syntax

```
set manageddevice index <number> <one or more parameters>
```

Parameters

Type `'show manageddevice all'` to get index.

```
set manageddevice index <number> fuse
ethernetdevice <EthernetDeviceName|IP>
[port <Port Name|Port Number>]
set manageddevice index <number> defuse
[device|serial|kvm|power1|power2]
```

Examples

```
set ma config port-1 name waimea-port-1
set ma config slp-sunset-port1 powerport 1 state off
set ma index 1 delete
set ma index 1 dialout myaccount modem pci-s4 phone 3334444
```

If you set `dialout myaccount` first and then decide to set `modem` and `phonenumber` later, you still must specify `dialout myaccount` or `dialout enable`.

```
set ma index 1 dialout myaccount
set ma index 1 dialout enable modem pci-s4 phone 3334444
set ma index 1 disconnect modem
```

Description

Find managed device by index and fuse or defuse an Ethernet device or port.

```
set manageddevice index <number> defuse
```

Syntax

```
set manageddevice index <number> defuse device|serial|power1|power2|kvm
```

Description

Defuses an Ethernet device or port from an existing managed device.

```
set mgroup add <newManagedGroupName>
```

Syntax

```
set mgroup add <newManagedGroupName>
```

Description

Creates a new managed device group.

```
set mgroup delete <existingManagedGroupName>
```

Syntax

```
set mgroup delete <existingManagedGroupName>
```

Description

Deletes an existing managed device group. The group must be empty.

```
show device
```

Syntax

```
show device <device name>
```

Note: *Entries are not case sensitive.*

Description

Searches for and displays Ethernet or managed devices by device name. For example, if you specify `name slc`, the vSLM 2 secure management software searches for all Ethernet and managed devices whose name starts with `slc`.

```
show device all
```

Syntax

```
show device all  
show device
```

Description

Displays all Ethernet and managed devices.

```
show manageddevice account
```

Syntax

```
show manageddevice account <accountName>
```

Description

Displays all managed devices viewable by a user account.

show manageddevice accountgroup

Syntax

```
show manageddevice accountgroup <accountGroupName>
```

Description

Displays all managed devices viewable by an account group.

show manageddevice all

Syntax

```
show manageddevice all  
show manageddevice
```

Description

Displays information about all managed devices.

show manageddevice config

Syntax

```
show manageddevice config <Device Name>
```

Description

Displays the configuration of a managed device.

show manageddevice index

Note: Type *show manageddevice all* to display index.

Syntax

```
show manageddevice index <number>
```

Description

Displays managed devices by index.

show manageddevice list

Syntax

```
show manageddevice list
```

Description

Displays all managed devices in short form.

show manageddevice search

Syntax

```
show manageddevice search <one or more parameters>
```

Parameters

Note: Search entries are not case sensitive.

```
[name <Port Name>]
```

Example

```
show manageddevice search name waimea-port
```

Description

Displays all ports that match the criteria entered.

Managed Device Users

set manageddevice config

Syntax

```
set manageddevice config <Device Name> <one or more parameters>
```

Parameters

```
[name <New Name>]
```

```
[state <on|off|cyclepower>] (available for RPM/SLP, SLB and Spider Duo devices only)
```

Powers managed device on or off.

Examples

```
set ma config port-1 name waimea-port-1
```

Specifies a managed device name (`port-1`) and renames it to `waimea-port-1`.

```
set ma config slp-sunset-port1 state off
```

Specifies a managed device name (`slp-sunset-port1`) and turns the power off.

Description

Finds a managed device-by-device name and modifies device parameters.

set manageddevice index

Note: Type `show manageddevice all` to display index.

Syntax

```
set manageddevice index <number> <one or more parameters>
```

Parameters

```
name <New Name>
```

powerport <1|2> state <on|off|cyclepower>] (RPM/SLP, SLB and Spider Duo devices only)

Example

```
set ma port slp-sunset po 2 state on
```

Description

Finds managed device by index and modifies device parameters.

```
set manageddevice config <Device Name> disconnect modem
```

Syntax

```
set manageddevice config <Device Name> disconnect modem
```

Description

Finds managed device by name and disconnects modem.

11: Operation and Maintenance

Depending on permissions, the typical user employs vSLM 2 secure management software to:

- ◆ Search for SLC console managers and other Ethernet devices, ports, and managed devices.
- ◆ Connect by browser, SSH, or secure channel to vSLM 2 software and to the managed devices connected to their ports.
- ◆ Access notes and logs about the Ethernet devices and their ports.

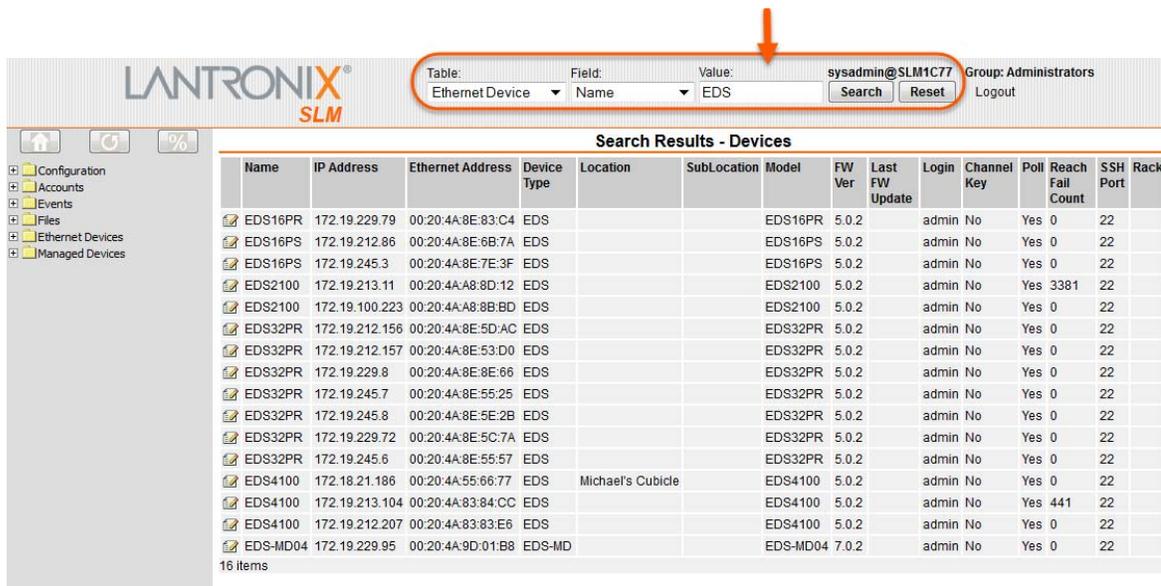
The administrator performs the following maintenance activities:

- ◆ Update vSLM 2 firmware and configurations
- ◆ Configure and manage log files
- ◆ Configure an SNMP agent
- ◆ View events
- ◆ Update SLC firmware

Searching for Ethernet Devices, Ports, Persistent Connections, Managed Devices, and Users

All pages in the web interface have three search fields at the top. Administrators and Ethernet Device Account groups can search by Ethernet device, port, and managed devices. Administrators with account rights can also search by user. Managed Device Account Groups can only search by managed device.

Figure 11-1 Search Fields



The screenshot shows the vSLM 2 web interface. At the top, there are search fields: "Table:" (set to "Ethernet Device"), "Field:" (set to "Name"), and "Value:" (set to "EDS"). There are "Search" and "Reset" buttons. The user is logged in as "sysadmin@SLM1C77" with the group "Administrators". Below the search fields is a table titled "Search Results - Devices". The table has columns: Name, IP Address, Ethernet Address, Device Type, Location, SubLocation, Model, FW Ver, Last FW Update, Login, Channel Key, Poll, Reach Fail Count, SSH Port, and Rack. The table contains 16 items, including various EDS models (EDS16PR, EDS16PS, EDS2100, EDS32PR, EDS4100, EDS-MD04) and their associated details.

Name	IP Address	Ethernet Address	Device Type	Location	SubLocation	Model	FW Ver	Last FW Update	Login	Channel Key	Poll	Reach Fail Count	SSH Port	Rack
EDS16PR	172.19.229.79	00:20:4A:8E:83:C4	EDS			EDS16PR	5.0.2		admin	No	Yes	0	22	
EDS16PS	172.19.212.86	00:20:4A:8E:6B:7A	EDS			EDS16PS	5.0.2		admin	No	Yes	0	22	
EDS16PS	172.19.245.3	00:20:4A:8E:7E:3F	EDS			EDS16PS	5.0.2		admin	No	Yes	0	22	
EDS2100	172.19.213.11	00:20:4A:A8:8D:12	EDS			EDS2100	5.0.2		admin	No	Yes	3381	22	
EDS2100	172.19.100.223	00:20:4A:A8:8B:BD	EDS			EDS2100	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.212.156	00:20:4A:8E:5D:AC	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.212.157	00:20:4A:8E:53:D0	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.229.8	00:20:4A:8E:8E:66	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.245.7	00:20:4A:8E:55:25	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.245.8	00:20:4A:8E:5E:2B	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.229.72	00:20:4A:8E:5C:7A	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.245.6	00:20:4A:8E:55:57	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS4100	172.18.21.186	00:20:4A:55:66:77	EDS	Michael's Cubicle		EDS4100	5.0.2		admin	No	Yes	0	22	
EDS4100	172.19.213.104	00:20:4A:83:84:CC	EDS			EDS4100	5.0.2		admin	No	Yes	441	22	
EDS4100	172.19.212.207	00:20:4A:83:83:E6	EDS			EDS4100	5.0.2		admin	No	Yes	0	22	
EDS-MD04	172.19.229.95	00:20:4A:9D:01:B8	EDS-MD			EDS-MD04	7.0.2		admin	No	Yes	0	22	

To view or make changes to any item returned in a search, click the **Edit**  icon in the leftmost column. (If the search returns the item, you have rights to edit it.)

To clear the search fields, click the **Reset** button. To re-sort the list (e.g., alphabetically by name), click the header of the column you want to sort by.

All searches are case insensitive.

Search for an Ethernet Device

There are several criteria to use to search for an Ethernet device.

To search for Ethernet devices on the network:

1. From the Table drop-down list at the top of any page, select Ethernet Device.
2. From the Field drop-down list, select one of the following search fields and enter the corresponding Value. If you omit the value, the search returns all devices.

Note: Searches are not case sensitive.

Table 11-2 Available Search Fields

Ethernet Device Setting	Description
Device Fields	<p>Name: The name of the device for which you are searching. You need type only as many characters as will identify the device. For example, s returns all devices with names starting with s.</p> <p>IP Address: The IP address of the device for which you are searching. You need enter only as many octets as will identify the device or group of devices.</p> <p>Location: The location of the device (or devices), for example, a room or building. You need type only as many characters as will identify the location. Thus, Irv returns all devices with locations starting with Irv, for example, Irvine. The sub-location can also used as part of the search by entering "Location/Sub-location". Only a few characters of the sub-location need to be entered to match the sub-location. Case insensitive.</p> <p>Model: Model name of the device(s) (e.g., SLC16, SLM 2.0 devices).</p> <p>Firmware: Version of the device's firmware (e.g., 4.0).</p>

3. Click the **Search** button. The Search Results - Devices page opens, listing all devices that meet the search criteria that you have permission to see.

Figure 11-3 Example of a Search by “EDS” Ethernet Device

Name	IP Address	Ethernet Address	Device Type	Location	SubLocation	Model	FW Ver	Last FW Update	Login	Channel Key	Poll	Reach Fail Count	SSH Port	Rack
EDS16PR	172.19.229.79	00:20:4A:8E:83:C4	EDS			EDS16PR	5.0.2		admin	No	Yes	0	22	
EDS16PS	172.19.212.86	00:20:4A:8E:6B:7A	EDS			EDS16PS	5.0.2		admin	No	Yes	0	22	
EDS16PS	172.19.245.3	00:20:4A:8E:7E:3F	EDS			EDS16PS	5.0.2		admin	No	Yes	0	22	
EDS2100	172.19.213.11	00:20:4A:A8:8D:12	EDS			EDS2100	5.0.2		admin	No	Yes	3381	22	
EDS2100	172.19.100.223	00:20:4A:A8:8B:BD	EDS			EDS2100	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.212.156	00:20:4A:8E:5D:AC	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.212.157	00:20:4A:8E:53:D0	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.229.8	00:20:4A:8E:8E:66	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.245.7	00:20:4A:8E:55:25	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.245.8	00:20:4A:8E:5E:2B	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.229.72	00:20:4A:8E:5C:7A	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS32PR	172.19.245.6	00:20:4A:8E:55:57	EDS			EDS32PR	5.0.2		admin	No	Yes	0	22	
EDS4100	172.18.21.186	00:20:4A:55:66:77	EDS	Michael's Cubicle		EDS4100	5.0.2		admin	No	Yes	0	22	
EDS4100	172.19.213.104	00:20:4A:83:84:CC	EDS			EDS4100	5.0.2		admin	No	Yes	441	22	
EDS4100	172.19.212.207	00:20:4A:83:83:E6	EDS			EDS4100	5.0.2		admin	No	Yes	0	22	
EDS-MD04	172.19.229.95	00:20:4A:9D:01:B8	EDS-MD			EDS-MD04	7.0.2		admin	No	Yes	0	22	

The following information (if available) displays for each device retrieved by the search:

Table 11-4 Device Search Results

Device Setting	Description
Name	Name of the device (e.g., SLC 4.0 device).
IP Address	IP address of the device.
Ethernet Address	Hardware or MAC address.
Device Type	SLC console manager, vSLM 2 secure management software, Spider device, etc.
Location	Place at the site, such as a room or a closet, where the unit is installed.
Model	Model name of the device (e.g., SLC48 console manager).
Firmware Version	Firmware release number (e.g., 2.1).
Last FW Update	Date of the last firmware update for the device.
Login	User name for accessing the device.
Channel Key	Yes indicates that a secure channel has been established between the vSLM 2 secure management software and the device. The Channel Key does not indicate whether or not there is an active secure channel communication session, but instead indicates whether or not a secure channel was established to the device in the past, enabling the vSLM 2 software to connect to the device without using a password. Note: Behind the scenes, the secure channel uses SSH keys for authentication.
Poll	Yes indicates that the device may be polled.
Reach Fail Count	During polling, the vSLM 2 secure management software keeps track of the number of consecutive failures. If that count exceeds the threshold specified in Auto Connection Fail Count (on the Polling tab of the Ethernet Devices page), the icon for that device shows a red stripe. If that device is configured for auto-modem connect, the vSLM 2 software will attempt to connect to that device over telephone lines.
SSH Port	Port assigned for SSH access, if applicable.
Rack	The name of the rack (RrrCccPpp, where rr = row, cc = cluster and pp = position) in the form of a link that will take you to the Device Locator page.

The Search Results - Devices page opens, listing all devices that meet the search criteria that you have permission to see.

Search for Ports

To search for a port, you can use two criteria.

To search for a port:

1. From the **Table** drop-down list at the top of any page, select **Port**.
2. From the **Field** drop-down list, select one of the following and enter the corresponding **Value**. If you omit the value, the search returns all ports.

Note: All searches are case insensitive.

Table 11-5 Search by Port

Port Setting	Description
Port Fields	<p>Name: The name of the port for which you are searching. You need type only as many characters as will identify the port. For example, s returns all devices with names starting with s.</p> <p>Number: Number of the port for which you are searching.</p>

3. Click the **Search** button. The Search Results - Ports page opens, listing all ports that meet the search criteria that you have permission to see.

Figure 11-6 Example of a Search by Port

The screenshot shows the LANTRONIX SLM search interface. At the top, there is a search form with the following fields: Table (set to 'Port'), Field (set to 'Name'), and Value (set to '3'). There are 'Search' and 'Reset' buttons, and a 'Logout' link. The user is identified as 'sysadmin@SLM1C77' with the group 'Administrators'. Below the search form, the search results are displayed in a table titled 'Search Results - Ports'. The table has the following columns: Name, Port Number, Console, Log Enabled, Log Time Frame, Max Log Size (KB), and Byte Threshold. One result is shown: Name '3ComSuperStack 1', Port Number '1', Console 'SecureLinuxSLP_8b0133', Log Enabled 'No', Log Time Frame '0', Max Log Size (KB) '0', and Byte Threshold '0'. A '1 item' indicator is shown below the table. On the left side, there is a navigation menu with options like Configuration, Accounts, Events, Files, Ethernet Devices, and Managed Devices.

The following information (if available) displays for each port retrieved by the search that you have permission to see:

Table 11-7 Search Results - Ports

Port Setting	Description
Name	Name of the device connected to the port.
Port Number	Number of the port.
Console	Name of the Ethernet device.
Log Enabled	Shows logging status for SLC/SLB devices.
Log Time Frame	<p>For SLC v3.1 and later v3.x (but not v4.0): The maximum time frame in hours before a new log file is created. The default setting is 1 hour.</p> <p>For SLC v4.0 and later: The maximum time frame in seconds before the SLC console manager sends data to the vSLM 2 secure management software. The default setting is 30 seconds.</p>

Port Setting	Description
Max Log Size (KB)	Maximum size of each log file in kilobytes. Once it is reached, a new log file is created.
Byte Threshold	The number of bytes of data the port receives before the Ethernet device captures log data and sends a notification regarding this port.

- The Search Results - Ports page opens, listing all ports that meet the search criteria that you have permission to see.

Search for Persistent Connections

You can search for persistent connections to which you have rights. To search for persistent connections:

- From the **Table** drop-down list at the top of any page, select **Persistent Connection**.
- From the **Field** drop-down list, select **Name** and the corresponding **Value** (name of the connection). If you omit the value, the search returns all persistent connections.

Note: All search fields are case insensitive.

- Click the **Search** button. The Search Results - Persistent Connections page lists all persistent connections that meet the search criteria and that you have permission to see.

Figure 11-8 Example of a Search by Persistent Connection

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with the following fields: Table (set to 'Persistent Connec'), Field (set to 'Name'), and Value (set to 'Cisco'). There are 'Search' and 'Reset' buttons, and a 'Logout' link. Below the search bar, the page title is 'Search Results - Persistent Connections'. On the left, there is a navigation menu with items like Configuration, Accounts, Events, Files, Ethernet Devices, and Managed Devices. The main content area displays a table with the following data:

Name	Console	Protocol	Time Established	Managed Device Available	Logging Enabled	Connection Enabled	Status
CiscoSwitch_1	CiscoSwitch	Telnet	2014-12-12 04:07:10	Yes	Yes	Yes	Connecting
CiscoSwitch_2	CiscoSwitch	Telnet	2014-12-12 04:07:31	Yes	Yes	Yes	Connecting

Below the table, it says '2 items'.

Note: To clear the search fields, click the **Reset** button. To re-sort the list (e.g., alphabetically by name), click the header of the column you want to sort by.

The following information (if available) displays for each persistent connection:

Table 11-9 Search by Persistent Connection

Persistent Connection Setting	Description
Name	Name of the persistent connection.
Console	Ethernet device to which the vSLM 2 secure management software is connected.
Protocol	Protocol used to make the persistent connection.
Time Established	Time the persistent connection was initiated.
Managed Device Available	If the parent Ethernet Device on this persistent connection is being managed as part of a managed device, users with access to the managed device also have access to this persistent connection.
Logging Enabled	Indicates whether the vSLM 2 secure management software is enabled to log the persistent connection.

Persistent Connection Setting	Description
Connection Enabled	Indicates whether the connection has been enabled and ready to activate.
Status	Indicates whether the connection is active.

Search for Managed Devices

To search for a managed device, Administrators, Ethernet Device Account group members, and Managed Device Account Group members can search by name.

To search for managed devices on the network:

1. From the **Table** drop-down list at the top of any page, select **Managed Device**.
2. From the **Field** drop-down list, select **Name** and the corresponding **Value**. If you omit the value, the search returns all managed devices.
3. Click the **Search** button. The Search Results - Devices page opens, listing all managed devices that meet the search criteria that you have permission to see.

Figure 11-10 Example of a Search by Managed Device

Name	Serial Port	Power Port 1	Power Port 2	KVM Port	Device	Managed Device Type	Managed Group	Modem	Connection	Modem App	Phone	Poll	Reachable
CiscoSwitch	Device-1	PowerOutlet-2	PowerOutlet-3		CiscoSwitch	Unknown	mggroup_2			None		No	No
MD-linux20	slcPort-1	PowerOutlet-1	Glenn-PowerOutlet-5	TS-1	linux20	Unknown	mggroup_1			None		No	No
MD-linux21	slcPort-1	PowerOutlet-2	Glenn-PowerOutlet-6	SLS-KVM-1	linux21	Unknown	mggroup_2			None		No	No
MD-linux22	slcPort-1	PowerOutlet-3	Glenn-PowerOutlet-7	SLS-KVM-1	linux22	Unknown	mggroup_3			None		No	No
MD-linux242	slcPort-1	PowerOutlet-4	Glenn-PowerOutlet-8	SLS Duo-KVM-1	linux242	Unknown	mggroup_4			None		No	No
MD-PowerOutlet-1		PowerOutlet-1	SLC8008PowerOutlet-2			Unknown	mggroup_1			None		No	No
MD-PowerOutlet-3		SLC8024PowerOutlet-3				Unknown	mggroup_1			None		No	No
MD-PowerOutlet-4		PowerOutlet-4				Unknown	mggroup_1			None		No	No
MD-PowerOutlet-5		PowerOutlet-5				Unknown	mggroup_1			None		No	No
MD-PowerOutlet-6		PowerOutlet-6				Unknown	mggroup_1			None		No	No
MD-PowerOutlet-7		PowerOutlet-7				Unknown	mggroup_1			None		No	No
MD-PowerOutlet-8		PowerOutlet-8				Unknown	mggroup_1			None		No	No
TSXPVIRTUAL	Port-6	PowerOutlet-3	PowerOutlet-4		TSXPVIRTUAL	Unknown	mggroup_7			None		No	No

The following information (if available) displays for each managed device retrieved by the search that you have permission to see:

Table 11-11 Search by Managed Device

Device Setting	Description
Name	Name of the managed device.
Serial Port	Number or name of the Ethernet device's serial port (e.g., a number between 1 and 48 for the SLC 48 console manager) that is connected to the managed device's console port.
Power Port 1	Number or name of an RPM/SLP power port that is connected to the managed device's power connector.
Power Port 2	Number or name of an RPM/SLP power manager's second power port that is connected to the managed device's power connector.
KVM Port	Number or name of an Spider or SLK KVM port that is connected to the managed device's KVM port.
Device	Name of the Ethernet device.

Device Setting	Description
Managed Device Type	Type of managed device (e.g., Solaris Server or Linux Server).
Managed Group	Name of the Managed Device Group to which the managed device belongs.
Modem	Name of the modem to be used when connecting to the managed device.
Connection	Type of connection to make when using the modem.
Modem App	Application to invoke for the connection (e.g., Secure Channel, SSH, Telnet).
Phone	Telephone number of the modem on the managed device.
Poll	Indicates whether to check the managed device for modem connectivity during modem polling testing.
Reachable	Indicates whether a connection to the modem on this managed device was successful the last time it was tested.

Search for Users

To search for users, administrators with account rights can search using two criteria.

To search for users on the network:

1. From the **Table** drop-down list at the top of any page, select **User**.
2. From the **Field** drop-down list, select one of the following search fields and enter the corresponding **Value**. If you omit the value, the search returns all devices.

Note: Searches are not case sensitive.

Table 11-12 Search for Users

User Setting	Description
User Fields	<p>Name: The name of the user for whom you are searching. You need type only as many characters as will identify the user. For example, s returns all users with names starting with s.</p> <p>E-Mail: E-mail address of the user for whom you are searching.</p>

3. Click the **Search** button. The Search Results - Users page opens, listing all users who meet the search criteria.

Figure 11-13 Example of a Search by User

LANTRONIX [®] SLM		Table:	Field:	Value:	sysadmin@SLM1C77	Group: Administrators								
		User	Name	glenn	Search	Reset Logout								
Search Results - Users														
Name	Email Address	Config Network	Config Authentication	Config Services	Device Management	Config Accounts	Config Events	Config Log Files	Authentication	Password Change	Password Expire	Next Login	Synchronize	Last Access
glenn	glenn@test.com	No	No	No	No	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:40:40
glenn_1	glenn_1@test.com	No	No	No	Yes	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:33:49
glenn_2	glenn_2@test.com	No	No	No	Yes	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:34:37
glenn_3	glenn_3@test.com	No	No	No	Yes	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:35:32
glenn_4	glenn_4@test.com	No	No	No	Yes	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:36:20
glenn_5	glenn_5@test.com	No	No	No	Yes	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:37:17
glenn_6	glenn_6@test.com	No	No	No	Yes	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:38:04
glenn_7	glenn_7@test.com	No	No	No	Yes	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:39:01
glenn_8	glenn_8@test.com	No	No	No	Yes	No	No	No	Local Only	Yes	Yes	No	No	2014-12-01 00:39:49
glenn_ad	glenn_ad@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:44
glennkrb	glennkrb@test.com	No	No	No	Yes	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:35
glennnis	glennnis@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:41
glenn_rd	glenn_rd@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-01 00:47:41
glennmtcac	glennmtcac@test.com	No	No	No	No	No	No	No	Remote Only	No	No	No	No	2014-12-02 09:33:51
14 items														

The following information (if available) displays for each user retrieved by the search.

Table 11-14 Search Results - Users

User Setting	Description
Name	The user name for logging in to the vSLM 2 secure management software.
Email Address	User's email address; may be used for event notification.
Config Network	Yes indicates the user can open the Network Settings page and configure network settings.
Config Authentication	Yes indicates the user can select and prioritize authentication methods and related settings.
Config Services	Yes indicates the user can configure services such as date and time and SNMP Agent & syslog and update SLC console managers to which the user has access.
Device Management	Yes indicates the user can configure settings for auto-detecting devices and ports and for managing alternate vSLM 2 software.
Config Accounts	Yes indicates the user can add, update, and delete all accounts and grant account permissions.
Config Events	Yes indicates the user can set alarms and triggers.
Config Log Files	Yes indicates the user can view, copy, and delete various log files.
Authentication	Indicates whether authentication for this user is Local Only , Remote Only , Local & Remote , or Disabled .
Password Change	Yes indicates that the user can use the current password indefinitely. Selected by default.
Password Expire	No allows the user to keep a password indefinitely.
Next Login	Yes requires the user to change the password the next time the user logs in. (You may change this setting at any time.)
Synchronize	Yes indicates that if the user's password has changed since the last synchronization, the vSLM 2 secure management software will update that new password on all SLM , SLC, SCSxx05/20, and RPM/SLP devices.
Last Access	Date and time the user last logged into the vSLM 2 secure management software, or the date and time of account creation if the user has never logged in.

Using Wildcards

You can use SQL wildcards when conducting a search:

- ◆ Use the percent sign (%) to match zero or more instances of any character.
- ◆ Use the underscore (_) to match any one character.

Note: The vSLM 2 secure management software search automatically appends a percent sign to the end of all search strings, so you do not need to put one there. All searches are case insensitive.

Table 11-15 Searching with Wildcards

A search for <code>_abc</code> will find:	A search for <code>%abc</code> will find:	A search for <code>s__2</code> (three underscores) will find:
Aabc	aaaaaaaaabCcccccc	SLM32_device
BABCdef	ABCccccccccccccc	Sxx32
AabCghi	jjjjjjjjjjjabc	s2232_system
bAbC		
but not	but not	but not
aaabcdc	Aaaaaaaabbcccccc	SLM332_device
	Bccccccccccccccc	sAB16
	Jjjjjjjjjjjjab	Dev_2232

Search Commands

show account search email

Syntax

```
show account search email <email address>
```

Example

```
show account search email sys
```

Displays all accounts whose email address starts with "sys."

Description

Displays accounts that match the email address entered.

show account search name

Syntax

```
show account search name <user name>
```

Examples

```
show account search name sys
```

Displays all accounts whose name starts with "sys."

Description

Displays accounts that match the name entered.

show manageddevice search

Syntax

```
show manageddevice search <one or more parameters>
```

Parameters

Note: Search entries are not case sensitive.

[name <Port Name>]

Example

```
show manageddevice search name waimea-port
```

Description

Displays all ports that match the criteria entered.

Connecting to Ethernet and Managed Devices

Connections Overview

From the vSLM 2 secure management software, you can connect to vSLM 2 software and other Ethernet devices just as you would if you logged into the device directly. You can also connect to Managed Devices.

Permissions set on the vSLM 2 secure management software for Ethernet devices and managed devices, in addition to granting access to device information in the vSLM 2 database, determine whether an account group can manage or just listen to the device.

Connection methods offered on a Managed Device depend on what is being managed, as well as the device types doing the management. For instance, if a Linux Server is being managed, then a VPN connection button displays. If a Windows box is being managed, then Remote Desktop is offered. Other connection methods are offered according to the device type specified in the table above.

Note: Some buttons on Device and Port pages may be inactive, depending on the type of device. On the Managed Device page, only active buttons display.

Ethernet Devices - Connection Methods

The table below shows the methods available for connecting to an Ethernet device.

Table 11-16 Methods of Connecting to Ethernet Devices

Ethernet Device	Browse HTTP	Browse HTTPS	Secure Channel	Web Channel	SSH	Telnet	TN3270
SLM	X	X	X		X	X	
SLC		X	X	X	X	X	
SLK	X	X				X	
RPM/SLP	X	X			X	X	
SLB		X	X	X	X	X	
Spider	X	X	X	X	X	X	
SCS05/20		X			X	X	
SCSxx00	X	X			X	X	

Ethernet Device	Browse HTTP	Browse HTTPS	Secure Channel	Web Channel	SSH	Telnet	TN3270
WiBox	X					X	
UDS/SDS	X					X	
EDS	X	X			X	X	
EDS-MD	X	X			X	X	
XPort	X	X			X	X	
PremierWave	X	X			X	X	
Other Lantronix	X	X			X	X	
Other Devices (Non-Lantronix)	X	X			X	X	X

Managed Devices - Connection Methods

The following table shows the methods available for connecting to a managed device.

Table 11-17 Methods of Connecting to Managed Devices

Managed device connected to:	Connection Methods
Non-Lantronix, SCS05/20, SCSxx00, Other Lantronix	By means of SSH when connected by serial; when a local Ethernet device is being managed, then HTTP, HTTPS, SSH, Secure Channel, Telnet, and Remote Desktop may be offered, depending on the type of Ethernet device.
Spider	HTTPS; Web Channel
SLK	HTTP or HTTPS
SLC, SLB and SLM	Secure Channel; also Web Channel for SLC/SLB device.

Browsing to an Ethernet or Managed Device's Web Page

Users can browse directly to the home page of a vSLM 2 secure management software or other discovered Ethernet device.

Note: If the **Login** and **Password** fields in the device record have been completed, the vSLM 2 software uses them for an automatic login when you browse to secure devices. However, if you use Microsoft Internet Explorer on the client machine, you must change the registry to use this feature. Firefox does not have this problem. You can change the Windows registry with the file, *iefix.reg*, which can be downloaded under the Management Platform product group at the Lantronix website: www.lantronix.com/support/downloads. You must run this file on the client machine that runs IE. Further, some non-Lantronix devices (notably the Avocet DSR1022) require IE 7 to support the browsing feature (from vSLM 2 secure management software to other device).

To access the Ethernet device's web page interface:

1. On the Device page, click the **Browse http** or **Browse https** button.
2. If required, enter the user name and password for accessing the device. The device's home

page opens.

3. Configure or manage the device as directed by the device's User Guide or online Help.

Making a Secure Channel Connection to an SLC, SLM, or SLB Device

You can use a Lantronix secure channel connection from the web interface to the command line interface of another vSLM 2 secure management software or an SLC console manager and its ports and managed devices.

Secure channel is actually a special form of SSH connection. If you use the secure channel, you need only supply the password when logging into the vSLM 2 secure management software. If you use SSH, you have to supply the password every time.

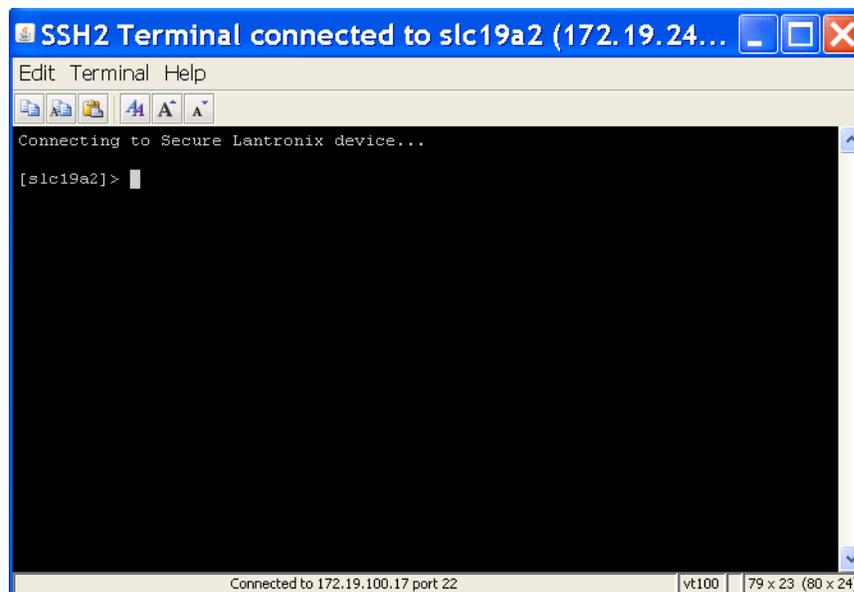
Before connecting to an SLC console manager or to another vSLM 2 secure management software through the secure channel, the administrator must first establish the secure channel connection to the Ethernet device (SLC or vSLM 2 software only). The administrator attempts to connect to the Ethernet device through the vSLM 2 secure channel connection and supplies the sysadmin password for the SLC console manager. After this, any authenticated user who has permission to connect to the Ethernet device can connect to it through the vSLM 2 secure channel without further authentication.

Configure or manage the device as directed by the product's User Guide or online Help.

To make a secure channel connection to an SLC or vSLM 2 software:

1. To log in to the SLC, SLB, or vSLM 2 software, click the Secure Channel button on its Ethernet device page. A Java applet runs, and then the "Connected to vSLM 2" message displays.

Figure 11-18 Secure Channel Connection to an SLC Console Manager



2. If prompted to enter a key, type `Yes` to continue.
3. If prompted, enter your current sysadmin password for the SLC device.
4. Configure or manage the device as directed by the product's User Guide or online Help.

Following is a list of error codes that may display:

Table 11-19 Secure Channel Error Codes

Major Code	Minor Code	Description
1	40	Could not connect to SLC module.
1	41	Network connection to SLC device broken during login
1	50	Error opening secure channel key
1	51	Error reading secure channel key
3	62	Error removing old secure channel key from SLC console manager
3	64	Error importing secure channel key to SLC device
4	68	Error importing secure channel key to SLC console manager
4	80	Error assigning user permissions
6	81	Timeout connecting to device port
6	101	Error connecting to device port (the port may already be in use)
6	102	Error listening to device port. (the port may not be connected)
8	200	Error getting key data from SLC device
8	202	Error establishing secure channel session to SLC console manager
8	203	Error establishing connection to SLC device
10	204	Error updating secure channel status
11	205	Error setting user permissions (for a connection to a device port)
X	207	Error exiting device port access
X	301	Error exiting listen mode
X	600	Error setting user permissions (for a connection to the CLI)
X	800	Error clearing command history on SLC console manager
<i>Note: Error codes display in the format: <Major Code>,<Minor Code>. An X indicates a variable major code.</i>		

Making an SSH Connection to an Ethernet or Managed Device

Users can use SSH from the web page of a Java-enabled web browser to connect to the command line interface of any vSLM 2 secure management software or other discovered Ethernet device.

SSH is a connection protocol that requires all data sent to be encrypted. SSH accomplishes this by using public and private keys generated by the client and the server. Both sides have a pair of keys. The private key encrypts the data being sent; for the receiver to decrypt the received encrypted data, it must have the sender's public key.

The received host key is saved in a file called `known_hosts` in the SSH directory of users. Upon reconnection to the same host, the receiver compares the newly received host key to the previously received key that was stored in the `known_host` file.

If the newly received host key matches the key in the `known_host` file, then the authentication process (login and password) continues.

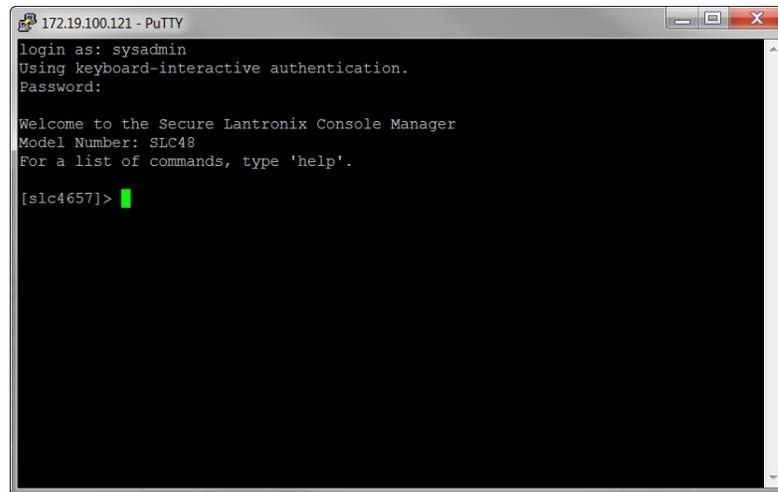
If the newly received host key does not match the key in the `known_host` file, then the user receives a warning that they do not match and is asked whether to replace the old host key information with the new key. (There could be someone trying to impersonate the known host.)

If the newly received host key does not exist in the known_host file, the device warns the user that the host does not exist (first-time connection) and asks the user if it should add the new key to the known_host file.

To make an SSH connection to the device CLI:

1. To log in to a vSLM 2 secure management software using SSH, click the SSH Connection button. A Java applet runs.
2. In response to the prompts, enter the user name and password for the device.

Figure 11-20 SSH Login to SLC Console Manager



```
172.19.100.121 - PuTTY
login as: sysadmin
Using keyboard-interactive authentication.
Password:

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

[slc4657]>
```

3. Configure or manage the device as directed by the device's User Guide or online Help.

Making a Web Channel Connection to an SLC Console Manager

The web channel feature uses the existing secure channel key to the SLC device to authenticate through the web interface. This enables a vSLM 2 user to connect to the web interface on an SLC module without having to enter a username and password. The web connection to the SLC filters through the vSLM 2 secure management software. The **Web Channel** button is only active for SLC console managers that already have a secure channel. No other device types currently support this feature.

To make a web channel connection:

1. On an SLC console manager that has been set up for a secure channel, click the **Web Channel** button. The SLC Web Home Page displays.

Figure 11-21 Web Channel Connection to an SLC Device



Welcome to the Secure Lantronix Console Manager



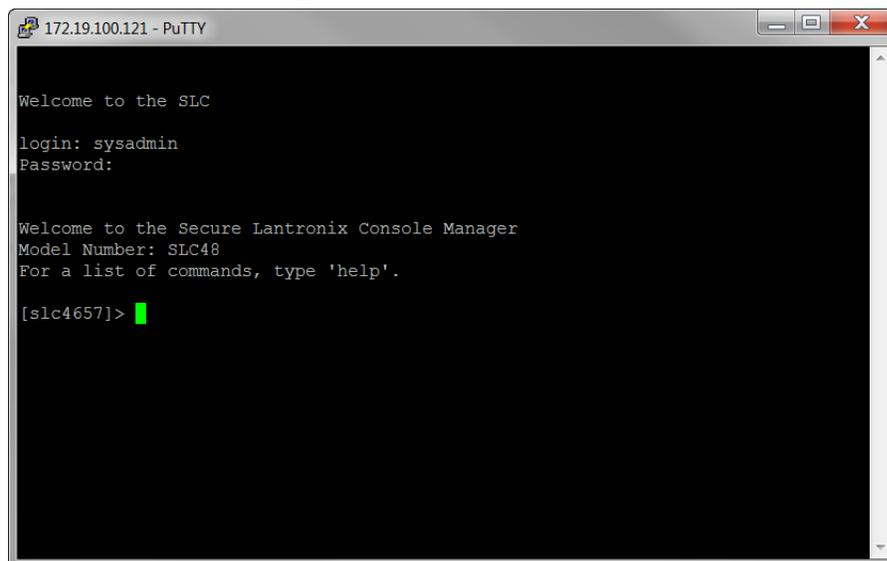
Making a Telnet Connection to an Ethernet device

You can make a Telnet connection to the command line interface of any discovered Ethernet device.

To make a Telnet connection:

1. Click the **Telnet** button. A Java applet runs, and then the Telnet command line interface displays.

Figure 11-22 Telnet Connection



2. Configure or manage the device as directed by the device's User Guide or online Help.

Connection Commands

Administrators, Ethernet Users and Menu Only Users

connect device

Syntax

```
connect device <Device Name or IP Address> <one or more parameters>
```

Parameters

```
[<secure|ssh|telnet|tn3270|serial|modem|modemssh|modemtelnet>
modemcallback] [port <port>]
```

Specify `secure` to connect through a secure channel. Secure channel is the default method of connection for SLC/SLB device, SLC ports, and vSLM 2 secure management software, and SSH is the default for other devices.

`port` is the number of a physical port on the SLC.

SLC48 has ports 1 to 48.

Modem connection is available for managed devices only.

With the `modemssh` option, the vSLM 2 secure management software dials out to the managed device in PPP, and then connects it via SSH.

With `modemtelnet` option, the vSLM 2 software dials out to the managed device in PPP, and then connects it via Telnet.

With the `modemcallback` option, when the vSLM 2 secure management software user calls an SLC console manager and logs in, the SLC device hangs up and calls the user back. The vSLM 2 software then logs in again. This feature is currently available in text mode only.

Examples

```
connect device slc-waimea
connect device slc-waimea-port-1
connect device slc-waimea ssh
connect device slc-waimea port 4
connect device slc-waimea modemssh
connect device slc-waimea modemcallback
```

Description

Connects to an Ethernet device, managed device, or device port.

connect index

Note: Type `show device all` to display the index.

Syntax

```
connect index <number> <one or more parameters>
```

Parameters

```
<secure|ssh|telnet|serial|modem|modemssh|modemtelnet| modemcallback>]
```

Description

Connects a device by index number.

connect persistent**Syntax**

```
connect persistent <persistentConnectionName> [device <devname|IP>]
```

Notes: The device parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name.

The <devname> following device may be the name of an Ethernet device or the name of a managed device. Persistent connections automatically belong to managed devices that have an Ethernet device component that has persistent connections defined.

Description

Connect to an existing persistent connection.

connect ssh**Syntax**

```
connect ssh <IP Address or Name> [tcpport <TCP Port>] [<SSH flags>]
```

Parameters

<SSH flags> is one or more of:

```
user <Login Name>
version <1|2>
escape <Character>
```

The TCP PORT parameter is the TCP port number; the default is **22**.

Description

Connect to any machine/device using standard SSH V1 or V2 protocol.

connect telnet**Syntax**

```
connect telnet <IP Address or Name> [tcpport <TCP Port>] [user <Login Name>]
```

tcpport is the TCP port number; the default is 23.

Description

Connects to a device by means of standard Telnet.

connect tn3270**Syntax**

```
connect tn3270 <IP Address> [tcpport <TCP Port>] [user <Login Name>]
```

Description

The `tcpport` parameter is the TCP port number and default is 23.

show connection list**Syntax**

```
show connection list
```

Description

Displays the active user connections in short form.

Managed Device Users**connect device****Syntax**

```
connect device <Device Name>
[<secure|ssh|telnet|serial|modem|modemssh|modemtelnet|
modemcallback>][port <port>]
```

Specify `secure` to connect through a secure channel. Secure channel is the default method of connection for SLC/SLB device, SLC ports, and vSLM 2 secure management software, and SSH is the default for other devices.

Port is the number of a physical port on the SLC device.

SLC48 console manager has ports 1 to 48.

Modem connection is available for managed devices only.

With the `modemssh` option, the vSLM 2 secure management software dials out to the managed device in PPP, and then connects it via SSH.

With `modemtelnet` option, the vSLM 2 software dials out to the managed device in PPP, and then connects it via Telnet.

With the `modemcallback` option, when the vSLM 2 secure management software user calls an SLC console manager and logs in, the SLC module hangs up and calls the user back. The vSLM 2 software then logs in again. This feature is currently available in text mode only.

Examples

```
connect device slc-waimea
connect device slc-waimea-port-1
connect device slc-waimea ssh
connect device slc-waimea port 4
connect device slc-waimea modemssh
connect device slc-waimea modemcallback
```

Description

Connects to a managed device through a secure channel.

connect index

Note: Type `show managedevice all` to display the index.

Syntax

```
connect index <number>
```

Parameters

```
[<secure|ssh|telnet|serial|modem|modemssh|modemtelnet| modemcallback>]
[<SSH flags>]
```

<SSH flags> is one or more of: user <Login Name>
version <1|2>
escape <Character>

Description

Connects to a device by index number.

Services

The SLM Services page allows administrators to define ways to access the vSLM 2 secure management software, to configure the banner for the CLI, and to enable an audit log of the vSLM 2 software.

To configure services:

1. On the menu, click **Configuration > Services**. The following page opens:

Figure 11-23 SLM Services Page

The screenshot shows the LANTRONIX SLM Services configuration page. At the top, there is a user interface with 'Table: User', 'Field: Name', and 'Value: glenn', along with 'Search' and 'Reset' buttons. The 'Services' configuration includes checkboxes for 'HTTPS Only', 'Enable WAP', 'Enable SSH Logins', 'Enable Telnet Logins', 'Enable Audit Log', 'Enable SSH V1 Logins', and 'Enable Session Logging'. There is also a text input for 'SSH Port' (set to 22) and a dropdown for 'Java Terminal Deployment' (set to 'Java Web Start'). A 'Java Terminal Buffer Size' input is set to 1000. 'Update' and 'Reset' buttons are at the bottom.

2. Enter the following information:

Table 11-24 SLM Services - Configure Tab

SLM Service Setting	Description
HTTPS Only	If selected, allows access to the vSLM 2 secure management software through HTTPS only and disallows access through HTTP. Requires a reboot to take effect. Selected by default.
Enable Telnet Logins	If selected, allows access to the vSLM 2 software through Telnet. Disabled by default.
Enable WAP	If selected, allows you to access the system through a cell phone. For more information about WAP, see Using the SLM Mobile Browser (on page 307) .
Enable Audit Log	If selected, enables the vSLM 2 secure management software to log all actions that have changed the configuration of the vSLM 2 software. Disabled by default.
Enable SSH Logins	If selected, enables the vSLM 2 software to allow users to access the CLI using SSH. Enabled by default.
Enable SSH v1 Logins	If selected, enables the vSLM 2 secure management software to allow users to access the CLI using SSH version 1.
SSH Port	Allows you to change the SSH TCP port to a value in the range of 1 - 65535. The default is 22 .
Enable Session Logging	If selected, enables the vSLM 2 software to log data going back and forth between the user and a device or port.
Java Terminal Deployment	When starting Java, should the vSLM 2 secure management software use Java Web Start (stand alone) or a Java Applet?
Java Terminal Buffer Size	Number of lines in the Java terminal buffer

3. Click the **Update** button.

Banners

You can maintain text that is used for the CLI.

To enter banner text:

1. On the Services page, click the **Banners** tab. The following page displays:

Figure 11-25 Services Page - Banners Tab

The screenshot shows the LANTRONIX SLM Services page with the Banners tab selected. The page header includes the user 'sysadmin@SLM1C77' and the group 'Administrators'. The left sidebar shows a navigation menu with 'Services' highlighted. The main content area has three sections: 'Welcome', 'Login', and 'Logout'. Each section contains a text area with a sample banner message. The 'Update' and 'Reset' buttons are located at the bottom of the page.

2. Enter the following information:

Table 11-26 SLM Services - Banners

SLM Service Setting	Description
Welcome	Enter the text to display at CLI connection.
Login	Enter the text to display upon successful login to the CLI.
Logout	Enter the text to display upon logout from the CLI.

3. Click the **Update** button.

Note: Use the **Reset** button to clear the entries.

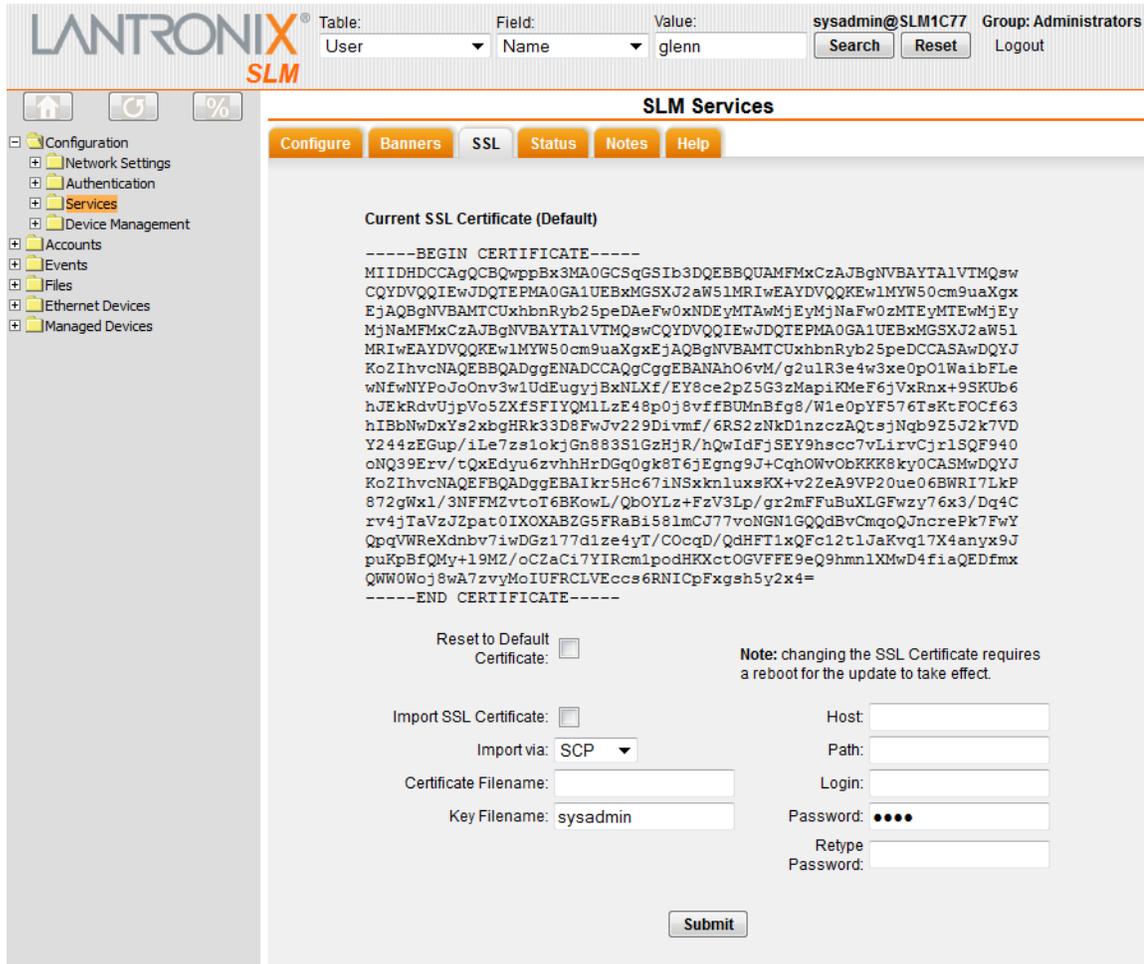
SSL

The vSLM 2 secure management software has a default Secure Socket Layer (SSL) certificate. The SSL tab enables administrators to view and update SSL certificate information. The SSL certificate, consisting of a public/private key pair used to encrypt HTTP data, is associated with the web server. You can import a site-specific SSL certificate, if desired.

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

1. On the Services page, click the **SSL** tab. The current certificate displays.

Figure 11-27 Services - SSL Tab



2. Enter the following:

Table 11-28 SLM Services - SSL Tab

SSL Certificate Setting	Description
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.

SSL Certificate Setting	Description
Import via	From the drop-down list, select the method of importing the certificate (SCP or SFTP). The default is SCP .
Certificate Filename	Filename of the certificate.
Key Filename	Filename of the private key for the certificate.
Host	Host name or IPAddress of the host from which to import the file.
Path	Path of the directory where the certificate will be stored.
Login User	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 **Submit** button.

Note: You must reboot the vSLM 2 secure management software for the update to take effect.

Status

Administrators can view the system status on the Status tab, and if they desire, email it to another person.

To view or email the system status:

1. On the Services page, click the **Status** tab. The following page displays the status information.

Figure 11-29 Services Page - Status Tab

The screenshot shows the LANTRONIX SLM web interface. At the top, there is a search bar with 'Table: User', 'Field: Name', and 'Value: glenn'. The user is logged in as 'sysadmin@SLM1C77' with the group 'Administrators'. The main content area is titled 'SLM Services' and has tabs for 'Configure', 'Banners', 'SSL', 'Status', 'Notes', and 'Help'. The 'Status' tab is active, showing the contents of '/tmp/simssystemstatus.txt'. The status information is as follows:

```

[SLM System Status Reports]

show datetime
-----
Date/Time: Fri Dec 12 04:36:03 2014
Timezone: US/Pacific
SLM Up time: 0 days, 8 hours, 12 minutes

admin version
-----
Model: SLM
Platform: vSLM
Firmware revision: 4.0.0.0
Release date: 12/09/2014 08:06:20 EST
MAC 1: 00:0C:29:A4:1C:77
MAC 2: 00:0C:29:A4:1C:81

Max number of seat: 25
Enhanced Lantronix update expiration: Dec2016

```

Continuation of [Figure 11-29](#) (part 2 of 5)

```

Copyright (c) 2003-2014, Lantronix, All rights reserved.

Lantronix Corporate Headquarters
167 Technology Drive
Irvine, CA 92618 USA
Tel: (800) 526-8766
Tel: +1 (949) 453-3990
Fax: +1 (949) 453-3995

Technical Support
Hours: 6:00a - 5:00p Pacific Time
Monday - Friday (excluding holidays)
Tel: (800) 422-7044 (US only)
Tel: (949) 453-7198
Fax: (949) 450-7226
FTP: ftp.lantronix.com

show sysinfo
-----
Max number of seat: 25
Hardware testing: 00
Ethernet address 1: 00:0C:29:A4:1C:77
Ethernet address 2: 00:0C:29:A4:1C:81
Hard Disk ID: (Unknown - Virtual Machine)

__Firmware update information__
(None)

__System file information__
(None)

show net all
-----
Port State      IP address      Subnet mask Mode      IPv4 filter
-----
1      DHCP           172.19.100.56  255.255.0.0 Auto-negotiate (None)
2      Disabled       0.0.0.0        0.0.0.0    Auto-negotiate (None)

Ethernet bonding      : disabled
Hostname              : SLMIC77
Default gateway       : 0.0.0.0
Port 1 DHCP gateway   : 172.19.0.1
Precedence            : Default
Alternate Gateway     : 0.0.0.0
Alternate Gateway IP Address to ping : 0.0.0.0
Alternate Gateway Ethernet Port for ping : Eth1
Alternate Gateway delay between pings : 3 Second(s)
Alternate Gateway # of failed pings : 10
Static DNS server #1 : 0.0.0.0
Static DNS server #2 : 0.0.0.0
Static DNS server #3 : 0.0.0.0
[port 1]
DHCP-Acquired DNS server #1 : 172.19.1.1
DHCP-Acquired DNS server #2 : 172.19.1.2
DHCP-Acquired DNS server #3 : 0.0.0.0

eth0      Link encap:Ethernet HWaddr 00:0C:29:A4:1C:77
          inet addr:172.19.100.56 Bcast:172.19.255.255 Mask:255.255.0.0
          inet6 addr: fe80::20c:29ff:fea4:1c77/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:298116 errors:0 dropped:0 overruns:0 frame:0
          TX packets:145323 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32949992 (31.4 MiB) TX bytes:80834188 (77.0 MiB)
          Interrupt:17 Base address:0x1080

eth1      Link encap:Ethernet HWaddr 00:0C:29:A4:1C:81
          BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
          Interrupt:18 Base address:0x1800

show service
-----
Audit log: Enabled
Session log: Enabled
Telnet login: Disabled
SSH login: Enabled
SSH version 1 login: Enabled
WAP access: Enabled
HTTPS only: Yes

Open SSH Version: 4.3p2
Open SSL Version: 0.9.8a
Linux Version: 2.6.15-1.2054_FC5smp
Server Version: Apache/2.2.3

show modem
-----
0 modem(s) found.

show account
-----
Idx User name Email address Account group Group type Assigned menu
-----
1 buguser buguser@test.co Administrators Administrator (None)

```

Continuation of [Figure 11-29](#) (part 3 of 5)

```

2 christi Long Group Name Device Perm (None)
3 eth1_1 eth1_1@test.com Ethgrp1 Ethernet user (None)
4 eth1_2 eth1_2@test.com Ethgrp1 Ethernet user (None)
5 eth1_3 eth1_3@test.com Ethgrp1 Ethernet user (None)
6 eth1_4 eth1_4@test.com Ethgrp1 Ethernet user (None)
7 eth2_1 eth2_1@test.com Ethgrp2 Ethernet user (None)
8 eth2_2 eth2_2@test.com Ethgrp2 Ethernet user (None)
9 eth2_3 eth2_3@test.com Ethgrp2 Ethernet user (None)
10 eth2_4 eth2_4@test.com Ethgrp2 Ethernet user (None)
11 eth3_1 eth3_1@test.com Ethgrp3 Ethernet user (None)
12 eth3_2 eth3_2@test.com Ethgrp3 Ethernet user (None)
13 eth3_3 eth3_3@test.com Ethgrp3 Ethernet user (None)
14 eth3_4 eth3_4@test.com Ethgrp3 Ethernet user (None)
15 glenn glenn@test.com Administrators Administrator (None)
16 glenn_1 glenn_1@test.co testmenu Menu user glenn8
17 glenn_2 glenn_2@test.co testmenu Menu user glenn8
18 glenn_3 glenn_3@test.co testmenu Menu user glenn8
19 glenn_4 glenn_4@test.co testmenu Menu user glenn8
20 glenn_5 glenn_5@test.co testmenu Menu user glenn8
21 glenn_6 glenn_6@test.co testmenu Menu user glenn8
22 glenn_7 glenn_7@test.co testmenu Menu user glenn8
23 glenn_8 glenn_8@test.co testmenu Menu user glenn8
24 glenn_ad glenn_ad@test.c Ethgrp1 Ethernet user (None)
25 glennkrb glennkrb@test.c Mnugrp1 Menu user glenn1
26 glennnis glennnis@test.c Mgdgrp2 Managed user (None)
27 glenn_rd glenn_rd@test.c Mgdgrp1 Managed user (None)
28 glenntacac glenntacac@test Ethgrp2 Ethernet user (None)
29 Kerberos Kerberos@test.c Administrators Administrator (None)
30 LDAP LDAP@test.com Administrators Administrator (None)
31 mgd1_1 mgd1_1@test.com Mgdgrp1 Managed user (None)
32 mgd1_2 mgd1_2@test.com Mgdgrp1 Managed user (None)
33 mgd1_3 mgd1_3@test.com Mgdgrp1 Managed user (None)
34 mgd1_4 mgd1_4@test.com Mgdgrp1 Managed user (None)
35 mgd2_1 mgd2_1@test.com Mgdgrp2 Managed user (None)
36 mgd2_2 mgd2_2@test.com Mgdgrp2 Managed user (None)
37 mgd2_3 mgd2_3@test.com Mgdgrp2 Managed user (None)
38 mgd2_4 mgd2_4@test.com Mgdgrp2 Managed user (None)
39 mgd3_1 mgd3_1@test.com Mgdgrp3 Managed user (None)
40 mgd3_2 mgd3_2@test.com Mgdgrp3 Managed user (None)
41 mgd3_3 mgd3_3@test.com Mgdgrp3 Managed user (None)
42 mgd3_4 mgd3_4@test.com Mgdgrp3 Managed user (None)
43 mnu1_1 mnu1_1@test.com Mnugrp1 Menu user glenn1
44 mnu1_2 mnu1_2@test.com Mnugrp1 Menu user glenn1
45 mnu1_3 mnu1_3@test.com Mnugrp1 Menu user glenn1
46 mnu1_4 mnu1_4@test.com Mnugrp1 Menu user glenn1
47 mnu2_1 mnu2_1@test.com Mnugrp2 Menu user glenn2
48 mnu2_2 mnu2_2@test.com Mnugrp2 Menu user glenn2
49 mnu2_3 mnu2_3@test.com Mnugrp2 Menu user glenn2
50 mnu2_4 mnu2_4@test.com Mnugrp2 Menu user glenn2
51 mnu3_1 mnu3_1@test.com Mnugrp3 Menu user glenn3
52 mnu3_2 mnu3_2@test.com Mnugrp3 Menu user glenn3
53 mnu3_3 mnu3_3@test.com Mnugrp3 Menu user glenn3
54 mnu3_4 mnu3_4@test.com Mnugrp3 Menu user glenn3
55 NIS NIS@test.com Administrators Administrator (None)
56 RADIUS RADIUS@test.com Administrators Administrator (None)
57 SecurID SecurID@test.co Administrators Administrator (None)
58 sysadmin Administrators Administrator (None)
59 TACACS TACACS@test.com Administrators Administrator (None)
60 vito ITM-Finance Device Perm (None)

60 users(s) found.

show connection
-----
Max number of seat: 25
Inbound sessions Outbound sessions
ID Type User Location Idle Time ID Type Destination Uptime MDev
-----
1 cli sysadmin Console 08:03:33
2 web sysadmin 172.20.197.103 00:00:01
3 cli sysadmin Unknown 00:00:00
3 inbound and 0 outbound connection(s) found.

admin showboot
-----
Current Bank: bank 1 Next Boot Bank: bank 1.
Bank 1: 4.0.0.0
Bank 2: 4.0.0.0

show dev all
-----
Ethernet device =====
Idx Name IP address Ethernet address Group Model SCC Vers
-----
1 ? 172.19.100.47 00:20:11:09:14:11 LTRX ??? No 1.0
2 ? 172.19.100.42 00:02:4A:9D:02:DF LTRX ??? No 7.0.
3 ? 172.19.100.132 00:20:4A:9D:03:95 LTRX ??? No 1.0
4 ? 172.19.100.162 00:80:A3:94:9F:45 LTRX ??? No 1.0.
5 ? 172.19.100.217 00:20:4A:9D:03:93 LTRX ??? No 1.0
6 ? 172.19.229.231 00:80:A3:98:02:1A LTRX ??? No 1.0.
7 ? 172.19.100.6 00:80:A3:98:00:26 LTRX ??? No 1.0.
8 ? 172.19.100.118 00:80:A3:9A:01:6D LTRX ??? No 7.0.
9 ? 172.19.100.128 00:80:A3:9A:23:6C LTRX ??? No 7.0.
10 ? 172.19.100.236 00:80:A3:A0:0F:EE LTRX ??? No 1.0.
11 ? 172.19.229.250 00:80:A3:A0:11:95 LTRX ??? No 1.0.
12 ? 172.19.100.241 00:80:A3:A0:10:FF LTRX ??? No 1.0.
13 ? 172.19.100.97 00:20:4A:9D:03:8B LTRX ??? No 1.0
14 ? 172.19.100.9 00:20:4A:9D:03:9B LTRX ??? No 1.0
15 AP541N-A-K9 172.18.0.110 BA:5B:A8:62:6D:D2 Other No
16 CiscoSwitch 172.19.39.40 00:02:B9:F4:F5:00 Other No

```

Continuation of [Figure 11-29](#) (part 4 of 5)

17	DSM-Access	172.19.39.248	00:80:A3:89:3F:07	SLB	SLB884	Yes	5.4
18	EDS16PR	172.19.229.79	00:20:4A:8E:83:C4	EDS	EDS16PR	No	5.0.
19	EDS16PS	172.19.245.3	00:20:4A:8E:7E:3F	EDS	EDS16PS	No	5.0.
20	EDS16PS	172.19.212.86	00:20:4A:8E:6B:7A	EDS	EDS16PS	No	5.0.
21	EDS2100	172.19.100.223	00:20:4A:A8:8B:BD	EDS	EDS2100	No	5.0.
22	EDS2100	172.19.213.11	00:20:4A:A8:8D:12	EDS	EDS2100	No	5.0.
23	EDS32PR	172.19.229.72	00:20:4A:8E:5C:7A	EDS	EDS32PR	No	5.0.
24	EDS32PR	172.19.245.6	00:20:4A:8E:55:57	EDS	EDS32PR	No	5.0.
25	EDS32PR	172.19.245.7	00:20:4A:8E:55:25	EDS	EDS32PR	No	5.0.
26	EDS32PR	172.19.245.8	00:20:4A:8E:5E:2B	EDS	EDS32PR	No	5.0.
27	EDS32PR	172.19.212.157	00:20:4A:8E:53:D0	EDS	EDS32PR	No	5.0.
28	EDS32PR	172.19.229.8	00:20:4A:8E:8E:66	EDS	EDS32PR	No	5.0.
29	EDS32PR	172.19.212.156	00:20:4A:8E:5D:AC	EDS	EDS32PR	No	5.0.
30	EDS4100	172.19.212.207	00:20:4A:83:83:E6	EDS	EDS4100	No	5.0.
31	EDS4100	172.18.21.186	00:20:4A:55:66:77	EDS	EDS4100	No	5.0.
32	EDS4100	172.19.213.104	00:20:4A:83:84:CC	EDS	EDS4100	No	5.0.
33	EDS-MD04	172.19.229.95	00:20:4A:9D:01:B8	EDSMD	EDS-MD04	No	7.0.
34	ETS_2393F2	172.18.18.130	00:80:A3:23:93:F2	Other		No	
35	Fedora-242-1	172.19.231.99	00:80:A3:8C:01:61	SPDR	SLS	Yes	3.3
36	GlennDell-XP-PC	172.19.100.229	00:80:A3:8C:47:D5	SPDR	SLS	Yes	3.0
37	HPProCurve2524	172.18.21.95	00:01:E6:13:C8:A1	Other		No	
38	Lantronix Tech S	172.18.0.106	00:22:57:FF:33:50	Other		No	
39	linux20	172.19.39.20	11:22:33:44:55:20	Other	Model	No	
40	linux21	172.19.39.21	00:15:F2:0B:24:10	Other	Model	No	
41	linux22	172.19.39.22	11:22:33:44:55:22	Other	Model	No	
42	linux242	172.19.242.1	11:22:33:44:52:42	Other	Model	No	
43	lyonslb	172.18.21.67	00:80:A3:8D:45:DF	SLB	SLB884-02	Yes	6.1.
44	MatchPort b/g Pr	172.19.100.170	00:20:4A:98:65:43	LTRX	MatchPort	No	5.0.
45	mlslc48	172.18.21.66	00:80:A3:8D:53:29	SLC	SLC48-03	No	6.1.
46	mlslc8048	172.18.21.61	00:20:4A:9D:03:64	SLC	SLC8048-01	No	7.1.
47	NPI2A1A49	172.18.0.104	00:01:E6:2A:1A:49	Other		No	
48	PAT-HostVM	172.19.100.168	00:20:41:80:8D:60	SPDR	SLS Duo	Yes	3.0
49	patlab_slb1	172.19.212.153	00:80:A3:8D:04:00	SLB	SLB0884	Yes	6.1.
50	patlab_slb2-1	172.19.229.253	00:80:A3:8D:20:F3	SLB	SLB0884	Yes	5.5a
51	Premier Wave EN	172.19.100.130	00:20:4A:DD:03:38	FWave	Premier Wa	No	7.0.
52	Premier Wave EN	192.168.0.2	00:80:A3:95:6D:E8	FWave	Premier Wa	No	7.0.
53	Premier Wave EN	172.19.100.124	00:80:A3:9A:34:73	FWave	Premier Wa	No	7.0.
54	Premier Wave EN	172.19.100.115	00:20:4A:DD:00:A4	FWave	Premier Wa	No	7.0.
55	Premier Wave EN	172.19.100.134	00:20:4A:DD:01:66	FWave	Premier Wa	No	7.0.
56	Premier Wave XN	172.19.100.204	00:80:A3:9A:32:E4	FWave	Premier Wa	No	7.0.
57	Premier Wave XN	172.19.100.12	00:80:A3:68:1B:32	FWave	Premier Wa	No	7.0.
58	Rexttron-Spider	172.19.38.96	00:20:4A:89:84:EE	SPDR	SLS Duo	Yes	3.3
59	SCS1600_glenn	172.19.39.123	00:80:A3:57:04:DF	SCSx	SCS1600	No	2.0/
60	SCS1620A	172.19.39.112	00:30:31:00:31:15	SCS	SCS1620	No	
61	SCS_57062F	172.18.21.51	00:80:A3:57:06:2F	SCSx	SCS3200	No	2.0/
62	SecureLinuxSLP_8b	172.18.21.65	00:80:A3:8B:00:0F	SLP	SLP	No	5.3q
63	SecureLinuxSLP_8b	172.19.39.44	00:80:A3:8B:00:26	SLP	SLP	No	5.3p
64	SecureLinuxSLP_8b	172.18.0.108	00:80:A3:8B:01:33	SLP	SLP	No	5.3q
65	ServerRm-RackPC	172.19.100.147	00:80:A3:8C:4F:64	SPDR	SLS Duo	Yes	3.3
66	slb08_250_54_1	172.19.39.250	00:80:A3:8D:52:6D	SLB	SLB0884	Yes	6.1.
67	slb792c	172.18.21.69	00:80:A3:94:79:2C	SLB	SLB882	Yes	6.1.
68	slb8Ref_120-6100	172.19.100.87	00:80:A3:94:DB:41	SLB	SLB882	Yes	6.1.
69	slbpccard71-P61R	172.19.250.55	00:80:A3:8D:04:CC	SLB	SLB0884	Yes	6.1.
70	slbRefreshVz251	172.19.39.251	00:80:A3:94:79:C6	SLB	SLB882	Yes	6.1.
71	slbvz249_glenn	172.19.39.249	00:20:4A:9D:02:FE	SLB	SLB882	Yes	6.1.
72	slc0737	172.19.100.251	00:80:A3:89:07:37	SLC	SLC8	No	6.1.
73	slc08_glenn-1	172.19.39.253	00:80:A3:89:07:01	SLC	SLC8	No	5.4
74	slc16_glenn	172.19.39.254	00:80:A3:89:07:03	SLC	SLC16	No	5.4
75	slc247	172.19.39.247	00:80:A3:89:42:7D	SLB	SLB884	Yes	6.1.
76	slc4657	172.19.213.8	00:80:A3:89:46:58	SLC	SLC48	No	6.1.
77	slc48_glenn_1	172.19.100.90	00:80:A3:8F:80:02	SLC	SLC48	No	6.1.
78	slc5e35	172.19.100.116	00:80:A3:8D:5E:35	SLC	SLC16	No	6.1
79	slca508	172.19.250.120	D4:AE:52:BC:AA:08	SLC	SLC8048	No	7.2.
80	slc-md-u	172.19.100.125	00:20:4A:9D:03:7C	SLC	SLC8048	No	7.2.
81	slcRef8008	172.19.100.221	00:80:A3:96:43:31	SLC	SLC8008	No	7.1.
82	slcRef8024	172.19.250.119	00:20:4A:9D:03:66	SLC	SLC8024	No	7.1.
83	slcRef8040	172.19.250.127	00:20:4A:9D:03:36	SLC	SLC8040	No	7.1.
84	slcRefreshR17_16	172.19.250.167	00:20:4A:9D:03:48	SLC	SLC8032	No	7.1.
85	slm02_glenn17	172.19.211.17	00:30:48:5B:6A:10	SLM	SLM	No	3.8
86	slm02_glenn3917	172.19.39.17	00:30:48:5B:6A:A6	SLM	SLM	No	4.0.
87	SLM115	172.18.0.115	00:30:48:9F:70:12	SLM	SLM	No	3.7
88	SLM117	172.18.0.117	00:30:48:61:49:80	SLM	SLM	No	3.7
89	SLM1F4F	172.19.100.169	00:0C:29:A8:87:30	SLM	SLM	No	3.4
90	slm211_19_37k	172.19.211.19	00:30:48:5B:41:F2	SLM	SLM	No	3.7
91	SLM2643	172.19.100.101	00:0C:29:3F:26:43	SLM	SLM	Yes	4.0.
92	SLM573E	172.19.100.165	00:30:48:5D:57:3E	SLM	SLM	No	3.4
93	SLP_Glenn_237_30	172.19.237.30	00:80:A3:8B:00:02	SLP	SLP	No	5.3p
94	SLS Duo	172.19.100.76	00:80:A3:8C:8B:51	SPDR	SLS Duo	No	3.0
95	SLS-PC3923	172.19.39.194	00:80:A3:8E:1E:9F	SPDR	SLS Duo	Yes	3.0
96	Solaris10	172.18.21.75	00:20:4A:80:8C:0A	SPDR	SLS	Yes	3.1
97	SpiderSLM117	172.18.21.78	00:80:A3:8C:16:76	SPDR	SLS	Yes	3.0
98	TEST1	172.19.39.23	00:17:31:47:19:71	Other		No	
99	TESTXP1	172.19.39.182	00:50:56:C0:00:08	Other		No	
100	TN3270	128.227.128.75	11:22:33:44:55:66	Other	Model	No	
101	TS	172.18.0.216	00:80:A3:88:27:4A	SLK	SLK	No	
102	TSFTP	172.18.21.76	00:80:A3:8C:00:40	SPDR	SLS	Yes	3.0
103	tslabel	172.18.0.103	00:40:01:23:A3:6A	Other		No	
104	tsslc32	172.18.0.107	00:30:31:FF:FF:54	SLC	SLC32	No	5.4
105	TSXPVIRTUAL	172.18.21.16	00:16:17:F8:3C:2A	Other		No	
106	Ubuntu	172.18.21.71	00:80:A3:FA:CE:DE	SPDR	SLS Duo	Yes	3.0
107	UDS2100	172.19.39.244	00:20:4A:9C:6A:EE	UDS	UDS2100	No	6.5
108	vsIm02_glenn2501	172.19.100.39	00:0C:29:F4:EF:A5	SLM	SLM	Yes	4.0.
109	WiBox b/g	172.19.210.210	00:20:4A:96:15:BF	WiBox	WiBox b/g	No	6.8
110	Windows2003	172.18.21.74	00:80:A3:8C:51:4C	SPDR	SLS Duo	Yes	3.0
111	Windows2012	172.18.21.77	00:80:A3:8C:56:64	SPDR	SLS Duo	Yes	3.1
112	Windows7	172.18.21.72	00:20:4A:80:8D:96	SPDR	SLS Duo	Yes	3.2
113	Windows81Pro	172.18.21.70	00:20:4A:80:8D:BD	SPDR	SLS Duo	Yes	3.0
114	WindowsXP	172.18.21.73	00:20:4A:80:8D:BC	SPDR	SLS Duo	Yes	3.2
115	XPort-03/04	172.19.212.62	00:20:4A:E3:96:5C	XPort	XPort-03/04	No	6.10

Continuation of [Figure 11-29](#) (part 5 of 5)

```

115 XPort-03/04      172.19.212.62  00:20:4A:E3:96:5C XPort XPort-03/0 No  6.10
Managed device -----
Idx Name           Group      Device      Serial Power1 Power2 KVM Modem
-----
116 CiscoSwitch    mgroup_2  CiscoSwitch Yes   Yes   Yes
117 MD-linux21     mgroup_2  linux21     Yes   Yes   Yes   Yes
118 MD-linux22     mgroup_3  linux22     Yes   Yes   Yes   Yes
119 TSXPVIRTUAL    mgroup_7  TSXPVIRTUAL Yes   Yes   Yes
120 MD-linux20     mgroup_1  linux20     Yes   Yes   Yes   Yes
121 MD-PowerOutlet-1 mgroup_1                Yes   Yes
122 MD-PowerOutlet-3 mgroup_1                Yes
123 MD-PowerOutlet-4 mgroup_1                Yes
124 MD-PowerOutlet-5 mgroup_1                Yes
125 MD-PowerOutlet-6 mgroup_1                Yes
126 MD-PowerOutlet-7 mgroup_1                Yes
127 MD-PowerOutlet-8 mgroup_1                Yes
128 MD-linux242    mgroup_4  linux242    Yes   Yes   Yes   Yes
115 ethernet device(s) and 13 managed device(s) found.

show persistent-----
Idx Name           Parent      Protocol Last Established Active Status
-----
1 CiscoSwitch_1    CiscoSwitch Telnet  12/12/2014 04:35: Yes  Connect
2 CiscoSwitch_2    CiscoSwitch Telnet  12/12/2014 04:35: Yes  Connect
3 judytest        Fedora-242-1 Secure  12/11/2014 21:04: Yes  Up
4 linux20_1       linux20     Telnet  12/12/2014 04:35: Yes  Connect
5 linux20_2       linux20     Telnet  12/12/2014 04:35: Yes  Connect
6 linux21_1       linux21     SSH     12/12/2014 04:35: Yes  Connect
7 linux21_2       linux21     SSH     12/12/2014 04:35: Yes  Connect
8 linux22_1       linux22     Telnet  12/12/2014 04:35: Yes  Connect
9 linux22_2       linux22     Telnet  12/12/2014 04:36: Yes  Connect
10 persist3921_1   DSM-Access SSH     12/12/2014 04:35: Yes  Connect
11 persist3921_10  DSM-Access SSH     12/12/2014 04:35: Yes  Connect
12 persist3921_11  DSM-Access SSH     12/12/2014 04:33: Yes  Up
13 persist3921_2   DSM-Access SSH     12/12/2014 04:33: Yes  Up
14 persist3921_3   DSM-Access SSH     12/12/2014 04:33: Yes  Up
15 persist3921_4   DSM-Access SSH     12/12/2014 04:33: Yes  Up
16 persist3921_5   DSM-Access SSH     12/12/2014 04:33: Yes  Up
17 persist3921_6   DSM-Access SSH     12/12/2014 04:33: Yes  Up
18 persist3921_7   DSM-Access SSH     12/12/2014 04:33: Yes  Up
19 persist3921_8   DSM-Access SSH     12/12/2014 04:33: Yes  Up
20 persist3921_9   DSM-Access SSH     12/12/2014 04:33: Yes  Up
21 test           slc247     SSH     12/11/2014 20:25: Yes  Up
22 TSXPVIRTUAL_1  TSXPVIRTUAL Telnet  12/11/2014 20:25: Yes  Down
23 TSXPVIRTUAL_2  TSXPVIRTUAL Telnet  12/11/2014 20:25: Yes  Down

[SLM System Status Reports End]

Email address:  

```

- To email the status, enter the recipient's email address and click the **Send Report** button.

Services Commands

```
set service auditlog
```

Syntax

```
set service auditlog <enable|disable>
```

Description

Enables or disables audit logging.

```
set service telnet
```

Syntax

```
set service telnet <enable|disable>
```

Description

Enables or disables Telnet logging to the vSLM 2 software.

set service ssh**Syntax**

```
set service ssh <enable|disable> version <1|2>
```

Description

Enables or disables SSH logging to the vSLM 2 secure management software.

set service sessionlog**Syntax**

```
set service sessionlog <enable|disable>
```

Description

Enables or disables session logging.

set service wap**Syntax**

```
set service wap <enable|disable>
```

Description

Enables or disables WAP access to the vSLM device.

set service httpsonly**Syntax**

```
set service httpsonly <enable|disable>
```

Description

Enables or disables https.

show service**Syntax**

```
show service
```

Description

Displays service settings.

Maintenance

The SLM Maintenance page allows administrators to:

- ◆ Reboot or shut down the vSLM 2 secure management software.
- ◆ Save a snapshot of all database settings (configuration, configured users, and discovered devices) on the vSLM 2 software or the user's client machine.
- ◆ Restore the configuration, either to a previously saved configuration or to the factory defaults.
- ◆ Update user passwords on selected vSLM 2/SLC/SLB/RPM/SLP and SCS05/20 vSLM 2 software (password synchronization).
- ◆ View the firmware version on two boot banks, and select the bank to boot from.

To configure maintenance activities:

1. On the menu, click **Services > Maintenance**. The following page opens:

Figure 11-30 SLM Maintenance Page

The screenshot displays the LANTRONIX SLM Maintenance page. At the top, there is a user login area with fields for 'Table: User', 'Field: Name', and 'Value: glenn', along with 'Search' and 'Reset' buttons. The user is identified as 'sysadmin@SLM1C77' in the 'Group: Administrators' section. The main navigation menu on the left includes 'Configuration', 'Network Settings', 'Authentication', 'Services', 'Maintenance' (highlighted), 'Date & Time', 'SNMP & Syslog', 'Firmware Updates', 'Device Management', 'Accounts', 'Events', 'Files', 'Ethernet Devices', and 'Managed Devices'. The 'SLM Maintenance' page has tabs for 'Configure', 'Versions', 'Notes', and 'Help'. The 'General' section contains 'Reboot' and 'Shutdown' checkboxes. The 'Password Synchronization' section has a 'Push Passwords' checkbox. The 'Boot Banks' section shows 'Bank 1: 4.0.0.0 (current)' and 'Bank 2: 4.0.0.0', with a 'Next Boot Bank: 1' and a 'Use Bank 2 on Next Boot' checkbox. The 'Configuration Management' section has radio buttons for 'Restore Configuration From Client', 'Restore Configuration From Local File', and 'Restore Factory Defaults'. There are also checkboxes for 'Preserve Network Settings', 'Preserve User Accounts', 'Preserve Devices & Ports', and 'Preserve SSH Keys'. At the bottom, there are radio buttons for 'Save Configuration To Client', 'Save Configuration To SLM', and 'No Save / Restore', along with an 'Overwrite existing file' checkbox and a 'Submit' button.

Table 11-31 SLM Maintenance - General Maintenance

General Maintenance Setting	Description
Reboot	Select this option to terminate all connections and reboot the vSLM 2 secure management software immediately.
Shutdown	Select this option to terminate all connections, shut down the vSLM 2 software immediately, and turn off the power.

Note: It is recommended that virtual vSLM 2 secure management software be shutdown or restarted using the vSLM 2 software reboot and shutdown commands available via the web or CLI, rather than using the virtualization manager to shutdown or restart the vSLM 2 secure management software.

Table 11-32 SLM Maintenance - Password Synchronization

Password Synchronization Setting	Description
Push Passwords	<p>When the Push Passwords check box on the Maintenance page is selected, the vSLM 2 secure management software uses the password on all accounts with Synchronize Password enabled to update accounts on remote SLM, SLC, SLB, RPM/SLP and SCSxx05/20 devices. The accounts must have access rights to and local user accounts on the devices.</p> <p>For the SCSxx05/20 and RPM/SLP devices, you must store the username and password for each target device in the vSLM 2 secure management software, enabling password(s) to be transferred by SSH.</p>

Table 11-33 SLM Maintenance - Boot Banks

Boot Banks Setting	Description
Bank 1	<p>Version of vSLM 2 firmware in bank 1.</p> <p>Note: The word "current" displays next to the bank the vSLM 2 secure management software booted from.</p>
Bank 2	Version of vSLM 2 firmware in bank 2.
Next Boot Bank	Current setting for bank to boot from at next reboot.
Use Bank n on Next Boot	If desired, select the alternate bank to boot from at next reboot. This option is disabled during the vSLM 30 day trial period.

From the option list, select one of the following:

Table 11-34 SLM Maintenance - Configuration Management

Configuration Management Setting	Description
Restore Configuration from Client	Returns the vSLM 2 settings to a previously saved configuration. If you select this option, the vSLM 2 secure management software reboots after you apply the update. If you select this option, the Browse button becomes available. Browse to the saved configuration.
Restore Configuration from Local File	Restores the configuration to one saved on the vSLM 2 software. Select the file from the drop-down list.

Configuration Management Setting	Description
Restore Factory Defaults	<p>Restores factory settings. If you select this option, the vSLM 2 secure management software reboots after you apply the update. To keep specific groups of settings rather than restoring defaults, select one or more of the following options:</p> <ul style="list-style-type: none"> ◆ Preserve Network Settings This option preserves the settings on the Network Settings and the Services page. ◆ Preserve User Accounts ◆ Preserve Devices & Ports This option preserves Ethernet and managed devices and their groups. ◆ Preserve SSH Keys This option preserves existing SSH Keys in the database for use with the restored system. <p>The four preserve options apply to any of the restore options. If you select a preserve option, then after restoration, all of the current "preserved" items are deleted, and the preserved items from before the restore are re-inserted.</p> <p>Example: You restore to a backup file but elect to preserve user accounts. The vSLM 2 secure management software is restored to the contents of the backup file, then all accounts (including any that were just restored) are deleted, and lastly, all the accounts, account groups, and notes about account groups that were present before the restore operation are added to the system.</p> <p>The same is true for devices and ports. If you preserve devices and ports, all associations with account groups are lost, even if both accounts and devices are preserved.</p> <p>Note: If you select any of the three Restore operations, the vSLM 2 secure management software saves the current configuration in the vSLM 2 Configuration Files directory using the name <code>autoConfigSaveYYMMDDHHMMSS.slm</code> before performing the restore command.</p>
Save Configuration to Client	<p>Saves all settings to a file on the client system, which you can back up to a location not on the vSLM 2 secure management software.</p> <p>The vSLM 2 software sends the file containing the state of the system to the client machine for storage. The default file name is <code>configsave.slm</code>, but you may save it using any name. This is the file uploaded to the vSLM 2 secure management software upon system restore.</p>
Save Configuration to SLM	<p>Saves all settings to the SLM device. If selected, enter the configuration file name. To overwrite the existing field with this configuration file, select the check box. Unselected by default.</p>
No Save/Restore	Does not save or restore a configuration.

Maintenance Commands

admin config

Syntax

`admin config factorydefaults`

Description

Restores the vSLM 2 configuration and device database settings to factory defaults.

admin config rebuilddatabase**Syntax**

```
admin config rebuilddatabase
```

Description

Removes and rebuilds the vSLM 2 configuration and database from scratch, in case of database corruption that cannot be fixed by the factory default.

admin config save file**Syntax**

```
admin config save file <filename>
```

Description

Saves the vSLM 2 configuration to the vSLM 2 Configuration Files directory.

admin config showfiles**Syntax**

```
admin config showfiles
```

Description

Shows saved configuration files.

admin locallog clear**Syntax**

```
admin locallog clear auditlog
admin locallog clear syslog
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, RPM, SCS, SCSx, SLB, SPDR, WiBox, UDS, EDS,
EDSMD, Xport, PWave, LTRX, or other
```

Description

Clears all of the entries in the auditlog, syslog, or traplog.

admin quicksetup**Syntax**

```
admin quicksetup
```

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command.

admin reboot**Syntax**

```
admin reboot
```

Description

Terminates all connections and reboots the vSLM 2 secure management software.

admin securechannel regenkey**Syntax**

```
admin securechannel regenkey
```

Description

Regenerates the secure channel key.

Note: *With this command, you lose access to established secure channels; therefore, the vSLM 2 secure management software first requests confirmation that you want to regenerate the securechannel key.*

admin shutdown**Syntax**

```
admin shutdown
```

Description

Terminates all connections, shuts down the vSLM 2 software, and turns off the power.

admin version**Syntax**

```
admin version
```

Description

Displays current application version information.

show progress**Syntax**

```
show progress
```

Description

Shows the progress of background tasks.

show sysconfig**Syntax**

```
show sysconfig [email <Email Address>]
```

Description

Displays a report of configurable parameters. The output can be emailed.

show sysinfo**Syntax**

```
show sysinfo
```

Description

Displays general system information.

Date and Time

You can specify the current date, time, and time zone at the vSLM 2 secure management software's location, or the vSLM 2 software can use NTP to synchronize with an NTP server on your network.

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

1. On the menu, click **Configuration > Services > Date & Time**. The following page opens:

Figure 11-35 Date & Time Page

2. Enter the following information:

Table 11-36 Date & Time - Configure Tab

Date & Time Setting	Description
Change Date/Time	Select the check box to manually enter the date and time at the vSLM 2 secure management software's location.
Date	From the drop-down lists, select the current month, day, and year.

Date & Time Setting	Description
Time	From the drop-down lists, select the current hour and minute.
Time Zone	From the drop-down list, select the appropriate time zone.
SLM Up Time	Indicates how long the vSLM 2 secure management software has been up and running.

- To save, click the **Update** button. When the update is complete, a confirmation message displays.

To synchronize the vSLM 2 secure management software with a remote timeserver using NTP:

- Enter the following:

Table 11-37 Date & Time - Configure NTP

Setting	Description
Enable NTP	Select the check box to enable NTP synchronization. NTP is disabled by default.
Synchronize via	Select one of the following: <ul style="list-style-type: none"> ◆ Broadcast from NTP Server: Enables the vSLM 2 secure management software to accept time information periodically transmitted by the NTP server. This is the default if you enable NTP. ◆ Poll NTP Server: Enables the vSLM 2 software to query the NTP Server for the correct time. If you select this option, complete one of the following: ◆ 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. We do not recommend this 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.) ◆ Local: Select this option if the NTP server is on a local network, and enter the IP address of the NTP server. This is the default, and we highly recommend it.

- To save, click the **Update** button. When the update is complete, a confirmation message displays.

Date and Time Commands

set datetime

Syntax

```
set datetime <one parameter>
```

Parameters

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

Description

Sets the local date, time, and time zone (one parameter at a time).

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

show datetime**Syntax**

```
show datetime
```

Description

Displays the local date, time, and time zone.

SNMP & Syslog

Administrators can configure a Simple Network Management Protocol (SNMP) agent to allow users read-only access to the system.

1. On the menu, click **Configuration > Services > SNMP & Syslog**. The following page opens:

Figure 11-38 SNMP & Syslog Page

The screenshot shows the LANTRONIX SLM web interface for configuring SNMP & Syslog. The page title is "SNMP & Syslog". The interface includes a navigation menu on the left with options like Configuration, Network Settings, Authentication, Services, Maintenance, Date & Time, and SNMP & Syslog. The main content area has tabs for "Configure", "Notes", and "Help". The configuration fields are as follows:

- SNMP Agent:
- NMS: 172.20.197.125
- Contact: Glenn Fountain
- V3 User: vslmuser
- Location: Irvine Ca, 92618
- Send Traps to Syslog:
- Enable Trap Reception:
- Read Community: public
- Trap Community: public
- V3 Password: ●●●●●●
- Password Retype: ●●●●●●
- Authentication: MD5 Encryption: DES
- SMTP Server: 172.16.1.22
- Remote Syslog Server:
- Syslog Server 1: 172.20.197.125
- Syslog Server 2: 0.0.0.0

Buttons for "Update" and "Reset" are located at the bottom of the configuration area.

2. Enter the following information:

Table 11-39 SNMP & Syslog - Configure

Setting	Description
SNMP Agent	Enables read-only access into the vSLM 2 secure management software. Disabled by default.
Enable Trap Reception	<p>Enables the vSLM 2 software to receive traps from outside and to store and display them on the Traps page. Disabled by default.</p> <p>Traps are notifications of certain critical events. This feature is applicable when SNMP is enabled. When the SLC or other secure IT management products (vSLM 2 secure management software, RPM/SLP power manager, or SLK device) configures the vSLM 2 software as its NMS, the vSLM 2 software receives these traps and displays them on the Traps page.</p> <p>The Traps page display has three levels:</p> <ul style="list-style-type: none"> ◆ Level 1: Ethernet device ◆ Level 2: vSLM 2/SLC/RPM/SLP/SLK ◆ Level 3: Individual device page

Setting	Description
NMS	When SNMP is enabled, an NMS acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP. The NMS can request information from the vSLM 2 secure management software and receive traps from the vSLM 2 software. Enter the IP address of the NMS server. Required if you selected SNMP Agent .
Read Community	An SNMP community is the group to which devices and management stations running SNMP belong. The default setting is public. <i>Note: Because SSH-to-RPM/SLP authentication may take a long time, this setting allows the user to choose SNMP support, which is faster.</i>
Contact (optional)	Description of the person responsible for maintaining the vSLM 2 secure management software, for example, a name.
Trap Community	Only management devices that are listening for the specified trap community process the trap. Management devices that are not listening for that trap community ignore the trap.
V3 User	SNMP v3 is secure and requires user-based authorization to access vSLM 2 MIB objects. Enter a user name. No defaults.
V3 Password and Password Retype	Password for accessing the SNMP v3. No defaults.
Location (optional)	Physical location of the vSLM 2 secure management software. Useful for managing the vSLM 2 software using SNMP.
Send Traps to Syslog	Enables the vSLM 2 secure management software to receive traps from outside and to display them in the syslog.
Authentication and Encryption	vSLM 2 software settings for SNMP v3 protocol. (Read only)
SMTP Server	IP address of your network's Simple Mail Transfer Protocol (SMTP) relay server.
Remote Syslog Server	Select to indicate that the vSLM 2 secure management software will act as a remote syslog server to receive syslogs from other Ethernet devices (devices that have the vSLM 2 software's IP Address specified as that device's syslog server).
Syslog Server 1 and Syslog Server 2	IP addresses of the main and secondary servers to which the vSLM 2 system logs are being forwarded.

- To save, click the **Update** button. When the update is complete, a confirmation message displays.

Device Firmware Updates

On these pages, you can update the firmware of Lantronix's Ethernet Devices.

1. On the main menu, click **Services > Firmware Updates**. The following page opens:

Figure 11-40 Device Firmware Update Page - SLM Tab

SLM Firmware

Note: One year of Auto SLM Update comes with your SLM installation. This feature automatically facilitates new firmware updates from a Lantronix server to your vSLM 2 secure management software. Please contact Lantronix Sales at 800-422-7055 for additional information on enabling this feature after the first included year.

To update SLM firmware:

1. Enter the following information:

Table 11-41 Device Firmware Update - SLM Tab

Setting	Description
Current Version (view only)	Number of the firmware release on the vSLM 2 secure management software.
Load Firmware via	From the drop-down list, select the method of loading the firmware. Options are FTP , SFTP , and Local File . FTP is the default. Note: The Local File option is active only when at least one file exists in the SLM FW Upgrade Files directory.
Firmware Filename	The name of the firmware update file downloaded from the Lantronix web site.
Key	If the user selects the firmware file from the SLM FW Upgrade Files directory, no entry is required. Otherwise, enter a key for validating the firmware file. Lantronix provides the key with the firmware file (32 hex characters).
Local File	From the drop-down list, select the firmware update (from the Files > SLM Upgrade Files directory).
Client File	Enter or browse to the file where the update is stored.

Setting	Description
Check Lantronix (Only displays for service plan holders)	If you have an active Lantronix service plan for your vSLM 2 secure management software, you can download update files directly from the Lantronix server onto your vSLM 2 software. If you select this checkbox, and click the Submit button, the vSLM 2 secure management software will interrogate the Lantronix Server to see if a firmware update file is available for your system. If one is present, then an additional option, Lantronix Server , displays in the Load Firmware via drop-down list.

Table 11-42 Device Firmware Update - SLM Tab - FTP/SFTP Server

Setting	Description
FTP Server	The IP address or host name of the server used for obtaining updates. May have up to 64 alphanumeric characters and may include hyphens and underscores.
Path	The default path on the server for obtaining firmware update files. May be blank.
Login	The user name for accessing the FTP server.
Password and Confirm Password	The FTP user password.
Connect Timeout (secs)	The number of seconds after which the connection attempt times out. Default is 60 .
Download Timeout (secs)	The number of seconds after which the download attempt times out. Default is 180 .

2. Click the **Update** button.

Note: To check the progress of the update, click the **Progress** button above the menu.

SLC/SLB Firmware

To update SLC/SLB firmware:

1. On the Device Firmware Updates page, click the **SLC/SLB** tab. The following page opens:

Figure 11-43 Device Firmware Update Page - SLC/SLB Tab

The screenshot shows the Lantronix SLM web interface for updating SLC/SLB firmware. The page title is "Device Firmware Update" and the selected tab is "SLC/SLB". The left sidebar contains a navigation tree with categories like Configuration, Services, Device Management, and Accounts. The main content area is titled "SLC/SLB Firmware Update" and contains the following fields and options:

- Load Firmware via:** A dropdown menu set to "FTP on SLM".
- Firmware Filename:** An empty text input field.
- Key:** An empty text input field.
- Local File:** A dropdown menu.
- Client File:** A "Browse..." button with the text "No file selected."
- FTP Server:** An empty text input field.
- Path:** An empty text input field.
- Login:** An empty text input field.
- Password:** A text input field with masked characters (dots).
- Retype Password:** A text input field with masked characters (dots).
- Connect Timeout (secs):** A text input field set to "60".
- Download Timeout (secs):** A text input field set to "180".
- SLC/SLB Devices to Update:** A list box containing the following devices: DSM-Access (172.19.39.248), lyonslb (172.18.21.67), mslc48 (172.18.21.66), mslc8048 (172.18.21.61), patlab_slb1 (172.19.212.153), patlab_slb2-1 (172.19.229.253), slb08_250_54_1 (172.19.39.250), slb792c (172.18.21.69), slb8Ref_120-6100 (172.19.100.87), and slbdb40 (172.19.39.253).
- Checkboxes:**
 - Use current configuration in new bank?
 - Reboot device after firmware update?
- Update:** A button at the bottom of the form.

2. Enter the following information:

Table 11-44 Device Firmware Update - SLC/SLB Tab

Setting	Description
Load Firmware via	<p>From the drop-down list, select the method of loading the firmware. You have the following options:</p> <p>FTP on SLC/SLB, SFTP on SLC/SLB, and TFTP on SLC/SLB: The SLM commands the SLC/SLB device to download the SLC/SLB firmware file directly from a server to the SLC/SLB module.</p> <p>FTP on SLM and SFTP on SLM: The vSLM 2 secure management software first checks to see whether the vSLM 2 firmware file already exists on the SLM local hard disk. If not, the vSLM 2 downloads it using FTP or SFTP. The vSLM 2 software stores the firmware file locally, securely copies the file to the selected SLC/SLB devices, and runs the firmware update on the SLC/SLB modules.</p> <p>HTTP From Client</p> <p>Note: The Local File option is active only when at least one file exists in the SLC/SLB FW Upgrade Files directory.</p>
Firmware Filename	The name of the firmware update file downloaded from the Lantronix web site.

Setting	Description
Key	If the user selects the firmware file from the SLC/SLB FW Upgrade Files directory, no entry is required. Otherwise, enter a key for validating the firmware file. Lantronix provides the key with the firmware file (32 hex characters).
Local File	From the drop-down list, select the firmware update (from the Files > SLC/SLB FW Upgrade Files directory.)
Client File	Enter or browse to the file where the update is stored.

Table 11-45 Device Firmware Update - SLC/SLB Tab - FTP/SFTP Server

Setting	Description
FTP Server	The IP address or host name of the server used for obtaining updates. May have up to 64 alphanumeric characters and may include hyphens and underscores.
Path	The default path on the server for obtaining firmware update files. May be blank.
Login	The user name for accessing the FTP server.
Password and Confirm Password	The FTP user password.
Connect Timeout (secs)	The number of seconds after which the connection attempt times out. Default is 60.
Download Timeout (secs)	The number of seconds after which the download attempt times out. Default is 180.
Apply firmware update to inactive bank?	Newer SLC console managers and SLB branch office managers use two partitions (should one fail, the user can fall back to the other). Check this option to apply the firmware update to the inactive partition.
Use current configuration in new bank?	If updating the inactive partition, this will take the configuration from the current (active) bank and apply it to the updated partition.
Reboot device after firmware update?	Use this option to force the SLC/SLB device to reboot (and come up using the new firmware version).

3. In the **SLC/SLB Devices to Update** area, select one or more of the SLC/SLB modules managed by the vSLM 2 secure management software. (Use **Ctrl+** click for multiple selections.)
4. To update the SLC/SLB devices, click the **Update** button. When the update is complete, a confirmation message displays.

Note: To check the progress of the update, click the **Progress** button above the menu.

RPM/SLP Firmware

To update RPM/SLP firmware:

1. On the Device Firmware Update page, click the **RPM/SLP** tab. The following page opens:

Figure 11-46 Device Firmware Update - RPM/SLP Tab

The screenshot displays the Lantronix SLM web interface for updating RPM/SLP firmware. The top navigation bar includes the Lantronix SLM logo, a search bar, and user information (sysadmin@SLM1F4F, Group: Administrators). The left sidebar shows a tree view of configuration options, with 'Firmware Updates' highlighted. The main content area is titled 'Device Firmware Update' and contains several tabs: SLM, SLC/SLB, RPM/SLP (selected), Spider, WiBox, UDS/SDS, Notes, and Help. The 'RPM/SLP Firmware Update' section includes a 'Load Firmware via' dropdown menu set to 'FTP on SLM'. Below this are fields for 'Firmware Filename', 'Key', 'Local File', and 'Client File' (with a 'Browse...' button). To the right, there are fields for 'FTP Server', 'Path', 'Login', and 'Password' (with a 'Retype Password' field). There are also input fields for 'Connect Timeout (secs): 60' and 'Download Timeout (secs): 180'. A list of 'RPM/SLP Devices to Update' is shown, with four entries: SecureLinuxSLP_8b000f (172.18.21.65), SecureLinuxSLP_8b0026 (172.19.39.44), SecureLinuxSLP_8b0133 (172.18.0.108), and SLP_Glenn_237_30 (172.19.237.30). An 'Update' button is located at the bottom right of the form.

2. Enter the following information:

Table 11-47 Device Firmware Update - RPM/SLP Tab

Setting	Description
Load Firmware via	<p>From the drop-down list, select the method of loading the firmware. You have the following options:</p> <p>Select FTP on RPM/SLP for the vSLM 2 secure management software to command the RPM/SLP power manager to download the RPM/SLP firmware file to the RPM/SLP unit directly from a server.</p> <p>Select FTP on SLM or SFTP on SLM for the vSLM 2 secure management software to first check to see whether the RPM/SLP firmware file already exists on the SLM local hard disk. If not, the SLM downloads it using FTP or SFTP. The vSLM 2 software stores the firmware file locally; then the vSLM 2 secure management software serves as the FTP server and allows the RPM/SLP power manager to download the firmware file from the vSLM 2 software, and then runs the firmware update.</p> <p>HTTP From Client</p> <p>Note: The Local File option is active only when at least one file exists in the SLP FW Upgrade Files directory.</p>

Setting	Description
Firmware Filename	The name of the firmware update file downloaded from the Lantronix web site.
Key	If the user selects the firmware file from the RPM/SLP FW Upgrade Files directory, no entry is required. Otherwise, enter a key for validating the firmware file. Lantronix provides the key with the firmware file (32 hex characters).
Local File	From the drop-down list, select the firmware update (from the Files > RPM/SLP Upgrade Files directory.)
Client File	Enter or browse to the file where the update is stored.

Table 11-48 Device Firmware Update - RPM/SLP Tab - FTP/SFTP Server

Setting	Description
FTP Server	The IP address or host name of the server used for obtaining updates. May have up to 64 alphanumeric characters and may include hyphens and underscores.
Path	The default path on the server for obtaining firmware update files. May be blank.
Login	The user name for accessing the FTP server.
Password and Confirm Password	The FTP user password.
Connect Timeout (secs)	The number of seconds after which the connection attempt times out. Default is 60 .
Download Timeout (secs)	The number of seconds after which the download attempt times out. Default is 180 .

3. In the **RPM/SLP Devices to Update** area, select one or more of the RPM/SLP power managers managed by the vSLM 2 secure management software. (Use **Ctrl+click** for multiple selections.)
4. To update the RPM/SLP units, click the **Update** button. When the update is complete, a confirmation message displays.

Note: To check the progress of the update, click the **Progress**  button above the menu.

Spider Firmware

1. On the Device Firmware Updates page, click the **Spider** tab. The following page opens.

Figure 11-49 Device Firmware Update Page - Spider Tab

2. Enter the following information:

Table 11-50 Device Firmware Update - Spider

Setting	Description
Load Firmware via	From the drop-down list, select the method of loading the firmware. You have the following options: HTTP From Client <i>Note:</i> The Local File option is active only when at least one file exists in the Spider FW Upgrade Files directory.
Local File	From the drop-down list, select the firmware update file stored on the vSLM 2 secure management software.
Client File	Enter or browse to the file where the update is stored.

3. In the **Spider Devices to Update** area, select one or more of the Spider units the vSLM 2 secure management software is managing. (Use **Ctrl+click** for multiple selections.)
4. To update the Spiders devices, click the **Update** button. When the update is complete, a confirmation message displays.

Note: To check the progress of the update, click the **Progress**  button above the menu.

WiBox Firmware

To update firmware on a WiBox:

1. On the Device Firmware Updates page, click the **WiBox** tab.

Figure 11-51 Device Firmware Update Page - WiBox Tab

2. Enter the following information:

Table 11-52 Device Firmware Update - WiBox

Setting	Description
Load Firmware via	From the drop-down list, select the method of loading the firmware. You have the following options: HTTP From Client <i>Note:</i> The <i>Local File</i> option is active only when at least one file exists in the <i>WiBox FW Upgrade Files</i> directory.
Local File	From the drop-down list, select the firmware update file stored on the vSLM 2 secure management software.
Client File	Enter or browse to the file where the update is stored.
WiBox File Code	Enter the 2-character firmware code that matches your WiBox device. <i>Note:</i> Not all WiBox units share the same code. See the User Guide for your WiBox to find the correct code.

3. In the **WiBox Devices to Update** area, select one or more of the WiBoxes the vSLM 2 secure management software is managing. (Use **Ctrl+click** for multiple selections.)
4. To update the WiBoxes, click the **Update** button. When the update is complete, a confirmation message displays.

Note: To check the progress of the update, click the **Progress** button above the menu.

UDS/SDS Firmware Updates

To update firmware on a UDS/SDS:

1. On the Device Firmware Updates page, click the **UDS/SDS** tab. The following page opens:

Figure 11-53 Device Firmware Update Page - UDS/SDS Tab

2. Enter the following information:

Table 11-54 Device Firmware Update - UDS/SDS

Setting	Description
Load Firmware via	From the drop-down list, select the method of loading the firmware. You have the following options HTTP From Client Note: The <i>Local File</i> option is active only when at least one file exists in the UDS/SDS FW Upgrade Files directory.
Local File	From the drop-down list, select the firmware update file stored on the vSLM 2 secure management software.
Client File	Enter or browse to the file where the update is stored.
UDS/SDS File Code	Enter the 2-character firmware code that matches your UDS/SDS. Note: Not all UDS/SDS units share the same code. See the User Guide for your UDS/SDS to find the correct code.

3. In the UDS/SDS Devices to Update area, select one or more of the UDS/SDS units the vSLM 2 secure management software is managing. (Use **Ctrl+** click for multiple selections.)
4. To update the UDS/SDS units, click the **Update** button. When the update is complete, a confirmation message displays.

Note: To check the progress of the update, click the **Progress**  button above the menu.

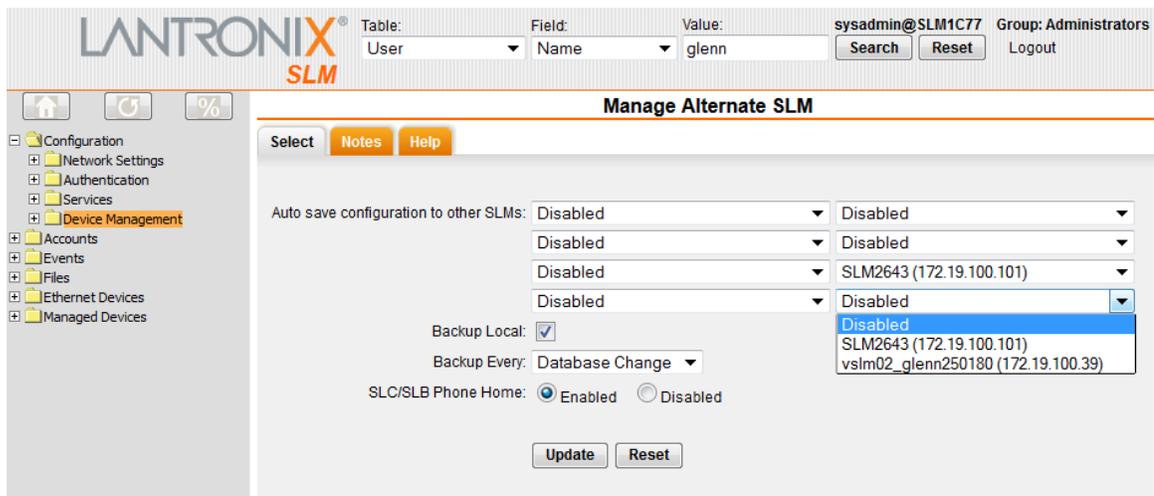
Managing Alternate SLM Devices

When **Auto save configuration to other SLMs** is enabled, the vSLM 2 secure management software immediately saves its own configuration to up to eight remote SLM units. After that, every time the vSLM configuration has changed, it waits 60 minutes to make sure there are no more changes before saving another configuration to the remote SLM appliances. The remote SLM units keep the most recent 10 configuration files saved by auto save configuration.

To auto-save a configuration:

1. On the menu, click **Configuration > Device Management**. The following page opens:

Figure 11-55 Auto Saving a Configuration



2. Enter the following information:

Table 11-56 Manage Alternate SLM Devices - Select Tab

Setting	Description
Auto save configuration to other SLMs	From the drop-down lists, select up to eight SLM devices on which automatically saved configuration files will be stored. (Disabled by default.) Note: For vSLM 2 software to populate the drop-down lists, they must have a secure channel connection with your SLM unit.
Backup Local	When creating saved configuration files, copy one to the local machine as well.
Backup Every	From the drop-down list, select how often to back up the configuration(s). You can back up the configuration(s) every time there is a database change or at specific daily intervals, regardless of whether there was a change.
SLC/SLB Phone Home	Allow SLC/SLB devices to automatically insert themselves into the SLM database without a discovery operation performed.

3. To save, click the **Update** button. When the update is complete, a confirmation message displays.

- To reset to original values, click the **Reset** button.

Managing Devices Through the Actions Tab

Administrators can reboot, shutdown, get log, status, and configuration files, restore configurations, and execute CLI commands.

Depending on the device, different options will be offered.

Using the Actions Tab

The Actions tab is active for the SLC, SLB, Spider and UDS Group pages. It allows you to perform many tasks related to the discovered devices. You can perform only one action at a time on a single device, but you may perform the same action on multiple or all devices or different actions on multiple devices.

- On the menu, click **Ethernet Devices** and select a specific device group. The Manage "selected device group" Group page opens.
- Click the **Actions** tab. The following page opens for SLC/SLB console manager. Note that this page will differ for Spider and UDS devices.

Figure 11-57 Manage "SLC" Group Actions Tab

The screenshot shows the LANTRONIX SLM web interface. The main content area is titled "Manage 'SLC' Group" and features several tabs: List, Add, Traps, Actions (selected), Port Access, Notes, and Help. Below the tabs, there are search filters for Location and Sub-Location. A table lists various SLC devices with columns for Name, IP addr, Reboot, Shutdown, Get Syslogs, Get Audit Log, Get Config, Get Sysconfig, Restore Config, Get SSH, Push SSH, Read Info, CLI Cmd, Get Groups, Push Groups, and Set Location. Each cell in the table contains a checkbox. Below the table is a CLI command input field and a note: "Multiple commands are separated by semi-colons".

Name	IP addr	Reboot	Shutdown	Get Syslogs	Get Audit Log	Get Config	Get Sysconfig	Restore Config	Get SSH	Push SSH	Read Info	CLI Cmd	Get Groups	Push Groups	Set Location
tssc32	172.18.0.107	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
m1slc8048	172.18.21.61	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
m1slc48	172.18.21.66	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slbdb40	172.19.39.253	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slc16_glenn	172.19.39.254	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slc48_glenn_1	172.19.100.90	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slc5e35	172.19.100.116	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slc-md-u	172.19.100.125	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slcRef250120	172.19.100.221	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slc4857	172.19.213.8	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slc4331	172.19.250.119	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slca508	172.19.250.120	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										
slcRefreshR17_167	172.19.250.167	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>										

- To perform an action on all of the listed SLC console managers, select the check box in the column header,

OR

To perform an action on multiple SLC devices, select the check box for each desired SLC module.

- To filter the list of SLC or SLB devices displayed by location and sub-location, enter a location and an optional sub-location in the location fields and select **Filter**.

Before performing an action on another group of devices, access the SLM auditlog or SLM syslog file.

Following are the available actions:

- ◆ Reboot
 - ◆ Shutdown
 - ◆ Get Syslogs
 - ◆ Get Audit Log
 - ◆ Get Config
 - ◆ Get Sysconfig
 - ◆ Restore Config
 - ◆ Get SSH/Push SSH
 - ◆ Read Info
 - ◆ CLI Cmd (For CLI Cmd, you may specify any number of devices.)
 - ◆ Get Groups
 - ◆ Push Groups
 - ◆ Set Locations
- Click the **Progress** button to view the status of your commands. For more details, view the SLM auditlog and SLM syslog.

Rebooting or Shutting Down

Use the Actions tab to reboot or shut down one or more SLC console managers.

To reboot or shut down:

- To reboot an SLC module, select the **Reboot** check box for the device,
OR
To shut down an SLC module, select the **Shutdown** check box for the device.
- Click the **Submit** button.

Getting a Log File

Use the **Actions** tab to get a syslog or audit log file from one or more SLC console managers.

Notes:

- ◆ The vSLM 2 secure management software stores files in the Files directories. You can display a file from the appropriate Files directory.
- ◆ The file name format is

*[first 8 characters of SLC host name] _[last 8 characters of MAC Address]-
YYMMDD_hhmm-[type of logfile].*

For example, the syslog file retrieved from SLC 'slc32glenn2' (MAC address:

00:11:11:00:11:11) at 15:11 Nov 2, 2006 is

'slc32gle_11001111-061102_1511-slcsyslog'.

To get a syslog or audit log file from an SLC device:

1. To get the syslog from an SLC console manager, select the type of syslog from the **Get Syslogs** drop-down list,
OR
To get the audit log from an SLC module, select the **Get Audit Log** check box for the SLC console manager.
2. Click the **Submit** button.

Getting or Restoring a Configuration File

Use the **Actions** tab to get a specific configuration file from one or more SLC modules or to restore a configuration to one or more SLC console managers.

Note: The vSLM 2 secure management software stores files in the Files directories. You can display a file from the appropriate Files directory.

To get a configuration file from an SLC device:

1. Select the **Get Config** check box for the SLC.
2. Click the **Submit** button.

To restore a configuration to an SLC module:

1. From the **Config file** drop-down list at the top of the page, select the desired configuration file.
2. Select the **Restore Config** check box for the SLC console manager.
3. Select the **Preserve** check boxes to retain the current configuration parameters after the configuration is restored. You may make multiple selections. (Options are Network, Services, Date/Time, Local Users, Device Ports, and **PC Care**.)
4. Click the **Submit** button.

Getting a Sysconfig File

Use the **Actions** tab to get a sysconfig file from one or more SLC modules.

To get a sysconfig (system status) file:

1. Select the **Get Sysconfig** check box for the SLC device.
2. Click the **Submit** button.

Getting or Pushing SSH Keys

Use the **Actions** tab to retrieve or export SSH keys from or to one or more SLC console managers.

Note: To view SSH keys, click **Configuration > Authentication > SSH Keys** on the menu, and then click the **SLC Keys** tab.

Get SSH key retrieves all the imported public SSH keys from the selected SLC device and stores them in the database. **Push SSH key** exports the selected SSH keys to the selected SLC console managers.

When an SLC module imports a public key (with a specific user and host name) from a host (could be an vSLM 2 secure management software or another PC), this SLC console manager allows that particular user to access the SLC device from that particular host. When you enable **Get SSH** keys from an SLC console manager, the vSLM 2 software retrieves all the imported public keys from that particular SLC device and stores them in the SLM database. Then you can push those public keys retrieved from one SLC console manager to other SLC modules, allowing those particular users to access other SLC devices from those particular hosts.

To get SSH keys:

Example: Following is an example of how the user may get and push SSH Keys.

SLC-1 console manager has three imported public keys:

- ◆ key1: [user-A@host-X](#)
- ◆ key2: [user-B@host-Y](#)
- ◆ key3: [user-C@host-Z](#)

The user enables **Get SSH key** from SLC-1 device on the vSLM 2 secure management software. As a result, the SLM database has the three keys above.

The user selects key1 and key3 on the SLC **Actions** tab on the vSLM 2 secure management software and enables **Push SSH Key** to SLC-20 and SLC-21 devices.

Now SLC-20 and SLC-21 console managers have both key1 and key3. This means that SLC-20 and SLC-21 devices allow user-A to access them from host-X, and allow user-C to access them from host-Z.

To get SSH keys:

1. To overwrite SSH keys with the same host and user name currently in the database, select the **Overwrite** check box at the top of the page.
2. Select the **Get SSH** check box for the SLC console manager.
3. Click the **Submit** button.

To push SSH keys:

1. To overwrite SSH keys with same user name and host name on the SLC device where you are exporting the SSH keys, select the **Overwrite** check box at the top of the page.
2. Select the **Push SSH** check box for the SLC module.
3. Click the **Submit** button.

Reading Information

Use the **Actions** tab to update the vSLM 2 software's database with SLC device and port information.

To read information from SLC console managers:

1. Select the checkboxes for the SLC devices to read.
2. Click the **Submit** button.

Note: This is the same as the **Read info from devices** check box on the SLC device page. On the **Actions** page, you can issue this action for multiple SLC devices at once.

Add Applet

For UDS only.

To send an applet file to one or more UDS devices:

1. Select the applet file from the drop down list. This file is found in the SLM folder "UDS Applet Files" under Configuration in the Files area. This applet file must be previously placed in this folder.
2. Check the "Add Applet" box for one or more UDS devices.
3. Click the **Submit** button.

Note: This applet file will be sent to page 0 of the UDS device. The ability to write to pages other than zero will be added to a future release.

Issuing a CLI Command

Use the **Actions** tab to issue a CLI command to one or more SLC console managers.

Note: Commands issued from the **Actions** tab are not interactive.

The following command will not work, because the SLC CLI requires confirmation to continue with group configuration commands:

```
set device port 1-3 baud 19200
```

The following commands will not work, because the SLC CLI requires confirmation to continue with admin maintenance configuration commands:

```
admin reboot
admin shutdown
admin config
```

The following commands will not work because the SLC CLI does not send status "settings successfully updated", which lets the vSLM 2 secure management software know that the command was successful:

```
show [anything]
```

Examples of commands that do work are:

```
se de po 1 baud 9600
set cli terminallines disable
```

To issue a CLI command:

1. Select the **CLI Cmd** check box for the SLC console manager.

Figure 11-58 Issuing a CLI Command

The screenshot shows the LANTRONIX SLM web interface. The main content area is titled "Manage 'SLC' Group" and features several tabs: List, Add, Traps, Actions, Port Access, Notes, and Help. The "Actions" tab is active. Below the tabs, there are input fields for "Location:" and "Sub-Location:" with a "Filter" button. A "SSH Keys:" section includes an "Overwrite" checkbox and a "Config file:" dropdown menu. To the right, there are "Preserve:" checkboxes for Network, Services, Date/Time, VIP, Local Users, Device Ports, and PC Card. A table lists SLC devices with columns for Name, IP addr, Reboot, Shutdown, Get Syslogs, Get Audit Log, Get Config, Get Sysconfig, Restore Config, Get SSH, Push SSH, Read Info, CLI Cmd, Get Groups, Push Groups, and Set Location. The "CLI Cmd" column has a checkmark for the device "tsslc32". At the bottom, a "CLI command:" field contains "set do po 1 baud 9600" and a note: "Multiple commands are separated by semi-colons". "Submit" and "Reset" buttons are at the bottom right.

Name	IP addr	Reboot	Shutdown	Get Syslogs	Get Audit Log	Get Config	Get Sysconfig	Restore Config	Get SSH	Push SSH	Read Info	CLI Cmd	Get Groups	Push Groups	Set Location
tsslc32	172.18.0.107	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
mlslc8048	172.18.21.61	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
mlslc48	172.18.21.66	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slbdb40	172.19.39.253	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slc16_glenn	172.19.39.254	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slc48_glenn_1	172.19.100.90	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slc5e35	172.19.100.116	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slc-md-u	172.19.100.125	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slcRef250120	172.19.100.221	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slc4657	172.19.213.8	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slc4331	172.19.250.119	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slca508	172.19.250.120	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
slcRefreshR17_167	172.19.250.167	<input type="checkbox"/>	<input type="checkbox"/>	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							

2. In the **CLI command** field at the bottom of the page, enter the command. You can issue multiple commands, separated by semicolons (;).
3. Click the **Submit** button.
4. Click **OK** to confirm this action in the popup window that appears.

Getting or Pushing Groups

Use the **Actions** tab to retrieve or export groups from or to one or more SLC console managers.

- ◆ **Get Groups** retrieves all the custom groups from the selected SLC device and stores them in the database as Device Permission groups.
- ◆ **Push Groups** exports all Device Permissions groups to the selected SLC console managers, creating a new custom group on the SLC.

To get groups:

1. To overwrite groups with the same name currently in the database, select the **Overwrite** check box at the top of the page.
2. Select the **Get Groups** check box for the SLC console manager.
3. Click the **Submit** button.

To push groups:

1. To overwrite custom groups with the same name on the SLC device where you are exporting the groups, select the **Overwrite** check box at the top of the page.
2. Select the **Push Groups** check box for the SLC module.
3. Click the **Submit** button.

Setting the Location and Sub-Location

Use the **Actions** tab to set the Location and Sub-Location for one or more SLC console manager.

To set the location:

1. Enter the location and an optional sub-location in the location fields at the top of the page.
2. Select the **Set Location** check box for the SLC module.
3. Click the **Submit** button.

Viewing Progress of Update FW and CLI Commands

You use the **Progress** button to view the progress of the **Update FW** and **CLI CMD** actions described above.

Note: For more detailed status, view the SLM auditlog in the Files folder.

To view the progress of actions running in the background:

1. Click the **Progress** button. The following page opens:

Figure 11-59 Viewing Progress of Update FW and CLI Commands

Background Task Progress				
Progress	Dev Status	Close	Notes	Help
Name	Status	Progress		
CLI Command		100%		
Device Auto Detect	64 devices found (63 new)	100%		
File Copy/Delete		100%		
Password Synchronization		100%		
SLC Update		100%		
SLP Update		100%		
SNMP Synchronization		100%		
Spider Update		100%		
WiBox/UDS/SDS Update		100%		
9 items				

2. View the following information about each task.

Table 11-60 Manage "SLC" Group - Actions Tab

Setting	Description
Name	Name of the task.
Status	Informational text.
Progress	Percentage of the task that is complete.

- To view details of the last device action status of the SLM/SLC/RPM/SLP/SCS devices, click the **Dev. Status** tab. The following page opens:

Figure 11-61 Background Task Progress - Dev Status Tab

Name	Command	Time Started	Status
avi-dsm	No action		
DSM-38-1	No action		
DSM-Access	Retrieve SLP status	09/18/2012 17:00	Success
Glenn-VMPC	No action		
patlab_slb1	Retrieve SLP status	09/18/2012 17:00	Success
patlab_slb2	Retrieve SLP status	09/17/2012 19:05	Success
PC-182	No action		
PCon-192	No action		
slb04cc	Retrieve SLP status	09/17/2012 19:05	Success
SLB_DW	Retrieve SLP status	09/17/2012 19:05	Success
slbusb_glenn	Retrieve SLP status	09/18/2012 17:00	Success
slc19a2	No action		
slc247	Retrieve SLP status	09/18/2012 17:00	Success
slc860d_Glenn	No action		
slm02_19	No action		
SLM6AA6	No action		
SLMC413	No action		
SLS	No action		
SLS4a808c06	No action		
SLSA38C4FD0	No action		
sls-sunset2	No action		
sls-sunset30	No action		
sls-sunset31	No action		
sls-sunset32	No action		
sls-sunset6	No action		
SpiderG-108	No action		
UDS2100	No action		
vslm_glenn19	No action		

28 items

Refresh

- To close the Background Task Progress page, click the **Close** tab.

Events

Administrators can configure alarms, triggers, and events on the vSLM 2 secure management software. Examples of events are receiving an SNMP trap, a system event like network failure, or a text string match in a certain log. There are several types of logs in the SLM system: data logs (device port buffering), syslogs, event logs, access logs (user access), and audit logs. The alarm could send an email to a user, send an SNMP trap, or write to a log file (local syslog or remote syslog).

Event Management

Administrators configure alarms and triggers. An alarm is a notification that may take the form of an email, trap, or syslog. A trigger is something that happens to set off an alarm assigned to that trigger. An event is a combination of a trigger and an alarm.

You can map one trigger to multiple alarms and/or multiple triggers to one alarm (saving you from having to define the same alarm repeatedly for each trigger).

To define alarms:

1. On the menu, click **Events**. The following page opens:

Figure 11-62 Event Management Page - Events Tab

2. Enter the following information:

Table 11-63 Event Management - Events Tab - Alarm Type

Setting	Description
Alarm Type	Select one of the following: email: Sends an email to the specified email address with details of the event that has been triggered. trap: Sends a notification of a critical event to a specified IP address. syslog: Writes an entry into the syslog with details of the event.
IP/email address	For an Email alarm: The email address where notifications go. For a trap: The IP address of the device to which notifications go. For a syslog: Leave blank.
Community	For a trap: The SNMP community of the device to which the trap is sent. The default is public. Example: If the alarm type is Trap, and the IP address is 172.19.100.123, the SNMP community name should be the SNMP community of the device 172.19.100.123. Otherwise the device will not receive the trap.

3. Click the **Define Alarm** button. The alarm displays in the **Alarm** list on the right.
4. Enter the following information:

Table 11-64 Event Management - Events Tab - Trigger Type

Setting	Description
Trigger Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> ◆ received device traps: An incoming trap from a specified IP address. ◆ port log string match (SLC/SLB): A defined string matches a monitored device's port log. The string match for the port log could be either an exact string match, or a regular expression. See the string field for an example. ◆ port connection: A defined string matches a monitored device's port connection. ◆ audit log string match (SLM): A defined string matches an entry in the audit log. ◆ SLM Ethernet down: A defined ethernet port has failed (for example, eth-port: 2). ◆ port log threshold %: The SLC port log files have reached a defined percentage of the SLC Portlog directory's capacity. ◆ audit log threshold %: The SLM or SLC audit log files have reached a defined percentage of the SLM Auditlog directory's capacity. ◆ syslog threshold %: The SLM or SLC syslog files have reached a defined percentage of the SLM Syslog directory's capacity. ◆ device reachability changed: If you specify the device's IP Address with this trigger type, the vSLM 2 secure management software sets the trigger should polling fail on this device. If you do not specify the device's IP Address, the vSLM 2 software sets the trigger on all the devices on which polling failed. When polling is enabled on a device (the Poll check box on the device page), the vSLM 2 secure management software constantly checks on the device to see if that device is reachable. ◆ syslog string match: Enter the text string for the string match in the oid / string / eth-port / % field. This is the trigger when a syslog string matches the specified string. ◆ This is a very powerful trigger because the vSLM 2 software can act as a syslog server by receiving a syslog from SLC console managers and other devices. You can do a string match to all kinds of syslog messages (e.g., for all SLC events that will send a message to syslog). ◆ current load threshold %: Enter the IP address and port number (optional) of the RPM/SLP or SLB device you want to monitor and its current load threshold %. For example, if the High Threshold value for a RPM/SLP expansion tower is configured to be 20 amps, and a trigger is defined for the same RPM/SLP for 90%, the event will trigger if the current load for the expansion tower exceeds 18 amps. ◆ If you specify a port number, the trigger is set when the current load (outletLoad) of the outlet # (port #) reaches the outletLoad threshold on that particular RPM/SLP or SLB device. ◆ If you do not specify a port number, the trigger is set when the current load (infeedLoad) of the whole RPM/SLP or SLB tower or unit reaches the infeedLoad threshold. ◆ hard disk threshold %: Enter the percentage of the hard disk threshold of the vSLM 2 secure management software. The vSLM 2 software sends out the alarm when the hard disk usage reaches this threshold. ◆ persistent connection state change: A persistent connection that has changed from active to inactive or vice versa.
IP Address[:port]	<p>For a trap, port log, or port connection: Enter the IP address followed by an optional port number 1-48, for example, 172.19.39.19:15.</p> <p><i>Note:</i> The brackets indicate that: port is not always required.</p>

Setting	Description
oid / string / eth-port /%	<p>Depending on the trigger type selected, enter one or more of the following:</p> <p>oid: 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.</p> <p>string: Series of characters that match a monitored device's audit log, syslog, or port log. The OID string match supports partial match. The string match for a port log could be an exact string or a regular expression. For example:</p> <ul style="list-style-type: none"> ◆ String "reboot" will match port logs containing "reboot." ◆ String "RE:abc[0-9]" will match port logs containing any string that matches the regular expression "abc[0-9]." ◆ OID .3.6.1.4.1.244.1.1 will match any SLC custom traps with OID: .3.6.1.4.1.244.1.1.0.1 to 1.3.6.1.4.1.244.1.1.0.4. <p>eth-port: Ethernet port that is down (for example, 2).</p> <p>%: Defined percentage of the SLC port log file's capacity.</p> <p>For detailed instructions on completing the OID for a trap, see the Lantronix web site www.lantronix.com/support.</p>

5. In the **Alarms** list to the right, select the alarm(s) to be associated with the selected trigger.
6. Click the **Define Event** button. The event displays in the format Trigger: Alarm in the Events list on the page. The trigger displays in the Events menu tree.

Figure 11-65 SNMP Trap Configuration (from Lantronix Tech Support FAQ)

SNMP trap configuration on an SLM

Published 08/03/2006 03:23 PM | Updated 01/21/2009 08:15 AM

How do I configure SNMP Trap Event Triggers on an SLM? Do I need to specify the full OID for every trap I want to use as a trigger?

This answer applies to SLM firmware v2.0 and higher.

On the SLM Events page, when you setup a "Trap" as an Event Trigger, you don't have to explicitly describe the OID down to the last digit.

Example 1:
If you define a trap as shown below:

```
Trigger Type
[v] Trap          IP Address: 172.19.237.10
                  OID: 1.3.6.1.4.1.244.1.1
```

It will match all SLC custom traps received from the specified IP address(172.19.237.10). These include:

```
1.3.6.1.4.1.244.1.1.0.1 (power supply)
1.3.6.1.4.1.244.1.1.0.2 (sysadmin password)
1.3.6.1.4.1.244.1.1.0.3 (shutdown)
1.3.6.1.4.1.244.1.1.0.4 (device port data)
```

Example 2:
If you define a trap as shown below:

```
Trigger Type
[v] Trap          IP Address: 172.19.237.10
                  OID: 1.3.6.1.6.3.1.1.5
```

It will match all generic SNMP traps received from the specified IP address(172.19.237.10). These include:

```
1.3.6.1.6.3.1.1.5.1 (cold start)
1.3.6.1.6.3.1.1.5.2 (warm start)
1.3.6.1.6.3.1.1.5.3 (link down)
1.3.6.1.6.3.1.1.5.4 (link up)
1.3.6.1.6.3.1.1.5.5 (auth failure)
1.3.6.1.6.3.1.1.5.6 (egpNeighborLoss)
```

Example 3:
If you define a trap as shown below:

```
Trigger Type
[v] Trap          IP Address: 172.19.237.10
                  OID: 1.3.6.1.4.1.244.1.1.0.1
```

This will only match SLC power supply trap received from the specified IP address(172.19.237.10).

Updating and Deleting Events

Administrators and authorized users can update triggers and delete or add alarms for defined events.

To update information about the alarm, trigger, or event:

1. On the menu, open the **Events** menu tree and select the event to be managed. The following page opens:

Figure 11-66 Manage Event Page -Event Tab

2. Update the information about the alarm, trigger, or combination of alarm and trigger as desired.

Note: If you deactivate an event, it remains in the system but will not send alarms until it is reactivated.

3. Click the **Update** button.

To add an additional alarm:

You may add an alarm only if there are available alarms that are not already assigned to the trigger. You can add more alarms on the main Event Management page.

1. From the **Available Alarms** list, select another alarm.
2. Click the **Add Alarm** button. The alarm now displays in the Current Alarms list.

To delete an alarm:

On the Manage Event page you can remove an alarm only if there are more than two alarms to start with (you may not leave a trigger without an alarm).

1. Select the alarm from the **Current Alarms** list and click the **Remove Alarm** button. A confirmation message displays.
2. Click **OK**. The alarm is no longer in the **Alarms** list or in any events that use that alarm.

To delete an event:

1. Select the event from the **Events** list and click the **Remove Event** button. A confirmation message displays.
2. Click **OK**. The event is no longer in the **Events** list.

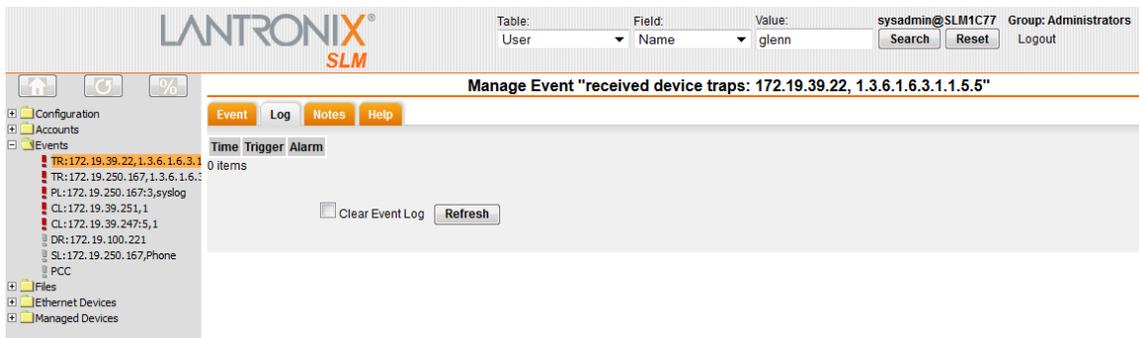
Viewing the Event Log

Administrators and authorized users view a list of all defined events.

To view all device events:

1. On the menu, click **Events** and then click the **Log** tab. The following page opens:

Figure 11-67 Event Management Page - Log Tab



Clearing the Event Log

Administrators can clear the event log.

To display current log information:

1. Click the **Refresh** button.

To clear the event log:

1. Click the **Clear Event Log** button. A message requesting confirmation displays.
2. In response to the confirmation message, click **OK**.

Files

Administrators can display and manage log, upgrade, configuration, session, and trap files of Ethernet devices.

Note: To retrieve files from the SLC console manager, use the *Manage SLC Group Actions* tab.

File Types

You can view and store the following files in the SLM database. You can also import or export them by means of an NFS or CICS mount.

Firmware Upgrade

- ◆ **vSLM 2 FW Upgrade Files:** Files for upgrading the vSLM 2 firmware.
- ◆ **SLC/SLB FW Upgrade Files:** Files for upgrading the SLC/SLB firmware.
- ◆ **RPM/SLP FW Upgrade Files:** Files for upgrading the RPM/SLP firmware.
- ◆ **Spider FW Upgrade Files:** Files for upgrading the Spider firmware.
- ◆ **UDS/SDS FW Upgrade Files:** Files for upgrading the UDS firmware.
- ◆ **WiBox FW Upgrade Files:** Files for upgrading the WiBox firmware.

Note: You can obtain the most up-to-date firmware and release notes for the unit from the Lantronix web site (www.lantronix.com) or by using anonymous FTP ([ftp.lantronix.com](ftp://lantronix.com)).

Configuration Files

- ◆ **SLM Configuration Files:** Contain all of the vSLM 2 secure management software's settings that have been saved to file. They can be backed up to a location that is not on the vSLM 2 software.
- ◆ **SLC/SLB Configuration Files:** Contain all of the SLC console manager's settings that have been saved to file. They can be backed up to a location that is not on the SLC device.
- ◆ **SLC/SLB Sysconfig Files:** Contain status information about the SLC console manager.
- ◆ **Spider Configuration Files:** Contains all of a Spider device's settings saved in a file. This can be used to restore another Spider unit to the same settings, or backed up and later used to restore the original Spider device.
- ◆ **Spider Sysconfig Files:** Viewable system configuration of vSLM 2 secure management software managed Spider devices.
- ◆ **UDS/SDS Sysconfig Files:** Viewable system configuration of SLM managed UDS devices.
- ◆ **UDS/SDS Applet Files:** Applet files for installation on UDS devices.

Log Files

- ◆ **SLM Syslog Files:** Contain information about all activity on the vSLM 2 secure management software (for example, login attempts, alarms, and diagnostics).
- ◆ **SLM Auditlog Files:** Every successful login, logout, and command on the command line interface and web is logged into a database table. The administrator reads this information from the CLI or web and creates an audit report for one or multiple users.
- ◆ **SLC/SLB Syslog Files:** Contain information about all activity on the SLC device, for example, login attempts, alarms, and diagnostics.
- ◆ **SLC/SLB Auditlog Files:** Contain a log of all actions that have changed the configuration of the SLC console manager.
- ◆ **SLC/SLB Portlog Files:** Contain a log of all actions and data on a specific port.
- ◆ **Persistent Log Files:** Contain data about the activity of persistent connections.

Session Files

- ◆ **SLC/SLB Port Active Files:** Contain session log files for currently active Secure Channel sessions to SLC device ports.
- ◆ **SLC/SLB Port Saved Files:** Contain archived session log files for Secure Channel sessions to SLC device ports. The files in the SLC/SLB Port Active Files directory move into the SLC/SLB Port Saved Files directory after the session ends.
- ◆ **SCS05/20 Port Session Files:** Contain session log files for SSH sessions to SCS05/20 device ports. There is no distinction between active and inactive sessions.
- ◆ **Device Session Files:** Contain session log files for Telnet/SSH/Secure Channel port sessions. There is no distinction between active and inactive sessions.

Note: Session log files can be accessed from the **Logs** tab of Ethernet devices and certain (SLC, SCS05/20) device ports, as well as through the appropriate folders under **Files>Session**.

Trap Files

- ◆ **SLM Exported Trap Files:** Contains all or part of the trap log files as specified on the Traps tab of the All Ethernet Devices page.

File Format

The names of Device Session Files, SLC Port Saved Files, SCS05/20 Port Session Files, Device Session Files, and SLC Port Active Files have the following format:

```
<hostname>_<host_mac_address>-  
<device_port_number>=<username>=<connection_type>-<date_and_time>.log,
```

where:

Table 11-68 File Format

Setting	Description
<hostname>	Up to the first 8 characters of the hostname of the Ethernet device. If the hostname is shorter than 8 characters, the hostname section is padded with ~ characters to reach this length.
<host_mac_address>	MAC Address of the Ethernet device. This is used by the vSLM 2 secure management software to correlate log files to their corresponding Ethernet devices.
<device_port_number>	Device port number connected to for this session. This field is set to 0 "00" for connections directly to the Ethernet device.
<username>	The vSLM 2 software user ID that initiated this session.
<connection_type>	Session connection type: tnt for telnet, ssh for ssh, or scc for secure channel.
<date_and_time>	Date and time string in the format YYMMDD_HHMMSS

For edge device based logging, the filename is made up of only three of these fields:

```
<hostname>_<host_mac_address>-<device_port_number>.log
```

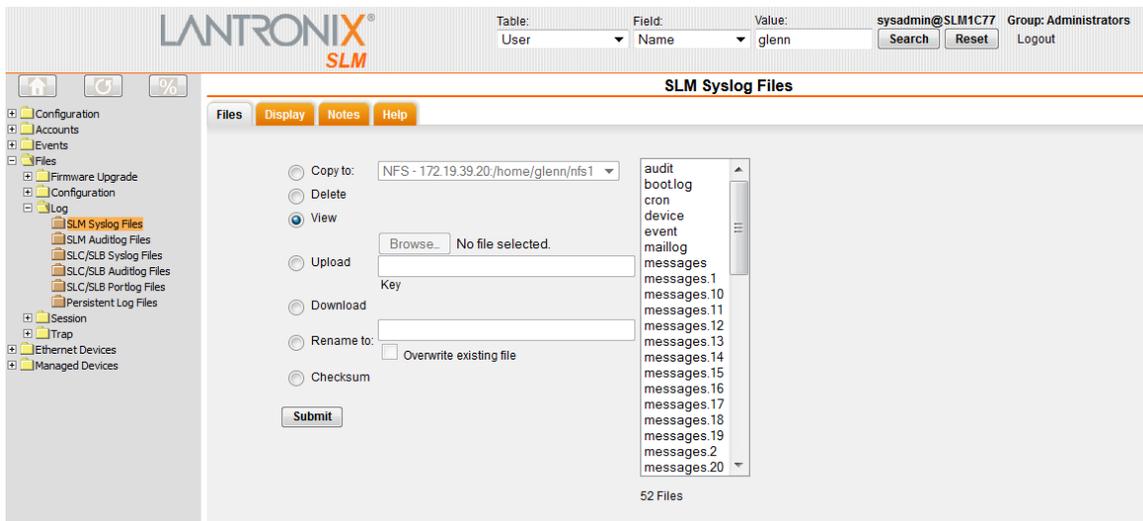
Viewing, Deleting, and Renaming Files

In this section, we show how to view, delete, and rename files. In our example, we use an SLM syslog file.

To view a file:

1. On the menu, click **Files** and then the file type you want to view. The following page opens:

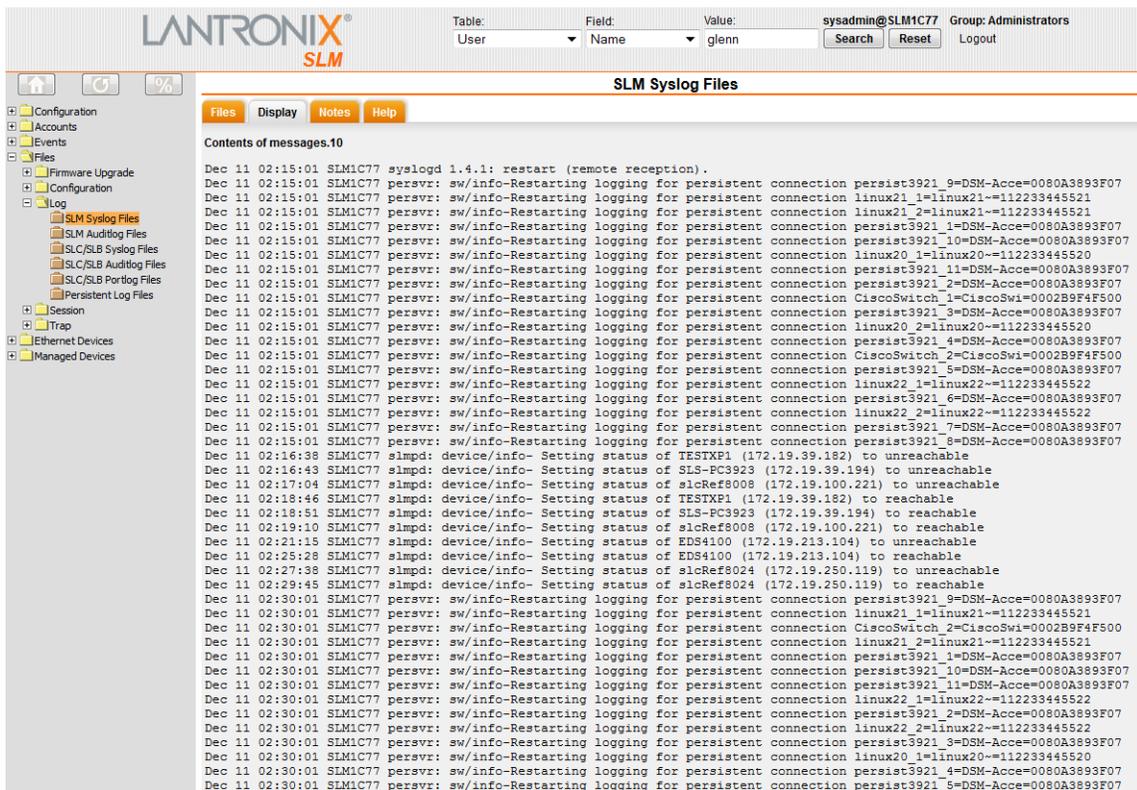
Figure 11-69 SLM Syslog Files Page - Files Tab



The available files (of the selected type) display in the list box.

2. Select **View** and then the file you want to view.
3. Click the **Submit** button. The **Display** tab opens and shows the contents of the selected file.

Figure 11-70 SLM Syslog Files Page - Display Tab



To delete a file:

Note: You cannot delete an active syslog file.

1. On the menu, click **Files** and then the type of file. The files of that type in the database display in the list box.
2. Select **Delete** and then the file you want to delete. To select multiple files, use **Shift+click** or **Ctrl+click**.
3. Click the **Submit** button.
4. In response to the request for confirmation, click **OK**. The file is no longer in the list.
5. To see the status of the copy process if you are deleting multiple files at the same time, click the **Progress** button above the menu.

To rename a file:

Note: You cannot rename an active syslog file.

1. On the menu, click **Files** and then the type of file you want to rename. The files of that type display in the list box.
2. Select **Rename** and then the file you want to rename.
3. To rename a file to a name already in use in the directory, select the **Overwrite existing file** check box.

Note: If you try to rename a file to a name already in use in that directory, the rename will fail unless you select **Overwrite existing file** check box.

4. Click the **Submit** button. A confirmation message displays.

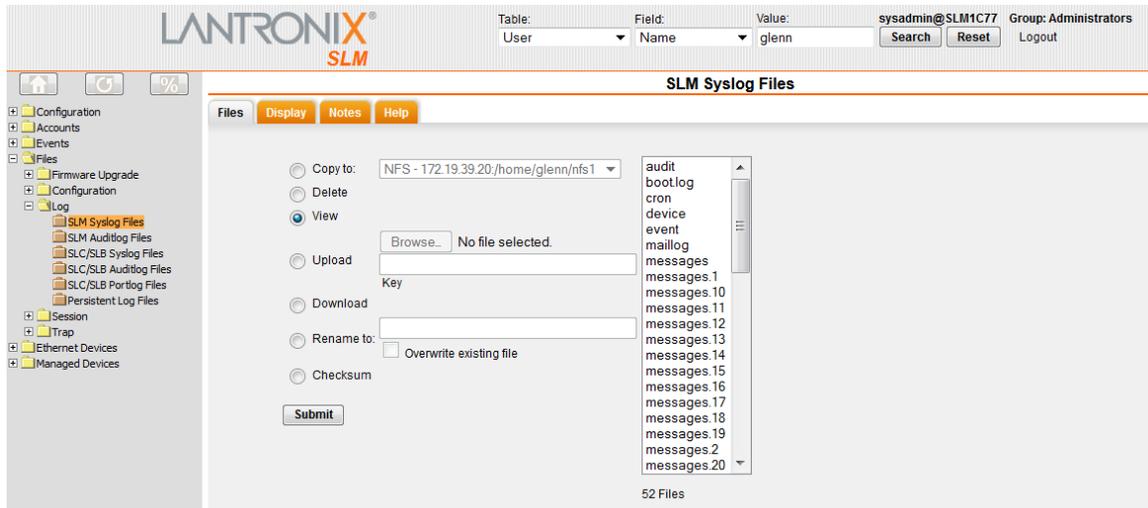
Exporting, Uploading, and Downloading Files

Administrators can export (copy), upload, and download files.

To open the Files page:

1. On the menu, click **Files** and then the file type you want to export. The following page opens:

Figure 11-71 Files Page



To export (copy) a file from the vSLM 2 secure management software to a mapped CIFS or NFS directory:

1. Select **Copy to**. The drop-down list box becomes active.

Note: *Copy To* is only active if CIFS or NFS has been configured or if USB flash memory is installed.

2. From the drop-down list, select the location of the file (NFS or CIFS).
3. From the list box to the right, select the destination directory for the file (CIFS or NFS), and click the **Submit** button. To select multiple files, use **Shift+click** or **Ctrl+click**. A confirmation message displays.
4. To see the status of the copy process if you are copying multiple files at the same time, click the **Progress** button above the menu.

To upload a file from the client machine to the vSLM 2 software:

1. On the menu, click **Files** and then the file type you want to upload.
2. Select **Upload**.
3. Click the **Browse** button and locate the file on your client machine to upload.
4. If this is an SLM FW Upgrade or SLC FW Upgrade (which also handles SLB branch office manager), enter the md5sum value for this file in the **Key** field.
5. Click the **Submit** button. The file displays in the list box.

To download a file from the vSLM 2 secure management software and to the client machine:

1. On the menu, click **Files** and then the file type you want to download.
2. Select **Download**.
3. Select the file to download from the files list.
4. Click the **Submit** button. A confirmation message displays.
5. If necessary, when requested by your browser, select the destination directory for the file on your client machine.

Copying Files

The administrator and other authorized users can download SLM and SLC firmware upgrade, configuration, and log files from an FTP/SFTP server.

To copy a file:

1. On the menu, click **Files**. The following page opens:

Figure 11-72 File Management Page - Copy Tab

2. Enter the following:

Table 11-73 File Management - Copy Tab

Setting	Description
File type to copy	From the drop-down list, select the type file to copy. The default setting is SLM FW Upgrade .
Copy file from	Select the type of server from which to copy. The default setting is SFTP. <i>Note: If you set up NFS and CIFS, or if a USB flash memory is installed, then they display in this list.</i>
Filename	Name of the firmware upgrade or configuration file.
Key	A key for validating the firmware file. The key comes with the firmware file (32 hex characters).

3. Enter the following information about the destination server:

Table 11-74 File Management - Copy Tab - FTP/SFTP Server

Setting	Description
Server	The IP address or host name of the server used for obtaining upgrades 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 upgrade files and getting and putting configuration save files.
Login	The user ID for accessing the FTP or SFTP server. May be blank.
Password and Retype	The FTP or SFTP user password.

Setting	Description
Connect Timeout (secs)	The number of seconds after which the connection attempt times out. Default is 60.
Download Timeout (secs)	The number of seconds after which the download attempt times out. Default is 180.

- To save, click the **Submit** button.
- To see the status of the copy process if you are copying multiple files at the same time, click the **Progress** button above the menu.

Setting up NFS

You can import files from or export files to a remote NFS server. The administrator defines the remote and local directories and read/write permissions.

To set up NFS:

- On the menu, click **Files** and then the **NFS** tab. The following page opens:

Figure 11-75 File Management Page - NFS Tab

The screenshot shows the LANTRONIX SLM File Management page, NFS Tab. The page has a navigation menu on the left with categories like Configuration, Accounts, Events, Files, Firmware Upgrade, Log, Session, Trap, Ethernet Devices, and Managed Devices. The main content area has tabs for Copy, NFS, CIFS, Logging, Notes, and Help. The NFS tab is selected. The page displays a table for configuring NFS shares. At the top, there is a search bar with 'User' selected, 'Name' as the field, and 'glenn' as the value. There are 'Search' and 'Reset' buttons, and a 'Logout' link. The table has columns for Remote directory, Local directory, Mount, Read-write, and NFSv4. There are three rows of configuration. Below the table are 'Update' and 'Reset' buttons. At the bottom, there is a section for 'Local directory to export' with two rows of configuration.

Remote directory	Local directory	Mount	Read-write	NFSv4
#1 172.19.39.20/home/glenn/nfs1	SLM Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
#2 172.19.39.20/home/glenn/nfs2	SLC/SLB FW Upgrade	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
#3 172.19.39.20/home/glenn/nfs3	SLC/SLB Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Local directory to export	Read-write
#1 Device Session /nfs/share1	<input checked="" type="checkbox"/>
#2 SLC/SLB Port Saved /nfs/share2	<input checked="" type="checkbox"/>

- Enter the following information for importing a file:

Note: The first three lines are for mounting remote NFS directories (the vSLM 2 secure management software functions as an NFS client). Once the directory is mounted, the vSLM 2 software can import files from that share point.

Table 11-76 File Management - NFS Tab - Remote Directory

Setting	Description
Remote directory	The remote NFS share directory in the format: <nfs_server_hostname_or_ipaddr>:/<nfs_mount_point> where <nfs_mount_point> is the path to the exported NFS directory on the remote NFS server.
Local directory	The local directory on the vSLM 2 secure management software on which to mount the remote directory. The vSLM 2 software creates the local directory automatically.
Mount	Select the check box to enable the vSLM 2 secure management software to import the file by means of the NFS server. Disabled by default.

Setting	Description
Read-write	If enabled, indicates that the user can read or write to the exported directory.
NFSv4	Use version 4 of NFS

- Enter the following information about exporting a file from the vSLM 2 software:

Note: This information is for exporting NFS shares (the SLM functions as an NFS server). This allows remote NFS clients to mount these shares and then view/update the files in the exported directories.

Table 11-77 File Management - NFS Tab - Local Directory

Setting	Description
Local directory to export #1 and #2	From the drop-down list, select up to two directories to export. Disabled by default.
Read-write	If enabled, indicates that the user can read or write to the exported directory.

- Click the **Update** button. When the update is complete, a confirmation message displays in the bottom part of the page.

Setting up CIFS

Administrators can import files from or export files to a local or remote CIFS server. You define the remote and local directories, passwords, and read/write permissions.

To set up CIFS:

- On the menu, click **Files** and then the **CIFS** tab. The following page opens:

Figure 11-78 File Management - CIFS Tab

The screenshot shows the LANTRONIX SLM File Management interface. At the top, there is a search bar with 'User' selected in the 'Table' dropdown, 'Name' in the 'Field' dropdown, and 'glenn' in the 'Value' field. The 'File Management' section has tabs for 'Copy', 'NFS', 'CIFS', 'Logging', 'Notes', and 'Help'. The 'CIFS' tab is selected. Below the tabs, there is a table with columns: Remote directory, Local directory, Username, Password, Retype, Mount, and Read-write. The table contains three rows for entries #1, #2, and #3. Below the table, there are fields for 'Local directory to share' (set to SLC/SLB Configuration), 'Workgroup' (set to workgroup), 'CIFS user password', 'Network port 1' (checked), and 'Network port 2' (checked). There are 'Update' and 'Reset' buttons at the bottom.

- Enter the following information for importing a file:

Note: The first three entries are for mounting remote CIFS/Samba shares (the vSLM 2 secure management software acts as a CIFS client). The username and password are required to authenticate users on the remote CIFS server. The second section on this page is for the CIFS share that we can export (the vSLM 2 software acts as a CIFS server).

Table 11-79 File Management - CFS Tab - Remote Directory

Setting	Description
Remote directory	The remote directory to be imported, in the format: //<server_name_or_ip>/<sharepoint>.
Local directory	The local directory on the vSLM 2 secure management software on which to mount the remote directory. The vSLM 2 software creates the local directory automatically.
Username	User name required to authenticate the user on the remote CIFS server.
Password and Retype	Password required to authenticate the user on the remote CIFS server.
Mount	Select the check box to enable the vSLM 2 secure management software to import the file from the CIFS server. Disabled by default.
Read-write	If enabled, indicates that the user can read and write to the imported directory. Disabled by default.

3. Enter the following information about exporting a file from the vSLM 2 software.

Note: This information is for the CIFS share that we can export (the vSLM 2 secure management software acts as a CIFS server).

Table 11-80 File Management - CFS Tab - Local Directory

Setting	Description
Local directory to share	From the drop-down list, select the directory you want the vSLM 2 secure management software to export. Disabled is the default setting.
Network port 1 and Network port 2	Select the network ports from which you can see the share. Normal usage is to make the share visible in both network ports, but the boxes are unchecked by default.
Workgroup	The Windows workgroup to which the PC importing the CIFS share belongs. Can have up to 15 characters.
CIFS user password and Retype	Only one special username (cifsuser) can access the CIFS share. Enter the CIFS user password in both password fields. The default user password is CIFSPASS . Note: More than one user can access the share at the same time with the cifsuser user name and password.

4. Click the **Update** button. When the update is complete, a confirmation message displays in the bottom part of the page.

Setting up Log Properties

The administrator specifies the properties of log files.

To set up log properties:

1. On the menu, click **Files** and then the **Logging** tab. The following page opens.

Figure 11-81 File Management Page - Logging Tab

The screenshot displays the LANTRONIX SLM File Management interface. At the top, there is a search bar with fields for 'Table' (User), 'Field' (Name), and 'Value' (glenn), along with 'Search' and 'Reset' buttons. The user is identified as 'sysadmin@SLM1C77' with the group 'Administrators'. The main content area is titled 'File Management' and has a navigation bar with tabs for 'Copy', 'NFS', 'CIFS', 'Logging', 'Notes', and 'Help'. The 'Logging' tab is active, showing configuration options for various log types:

- Port Logs:** Maximum log space (GB): 5. On log space exhausted: Stop logging, Overwrite oldest entries. Port Log Type: User session based, Edge device based.
- Audit Logs:** Max File Size (KB): 32. Maximum log space (GB): 2. On log space exhausted: Stop logging, Overwrite oldest entries.
- Session Logs:** Maximum log space (GB): 5.
- System Logs:** Max File Size (KB): 32. Max File Count: 500. Maximum log space (GB): 2.
- Persistent Connection Logs:** Max File Size (KB): 32. Max File Count: 50. Maximum log space (GB): 2. Keystroke Logging: .

At the bottom of the configuration area, there are 'Update' and 'Reset' buttons.

2. Enter the following:

Table 11-82 File Management - Logging Tab - Port Logs

Setting	Description
Maximum log space (30 GB available)	Maximum space used for all session log files in gigabytes. It is 30 GB for SLM-01 device and 60 GB for SLM-02 device.
On log space exhausted	Select one of the following actions the vSLM 2 secure management software should take when all port log space has been used: Stop logging: When log space is exhausted, logging stops. Overwrite oldest entries: When port log space is exhausted, logging overwrites the oldest entries.

Setting	Description
Port Log Type	Select from these options: User session based: each connection will generate it's own log file, even if multiple users are connected to the same edge device. Edge device based: one log file will be created for each edge device, and all user interaction will be merged into a single log file, and individual user keystrokes will be identified.

Table 11-83 File Management - Logging Tab - Audit Logs

Setting	Description
Maximum File Size (KB)	Maximum size for each SLM audit log file in kilobytes. The default is 64.
Maximum log space (GB)	Maximum space used for all SLM audit log files in gigabytes. The default is 5.
On log space exhausted	Select one of the following actions the vSLM 2 secure management software should take when all audit log space has been used: Stop logging: When audit log space is exhausted, logging stops. Overwrite oldest entries: When audit log space is exhausted, logging overwrites the oldest entries.

Table 11-84 File Management - Logging Tab - Session Logs

Setting	Description
Maximum log space (GB)	Maximum space used for all SLC session files in gigabytes. The default is 10.

Table 11-85 File Management - Logging Tab - System Logs

Setting	Description
Maximum File Size (KB)	Maximum size for each SLM system log file in kilobytes. The default is 64.
Max File Count	Maximum number of system log files before the vSLM 2 secure management software starts to overwrite the old ones. The default is 1000.
Maximum log space (GB)	Maximum space used for all SLM system log files in gigabytes. The default is 5.

Table 11-86 File Management - Logging Tab - Persistent Connection Logs

Setting	Description
Maximum File Size (KB)	Maximum size for each persistent connection log file in kilobytes. The default is 64.
Max File Count	Maximum number of persistent connection log files before the vSLM 2 secure management software starts to overwrite the old ones. The default is 100.
Maximum log space (GB)	Maximum space used for all persistent connection log files in gigabytes. The default is 5.

3. Click the **Update** button. When the update is complete, a confirmation message displays in the bottom part of the page.

Logging Commands

admin locallog

Syntax

```
admin locallog clear auditlog
admin locallog clear syslog
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, RPM, SCS, SLB, SPDR, WiBox, LTRX, UDS, or
other
```

Description

Clears all of the entries in the auditlog, syslog, or traplog.

show auditlog

Syntax

Displays the audit log from the bottom: `show auditlog`

```
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
```

Parameters

Type 'show auditlog' to get index.

List auditlog files by index number from top: `show auditlog index <number>`

Note: *Index is the number by the specified parameters 'lastminutes' and 'date'.*

List auditlog files in short form: `show auditlog list <parameters>`

List auditlog files: `show auditlog lastminutes 5`

List auditlog files modified in last 5 minutes: `show auditlog date 0205`

List auditlog files last modified on 0205: `show auditlog date 0205-0209`

List auditlog files last modified between 0205 and 0209: `show auditlog index 3`

Description

Displays the audit log.

show portlog

Syntax

```
show portlog
```

Lists all port log files.

```
show portlog <parameters>
```

Lists port log files as specified by parameters.

Parameters

[tail <number of lines>]

[lastminutes <minutes>]

[date <MMDD>]

[date <MMDD-MMDD>]

Description

Lists portlog files.

Examples

```
show portlog lastminutes 5
```

Lists portlog files modified in last 5 minutes.

```
show portlog date 0205
```

Lists portlog files last modified on 0205.

```
show portlog date 0205-0209
```

Lists portlog files last modified between 0205 and 0209.

show portlog file

Note: Type `show portlog` to display index.

Syntax

```
show portlog file <index>
```

Shows the port log from the top.

```
show portlog file <index> tail
```

Displays the port log from the bottom (tail).

```
show portlog file <index> top
```

Displays the port log from the top.

Description

Displays the contents of the portlog file by index. Default is top.

show portlog index

Syntax

Note: Type `show portlog` to display index.

```
show portlog index <number>
```

Displays part of portlog by index from the top.

Index is the number specified by lastminutes and date.

```
show portlog index <number> <parameters>
```

Parameters

```
[tail <number of lines>]
```

Displays the part of the portlog by index from the end.

```
[lastminutes <minutes>]
```

```
[date <MMDD>]
```

```
[date <MMDD-MMDD>]
```

Description

Displays the contents of the portlog file by index.

Note: *Index is the number specified by parameters lastminutes and date. If you specify 0 as number of lines, all lines display. If you specify both date and time, the vSLM 2 secure management software ignores the date option.*

Examples

```
show portlog index 3
```

Displays the specified portlog from top.

```
show portlog index 3 top 10
```

Displays the first 10 lines of specified portlog from top.

```
show portlog index 3 tail 15
```

Displays the last 15 lines of specified port log from tail.

```
show portlog index 3 lastminutes 5
```

Displays port log by the index '3'.

To get this index, type show portlog lastminutes 5.

```
show portlog index 3 date 0205
```

Displays port log by the index '3'.

To get this index, type show portlog date 0205.

```
show portlog index 3 date 0205-0209
```

Displays port log by the index '3'.

To get this index, type show portlog date 0205-0209.

```
show portlog index 3 top 10 lastminutes 5
```

Displays the first 10 lines of portlog by the index '3'.

To get this index, type show portlog lastminutes 5.

```
show portlog index 3 tail 0 lastminutes 5
```

Displays the portlog by the index '3' from tail.

To get this index, type show portlog lastminutes 5.

show portlog list**Syntax**

```
show portlog list
show portlog list <parameters>
```

Parameters

```
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
```

Description

Lists portlog files in short form.

show sessionlog**Syntax**

```
show sessionlog type <sessiontype> <parameters>
sessiontype: <slcportactive|slcportsaved|scsport|device>
```

Parameters

```
[top <number of lines>]
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
```

Description

Lists session log files.

Examples

```
show sessionlog
```

Lists device session log files.

```
show sessionlog type slcportsaved lastminutes 5
```

Lists archived SLC port session log files modified in last 5 minutes.

```
show sessionlog date 0205
```

Lists session log files last modified on 0205.

```
show sessionlog type scsport index 3
```

Displays the specified SCS05/20 port session log from the top.

```
show sessionlog type device index 3 top 10
```

Displays the first 10 lines of the specified device session log from the top.

```
show sessionlog type device index 3 tail 15
```

Displays the last 15 lines of specified device session log from the end.

```
show sessionlog type device index 3 lastminutes 5
```

Displays device session log by the index '3'.

To get this index, type show portlog lastminutes 5.

```
show sessionlog type slcportsaved index 3 date 0205
```

Displays archived SLC port sessionlog by the index '3'.

To get this index, type show sessionlog type slcportsaved date 0205.

```
show sessionlog type device index 3 date 0205-0209
```

Displays device session log by the index '3'.

To get this index, type show sessionlog type device date 0205-0209.

```
show sessionlog type device index 3 top 10 lastminutes 5
```

Displays the first 10 lines of device session log by the index '3'.

To get this index, type show sessionlog type device lastminutes 5.

show syslog

Syntax

```
show syslog
```

Shows the syslog information.

Parameters

```
[lastminutes <minutes>]
```

```
[date <MMDD>]
```

```
[date <MMDD-MMDD>]
```

Description

Shows the syslog information.

show syslog index

Syntax

Type 'show syslog' to get index.

```
show syslog index <number>
```

Display the part of syslog by index from top:

Index is the number by the specified parameters 'lastminutes' and 'date'.

If you specify '0' at number of lines, display all.

```
show syslog index <number> <parameters>
```

Parameters

```
[top <number of lines>]
```

```
[lastminutes <minutes>]
```

```
[date <MMDD>]
```

```
[date <MMDD-MMDD>]
```

```
[loglastminutes <minutes>]
```

```
[logdate <MMDD>]
```

```
[logdate <MMDD-MMDD>]
```

Display the part of syslog by index from tail:

Index is the number by the specified parameters 'lastminutes' and 'date'.

If you specify '0' at number of lines, display all.

```
show syslog index <number> <parameters>
```

Parameter

```
[tail <number of lines>]
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
[loglastminutes <minutes>]
[logdate <MMDD>]
[logdate <MMDD-MMDD>]
```

Note: If you specify both date and time, ignore the date.

Description

Display the contents of the syslog file by index. Default starts from top.

show traplog index

Syntax

```
show traplog index <number> <parameters>
```

Parameters

```
[top <number of lines>]
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
[loglastminutes <minutes>]
[logdate <MMDD>]
[logdate <MMDD-MMDD>]
```

Description

Displays all current trap log information. The index number displays detailed information about a selected trap log.

show traplog device

Note: Type show traplog to display the index.

Syntax

```
show traplog device <Device Name or IP address> [index <number>]
```

Description

Displays the current trap log information for an Ethernet device using name, IP address, or index number.

show traplog group

Note: Type *show traplog* to display the index.

Syntax

```
show traplog group <Device Group Name> [index <number>]  
Group name: SLM, SLC, SLK, RPM, SCS, SLB, SPDR, WiBox, LTRX, or other
```

Description

Displays the current trap log information for an Ethernet device group by index number.

12: Using vSLM 2 Software on a Mobile Browser

The vSLM 2 secure management software's WAP technology enables you to access the status of your vSLM 2 software from your mobile phone. This chapter familiarizes you with how to do this. For more detailed information about the options, please see the other chapters in this user guide.

Requirements

- ◆ To access vSLM 2 secure management software for mobile web browsers, your phone must meet the following minimum requirements:
- ◆ Your phone's web browser must be XHTML Mobile 1.0-compliant, which most mobile browsers are.
- ◆ If you want to access the SLM WAP site via SSL (https), your phone browser must support SSL. An example of such a browser is Opera® Mini.
- ◆ Your phone's browser does not need to support cookies or JavaScript.
- ◆ Your wireless provider may charge you, Depending on your service plan, Check with your provider for more information about fees associated with accessing the Internet from your mobile phone.

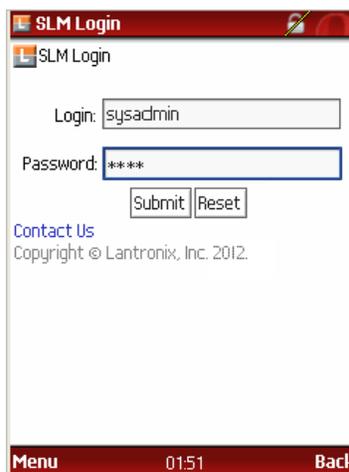
Using the SLM Mobile Browser

Logging in to the vSLM 2 Software

To log into the vSLM 2 software:

1. Enter `http://(vSLM 2 software's IP address)/wap` or `https://(vSLM 2 IP address)/wap` in your phone's web browser to log in to vSLM 2 secure management software.

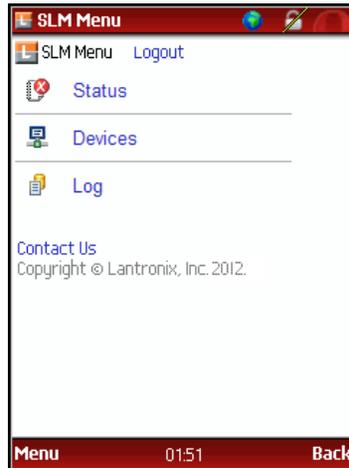
The Login page displays.



2. Enter your SLM login name and password.

3. Move the cursor to the **Submit** button and select it.

The SLM main menu (Home page) displays a list of options:



Using Links to Select Options

To select an option:

1. Click the link (blue). For example, click **Log** on the Home page to display a menu of logs.

Using the Keypad to Select Options

Note: *Shortcut keys only work with a true WAP browser (not browsers such as IE or FireFox).*

1. When a number precedes an option, tap the number on the keypad to open the link.



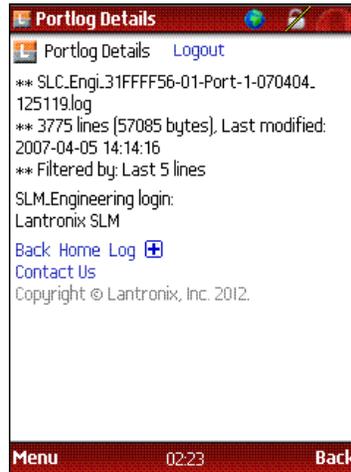
For example, to select **Managed Devices** in the example above, tap the **3** key.

Obtaining More Data

A + (plus) and/or a - (minus) button may display at the bottom of a page.

- ◆ If there is a +, select it or tap the * (star key) to advance to the next page of details.

- ◆ If there is - (minus), select it or tap the # (pound key) to return to the previous page. For example, towards the bottom of the Portlog Details page, the + symbol displays.



If you select the +, further details display.



If you select the -, the previous page of details displays.

Logging Out

To log out of the vSLM 2 secure management software:

1. Select **Logout** (at the top right of each page).

Table 12-1 Navigation Summary

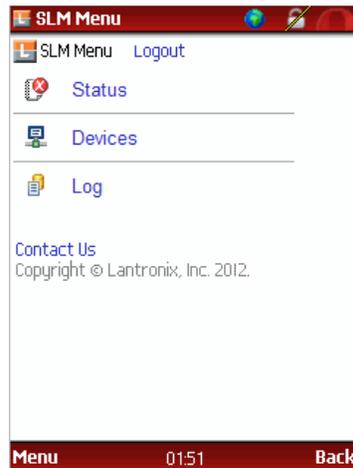
To	Select on the browser page	Tap on the keypad
Return to the Home page	Home (bottom of page)	0 (zero)
Select menu option	Link (blue)	When a number precedes an option, the number on the keypad.
See more details (if available)	+	* (star key)
Return to previous details	-	# (pound key)

To	Select on the browser page	Tap on the keypad
Return to the previous page	Back (bottom of page)	Back or its equivalent on your phone
Return to a menu	Name of menu (if at bottom of page)	
Log out	Logout (top of any page)	

Main Menu

To use the SLM Menu (main menu):

- To use the main menu, select one of the following links:
 - ◆ **Status:** Displays the status of the vSLM 2 secure management software.
 - ◆ **Devices:** Displays information about Ethernet and Managed devices.
 - ◆ **Log:** Displays audit, port, system, and trap logs.



The menu for the selected category opens.

Status Menu

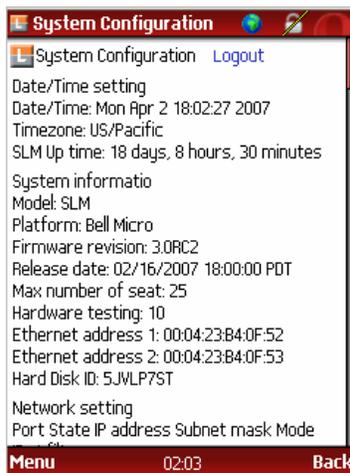
The SLM Status menu has three options: System Information, Connections, and Routes.



System Information

To view the status of the system:

1. On the Status Menu, select **System Information** or tap the **1** key. The system configuration displays.



Connections

To view information about the vSLM 2 software's connections:

1. On the Status Menu, select **Connections** or tap the **2** key. The Connections menu displays.



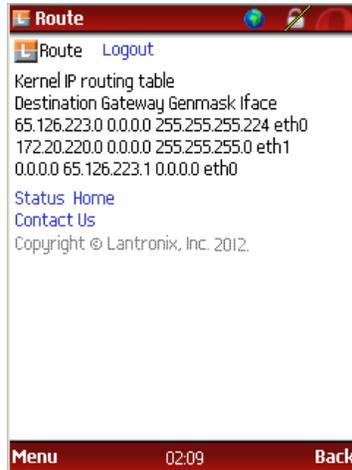
2. To view individual connections, click the blue link on the Connections menu or tap the key number displayed to the left of the option.



Route Information

To view SLM route information:

1. On the Status Menu, select **Routes**, or tap the **3** key.



Device Menu

The Device Menu provides access to Ethernet devices, unreachable Ethernet devices, and Managed Devices.

To view information about the devices the vSLM 2 secure management software is managing:

1. On the Main menu, select **Devices**. The Devices menu displays.



Ethernet Devices

To view information about an Ethernet device:

1. From the Devices menu, select **Ethernet Devices**.



The green icon to the right of a device indicates that the device is reachable; the red indicates that the device is unreachable.

2. Select the unit you want to view. Details about the device display.



Ethernet Unreachable Devices

To view Ethernet devices to which the vSLM 2 secure management software has not been able to connect:

1. On the Devices menu, select **Ethernet Unreachable Devices**. The Ethernet Unreachable Devices page displays a list of unreachable devices.



2. To view device details, select the device.



Managed Devices

To obtain information about managed devices:

1. Select **Managed Devices** on the Devices menu. The Managed Devices page displays a list of managed devices.



2. Select a managed device to view its details.



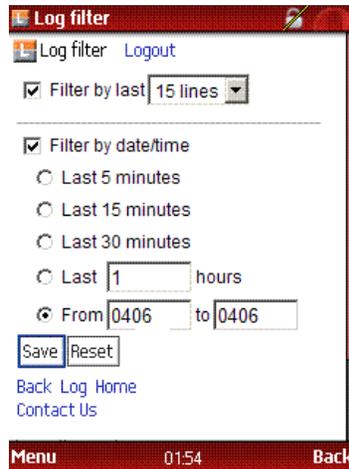
Log Menu

Filtering Logs

The Log filter page enables you to view logs matching specified criteria (number of lines and date/time). The settings are for the current session only. Once you save the filter, it applies for all log commands and is available as long as you are on the system (until logout or timeout).

To define a filter:

1. Click the **Filter** link at the bottom of the Log menu. The Log Filter page displays.



2. Select one or both of the following:

Table 12-2 Log Filter by Last and Date/Time

Setting	Description
Filter by last	Select the check box and from the drop-down list, select the number of lines at the end of the log you want to see.
Filter by date/time	Select the check box and time period you want to see.

3. Select the **Save** button.

Example:

If you set Filter by last to 5 in log filter page and enable the filter, only the last 5 lines of a log file displays.

When you select +, it displays 10 (2X5), if available

When a user select + again, it displays 15 (3X5), if available

Minus works in the other direction.

View Logs

To view audit, trap, system, or port logs:

1. Select **Log** on the Main menu. The SLM Log menu displays.



2. Select the type of log you want to see (e.g., tap **2** to see the vSLM 2 software's audit logs).



3. Select the log to view details.



4. Select the + button to see more details.



5. Select the + to scroll to see more lines of details.

Note: You can set the number of lines you see at a time on the Log filter page.

Appendix A: Command Reference

After an introduction to using commands, this chapter lists and describes all of the commands available on the SLM command line interface accessed through SSH, secure channel (SLC console manager only), Telnet, or a serial connection. The commands are in alphabetical order by category.

Introduction to Commands

Command Syntax

Commands have the following format:

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

where

<action> is set, show, connect, diag, admin, or logout.

<category> is a group of related parameters you want to configure or view. Examples are devicegroup, account, and network.

<parameter(s)> is one or more name-value pairs in one of the following formats:

Table A-1 Command Syntax

	Description
<parameter name> <aa bb>	Specify one of the values (aa or bb) separated by a vertical line (). The values are all lowercase and must be entered exactly as shown. Bold indicates a default value.
<parameter name> <Value>	Specify an appropriate value, for example, a device group name. This User Guide shows parameter values in mixed case to indicate they are case sensitive. For example, if you saved a device group name in mixed case, you must enter it in mixed case; if you saved it in lowercase, you must enter it in lowercase.
Square brackets []	Indicate optional parameters.

Table A-2 Actions and Category Options

Action	Category
set	network service ipfilter account accountgroup auth nis ldap radius kerberos tacacs+ ethernetdevice manageddevice mgroup datetime cli menu sshkey history modem dialaccount persistent ipmi ilo
show	network service ipfilter iptables account accountgroup auth nis ldap radius kerberos tacacs+ device port ethernetdevice manageddevice auditlog syslog portlog traplog eventlog sessionlog datetime cli menu sshkey history connection progress sysconfig sysinfo modem dialaccount routing persistent ipmi ilo user

Action	Category
connect	device remote index ssh telnet tn3270 terminate persistent wakeonlan
diag	ping ping6 arp traceroute netstat nettrace internals
admin	autodetect locallog version option showoptions config quicksetup securechannel signature banner reboot shutdown showbootbank switchbank copybank web
logout	Terminates CLI session.

Command Help

For general command help, type: `help`

For more information about a specific command, type `help` followed by the command, for example:

```
help set network
```

OR

type `?` after the command:

```
set network ?
```

Tips

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


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

 can be shortened 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** to complete the name if only one is possible, or to display the possible names if more than one is possible.
- ◆ Should you make a mistake while typing, backspace by pressing the **Backspace** key 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.
- ◆ When the number of lines displayed by a command exceeds the size of the window (the default is 20), the "--Type 'm' (more) to see the next page--" message displays. To display the next page, type `more` and press **Enter**. You can override the number of lines (or disable the feature altogether) with the `set cli` command.
- ◆ To clear an IP address, type `0.0.0.0`.

Authentication Commands

set auth

Syntax

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

Parameters

```
local <1-6>
nis <1-6>
ldap <1-6>
radius <1-6>
kerberos <1-6>
tacacs+ <1-6>
authusenextmethod <enable|disable>
limitsysadmin <enable|disable>
```

Description

Sets ordering of authentication methods and how authentication methods are used.

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

Any methods omitted from the `set auth` command will be disabled if at least one method is selected

set ldap

Syntax

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

Parameters

```
state <enable|disable>
server <IP Address or Name>
port <TCP Port>
base <LDAP Base>
bindname <Bind Name>
bindpassword <Bind Password>
adsupport <enable|disable>
encrypt <starttls|ssl|disable>
filteruser <User Login Attribute|CLEAR>
filtergroup <Group Filter Objectclass|CLEAR>
grmemberattr <Group Member Attribute|CLEAR>
grmembervalue <dn|name>
```

Description

Configures the vSLM 2 secure management software to use LDAP to authenticate users who log in to the vSLM 2 software via SSH, Telnet, the web, or the console port.

set nis**Syntax**

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

Parameters

```
state <enable|disable>
domain <NIS Domain Name>
broadcast <enable|disable>
master <IP Address or Name>
slave1 <IP Address or Name>
slave2 <IP Address or Name>
slave3 <IP Address or Name>
slave4 <IP Address or Name>
slave5 <IP Address or Name>
```

Description

Configures the vSLM 2 secure management software to use NIS to authenticate users who log in to the vSLM 2 software via SSH, Telnet, the web, or the console port.

set radius**Syntax**

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

Parameters

```
state <enable|disable>
timeout <1-30 seconds>
server1 <IP Address or Name>
port1 <TCP Port>
secret1 <Secret>
server2 <IP Address or Name>
port2 <TCP Port>
secret2 <Secret>
```

Description

Configures the vSLM 2 secure management software to use RADIUS to authenticate users who login to the vSLM 2 software via SSH, Telnet, the web, or the console port.

set sshkey copybank dest**Syntax**

```
set sshkey copybank dest <alt|cur>
```

Description

Copy ssh keys between boot banks.

set sshkey delete**Syntax**

```
set sshkey delete keyuser <SSH Key User> keyhost <SSH Key Host>
```

Description

Deletes an imported SSH key.

set sshkey import**Syntax**

```
set sshkey import <copypaste>
```

Note: RSA keys must be 1024 bits

Description

Imports an SSH key.

set ilo**Syntax**

```
set ilo
```

Parameters

```
led <on | off>  
ipaddr <IP Address>  
user <User Name>  
[password <Password>]
```

Description

Control LED of HP iLO remote device.

set persistent ipmi**Syntax**

```
set ipmi power <on|off|cycle|reset|diag>
```

Parameters

```
ipaddr <IP Address>  
[user <User Name>]  
[password <Password>]
```

Description

Control an IPMI-remote enabled remote device.

show auth**Syntax**

```
show auth
```

Description

Displays ordering of authentication methods and how authentication methods are used.

show ipmi**Syntax**

```
show ipmi chassis <power|status>
```

Parameters

```
ipaddr <IP Address>  
[user <User Name>]  
[password <Password>]
```

Description

Display status of an IPMI enable remote device.

show ldap**Syntax**

```
show ldap
```

Description

Displays all LDAP information used to authenticate users who login to the SLM via SSH, Telnet, the Web or the Console Port.

show nis**Syntax**

```
show nis
```

Description

Displays all NIS information used to authenticate users who login to the SLM via SSH, Telnet, the Web or the Console Port.

show radius**Syntax**

```
show radius
```

Description

Displays all RADIUS information and configure the SLM to NIS to authenticate users who login to the SLM via SSH, Telnet, the Web or the Console Port.

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 imported SSH keys.

show sysinfo**Syntax**

```
show sysinfo
```

Description

Displays system file changes.

show ilo**Syntax**

```
show ilo led status
show ilo health <sensor | fan | all>
```

Parameters

```
ipaddr <IP Address>
user <User Name>
[password <Password>]
```

Description

Display health status of HP iLO remote device.

Account Commands

Use the following commands to configure local accounts (including sysadmin) to authenticate users who login to the vSLM 2 secure management software by means of SSH, Telnet, the web, or the console port.

set account add**Syntax**

```
set account add <User Name> group <Group Name|admin> <parameters>
```

Parameters

```
[email <Email Address>]
[auth <local|remote|localremote|disable>]
[allowdialback <enable|disable>]
```

```
[dialbacknumber <dial-back number>]
[allowpwchange <enable|disable>]
[pwneverexpires <enable|disable>]
[changepwnextlogin <enable|disable>]
```

Description

Creates a new user account.

set account delete**Syntax**

```
set account delete <User Name>
```

Description

Deletes a user account.

set account edit**Syntax**

```
set account edit <User Name> <parameters>
```

Parameters

```
[email <Email Address|CLEAR>]
[auth <local|remote|localremote|disable>]
[allowdialback <enable|disable>]
[dialbacknumber <dial-back number|CLEAR>]
[allowpwchange <enable|disable>]
[pwneverexpires <enable|disable>]
[changepwnextlogin <enable|disable>]
```

Description

Modifies a user account.

set account password**Syntax**

```
set account password <User Name>
```

Note: Administrators with permission to change passwords must enter the username. Other users may not enter a username (they are changing their own password).

Description

Configures a user account's password for the vSLM 2 secure management software.

show account**Syntax**

```
show account <User Name>
show account user <User Name>
```

Description

Displays account information by user name.

```
show account all
```

Syntax

```
show account all  
show account
```

Description

Displays all account names and information.

```
show account index
```

Note: Type `show account all` to display the index.

Syntax

```
show account index <number>
```

Description

Displays accounts by index number.

```
show account search
```

Syntax

Note: All searches are case insensitive.

```
show account search name <name>  
show account search email <email address>
```

Examples

```
show account search name sys
```

Description

Searches for accounts by name or email address.

Account Group Commands

```
set accountgroup add
```

Syntax

```
set accountgroup add <Group Name> type <ethernet|managed|menu|device>  
<parameters>
```

Parameters

```
[menu <Menu Name>]  
[dataports <Port List>]
```

```
[listenports <Port List>]
[clearports <Port List>]
[accessoutlets <Outlet List>]
[escapeseq <1-10 Chars>]
[breakseq <1-10 Chars>]
[custommenu <Menu Name>]
[displaymenu <enable|disable>]
[allowdialback <enable|disable>]
[dialbacknumber <Phone Number>]
[permissions <Permission List>]
```

Description

Creates a local account group. Group type is Administrators, Ethernet, Managed, or Menu User.

set accountgroup edit**Syntax**

```
set accountgroup edit <Group Name> <one or more parameters>
```

Parameters

```
[name <new name>]
[menu <Menu Name|CLEAR>]
[dataports <Port List|CLEAR>]
[listenports <Port List|CLEAR>]
[clearports <Port List|CLEAR>]
[accessoutlets <Outlet List|CLEAR>]
[escapeseq <1-10 Chars>]
[breakseq <1-10 Chars>]
[custommenu <Menu Name|CLEAR>]
[displaymenu <enable|disable>]
[allowdialback <enable|disable>]
[dialbacknumber <Phone Number|CLEAR>]
[permissions <Permission List|CLEAR>]
```

Description

Modifies an account group. Group type is Administrators, Ethernet User, Managed User, or Menu User. CLEAR removes the current menu assignment.

show accountgroup**Syntax**

```
show accountgroup <Group Name>
show accountgroup name <Group Name>
```

Description

Displays account group information.

show accountgroup all**Syntax**

```
show accountgroup all
show accountgroup
```

Description

Displays information about all account groups.

show accountgroup index

Note: Type `show accountgroup all` to display the index.

Syntax

```
show accountgroup index <number>
```

Description

Displays account groups by index number.

Administrative Commands

admin autodetect filter

Syntax

```
admin autodetect filter delete
```

Deletes one of the current auto-detect search filters. The command displays an index of current filters. Type the index number of the filter you want to delete and press **Enter**.

```
admin autodetect filter ltrx <IP subnet>
```

Sets Lantronix discovery protocol search filters.

```
admin autodetect filter scs <IP range> [timeout <number of milliseconds>]
```

Sets SCS discovery protocol search filters.

Example

```
IP range: 192.168.0.1-192.168.0.155
timeout : 100ms (default)
```

```
admin autodetect filter snmp <IP range> [community <name>][timeout
<number of milliseconds>]
```

Sets SNMP protocol search filters.

Example

```
IP range: 192.168.0.1-192.168.0.155
name: public (default)
```

```
admin autodetect filter show
```

Displays the current auto-detect search filters.

Description

Configures or displays the protocol and filters.

admin autodetect start**Syntax**

```
admin autodetect start
```

Description

Starts the SLM auto-detect device process, using the protocol and filters configured.

admin banner**Syntax**

```
admin banner welcome <Banner Text>  
admin banner login <Banner Text>  
admin banner logout <Banner Text>
```

Description

Configures the banner displayed before login (welcome), after login, or after logout. To insert line feeds in the banner, use the '\\n' character sequence.

admin banner show**Syntax**

```
admin banner show
```

Description

Displays the banner configuration.

admin copybank**Syntax**

```
admin copybank
```

Description

Copies the SLM firmware running in the current bank to the other bank.

admin config**Syntax**

```
admin config factorydefaults
```

Description

Restores the SLM configuration and device database settings to factory defaults.

admin config rebuilddatabase**Syntax**

```
admin config rebuilddatabase
```

Description

Removes and rebuilds the SLM configuration and database from scratch, in case of database corruption that cannot be fixed by the factory default.

admin config save**Syntax**

```
admin config save file <filename>
```

Description

Save the vSLM configuration to the vSLM Configuration Files directory.

admin locallog**Syntax**

```
admin locallog clear auditlog
admin locallog clear syslog
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, RPM, SCS, SLB, SPDR, WiBox, LTRX, or other
```

Description

Clears all of the entries in the auditlog or syslog or traplog.

admin option**Syntax**

```
admin option <Option Name> value <Option Value>
```

Description

Adds license options.

admin quicksetup**Syntax**

```
admin quicksetup
```

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command. Runs the Quick Setup script to configure network settings, gateway, hostname, date & time, time zone, and sysadmin password.

admin reboot**Syntax**

```
admin reboot
```

Description

Terminates all connections and reboots the vSLM 2 secure management software.

admin securechannel regenkey**Syntax**

```
admin securechannel regenkey
```

Description

Regenerates the secure channel key.

Note: *With this command, you lose access to established secure channels; therefore, the vSLM 2 software first requests confirmation that you want to regenerate the secure channel key.*

admin showbootbank**Syntax**

```
admin showbootbank
```

Description

Displays the SLM boot bank.

admin showoptions**Syntax**

```
admin showoptions
```

Description

Display license options.

admin shutdown**Syntax**

```
admin shutdown
```

Description

Terminates all connections, shuts down the vSLM 2 secure management software, and turns off the power.

admin switch bank**Syntax**

```
admin switchbank bank [1|2]
```

Description

Switches the vSLM 2 software to the next boot bank.

admin signature restore**Syntax**

```
admin signature restore
```

Description

Restores signature information to the system.

admin signature show**Syntax**

```
admin signature show
```

Description

Displays signature information.

admin version**Syntax**

```
admin version
```

Description

Displays current application version information.

admin web certificate**Syntax**

```
admin web certificate reset  
admin web certificate show
```

Description

Reset SSL web certificate to default.

Displays current SSL web certificate.

show progress**Syntax**

```
show progress
```

Description

Shows the progress of background tasks.

show sysconfig**Syntax**

```
show sysconfig [email <Email Address>]
```

Description

Displays a report of configurable parameters. The output can be emailed.

All Devices Commands

show device

Note: Entries are not case sensitive.

Syntax

```
show device <device name>
```

Description

Searches for and displays Ethernet or managed devices by device name. For example, if you specify `name slc`, the vSLM 2 secure management software searches for all Ethernet and managed devices whose name starts with `slc`.

show device all

Syntax

```
show device all  
show device
```

Description

Displays all Ethernet and managed devices.

show device index

Note: Type `show device all` to display the index.

Syntax

```
show device index <number>
```

Description

Displays Ethernet or managed devices by index.

Auto-Detect Commands

admin autodetect filter delete

Syntax

```
admin autodetect filter delete
```

The command displays an index of current filters. Type the index number of the filter you want to delete and press **Enter**.

Description

Deletes one of the current auto-detect search filters.

admin autodetect filter ltrx**Syntax**

```
admin autodetect filter ltrx <IP range> [timeout <number of milliseconds>]
```

Example

```
IP range: 192.168.0.1-192.168.0.155 timeout 1500  
timeout: default is 1000 ms; range is 1000-60000 ms
```

Description

Sets Lantronix discovery protocol search filters. The ending IP address is optional.

admin autodetect filter scs**Syntax**

```
admin autodetect filter scs <IP range> [timeout <number of milliseconds>]
```

Example

```
IP range: 192.168.0.1-192.168.0.155  
timeout: default is 100ms; range is 100-60000ms
```

Description

Sets SCS discovery protocol search filters.

admin autodetect filter show**Syntax**

```
admin autodetect filter show
```

Description

Displays the current auto-detect search filters.

admin autodetect filter snmp**Syntax**

```
admin autodetect filter snmp <IP range> [community <name>] [timeout <number of milliseconds>]
```

Example

```
IP range: 92.168.0.1-192.168.0.155  
name: public (default)  
timeout: default is 100ms; range is 100-60000ms
```

Description

Sets SNMP protocol search filters.

admin autodetect start**Syntax**

```
admin autodetect start <one or more parameters>
```

Parameters

```
[securechannel <default|password>]  
[option <ltrxonly|delnonltrx>]
```

`ltrxonly` detects only Lantronix devices

`delnonltrx` detects only Lantronix devices and removes existing non-Lantronix devices.

Examples

```
admin autodetect start securechannel default
```

Attempts secure channel using the default password

```
admin autodetect start securechannel mypass option delnonltrx
```

Attempts secure channel using password `mypass`. Detects only Lantronix devices and removes existing non-Lantronix devices.

Description

Starts the vSLM 2 secure management software auto-detect device process, using the protocol and filters configured.

show progress**Syntax**

```
show progress
```

Description

Shows the progress of background tasks.

CLI Commands

The following commands relate to the CLI itself.

set cli terminallines**Syntax**

```
set cli terminallines <disable|1-1000>
```

Description

Sets the number of lines that display in a page for the auditlog, syslog, and device list. Default is **20**.

set history clear**Syntax**

```
set history clear
```

Description

Clears the CLI command history.

show cli

Syntax

show cli

Description

Displays the terminal lines settings.

show history

Syntax

show history

Description

Displays the 100 most recent CLI commands.

Connection Commands

Administrators, Ethernet Users and Menu Only Users

connect device

Syntax

connect device <Device Name or IP Address> <one or more parameters>

Parameters

[<secure|ssh|telnet|tn3270|serial|modem|modemssh|modemtelnet>
modemcallback>] [port <port>]

Specify *secure* to connect through a secure channel. Secure channel is the default method of connection for SLC/SLB devices, SLC ports, and vSLM 2 secure management software, and SSH is the default for other devices.

Port is the number of a physical port on the SLC console manager.

SLC48 console manager has ports 1 to 48.

Modem connection is available for managed devices only.

With the *modemssh* option, the vSLM 2 secure management software dials out to the managed device in PPP, and then connects it via SSH.

With *modemtelnet* option, the vSLM 2 software dials out to the managed device in PPP, and then connects it via Telnet.

With the *modemcallback* option, when the SLM user calls an SLC device and logs in, the SLC module hangs up and calls the user back. The vSLM 2 secure management software then logs in again. This feature is currently available in text mode only.

Examples

```
connect device slc-waimea
connect device slc-waimea-port-1
connect device slc-waimea ssh
connect device slc-waimea port 4
connect device slc-waimea modemssh
connect device slc-waimea modemcallback
```

Description

Connects to an Ethernet device, managed device, or device port.

connect index

Note: Type `show device all` to display the index.

Syntax

```
connect index <number> <one or more parameters>
```

Parameters

```
[<secure|ssh|telnet|serial|modem|modemssh|modemtelnet| modemcallback>]
[<SSH flags>]
<SSH flags> is one or more of: user <Login Name>
                                version <1|2>
                                escape <Character>
```

Description

Connects a device by index number.

connect persistent**Syntax**

```
connect persistent <persistentConnectionName> [device <devname|IP>]
```

Notes: The `device` parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name.

The `<devname>` following device may be the name of an Ethernet device or the name of a managed device. Persistent connections automatically belong to managed devices that have an Ethernet device component that has persistent connections defined.

Description

Connect to an existing persistent connection.

connect ssh**Syntax**

```
connect ssh <IP Address or Name> [tcpport <TCP Port>] [<SSH flags>]
```

Parameters

<SSH flags> is one or more of:

```

user <Login Name>
version <1|2>
escape <Character>

```

The TCP `PORT` parameter is the TCP port number; the default is **22**.

Description

Connect to any machine/device using standard SSH V1 or V2 protocol.

connect telnet

Syntax

```
connect telnet <IP Address> [tcpport <TCP Port>] [user <Login Name>]
```

`tcpport` is the TCP port number; the default is **23**.

Description

Connects to a device by means of standard Telnet.

connect tn3270

Syntax

```
connect tn3270 <IP Address or Name> [tcpport <TCP Port>] [user <Login Name>]
```

Description

The `tcpport` parameter is the TCP port number and default is 23.

show connection list

Syntax

```
show connection list
```

Description

Displays the active user connections in short form.

Managed Device Users

connect device

Syntax

```
connect device <Device Name or IP Address> <one or more parameter>
[<secure|ssh|telnet|serial|modem|modemssh|modemtelnnet|modemcallback>][po
rt <port>]
```

Specify `secure` to connect through a secure channel. Secure channel is the default method of connection for SLC/SLB device, SLC ports, and vSLM 2 secure management software, and SSH is the default for other devices.

Port is the number of a physical port on the SLC console manager.

SLC48 console manager has ports 1 to 48.

Modem connection is available for managed devices only.

With the `modemssh` option, the vSLM 2 software dials out to the managed device in PPP, and then connects it via SSH.

With `modemtelnet` option, the vSLM 2 secure management software dials out to the managed device in PPP, and then connects it via Telnet.

With the `modemcallback` option, when the vSLM 2 software user calls an SLC device and logs in, the SLC module hangs up and calls the user back. The vSLM 2 secure management software then logs in again. This feature is currently available in text mode only.

Examples

```
connect device slc-waimea
connect device slc-waimea-port-1
connect device slc-waimea ssh
connect device slc-waimea port 4
connect device slc-waimea modemssh
connect device slc-waimea modemcallback
```

Description

Connects to a managed device through a secure channel.

connect index

Note: Type `show managedevice all` to display the index.

Syntax

```
connect index <number>
[<secure|ssh|telnet|serial|modem|modemssh|modemtelnet| modemcallback>]>
[<SSH flags>]
    <SSH flags> is one or more of: user <Login Name>
                                version <1|2>
                                escape <Character>
```

Description

Connects to a device by index number.

connect remote

Syntax

```
connect remote show connections <Device Name or IP Address>
connect remote terminate <Device Name or IP Address> (id <connectionId>)
```

Parameters

```
<Device Name or IP Address>
id <connectionid>
```

Description

Displays or terminates user connections on a remote Ethernet device. The specified device must exist in the SLM database.

connect wakeonlan**Syntax**

```
connect wakeonlan
```

Parameters

```
Device <Device Name or IP Address> (password <Password>)
```

Description

Send a Wake On LAN packet to an Ethernet device. The specified device must exist in the SLM database.

Date and Time Commands

set datetime**Syntax**

```
set datetime <one parameter>
```

Parameters

```
date <MMDDYYhhmm[ss]>
```

```
timezone <Time Zone>
```

Description

Sets the local date, time, and time zone (one parameter at a time).

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

show datetime**Syntax**

```
show datetime
```

Description

Displays the local date, time, and time zone.

Diagnostic Commands

diag arp**Syntax**

```
diag arp
```

Description

Displays the ARP table for mapping IP addresses to hardware addresses.

diag netstat**Syntax**

```
diag netstat [<tcp|udp|all>] [statistics]
```

Description

Displays output IP routing table, and optionally, network connections and statistics.

diag nettrace**Syntax**

```
diag nettrace <one or more parameters>
```

Parameters

```
[ethport <1|2>]
[protocol <tcp|udp|icmp>]
[host <IP Address or Name>]
[numpackets <number of packets>] [snaplen <capture bytes>]
[verbose <0|1|2|3>]
```

Defaults: ethport=1, verbose=1

Example

```
diag nettrace protocol udp verbose 2
```

Description

Displays all network traffic, applying optional filters.

diag ping**Syntax**

```
diag ping <IP Address or Name> <one or more parameters>
```

Parameters

```
count <Number of Times to Ping>
```

Default is 5.

```
packetsize <Size in Bytes>
[packetsize <size in bytes>]
```

Defaults: count=5, packetsize=64.

Description

Verifies that the vSLM 2 secure management software can reach a host over the network.

diag ping6**Syntax**

```
diag ping6 <IP Address or Name> <one or more parameters>
```

Parameters

```
interface <interface name>
count <Number of Times to Ping>
[packetize <size in bytes>]
```

Defaults: count=5, packetize= 64.

```
packetize <Size in Bytes>
```

Default is 64.

Examples

```
diag ping6 fe80::214:85ff:fec0:928e interface eth1
```

Description

Verifies that the vSLM 2 software can reach a host over the network.

diag traceroute**Syntax**

```
diag traceroute <IP Address or Name>
```

Description

Displays the route that packets take to get to a network host.

diag internals**Syntax**

```
diag internals
```

Description

Displays information on the internal memory, storage and processes of the vSLM 2 secure management software.

Dial Account Commands

set dialaccount add**Syntax**

```
set dialaccount add <Dial Account Name> <parameters>
```

Parameters

```
modemmode <text|ppp>
```

Note: If you select `text`, all other parameters except `timeout` are ignored.

```
modemmode <text|ppp>
localipaddr <negotiate|IP Address>
remoteipaddr <negotiate|IP Address>
auth <pap|chap>
```

```
username <User Name>
password <Password>
nat <enable|disable>
timeout <disable|1-30 minutes>
```

Default is 20.

Description

Creates a new dial account.

set dialaccount delete

Syntax

```
set dialaccount delete <Dial Account Name>
```

Description

Delete a dial account.

set dialaccount edit

Syntax

```
set dialaccount edit <Dial Account Name> <parameters>
```

Parameters

```
modemmode <text|ppp>
localipaddr <negotiate|IP Address>
remoteipaddr <negotiate|IP Address>
auth <pap|chap>
username <User Name>
password <Password>
nat <enable|disable>
forcedialback <disable|enable> (applies only to text mode)
callback <disable|enable> (text mode for SLC dialback)
dialbacknumber <dial-back number|CLEAR> (applies only to text mode)
```

CLEAR removes the dial-back number.

```
useraccount <disable|enable> (text mode dialback)
```

Uses local user-defined dial-back configuration.

```
timeout <disable|1-30 minutes>
```

Note: The parameter "dialbacknumber CLEAR" remove the dial-back number. The parameter "useraccount enable" use local user defined dial-back configuration.

Description

Modifies a dial account's settings.

set manageddevice config**Syntax**

```
set manageddevice config <Device Name> [dialout <Dial Account
Name|enable|disable> modem <Modem Name> phonenumber <phonenumber>]
application <ssh|telnet|http|none>]
```

Description

Configures modem and dial account settings for a managed device.

set manageddevice index

Note: Type `show manageddevice all` to display index.

Syntax

```
set manageddevice index <number> [dialout <Dial Account
Name|enable|disable> modem <Modem Name> phonenumber <phonenumber>]
application ssh|telnet|http|none]
```

Description

Finds managed device by index and modifies dial account settings.

To set modem parameters, you must specify a dial-out option.

set modem edit**Syntax**

```
set modem edit <Modem Name> <parameters>
```

Parameters

```
name <New Name>
baud <300-115200>
flowcontrol <none|xon/xoff|rts/cts>
speaker <enable|disable>
initscript <Modem Initialization Script>
defaultinitscript <Modem Default Initialization Script>
dialin <Dial Account Name|CLEAR|disable|enable>
ipfilter <IPv4 Filter Name|CLEAR>
number <modem telephone number|CLEAR>
```

Note: The parameter "ipfilter CLEAR" remove the ipfilter assignment. The parameter "dialin CLEAR" remove the dial account assignment. The parameter "dialin disable" disable dialin. The parameter "dialin enable" enable dialin.

Description

Configures a curently loaded modem.

show dialaccount

Note: Type `show dialaccount` to display index.

Syntax

```
show dialaccount <parameters>
```

Parameters

```
[name <Dial Account Name>]
[index <number>]
```

Examples

```
show dialaccount
show dialaccount name ppp-pap
show dialaccount index 2
```

Description

Displays dial account settings.

show dialaccount mapping**Syntax**

```
show dialaccount mapping
```

Description

Shows dial account used by dial-in and dial-out.

Ethernet Device Commands

set ethernetdevice**Syntax**

```
set ethernetdevice add <New Device Name> mac <MAC> ipaddr <IP Address>
    type <slm|slc|slc80xx|slk|rpm|slb|spider|scs0520|scsxx00|
        wibox|uds|eds|edsmd|xport|pwave|other|non>
    [portcount <# of ports>] (default 0)
set ethernetdevice assign
```

Description

Create a new ethernet device and optional ports.

set ethernetdevice assign**Syntax**

```
set ethernetdevice assign <ethernetDevice|IP> group
<ethernetAccoutGroup> [remove]
```

Description

Assigns or removes permissions for an Ethernet device by name.

set ethernetdevice config**Syntax**

```
set ethernetdevice config <Device Name or IP Address> <one or more
parameters>
```

Parameters

```
[delete]
[dialout <Dial Account Name|enable|disable> phonenumber <phone number>]
[disconnect modem]
[name <Device Name>]
[ipaddr <IP Address>]
[location <Location|CLEAR>]
[sublocation <Sub-Location|CLEAR>]
[login <Loginname>]
[model <Model>]
[readinfo]
[sshport <TCP Port for SSH>]
[tnport < TCP Port for Telnet>]
[tn3270lu <Logical Unit>]
[version <Version>]
```

Description

Finds Ethernet devices by device name or IP address and modifies device parameters.

set ethernetdevice delete**Syntax**

```
set ethernetdevice delete <Device Name or IP Address>
```

Finds Ethernet device using device name or IP address and deletes the device.

```
set ethernetdevice delete <Device Name or IP Address> portnumber <port
number or port number range>
```

port number range, for example, 1-4

Finds a port by Ethernet device name or IP address with the port number and deletes the port.

Examples

```
set eth delete slc-waimea
set eth delete slc-waimea port 5
set eth delete slc-waimea port 1-5
set eth conf slc-waimea delete
```

Description

Finds Ethernet device or Ethernet device port and deletes it.

set ethernetdevice port**Syntax**

```
set ethernetdevice port <Device Name or IP Address> portnumber <port
number or list> <one or more parameters>
```

Parameters

```
[name <New Port Name>]
```

```
[state <on|off|cyclepower>] (available for RPM/SLP power manager only)
```

Powers Ethernet device port on or off.

Note: Only RPM/SLP outlet action supports a port list.

Examples

To power up RPM/SLP outlet 2:

```
set eth port slp-sunset po 2 state on
```

To power up RPM/SLP outlet port list 1-3,6,8-14

```
set eth port slp-sunset po 1-3,6,8-14 state on
```

Description

Finds a port by device name or IP address with the port number and modifies port parameters.

set ethernetdevice sync**Syntax**

```
set ethernetdevice sync <Device Name or IP Address> action <read|write>
```

Description

Finds an Ethernet device-by-device name or IP address and synchronizes device information.

show device

Note: Entries are not case sensitive.

Syntax

```
show device <device name>
```

Description

Searches for and displays Ethernet or managed devices by device name.

show device all**Syntax**

```
show device all
show device
```

Description

Displays all Ethernet and managed devices.

show ethernetdevice account**Syntax**

```
show ethernetdevice account <accountName>
```

Description

Displays all Ethernet devices viewable by the specified user account.

show ethernetdevice accountgroup**Syntax**

```
show ethernetdevice accountgroup
```

Description

Displays all Ethernet devices viewable by users whose accounts belong to the specified account group.

show ethernetdevice all**Syntax**

```
show ethernetdevice all
```

Description

Displays all Ethernet device information.

show ethernetdevice config**Syntax**

```
show ethernetdevice config <Device Name or IP Address>
```

Description

Finds an Ethernet device-by-device name or IP address and displays device information.

show ethernetdevice firmware**Syntax**

```
show ethernetdevice firmware
```

Description

Displays firmware versions of all Ethernet devices managed by the vSLM 2 secure management software.

show ethernetdevice group**Syntax**

```
show ethernetdevice group <Group Name> [firmware]
group name: SLM, SLC, SLK, RPM, SCS, SLB, SPDR, WiBox, UDS, EDS, EDSMD,
XPORT, PWAVE, LTRX, or other
```

Note: Ethernet device group names are not case sensitive.

Description

Displays Ethernet devices by device group.

show ethernetdevice index**Syntax**

```
show ethernetdevice index <number>
```

Description

Displays Ethernet devices by index.

show ethernetdevice list**Syntax**

```
show ethernetdevice list
```

Description

Displays all Ethernet devices in short form.

show ethernetdevice port**Syntax**

```
show ethernetdevice port <Device Name or IP Address> all
show ethernetdevice port <Device Name or IP Address> portnumber
<Port Number>
```

Description

Finds an Ethernet device using device name or IP address and displays port information.

show ethernetdevice search device**Syntax**

```
show ethernetdevice search device <one or more parameters>
```

Parameters

```
[name <Device Name>]
[ipaddr <IP Address>]
[location <location>] [firmware <version number>]
```

Note: Search entries are not case sensitive.

Example

```
show ethernetdevice search device name slc firmware 4
```

Description

Displays all devices that match the criteria entered. For example, if you specify name slc, the vSLM 2 secure management software searches for all devices whose name starts with slc.

show ethernetdevice unreachablelist

Syntax

```
show ethernetdevice unreachablelist
```

Description

Displays unreachable Ethernet devices in short form.

```
show ethernetdevice unreachablelist index
```

Note: Type `show ethernetdevice unreachablelist` to display index.

Syntax

```
show ethernetdevice unreachablelist index <number>
```

Description

Displays unreachable ethernet devices by index.

IPv4 Filter Commands

```
set ipfilter delete
```

Syntax

```
set ipfilter delete <Name>
```

Example

```
set ipfilter delete MyFilter
```

Description

Deletes IPv4 filter set by specified name.

```
set ipfilter delete all
```

Syntax

```
set ipfilter delete all
```

Description

Deletes all references to filters.

```
set ipfilter delete interactive
```

Syntax

```
set ipfilter delete interactive
```

Description

Deletes IPv4 filters by interactive mode.

```
set ipfilter name delete
```

Note: Type `show ipfilter name <Name>` or `show ipfilter index <number>` to display the rule number.

Syntax

```
set ipfilter delete name <Name> [rule <rule number>]
```

Example

```
set ipfilter delete MyFilter rule 3
```

Description

Deletes IPv4 filter rule by specified name and rule number.

set ip filter state**Syntax**

```
set ipfilter state <enable|disable>
```

Description

Enables or disables IPv4 filters.

set ipfilter test**Syntax**

```
set ipfilter test <number of minutes>
```

Description

Enables or disables IPv4 filter test mode.

show ipfilter

Note: Type `show ipfilter` to display index.

Syntax

```
show ipfilter <parameters>
```

Parameters

```
[name <Filter Name>]
```

```
[index <number>]
```

Examples

```
show ipfilter
```

```
show ipfilter name MyFilter
```

```
show ipfilter index 2
```

Description

Displays IPv4 filter information.

show iptables**Syntax**

```
show iptables
```

Description

Displays all IP filtering rules for all chains.

Logging Commands

admin locallog**Syntax**

```
admin locallog clear auditlog
admin locallog clear syslog
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, RPM, SCS, LTRX, SLB, SPDR, WiBox, or other
```

Description

Clears all of the entries in the auditlog, syslog, or traplog.

Audit Log

show auditlog**Syntax**

```
show auditlog <parameters>
```

Parameters

```
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
```

Description

Lists audit log files.

show auditlog list**Syntax**

```
show auditlog list <parameters>
```

Parameters

```
lastminutes <minutes>
date <MMDD>
date <MMDD-MMDD>
```

Description

Lists auditlog files in short form.

show auditlog index

Syntax

```
show auditlog index <number> <parameters>
```

index is the number of lines of the log specified by lastminutes and date. If you specify 0 at number of lines, all lines display.

Parameters

```
[top <number of lines>]
[tail <number of lines>]
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
[loglastminutes <minutes>]
[logdate <MMDD>]
[logdate <MMDD-MMDD>]
```

If you specify both the date and time, the vSLM 2 secure management software ignores the date.

Description

Displays the specified part of the auditlog by index.

Examples

```
show auditlog
```

Lists auditlog files.

```
show auditlog lastminutes 5
```

Lists auditlog files modified in the last 5 minutes.

```
show auditlog date 0205
```

Lists auditlog files last modified on 0205.

```
show auditlog date 0205-0209
```

Lists auditlog files last modified between 0205 and 0209.

```
show auditlog index 3
```

Displays index 3 from the top.

```
show auditlog index 3 top 10
```

Displays the first 10 lines of index 3 from the top.

```
show auditlog index 3 tail 15
```

Displays the last 15 lines of index 3 from the tail.

```
show auditlog index 3 lastminutes 5
```

Displays the lines in index 3 from the last 5 minutes of.

```
show auditlog index 3 date 0205
```

Displays the audit log in index 3 for the date 0205.

```
show auditlog index 3 date 0205-0209
```

Displays the auditlog by the index 3 between the dates 0205 to 0209.

```
show auditlog index 3 top 10 lastminutes 5
```

Displays the first 10 lines of index 3 of the auditlog from the last 5 minutes.

```
show auditlog index 3 tail 0 lastminutes 5
```

Displays all lines of the auditlog in index 3 from the tail.

```
show auditlog index 3 lastminutes 5 logminutes 10
```

Displays the part of auditlog in index 3 times tamped in the last 10 minutes.

```
show auditlog index 3 date 0205
```

Displays the part of auditlog in index 3 time- stamped on 0205.

Event Log

```
show eventlog
```

Syntax

```
show eventlog
```

Description

Lists the event log files.

Port Log

```
show portlog
```

Syntax

```
show portlog
```

Lists all port log files.

```
show portlog <parameters>
```

Lists port log files as specified by parameters.

Parameters

```
[lastminutes <minutes>]
```

```
[date <MMDD>]
```

```
[date <MMDD-MMDD>]
```

Description

Lists portlog files.

Examples

```
show portlog lastminutes 5
```

Lists portlog files modified in last 5 minutes.

```
show portlog date 0205
```

Lists portlog files last modified on 0205.

```
show portlog date 0205-0209
```

Lists portlog files last modified between 0205 and 0209.

show portlog file

Note: Type `show portlog` to display index.

Syntax

```
show portlog file <index>
```

Shows the port log from the top.

```
show portlog file <index> tail
```

Displays the port log from the bottom (tail).

```
show portlog file <index> top
```

Displays the port log from the top.

Description

Displays the contents of the portlog file by index. Default is `top`.

show portlog index

Syntax

Note: Type `show portlog` to display index.

```
show portlog index <number>
```

Displays part of portlog by index from the top.

Index is the number specified by lastminutes and date.

```
show portlog index <number> <parameters>
```

Parameters

```
[top <number of lines>]
```

Displays the part of portlog by index from the top.

```
[tail <number of lines>]
```

Displays the part of the portlog by index from the end.

```
[lastminutes <minutes>]
```

```
[date <MMDD>]
```

```
[date <MMDD-MMDD>]
```

```
[loglastminutes <minutes>]
```

```
[logdate <MMDD>]
```

```
[logdate <MMDD-MMDD>]
```

Description

Displays the contents of the portlog file by index.

Note: Index is the number specified by parameters `lastminutes` and `date`. If you specify 0 as number of lines, all lines display. If you specify both date and time, the vSLM 2 secure management software ignores the date option.

Examples

```
show portlog index 3
```

Displays the specified portlog from top.

```
show portlog index 3 top 10
```

Displays the first 10 lines of specified portlog from top.

```
show portlog index 3 tail 15
```

Displays the last 15 lines of specified port log from tail.

```
show portlog index 3 lastminutes 5
```

Displays port log by the index '3'.

To get this index, type `show portlog lastminutes 5`.

```
show portlog index 3 date 0205
```

Displays port log by the index '3'.

To get this index, type `show portlog date 0205`.

```
show portlog index 3 date 0205-0209
```

Displays port log by the index '3'.

To get this index, type `show portlog date 0205-0209`.

```
show portlog index 3 top 10 lastminutes 5
```

Displays the first 10 lines of portlog by the index '3'.

To get this index, type `show portlog lastminutes 5`.

```
show portlog index 3 tail 0 lastminutes 5
```

Displays the portlog by the index '3' from tail.

To get this index, type `show portlog lastminutes 5`.

show portlog list

Syntax

```
show portlog list
show portlog list <parameters>
```

Parameters

```
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
```

Description

Lists portlog files in short form.

Session Log

show sessionlog

Syntax

```
show sessionlog
show sessionlog type <sessiontype> index <number>
sessiontype: <slcportactive|slcportsaved|scsport|device>
```

Parameters

```
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
```

Description

Lists session log files.

Note: Edge device log files do not use the date as part of the filename makeup.

Examples

```
show sessionlog
```

Lists device session log files.

```
show sessionlog type slcportsaved lastminutes 5
```

Lists archived SLC port session log files modified in last 5 minutes.

```
show sessionlog date 0205
```

Lists session log files last modified on 0205.

```
show sessionlog type scsport index 3
```

Displays the specified SCS05/20 port session log from the top.

```
show sessionlog type device index 3 top 10
```

Displays the first 10 lines of the specified device session log from the top.

```
show sessionlog type device index 3 tail 15
```

Displays the last 15 lines of specified device session log from the end.

```
show sessionlog type device index 3 lastminutes 5
```

Displays device session log by the index '3'.

To get this index, type `show portlog lastminutes 5`.

```
show sessionlog type slcportsaved index 3 date 0205
```

Displays archived SLC port sessionlog by the index '3'.

To get this index, type `show sessionlog type slcportsaved date 0205`.

```
show sessionlog type device index 3 date 0205-0209
```

Displays device session log by the index '3'.

To get this index, type `show sessionlog type device date 0205-0209`.

```
show sessionlog type device index 3 top 10 lastminutes 5
```

Displays the first 10 lines of device session log by the index '3'.

To get this index, type `show sessionlog type device lastminutes 5`.

System Log

show syslog

Syntax

```
show syslog <parameters>
```

Parameters

```
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
```

Description

Lists syslog files.

show syslog list

Syntax

```
show syslog list <parameters>
```

Parameters

```
lastminutes <minutes>
date <MMDD>
date <MMDD-MMDD>
```

Description

Lists syslog files in short form.

show syslog index

Syntax

```
show syslog index <number> <parameters>
```

`index` is the number of lines of the log specified by `lastminutes` and `date`. If you specify 0 at number of lines, all lines display.

Parameters

```
[top <number of lines>]
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
[loglastminutes <minutes>]
[logdate <MMDD>]
[logdate <MMDD-MMDD>]
```

If you specify both the date and time, the vSLM 2 secure management software ignores the date.

Description

Displays the specified part of the syslog by index.

Examples

```
show syslog
```

Lists syslog files.

```
show syslog lastminutes 5
```

Lists syslog files modified in the last 5 minutes.

```
show syslog date 0205
```

Lists syslog files last modified on 0205.

```
show syslog date 0205-0209
```

Lists syslog files last modified between 0205 and 0209.

Note: *If both date and time are specified, ignore the date option.*

```
show syslog index 3
```

Displays index 3 from the top.

```
show syslog index 3 top 10
```

Displays the first 10 lines of index 3 from the top.

```
show syslog index 3 tail 15
```

Displays the last 15 lines of index 3 from the tail.

```
show syslog index 3 lastminutes 5
```

Displays the lines in index 3 from the last 5 minutes of.

```
show syslog index 3 date 0205
```

Displays the audit log in index 3 for the date 0205.

```
show syslog index 3 date 0205-0209
```

Displays the syslog by the index 3 between the dates 0205 to 0209.

```
show syslog index 3 top 10 lastminutes 5
```

Displays the first 10 lines of index 3 of the syslog from the last 5 minutes.

```
show syslog index 3 tail 0 lastminutes 5
```

Displays all lines of the syslog in index 3 from the tail.

```
show syslog index 3 lastminutes 5 logminutes 10
```

Displays the part of syslog in index 3 time- stamped, in the last 10 minutes.

```
show syslog index 3 date 0205
```

Displays the part of syslog in index 3 time stamped, on 0205.

Trap Log

show traplog

Syntax

```
show traplog <parameters>
```

Parameters

```
[device <Device Name or IP Address>]  
[group <group name>]  
[lastminutes <minutes>]  
[date <MMDD>]  
[date <MMDD-MMDD>]
```

Description

Lists traplog files.

show traplog group

Note: Type `show traplog group` to display the index.

Syntax

```
show traplog group <Device Group Name> [index <number>]  
Group name: SLM, SLC, SLK, RPM, SCS, SLB, SPDR, WiBox, LTRX, or other
```

Description

Displays the current trap log information.

show traplog list

Syntax

```
show traplog list <parameters>
```

Parameters

```
[device <Device Name or IP Address>]  
[group <group name>]  
lastminutes <minutes>  
date <MMDD>  
date <MMDD-MMDD>
```

Description

Lists traplog files in short form.

show traplog index

Syntax

```
show traplog index <number> <parameters>
```

index is the number of lines of the log specified by lastminutes and date. If you specify 0 at number of lines, all lines display.

Parameters

```
[device <Device Name or IP Address>]
[group <group name>]
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
```

If you specify both the date and time, the vSLM 2 secure management software ignores the date.

Description

Displays the specified part of the traplog by index.

Examples

```
show traplog
```

Lists traplog files.

```
show traplog lastminutes 5
```

Lists traplog files modified in the last 5 minutes.

```
show traplog date 0205
```

Lists traplog files last modified on 0205.

```
show traplog date 0205-0209
```

Lists traplog files last modified between 0205 and 0209.

```
show traplog index 3
```

Displays index 3 from the top.

```
show traplog index 3 top 10
```

Displays the first 10 lines of index 3 from the top.

```
show traplog index 3 tail 15
```

Displays the last 15 lines of index 3 from the tail.

```
show traplog index 3 lastminutes 5
```

Displays the lines in index 3 from the last 5 minutes of.

```
show traplog index 3 date 0205
```

Displays the audit log in index 3 for the date 0205.

```
show traplog index 3 date 0205-0209
```

Displays the traplog by the index 3 between the dates 0205 to 0209.

```
show traplog index 3 top 10 lastminutes 5
```

Displays the first 10 lines of index 3 of the traplog from the last 5 minutes.

```
show traplog index 3 tail 0 lastminutes 5
```

Displays all lines of the traplog in index 3 from the tail.

```
show traplog index 3 lastminutes 5 logminutes 10
```

Displays the part of traplog in index 3 times tamped in the last 10 minutes.

```
show traplog index 3 date 0205
```

Displays the part of traplog in index 3 times stamped on 0205.

Maintenance Commands

admin config

Syntax

```
admin config factorydefaults
```

Description

Restores the vSLM configuration and device database settings to factory defaults.

admin config rebuilddatabase

Syntax

```
admin config rebuilddatabase
```

Description

Removes and rebuilds the vSLM configuration and database from scratch, in case of database corruption that cannot be fixed by the factory default option.

admin config showfiles

Syntax

```
admin config showfiles
```

Description

Shows saved configuration files.

admin config save file

Syntax

```
admin config save file <filename>
```

Description

Saves the vSLM configuration to the vSLM configuration files directory.

admin locallog clear

Syntax

```
admin locallog clear auditlog
admin locallog clear syslog
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, RPM, SCS, LTRX, SLB, SPDR, WiBox, UDS, or
other
```

Description

Clears all of the entries in the auditlog, syslog, or traplog.

admin quicksetup**Syntax**

```
admin quicksetup
```

Description

Runs the Quick Setup script to configure network settings, gateway, hostname, date & time, time zone, and sysadmin password.

admin reboot**Syntax**

```
admin reboot
```

Description

Terminates all connections and reboots the vSLM 2 secure management software.

admin securechannel regenkey**Syntax**

```
admin securechannel regenkey
```

Description

Regenerates the secure channel key.

Note: *With this command, you lose access to established secure channels; therefore, the vSLM 2 software first requests confirmation that you want to regenerate the securechannel key.*

admin shutdown**Syntax**

```
admin shutdown
```

Description

Terminates all connections, shuts down the vSLM 2 secure management software, and turns off the power.

admin version**Syntax**

```
admin version
```

Description

Displays current application version information.

show progress**Syntax**

```
show progress
```

Description

Shows the progress of background tasks.

show sysconfig**Syntax**

```
show sysconfig [email <Email Address>]
```

Description

Displays a report of configurable parameters. The output can be emailed.

show user**Syntax**

```
show user
```

Description

Displays information about the currently logged in user, including a list of groups retrieved from a remote authentication server and the actual group the user has inherited rights and attributes.

Managed Devices

Administrators, Ethernet Account Users and Menu Only Users

set manageddevice add**Syntax**

```
set manageddevice add <Device Name> group <Managed Device Group Name>  
<parameters>
```

Parameters

```
ethernetdevice <ethernetDevice|IP>  
[port <portName|portNumber>]
```

Description

Create a new managed device from the specified Ethernet device or port.

set manageddevice assign**Syntax**

```
set manageddevice assign <managedDeviceName> group <managedDeviceGroup>
[write|remove]
```

Description

Assigns or removes permissions for a managed device.

set manageddevice config**Syntax**

```
set manageddevice config <Device Name> <one or more parameters>
```

Parameters

```
name <New Name>
powerport <1|2> state <on|off|cyclepower>]
[dialout <Dial Account Name|enable|disable>
modem <Modem Name>
```

To set modem parameters, you must specify the dial-out option.

```
disconnect modem
delete
phonenumber <phone number>]
application <ssh|telnet|http|none>]
```

Examples

```
set ma config port-1 name waimea-port-1
```

Specifies a managed device name (port-1) and renames it to waimea-port-1.

```
set ma config slp-sunset-port1 state off
```

Specifies a managed device name (slp-sunset-port1) and turns the power off.

Description

Finds a managed device-by-device name and modifies device parameters.

set manageddevice defuse**Syntax**

```
set manageddevice defuse <Device Name> device|serial|power1|power2|kvm
```

Description

Defuses an Ethernet device or port from an existing managed device.

set manageddevice fuse**Syntax**

```
set manageddevice fuse <managedDeviceName> ethernetdevice
<EthernetDevice|IP> [port <Port Name|Port Number>]
```

Description

Fuses an Ethernet device or port to an existing managed device.

set manageddevice index

Note: Type `show manageddevice all` to display index.

Syntax

```
set manageddevice index <number> <one or more parameters> ethernetdevice
<EthernetDeviceName|IP> [port <Port Name|Port Number>]
```

```
set manageddevice index <number> defuse
[device|serial|kvm|power1|power2]
```

Parameters

```
assign group <managedDeviceGroup> [write|remove]
```

Assigns or removes permissions.

```
name <New Name>
```

```
powerport <1|2> state <on|off|cyclepower> (RPM/SLP power manager only)
```

```
delete
```

```
dialout <Dial Account Name|enable|disable>
```

```
modem <Modem Name>
```

To set modem parameters, you must specify the dial-out option.

```
disconnect modem
```

```
phonenumber <phone number>
```

```
application <ssh|telnet|http|none>
```

Examples

```
set ma config port-1 name waimea-port-1
set ma config slp-sunset-port1 powerport 1 state off
set ma index 1 delete
set ma index 1 dialout myaccount modem pci-s4 phone 3334444
```

If you set `dialout myaccount` first and then decide to set `modem` and `phonenumber` later, you still must specify `dialout myaccount` or `dialout enable`.

```
set ma index 1 dialout myaccount
set ma index 1 dialout enable modem pci-s4 phone 3334444
set ma index 1 disconnect modem
```

Description

Finds managed device by index and modifies device parameters.

set manageddevice index <number> fuse**Syntax**

```
set manageddevice index <number> fuse
```

Parameters

Type 'show manageddevice all' to get index.

```
set manageddevice index <number> fuse
    ethernetdevice <EthernetDeviceName|IP>
    [port <Port Name|Port Number>]
```

Description

Find managed device by index and fuse or defuse an Ethernet device or port:

set manageddevice index <number> defuse

Syntax

```
set manageddevice index <number> defuse device|serial|power1|power2|kvm
```

Description

Defuses an Ethernet device or port from an existing managed device.

set mgroup add

Syntax

```
set mgroup add <newManagedDeviceGroupName>
```

Description

Creates a new managed device group.

set mgroup delete

Syntax

```
set mgroup delete <existingManagedDeviceGroupName>
```

Description

Deletes an existing managed device group. The group must be empty.

show device

Syntax

```
show device <device name>
```

Note: Entries are not case sensitive.

Description

Searches for and displays Ethernet or managed devices by device name. For example, if you specify name `slc`, the vSLM 2 software searches for all Ethernet and managed devices whose name starts with `slc`.

show device all**Syntax**

```
show device all
show device
```

Description

Displays all Ethernet and managed devices.

show manageddevice account**Syntax**

```
show manageddevice account <accountName>
```

Description

Displays all managed devices viewable by a user account.

show manageddevice accountgroup**Syntax**

```
show manageddevice accountgroup <accountGroupName>
```

Description

Displays all managed devices viewable by an account group.

show manageddevice all**Syntax**

```
show manageddevice all
show manageddevice
```

Description

Displays information about all managed devices.

show manageddevice config**Syntax**

```
show manageddevice config <Device Name>
```

Description

Displays the configuration of a managed device.

show manageddevice index

Note: Type *show manageddevice all* to display index.

Syntax

```
show manageddevice index <number>
```

Description

Displays managed devices by index.

show manageddevice list

Syntax

```
show manageddevice list
```

Description

Displays all managed devices in short form.

show manageddevice search

Syntax

```
show manageddevice search <one or more parameters>
```

Parameters

Note: Search entries are not case sensitive.

```
[name <Port Name>]
```

Example

```
show manageddevice search name waimea-port
```

Description

Displays all ports that match the criteria entered.

Managed Device Users

set manageddevice config

Syntax

```
set manageddevice config <Device Name> <one or more parameters>
```

Parameters

```
[name <New Name>]
```

```
[state <on|off|cyclepower>] (available for RPM/SLP power manager only)
```

Powers managed device on or off.

Examples

```
set ma config port-1 name waimea-port-1
```

Specifies a managed device name (port-1) and renames it to waimea-port-1.

```
set ma config slp-sunset-port1 state off
```

Specifies a managed device name (slp-sunset-port1) and turns the power off.

Description

Finds a managed device-by-device name and modifies device parameters.

set manageddevice index

Note: Type `show manageddevice all` to display index.

Syntax

```
set manageddevice index <number> <one or more parameters>
```

Parameters

```
name <New Name>
powerport <1|2> state <on|off|cyclepower>] (RPM/SLP power manager only)
[delete]
[dialout <Dial Account Name|enable|disable>
modem <Modem Name>
phonenumber <phone number>]
application <ssh|telnet|http|none>]
```

Example

```
set ma index 1 delete
set ma index 1 dialout myaccount modem pci-s4 phone 3334444
set ma index 1 assign group MD-group write
```

Description

Finds managed device by index and modifies device parameters.

set manageddevice config**Syntax**

```
set manageddevice config <Device Name> disconnect modem
```

Description

Finds managed device by name and disconnects modem.

set manageddevice index

Note: Type `show manageddevice all` to display index.

Syntax

```
set manageddevice index <number> disconnect modem
```

Example

```
set ma index 2 disconnect modem
```

Description

Finds a managed device by index number and disconnects modem.

Menu Commands

Users can have custom user menus as their command line interface rather than the standard CLI command set. Each custom user menu can contain up to 50 commands (`logout` is always the last command). Instead of typing each command, the user enters the number associated with the command. Each command can also have an associated nickname that can be displayed in the menu instead of the command. You can use the `showmenu <Menu Name>` and `returnmenu` commands to display another menu from a menu or to return to the prior menu.

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 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 menu edit

Syntax

```
set menu edit <Menu Name> command <command number>
```

Changes a command within an existing custom user menu.

```
set menu edit <Menu Name> nickname <command number>
```

Changes a nickname within an existing custom user menu.

```
set menu edit <Menu Name> title <Menu Title>
```

Sets the optional title for a menu.

```
set menu edit <Menu Name> shownicknames <enable|disable>
```

Enables or disables display of command nicknames instead of commands.

```
set menu edit <Menu Name> redisplaymenu <enable|disable>
```

Enables or disables redisplay of menu before each prompt.

Description

Changes menu properties.

show menu

Syntax

```
show menu <Menu Name>
```

```
show menu name <Menu Name>
```

```
show menu
show menu all
```

Description

Shows a list of all menu names or all commands for a specific menu.

Note: To see assignments to account group, type `help show accountgroup`.

Modem Commands

reset modem connection

Note: You may only use this command when the modem is completely stuck. Wait for minimum timeout period (3 minutes) before you use this command when:

- ◆ You dial out via PPP and encounter no dial tone.
- ◆ You dial out via PPP and encounter a busy signal.

Syntax

```
reset modem connection
```

Description

Resets a modem connection.

set modem scan**Syntax**

```
set modem scan
```

Description

Scans a modem.

set modem disconnect

Note: Type `show modem` to view the current modem connections.

Syntax

```
set modem disconnect <Name>
```

Example

```
set modem disconnect MyPCIModem
```

Description

Terminates modem dial-out connection.

set modem edit**Syntax**

```
set modem edit <Modem Name> <parameters>
```

Parameters

```
name <New Name>
baud <300-115200>
flowcontrol <none|xon/xoff|rts/cts>
speaker <enable|disable>
initscript <Modem Initialization Script>
defaultinitscript <Modem Default Initialization Script>
dialin <Dial Account Name|CLEAR|disable|enable>
number <modem telephone number|CLEAR>
```

CLEAR removes the dial account assignment.

disable disables dial-in.

enable enables dial-in

```
ipfilter <IPv4 Filter Name|CLEAR>
```

ipfilter CLEAR removes the ipfilter assignment.

Description

Configures a currently loaded modem.

show modem**Syntax**

```
show modem
```

Description

Displays all current modem connections.

show modem connection**Syntax**

```
show modem connection <parameters>
```

Parameters

```
[index <number>]
```

Description

Displays active (established) modem connections.

show modem settings**Syntax**

```
show modem <parameters>
```

Parameters

```
[name <Modem Name>]
```

[index <number>]

Description

Displays modem settings.

show modem status

Syntax

show modem status

Description

Displays the status of the modem.

Network Commands

admin quicksetup

Syntax

admin quicksetup

Description

Runs the Quick Setup script to configure network settings, gateway, hostname, date & time, time zone, and sysadmin password.

set network bonding

Syntax

set network bonding <disabled|active-backup|802.3ad-2|802.3ad-34|adaptive-balancing>

Description

Configures Ethernet bonding.

set network dns

Syntax

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

Description

Configures up to three DNS servers.

set network gateway

Syntax

set network gateway <parameters>

Parameters

default <IP Address>

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

Description

Sets the default gateway.

set network host**Syntax**

```
set network host <Hostname>
```

Description

Sets the SLM hostname.

set network port**Syntax**

```
set network port <1|2> <parameters>
```

Parameters

```
state <dhcp|bootp|static|disable>  
[ipaddr <IP Address> mask <Mask>]  
mode <auto|10mbit-half|100mbit-half|10mbit-full|100mbit-full>  
[ipfilter <IPv4 Filter Name | CLEAR>]  
ip filter CLEAR removes the IP filter assignment.
```

Description

Configures Network Port 1 or 2.

show network all**Syntax**

```
show network all
```

Description

Displays all network settings.

show network bonding**Syntax**

```
show network bonding
```

Description

Displays network bonding information.

show network port**Syntax**

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

Description

Displays Network Port 1 and Network Port 2 connection information.

show network settings**Syntax**

```
show network settings
```

Description

Displays all network settings.

show routing**Syntax**

```
show routing
```

Description

Display the kernel IP routing tables.

Persistent Connection Commands

set persistent add**Syntax**

```
set persistent add <persistentConnectionName> ethernetdevice
<ethernetDeviceName|IP>
```

Parameters

```
[protocol <Secure|SSH|Telnet|TN3270>] (default SSH)
[logging <enable|disable>] (default disable)
[managed <enable|disable>] (default enable)
[active <enable|disable>] (default enable)
[parentlogin <enable|disable>] (default disable)
[login <loginAccount>]
[password <loginPassword>]
[prompt <promptString>]
[application <applicationName>]
[escapesequence <escapeString>] (default is '\x1BC')
[reconnectdelay <1-999>] (default is 1)
[eoltranslation <lf | cr>] (default is LF)
```

Description

Creates a new persistent connection

set persistent edit**Syntax**

```
set persistent edit <persistentConnectionName> <one or more parameters>
```

Parameters

```
[ethernetdevice <ethernetDeviceName|IP>]
[protocol <Secure|SSH|Telnet|TN3270>]
[logging <enable|disable>]
[managed <enable|disable>]
[active <enable|disable>]
[parentlogin <enable|disable>]
[login <loginAccount>]
[password <loginPassword>]
[prompt <promptString>]
[application <applicationName>]
[escapesequence <escapeString>]
[reconnectdelay <1-999>]
[eoltranslation <lf | cr>]
```

Note: For the edit and delete commands, the ethernetdevice parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name.

Description

Modifies an existing persistent connection.

set persistent delete**Syntax**

```
set persistent delete <persistentConnectionName> [ethernetdevice
<ethernetDeviceName|IP>]
```

Note: For the delete command, the ethernetdevice parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name.

Description

Deletes a persistent connection.

show persistent**Syntax**

```
show persistent [[name] <persistentConnectionName>][device
<devname|IP>][all]
```

Note: The device parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name. The <devname> following device may be the name of an Ethernet device or the name of a managed device. Persistent connections automatically belong to managed devices that have an Ethernet device component that has persistent connections defined.

Description

Displays one or more persistent connections

connect persistent

Syntax

```
connect persistent <persistentConnectionName> [device <devname|IP>]
```

Note: The device parameter is necessary only to discriminate between two or more persistent connections that are visible to the current user and are using the same name. The <devname> following device may be the name of an Ethernet device or the name of a managed device. Persistent connections automatically belong to managed devices that have an Ethernet device component that has persistent connections defined.

Description

Connect to an existing persistent connection.

Port Commands

set ethernetdevice port

Syntax

```
set ethernetdevice port <Device Name or IP Address> portnumber <port number or list> <one or more parameters>
```

Parameters

[name <New Port Name>]

[state <on|off|cyclepower>] (available for RPM/SLP power manager only)

Powers Ethernet device port on or off.

Note: Only RPM/SLP outlet action supports a port list.

Examples

To power up RPM/SLP outlet 2:

```
set eth port slp-sunset po 2 state on
```

To power up RPM/SLP outlet port list 1-3,6,8-14

```
set eth port slp-sunset po 1-3,6,8-14 state on
```

Description

Finds a port by device name or IP address with the port number and modifies port parameters.

show ethernetdevice port

Syntax

```
show ethernetdevice port <Device Name or IP Address> all
show ethernetdevice port <Device Name or IP Address> portnumber
<Port Number>
```

Description

Finds an Ethernet device using device name or IP address and displays port information.

show ethernetdevice search port

Syntax

```
show ethernetdevice search port <one or more parameters>
```

Parameters

Note: Search entries are not case sensitive.

```
[name <Port Name>]
[portnumber <Port Number>]
```

Examples

```
show ethernetdevice search port name waimea-port
show ethernetdevice search port name waimea portnumber 2
```

Description

Displays all ports that match the criteria entered.

show port

Note: Type `show port all` to display index.

Syntax

```
show port <Port Name>
```

Example

```
show port slc displays all Ethernet ports whose name starts with "slc."
```

Description

Searches Ethernet ports by port name and displays port information.

show port all

Syntax

```
show port all
show port
```

Description

Displays all Ethernet ports.

show port index

Syntax

```
show port index <number>
```

Description

Displays Ethernet ports by index.

Search Commands

show account search email

Syntax

```
show account search email <email address>
```

Example

```
show account search email sys
```

Displays all accounts whose email address starts with "sys."

Description

Displays accounts that match the email address entered.

show account search name

Syntax

```
show account search name <user name>
```

Examples

```
show account search name sys
```

Displays all accounts whose name starts with "sys."

Description

Displays accounts that match the name entered.

show ethernetdevice search device

Syntax

```
show ethernetdevice search device <one or more parameters>
```

Parameters

Note: Search entries are not case sensitive.

```
[name <Device Name>]
```

```
[ipaddr <IP Address>]  
[location <location>] [firmware <version number>]
```

Example

```
show ethernetdevice search device name slc firmware 4
```

Description

Displays all devices that match the criteria entered. For example, if you specify `name slc`, the vSLM 2 secure management software searches for all devices whose name starts with `slc`.

show manageddevice search**Syntax**

```
show manageddevice search <one or more parameters>
```

Parameters

Note: Search entries are not case sensitive.

```
[name <Port Name>]
```

Examples

```
show manageddevice search name "waimea-port"
```

Description

Displays all ports that match the criteria entered.

Services Commands

set service auditlog**Syntax**

```
set service auditlog <enable|disable>
```

Description

Enables or disables audit logging.

set service httpsonly**Syntax**

```
set service httpsonly <enable|disable>
```

Description

Enable or disables HTTPS only.

set service telnet**Syntax**

```
set service telnet <enable|disable>
```

Description

Enables or disables Telnet logging to the vSLM 2 secure management software.

set service sessionlog**Syntax**

```
set service sessionlog <enable|disable>
```

Description

Enables or disables session logging.

set service ssh**Syntax**

```
set service ssh <enable|disable> version <1|2>
```

Description

Enables or disables SSH logging to the vSLM 2 software.

set service wap**Syntax**

```
set service wap <enable|disable>
```

Description

Enables or disables WAP access to vSLM 2 secure management software.

show service**Syntax**

```
show service
```

Description

Displays service settings.

Session Commands

connect terminate**Syntax**

```
connect terminate <connect ID> <one or more parameters>
```

Parameters

outbound <outbound ID>

You must specify connection ID (inbound ID) to terminate an outbound connection.

Use `show connection` to view the current connections and their ID.

Examples

```
connect terminate 3
connect terminate 3 outbound 1
```

Description

Terminates a user connection to the SLM session. Use `show connection` to view the current connections and IDs.

show connection**Syntax**

```
show connection
```

Description

Displays active user IDs.

SSH Key Commands

set sshkey delete**Syntax**

```
set sshkey delete keyuser <SSH Key User> keyhost <SSH Key Host>
```

Description

Deletes an imported SSH key.

set sshkey import**Syntax**

```
set sshkey import <copypaste>
```

Note: RSA keys must be 1024 bits

Description

Imports an SSH 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 imported SSH keys.

Task Progress Command

show progress

Syntax

```
show progress
```

Description

Shows the progress of background tasks.

Appendix B: Security Considerations

The vSLM 2 secure management software provides data path security by means of SSH, Web/SSL, and in the case of SLC console managers, secure channel. Even with the use of these protocols, 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 vSLM 2 secure management software, for example:

- ◆ A terminal to the vSLM 2 software may be secure, but the path from the vSLM 2 secure management software to the end device may not be secure.
- ◆ With the right tools, a person having physical access to open the vSLM 2 software 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 vSLM 2 secure management software attempts to service all requests and does not filter out potential denial-of-service attacks.

Available Services and Port Numbers

The vSLM 2 software supports the services listed below. When installing and configuring an vSLM 2 secure management software in an environment where such services are limited, please make sure network equipment configurations allow access to and from the listed port numbers.

Table B-1 Administration

Protocol	Port#	Type
SSH	22	TCP
HTTP	80	TCP
HTTPS (SSL)	443	TCP
Telnet	23	TCP

Table B-2 Management

Protocol	Port#	Type
SMTP	25	TCP
BOOTP/DHCP	67/68	TCP
NTP	123	TCP
NIS	111	TCP/UDP
SNMP	161/162	UDP
LDAP	389	TCP
RADIUS	1645/1812	TCP/UDP

Table B-3 Device Access

Protocol	Port#	Type
FTP	20/21	TCP/UDP
SSH/SCP	22	TCP
TFTP	69	UDP
SNMP	161/162	UDP
LDP	30718	UDP

Appendix C: Protocol Glossary

This glossary provides brief definitions of commonly used protocols.

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.

FTP (File Transfer Protocol)

A standard network protocol used to transfer files from one host or to another host over a TCP-based network, such as the Internet.

HTTPS

A widely used communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.

Kerberos

A network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

LDAP (Lightweight Directory Access Protocol)

A protocol for accessing directory information.

NAT (Network Address Translation)

An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This enables a company to shield internal addresses from the public Internet.

NFS (Network File System)

A protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer. You can use NFS to mount all or a portion of a file system. Users can access the portion mounted with the same privileges as the user's access to each file.

NIS (Network Information System)

System developed by Sun Microsystems for distributing system data such as user and host names among computers on a network.

NMS (Network Management Station)

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.

Secure Channel

The name that Lantronix gave to encrypted password-less connections on the vSLM 2 secure management software. These connections use public key encryption for authentication over SSH.

SMB/CIFS

(Server Message Block/Common Internet File System): Microsoft's protocol for allowing all applications as well as Web browsers to share files across the Internet. CIFS runs on TCP/IP and uses the SMB protocol in Microsoft Windows for accessing files. With CIFS, users with different platforms and computers can share files without having to install new software.

SFTP (Secure File Transfer Protocol)

SFTP is a network protocol that provides file access, file transfer, and file management functionalities over a secure SSH data stream.

SNMP (Simple Network Management Protocol)

A protocol that 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.

WAP (Wireless Application Protocol)

WAP is a technical standard for accessing information over a mobile wireless network.