

LANTRONIX®



EMG™ Edge Management Gateway User Guide

EMG 8500

Part Number PMD-00008
Revision A October 2019

Intellectual Property

© 2019 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries. *EMG* and *SLC* are trademarks of Lantronix, Inc.

Patented: <http://www.lantronix.com/legal/patents/>; additional patents pending.

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

Warranty

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

Contacts

Lantronix Corporate Headquarters

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: <https://www.lantronix.com/support>

Sales Offices

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

Open Source Software

Some applications are Open Source software licensed under the Berkeley Software Distribution (BSD) license, the GNU General Public License (GPL) as published by the Free Software Foundation (FSF), or the Python Software Foundation (PSF) License Agreement for Python 2.7.3 (Python License). Lantronix grants you no right to receive source code to the Open Source software; however, in some cases, rights and access to source code for certain Open Source software may be available directly from Lantronix' licensors. Your use of each Open Source component or software is subject to the terms of the applicable license. The BSD license is available at <http://opensource.org/licenses>. The GNU General Public License is available at <http://www.gnu.org/licenses>. The Python License is available at <http://cmpt165.csil.sfu.ca/Python-Docs/license.html>. Your use of each Open Source component or software is subject to the terms of the applicable license.

OPEN SOURCE SOFTWARE IS DISTRIBUTED WITHOUT ANY WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE APPLICABLE LICENSE AGREEMENT FOR ADDITIONAL INFORMATION.

Disclaimer & Revisions

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

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

Note: *This equipment has been tested and found to comply with the limits for Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user guide, may cause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.*

User Information

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

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

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

Revision History

Date	Rev.	Comments
October 2019	A	Initial release for EMG 8500

Table of Contents

Intellectual Property	2
Warranty	2
Contacts	2
Open Source Software	2
Disclaimer & Revisions	3
Revision History	4
Table of Contents	5
List of Figures	15
List of Tables	19
1: About this Guide	20
Purpose and Audience	20
Summary of Chapters	20
Additional Documentation	21
2: Introduction	22
EMG 8500 Overview	22
Key Features	22
Console Management	22
Performance Monitoring	23
Security	23
Power	23
Integration with Lantronix ConsoleFlow™	23
Applications	23
Protocol Support	24
Configuration Methods	24
Product Information Label	25
Hardware Components	26
System Features	28
Access Control	28
Device Port Buffer	28
Console Port Interface	28
Device Port Interfaces	29
I/O Modules	30
Network Connections	31
Connectivity Modules	32
Front Panel LEDs	33
Digital IO Port	33

3: Installation	35
Package Contents	35
Order Information	36
User Supplied Items	36
Customize an EMG	36
Hardware Specifications	37
Physical Installation	38
Rack Mount Installation	39
Wall Mounting Instructions	40
Connecting to a Device Port	41
Modular Expansion for I/O Module Bays	43
Connecting to Network Ports	44
Modular Expansion for Connectivity Module Bays	44
Connecting Terminals	45
Power Input	46
I/O Module Installation	47
Connectivity Module Installation	48
4: Quick Setup	50
Recommendations	50
IP Address	50
Lantronix Provisioning Manager	51
Method #1 Quick Setup on the Web Page	51
Network Settings	53
Date & Time Settings	54
Administrator Settings	54
Method #2 Quick Setup on the Command Line Interface	55
Next Step	58
Limiting Sysadmin User Access	58
5: Web and Command Line Interfaces	59
Web Manager	59
Logging in	61
Logging Out	61
Web Page Help	61
Command Line Interface	62
Logging In	62
Logging Out	62
Command Syntax	62
Command Line Help	63
Tips	63
General CLI Commands	64

6: Networking	66
Requirements	66
Network Port Settings	67
Ethernet Interfaces (Eth1 and Eth2)	70
Hostname & Name Servers	72
DNS Servers	72
DHCP-Acquired DNS Servers	72
TCP Keepalive Parameters	73
Gateway	73
Fail-Over Settings	73
Fail-Over Cellular Gateway Configuration	74
Advanced Cellular Gateway Configuration	75
Fail-Over Cellular Gateway Firmware	75
Load Cellular Gateway Firmware Options	76
Ethernet Counters	76
Network Commands	76
Cellular Modem Settings	77
Cellular Interface	78
Cellular Modem Configuration	78
Cellular Modem Firmware	78
Cellular Modem Commands	78
IP Filter	79
Viewing IP Filters	79
Mapping Rulesets	79
Enabling IP Filters	80
Configuring IP Filters	81
Rule Parameters	82
Updating an IP Filter	82
Deleting an IP Filter	83
IP Filter Commands	83
Routing	83
Dynamic Routing	84
Static Routing	84
Routing Commands	84
VPN Settings	84
Sample ipsec.conf Files	95
VPN Commands	100
Security	101
Performance Monitoring	103
Performance Monitoring - Add/Edit Probe	106
Performance Monitoring - Results	109
Performance Monitoring Commands	112
FQDN List	113

7: Services 114

System Logging and Other Services	114
SSH/Telnet/Logging	114
System Logging	115
Audit Log	116
SMTP	116
SSH	116
Telnet	117
Web SSH/Web Telnet Settings	117
SSH Commands	118
Logging Commands	118
SNMP	118
v1/v2c Communities	121
Version 3	121
V3 User Read-Only	121
V3 User Read-Write	122
V3 User Trap	122
Services Commands	122
NFS and SMB/CIFS	122
SMB/CIFS Share	124
NFS and SMB/CIFS Commands	124
Secure Lantronix Network	125
Browser Issues	127
Troubleshooting Browser Issues	128
Web SSH/Telnet Copy and Paste	130
Secure Lantronix Network Commands	130
Date and Time	131
Date and Time Commands	132
Web Server	133
Admin Web Commands	135
Services - SSL Certificate	135
Services - Web Sessions	138
ConsoleFlow	138
ConsoleFlow Commands	142

8: USB/SD Card Port 143

Set up USB/SD Card Storage	143
Manage Files	146
USB Commands	147
SD Card Commands	147

9: Device Ports 148

Connection Methods	148
Permissions	148
I/O Modules	149
Device Status	150
Device Ports	150
Telnet/SSH/TCP in Port Numbers	152
Device Port Global Commands	152
Device Ports - Settings	152
Device Port Settings	155
IP Settings	157
Data Settings	158
Hardware Signal Triggers	159
Modem Settings (Device Ports)	160
Modem Settings: Text Mode	161
Modem Settings: PPP Mode	162
Port Status and Counters	163
Device Ports - Power Management	163
Device Port - Sensorsoft Device	166
Device Port Commands	168
Device Commands	168
Interacting with a Device Port	168
Device Ports - Logging and Events	169
Local Logging	169
NFS File Logging	169
USB and SD Card Logging	170
Token/Data Detection	170
Syslog Logging	170
Token & Data Detection	171
Local Logging	173
Log Viewing Attributes	173
NFS File Logging	173
USB / SD Card Logging	173
Syslog Logging	173
Logging Commands	174
Console Port	174
Console Port Commands	175
DIO Port	175
DIO Commands	176
Xmodem	176
Xmodem Commands	179
Host Lists	180
Host Parameters	180

Host List Commands	183
Sites	183
Site Commands	186
Modem Dialing States	186
Dial In	186
Dial-back	187
Dial-on-demand	188
Dial-in & Dial-on-demand	188
Dial-back & Dial-on-demand	189
CBCP Server and CBCP Client	189
CBCP Server	190
CBCP Client	190
Key Sequences	191
10: Remote Power Managers	192
Devices - RPMs	192
RPMs - Add Device	195
RPMs - Manage Device	198
RPMs - Outlets	202
RPM Shutdown Procedure	202
Optimizing and Troubleshooting RPM Behavior	204
RPM Commands	205
11: Scripts	206
Script Commands	211
Batch Script Syntax	211
Interface Script Syntax	212
Primary Commands	213
Secondary Commands	214
Control Flow Commands	216
Custom Script Syntax	218
Example Scripts	219
12: Connections	235
Typical Setup Scenarios for the EMG unit	235
Terminal Server	235
Remote Access Server	236
Reverse Terminal Server	236
Multiport Device Server	237
Console Server	237
Connection Configuration	238
Connection Commands	240

13: User Authentication 241

Authentication Commands	243
User Rights	243
Local and Remote User Settings	245
Adding, Editing or Deleting a User	246
Shortcut	250
Local Users Commands	250
Remote User Rights Commands	250
NIS	251
NIS Commands	253
LDAP	254
LDAP Commands	258
RADIUS	259
RADIUS Commands	262
User Attributes & Permissions from LDAP Schema or RADIUS VSA	262
Kerberos	263
Kerberos Commands	266
TACACS+	266
TACACS+ Groups	267
TACACS+ Commands	270
Groups	271
Group Commands	274
SSH Keys	274
Imported Keys	274
Exported Keys	274
Imported Keys (SSH In)	276
Host & Login for Import	276
Exported Keys (SSH Out)	276
Host and Login for Export	277
SSH Commands	279
Custom Menus	279
Custom User Menu Commands	282

14: Maintenance 283

Firmware & Configurations	283
HTTPS Push Configuration Restore	283
Internal Temperature	286
Site Information	286
EMG Firmware	286
Boot Banks and Bootloader Settings	287
Load Firmware Via Options	288
Configuration Management	288

Manage Files	290
Administrative Commands	290
System Logs	291
System Log Commands	292
Audit Log	293
Audit Log Commands	294
Email Log	294
Logging Commands	294
Diagnostics	295
Diagnostic Commands	298
Status/Reports	298
View Report	298
Status Commands	300
Emailing Logs and Reports	300
Events	303
Events Commands	305
Banners	305
Administrative Banner Commands	306

15: Application Examples 307

Telnet/SSH to a Remote Device	308
Dial-in (Text Mode) to a Remote Device	309
Local Serial Connection to Network Device via Telnet	311

16: Command Reference 313

Introduction to Commands	313
Command	313
Command Line Help	314
Tips	314
Administrative Commands	315
Audit Log Commands	327
Authentication Commands	327
Kerberos Commands	328
LDAP Commands	329
Local Users Commands	331
NIS Commands	335
RADIUS Commands	336
TACACS+ Commands	337
User Permissions Commands	338
Remote User Commands	339
Cellular Modem Commands	341
ConsoleFlow Commands	342
CLI Commands	344

Connection Commands	346
Console Port Commands	349
Custom User Menu Commands	350
Date and Time Commands	351
Device Commands	353
Device Port Commands	354
DIO Commands	358
Diagnostic Commands	359
Events Commands	363
Groups Commands	365
Host List Commands	366
Internal Modem Commands	367
IP Filter Commands	368
Logging Commands	369
Network Commands	372
NFS and SMB/CIFS Commands	376
Performance Monitoring Commands	377
Routing Commands	381
RPM Commands	382
Script Commands	384
SD Card Commands	387
Security Commands	388
Services Commands	388
Site Commands	389
SLC Network Commands	390
SSH Key Commands	391
Status Commands	394
System Log Commands	395
USB Access Commands	396
USB Device Commands	396
USB Storage Commands	397
USB Modem Commands	399
VPN Commands	400
Temperature Commands	403
Xmodem Commands	403
Appendix A: Security Considerations	405
Security Practice	405
Factors Affecting Security	405
Appendix B: Safety Information	406
Safety Precautions	406
Fuse Caution Statement	406

Cover	406
Power Plug	406
Input Supply	407
Grounding	407
Rack Mounting	407
Wall Mounting	407
Port Connections	408
Appendix C: Adapters and Pinouts	409
Appendix D: Protocol Glossary	412
Appendix E: Compliance Information	415
RoHS, REACH and WEEE Compliance Statement	416

List of Figures

Figure 2-1 EMG 8500 Edge Management Gateway	22
Figure 2-2 EMG 8500 Product Label	25
Figure 2-3 EMG 8500 Unit (front side)	26
Figure 2-4 EMG 8500 Unit (back side)	27
Figure 2-5 Console Port (Front Side)	29
Figure 2-7 I/O Modules	30
Figure 2-9 Dual Ethernet Network Connection	31
Figure 2-10 Dual SFP Connection. Inserting the SFP transceiver	32
Figure 2-11 LTE Cellular Modem Module	33
Figure 2-13 Digital I/O Port	34
Figure 3-4 Rack Mount Dimensions	40
Figure 3-5 Wall Mount Dimensions	41
Figure 3-8 Sample Device Port Connections (Front Side)	43
Figure 3-10 Sample Connectivity Module Configuration (Back Side)	45
Figure 3-11 Power Input	46
Figure 4-2 Quick Setup	52
Figure 4-3 Quick Setup Completed in Web Manager	54
Figure 4-4 Home	55
Figure 4-5 Beginning of Quick Setup Script	55
Figure 4-6 Quick Setup Completed in CLI	57
Figure 5-1 Web Page Layout	59
Figure 5-2 Sample Dashboard	60
Figure 6-1 Network > Network Settings (1 of 2)	68
Figure 6-2 Network > Network Settings (2 of 2)	69
Figure 6-3 Network Settings > SFP NIC Information & Diagnostics	70
Figure 6-4 Network > Cellular Modem Settings Page	77
Figure 6-5 Network > IP Filter	79
Figure 6-6 Network > IP Filter Ruleset (Adding/Editing Rulesets)	81
Figure 6-7 Network > Routing	83
Figure 6-8 Network > VPN (1 of 2)	86
Figure 6-9 Network > VPN (2 of 2)	87
Figure 6-10 Network > Security	102
Figure 6-11 Network > Perf Monitoring	104
Figure 6-12 Performance Monitoring - Add/Edit Probe	106
Figure 6-14 Performance Monitoring - Operations	112

Figure 6-15 FQDN List	113
Figure 7-1 Services > SSH/Telnet/Logging	115
Figure 7-2 Services > SNMP	119
Figure 7-3 Services > NFS & SMB/CIFS	123
Figure 7-4 Services > Secure Lantronix Network	125
Figure 7-5 IP Address Login Page	126
Figure 7-6 SSH or Telnet CLI Session	126
Figure 7-7 Disabled Port Number Popup Window	127
Figure 7-8 Services > Secure Lantronix Network - Search Options	128
Figure 7-9 Services > Date & Time	131
Figure 7-10 Services > Web Server	133
Figure 7-11 Web Server - SSL Certificate	136
Figure 7-12 Web Server - Web Sessions	138
Figure 7-13 Services > ConsoleFlow	140
Figure 8-1 Devices > USB / SD Card	144
Figure 8-2 Devices > USB > Configure	145
Figure 8-3 Devices > SD Card > Configure	145
Figure 8-4 Firmware and Configurations - Manage Files	147
Figure 9-2 Devices > Device Status	150
Figure 9-3 Devices > Device Ports	151
Figure 9-4 Device Ports > Settings (1 of 2)	154
Figure 9-5 Device Ports > Settings (2 of 2)	155
Figure 9-7 Device Ports - Power Management	165
Figure 9-8 Devices > Device Ports - Sensorsoft	167
Figure 9-9 Sensorsoft Status	168
Figure 9-10 Devices > Device Ports - Logging & Events	171
Figure 9-11 Devices > Console Port	174
Figure 9-12 Devices > Host Lists	180
Figure 9-13 Devices > View Host Lists	182
Figure 9-14 Devices > Sites	184
Figure 10-1 Devices > RPMs	192
Figure 10-2 RPM Shutdown Order	193
Figure 10-3 RPM Notifications	194
Figure 10-4 RPM Raw Data Log	194
Figure 10-5 RPM Logs	195
Figure 10-6 RPM Environmental Log	195
Figure 10-7 Devices > RPMs - Add Device	196
Figure 10-8 RPMs - Manage Device	199

Figure 10-9 RPMs - Outlets	202
Figure 11-1 Devices > Scripts	206
Figure 11-2 Adding or Editing New Scripts	207
Figure 11-3 Scripts > Custom Scripts - Scheduler	209
Figure 12-1 Terminal Server	235
Figure 12-2 Remote Access Server	236
Figure 12-3 Reverse Terminal Server	236
Figure 12-4 Multiport Device Server	237
Figure 12-5 Console Server	238
Figure 12-6 Devices > Connections	239
Figure 12-7 Current Connections	240
Figure 13-1 User Authentication > Auth Methods	242
Figure 13-3 User Authentication > Local/Remote Users	245
Figure 13-4 User Authentication > Local/Remote User Settings	247
Figure 13-5 User Authentication > NIS	251
Figure 13-6 User Authentication > LDAP	255
Figure 13-7 User Authentication > RADIUS	259
Figure 13-8 User Authentication > Kerberos	264
Figure 13-9 User Authentication > TACACS+	268
Figure 13-10 User Authentication > Groups	272
Figure 13-11 User Authentication > SSH Keys	275
Figure 13-12 Current Host Keys	278
Figure 13-13 User Authentication > Custom Menus	280
Figure 14-1 Maintenance > Firmware & Configurations	285
Figure 14-2 Network > Firmware/Config > Manage	290
Figure 14-3 Maintenance > System Logs	291
Figure 14-4 View System Logs	292
Figure 14-5 Maintenance > Audit Log	293
Figure 14-6 Maintenance > Email Log	294
Figure 14-7 Maintenance > Diagnostics	295
Figure 14-8 Diagnostics Output	297
Figure 14-9 Maintenance > Status/Reports	298
Figure 14-10 Generated Status/Reports	300
Figure 14-11 Emailed Log or Report	301
Figure 14-12 About EMG	302
Figure 14-13 Maintenance > Events	303
Figure 14-14 Maintenance > Banners	305
Figure 15-1 EMG - Configuration	307

Figure 15-2 Remote User Connected to a SUN Server via the Console Manager	308
Figure 15-3 Dial-in (Text Mode) to a Remote Device	309
Figure 15-4 Local Serial Connection to Network Device via Telnet	311
Figure C-1 RJ45 Receptacle to DB25M DCE Adapter for the EMG Unit (PN 200.2066A)	409
Figure C-2 RJ45 Receptacle to DB25F DCE Adapter for the EMG Unit (PN 200.2067A)	410
Figure C-3 RJ45 Receptacle to DB9M DCE Adapter for the EMG Unit (PN 200.2069A)	410
Figure C-4 RJ45 Receptacle to DB9F DCE Adapter for the EMG Unit (PN 200.2070A)	411
Figure C-5 RJ45 Receptacle to DB25M DTE Adapter (PN 200.2073)	411

List of Tables

Table 2-6 Console (DTE) Port Pinout	29
Table 2-8 Device (DCE Reversed & DTE) Port Pinout	30
Table 2-12 Front Panel LED Indicators	33
Table 3-1 EMG 8500 Parts	35
Table 3-2 EMG 8500 Device Modules	35
Table 3-3 EMG Technical Specifications	37
Table 3-6 Console Port and Device Port - Reverse Pinout Disabled	42
Table 3-7 Device Port - Reverse Pinout Enabled (Default)	42
Table 3-9 Available I/O Module Configurations	44
Table 4-1 Methods of Assigning an IP Address	50
Table 5-3 SCS Commands	64
Table 5-4 CLI Keyboard Shortcuts	65
Table 6-13 Error Conditions Detected by Probes	111
Table 9-1 Supported I/O Module Configurations	149
Table 9-6 Port Status and Counters	163
Table 11-4 Interface Script Syntax Definitions	212
Table 11-5 Primary Commands	213
Table 11-6 Secondary Commands	215
Table 11-7 Control Flow Commands	216
Table 13-2 User Types and Rights	244
Table 16-1 Actions and Category Options	313

1: About this Guide

Purpose and Audience

This guide provides the information needed to install, configure, and use the Lantronix EMG™ edge management gateway. The EMG gateway is for IT professionals who must remotely and securely configure and administer servers, routers, switches, telephone equipment, or other devices equipped with a serial port for facilities that are typically remote branch offices or “distributed” IT locations.

Note: *EMG edge management gateways are referred to as either EMG or as EMG 8500 when referring to the specific series. Edge management gateway or console manager may be used to describe the EMG devices.*

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
Chapter 2: Introduction	Describes the EMG models, their main features, and the protocols they support.
Chapter 3: Installation	Provides technical specifications; describes connection form factors and power supplies; provides instructions for installing the EMG in a rack.
Chapter 4: Quick Setup	Provides instructions for getting your EMG unit up and running and for configuring required settings.
Chapter 5: Web and Command Line Interfaces	Describes the web and command line interfaces available for configuring the EMG. The configuration chapters (6-15) provide detailed instructions for using the web interface and include equivalent command line interface commands.
Chapter 6: Networking	Provides instructions for configuring network ports, firewall and routing settings, and VPN.
Chapter 7: Services	Provides instructions for enabling and disabling system logging, SSH and Telnet logins, SNMP, SMTP, and the date and time.
Chapter 8: USB/SD Card Port	Provides instructions for using the USB and SD Card ports.
Chapter 9: Device Ports	Provides instructions for configuring global device port settings, individual device port settings, and console port settings.
Chapter 10: Remote Power Managers	Provides instructions for using RPMs.
Chapter 11: Scripts	Provides instructions for creating scripts to automate tasks performed on the EMG command line interface (CLI) or on device ports.
Chapter 12: Connections	Provides instructions for configuring connections and viewing, updating, or disconnecting a connection.
Chapter 13: User Authentication	Provides instructions for enabling or disabling methods that authenticate users who attempt to log in via the web, SSH, Telnet, or the console port. Provides instructions for creating custom menus.

Chapter (continued)	Description
<i>Chapter 14: Maintenance</i>	Provides instructions for upgrading firmware, viewing system logs and diagnostics, generating reports, and defining events. Includes information about web pages and commands used to shut down and reboot the EMG.
<i>Chapter 15: Application Examples</i>	Shows three different configurations to set up and use the EMG unit.
<i>Chapter 16: Command Reference</i>	Lists and describes all of the commands available on the EMG command line interface.
<i>Appendix A: Security Considerations</i>	Provides tips for enhancing EMG security.
<i>Appendix B: Safety Information</i>	Lists safety precautions for using the EMG.
<i>Appendix C: Adapters and Pinouts</i>	Includes adapter and pinout diagrams.
<i>Appendix D: Protocol Glossary</i>	Lists the protocols supported by the EMG unit with brief descriptions.
<i>Appendix E: Compliance Information</i>	Provides information about the EMG unit's compliance with industry standards.

Additional Documentation

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

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

2: *Introduction*

The EMG edge management gateway enables IT system administrators to manage remote servers and IT infrastructure equipment securely over the Internet.

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

EMG 8500 Overview

The EMG 8500 is a modular edge management gateway that offers serial RJ45 and USB console connectivity with user swappable I/O modules and connectivity modules. The EMG unit can accommodate up to two user swappable I/O modules (4 port serial RJ45 and/or 4 port serial USB).

For connectivity, the EMG provides dual Ethernet or dual small form-factor pluggable (SFP) network ports and up to two user replaceable modules for one LTE cellular modem, and in a future release for one Wi-Fi modem or dialup modem.

Figure 2-1 EMG 8500 Edge Management Gateway



Key Features

Console Management

- ◆ Enables system administrators to remotely manage devices with serial and/or USB console ports with RS-232C (now EIA-232) or USB compatible serial consoles in a 1U-tall rack space.
- ◆ Provides up to 8 serial RJ45 RS-232 or USB Type A console connections.
- ◆ Dual 10/100/1000 Base-T Ethernet or dual 1 Gb SFP network ports for in-band network device access

- ◆ Local terminal or internal cellular modem (LTE cellular) for out-of-band network device access
- ◆ Modular design allows user to add or swap I/O modules (RJ45, USB) and connectivity modules (LTE cellular)
- ◆ Data logging, device port buffering, network performance monitoring, system event logs and console event notification via email
- ◆ Integrated automatic fail-over/failback mechanism for seamless connection to IT equipment
- ◆ Sun Break Safe compatible
- ◆ Remote power manager (RPM) control of UPS and PDU devices
- ◆ Scripting to automate tasks performed on the CLI or on device ports

Performance Monitoring

- ◆ Performance Monitoring probes to analyze network performance

Security

- ◆ Enterprise-grade security and secure user access control with local or remote authentication

Power

- ◆ An external Universal AC (90W, 100-240V, 50/60 Hz) power supply provides power to the unit DC power port. The DC power port supports 9 to 30Vdc.
- ◆ Convection cooled, silent operation, low power consumption

Integration with Lantronix ConsoleFlow™

- ◆ Compatible with Lantronix ConsoleFlow™ management software for an end-to-end Out-of-Band (OOB) management solution.

Applications

The EMG edge management gateway is suitable for remote and secure management of the following types of IT equipment:

- ◆ **Servers:** Unix, Linux, Windows, and others.
- ◆ **Networking equipment:** Routers, switches, storage networking.
- ◆ **Telecom:** PBX, voice switches.
- ◆ **Other systems with serial interfaces:** Heating/cooling systems, security/building access systems, uninterruptible power supply (UPS), medical devices.

Protocol Support

The EMG supports the following protocols:

- ◆ TCP/IP network protocol
- ◆ SSH, TLS, SSL, Telnet and TCP for connections in and out of device ports
- ◆ DHCP and BOOTP for dynamic IP address assignment
- ◆ DNS for IP address name resolution
- ◆ SNMP for remote monitoring and management
- ◆ SCP, FTP, and SFTP for file transfers and firmware upgrades
- ◆ TFTP for firmware upgrades
- ◆ SMTP for mail transfer
- ◆ HTTPS (SSL) for secure browser-based configuration
- ◆ NTP for time synchronization
- ◆ UDP, PPP with PAP/CHAP, NFS and CIFS for data storage
- ◆ LDAP/AD, NIS, RADIUS with VSA support, CHAP, PAP, Kerberos, TACACS+, and SecurID (via RADIUS) for remote authentication
- ◆ Callback Control Protocol (CBCP) for PPP server callback
- ◆ StrongSwan IPsec for VPN access

For brief descriptions of these protocols, see [Appendix D: Protocol Glossary on page 412](#).

Configuration Methods

After installation, the EMG requires configuration. For the unit to operate correctly on a network, it must have a unique IP address on the network. This IP address references the specific unit.

For details on how to configure the unit with basic network settings, see [Chapter 4: Quick Setup](#).

The EMG provides the following methods for logging into the unit to configure EMG settings or monitor performance:

- ◆ **Web Manager:** View and configure all settings through a secure, encrypted web interface using most web browsers (Firefox, Chrome, or Internet Explorer with the latest browser updates). See [Chapter 5: Web and Command Line Interfaces](#).
- ◆ **Command Line Interface (CLI):** The command mode may be accessed through Telnet, SSH, Web Telnet/SSH or connecting a terminal (or a PC running a terminal emulation program) to the unit's console port. See [Chapter 5: Web and Command Line Interfaces](#).

Product Information Label

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

- ◆ Bar Code
- ◆ Product Part Number
- ◆ Product Revision
- ◆ Manufacturing Date Code
- ◆ Country of Manufacturing Origin
- ◆ Hardware Address (MAC address or serial number)
- ◆ Device ID (used to connect to ConsoleFlow central management software)

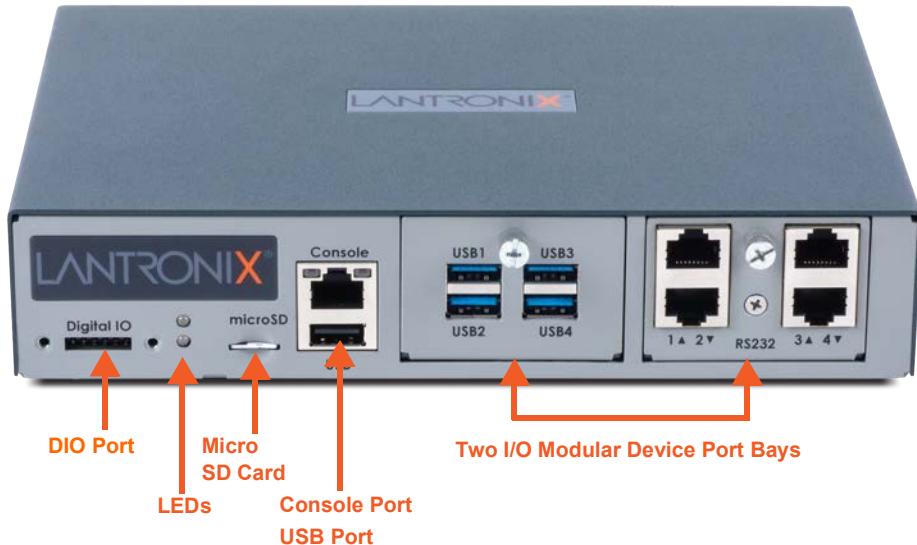
Figure 2-2 EMG 8500 Product Label



Hardware Components

- ◆ **EMG Chassis:** The EMG has a 1U-tall (1.75 inch), 212.6mm [8.37"] L x 167.68mm [6.60"] W x 43.21mm [1.70"] H chassis. Options for rack mounting and wall mounting are available.
- ◆ **Front Chassis:** [Figure 2-3](#) shows the front view of the EMG:

Figure 2-3 EMG 8500 Unit (front side)



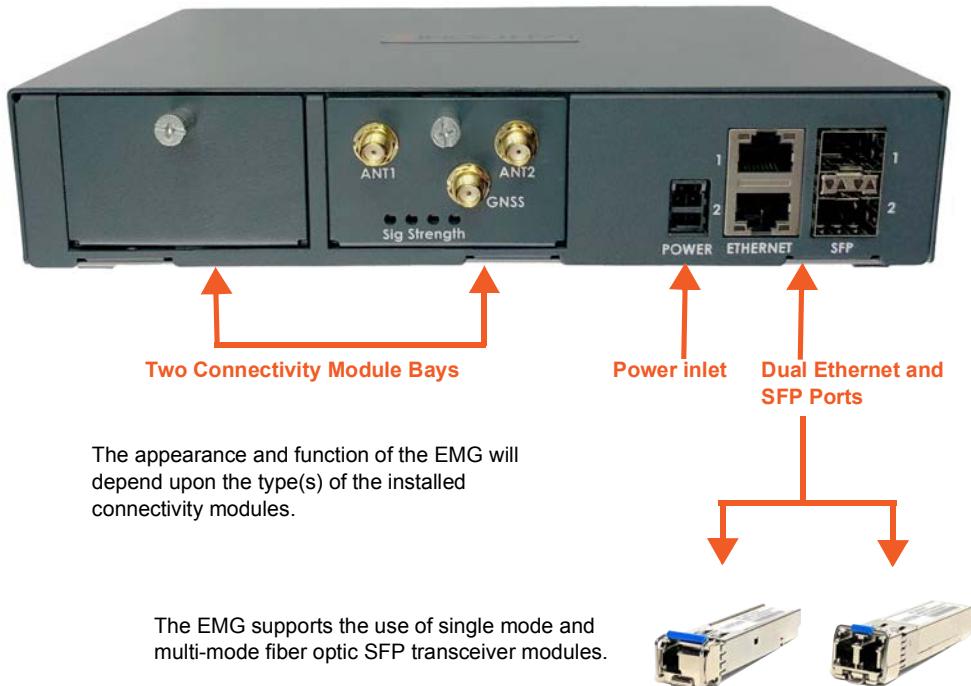
The front of the EMG unit appearance and function will depend upon the type(s) of I/O modules installed in Bay 1 and Bay 2.

- **Two I/O Module Bays** are available to accommodate a total of 8 device ports depending on the number of I/O modules installed. Configuration possibilities are listed below. See [Table 3-9 on page 44](#) which describes different I/O module configurations.
 - ◆ **Up to two 4 port RJ45 I/O modules** can be installed to provide a maximum of 8 serial RS-232C (EIA-232) device ports. The serial RJ45 ports match the RJ45 pinouts of the console ports of many popular devices found in a network environment, and where different can be converted using Lantronix adapters. The RJ45 ports have software reversible pinouts to switch between digital terminal equipment (DTE) and digital communications equipment (DCE) applications. See [Appendix C: Adapters and Pinouts on page 409](#) for more information on serial adapters and pin-outs.
 - ◆ **Up to two 4 port USB I/O modules** can be installed to provide a maximum of 8 USB type A device ports.
 - ◆ **A combination of 4 port USB I/O modules and 4 port RJ45 I/O modules** can be installed to provide up to 8 serial device ports.
- **One serial console port** (RJ45, RS-232) for VT100 terminal or PC with emulation with light emitting diode (LED) for activity indicators
- **One 2.0 USB type A port** (HS, FS, LS) for use with flash drive or external USB modem (V.92 dialup)

One Micro Secure Digital (micro SD) memory card slot for use with micro SD card to collect logs, save configurations, and update firmware. (Micro SD card provided by the user)

- **One digital IO (DIO) port** with two digital inputs and one relay output (terminal block) for use with sensors
- **LED indicators** for ethernet port status and connectivity module status
- ◆ **Back Chassis:** *Figure 2-4* shows the back view of the EMG 8500:

Figure 2-4 EMG 8500 Unit (back side)



- **Two Connectivity Module Bays** accommodate up to two connectivity modules. Configuration possibilities are listed below. See *Figure 3-10 on page 45* for a sample connectivity module configuration.
 - ◆ One LTE cellular modem module can be installed to provide cellular connectivity.
- **Network Interface: Dual 10/100/1000 Base-T Ethernet port I/F card.** Ethernet ports are referred to as Eth1 and Eth2 in the user interface and this user guide.
- **Network Interface: Dual 1 Gigabit-capable SFP port I/F card** to support single or multi-mode fiber optic SFP transceiver modules. SFP transceiver modules are referred to as SFP1 and SFP2 in the user interface and this user guide.

Note: EMG will recognize two network connections. Either Eth1 or SFP1 is active, but not both. Similarly, either Eth2 or SFP2 is active, but not both.

- ◆ *Lantronix offers SFP Transceivers (“modules”) for EMG 8500 edge management gateways and SLC 8000 console managers with fiber SFP ports. To learn more, go to <https://www.lantronix.com/products/sfp/>*
- ◆ *SFP transceiver modules are provided by users according to fiber mode and brand preferences.*

- ◆ Network ports and the SFP port have LEDs to indicate link and activity status. If a single mode and a multi-mode are both installed on the EMG unit, the device can be configured to utilize one mode at a time.
- **Power supply inlet:** The unit accepts a 9 to 30 Vdc power input via a back-panel connector. A universal AC power input (100-240V, 50/60 Hz) to 12 Vdc power supply brick is available for use with the unit.

System Features

This section describes system features, interfaces, and ports of the EMG.

Access Control

The system administrator controls access to attached servers or devices by assigning access rights to up to 128 user profiles. Each user has an assigned ID, password, and access rights. Other user profile access options may include externally configured authentication methods such as Radius, TACACS+, NIS, and LDAP. Groups are supported in LDAP, RADIUS (using VSA), and TACACS+ (using priv_lvl).

Device Port Buffer

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

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

Console Port Interface

The EMG unit supports local access through a dedicated front panel serial console port (see [Figure 2-3](#)). The console port supports the RS-232C (EIA-232) standard. RJ45 cabling (e.g., category 5 or 6 patch cabling) is used.

[Figure 2-5](#) and [Table 2-6](#) show the Console port and port pinout.

The console port supports the following baud rate options: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, and 921600 baud.

Figure 2-5 Console Port (Front Side)

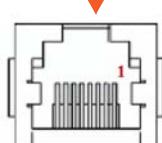


Table 2-6 Console (DTE) Port Pinout

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

Device Port Interfaces

RS-232 RJ45 Interface

The device ports are located on the front of the EMG unit in the I/O module device port bays (see [Figure 2-3](#)).

All devices attached to the RJ45 device ports must support the RS-232C (EIA-232) standard. For serial RJ45 device ports, RJ45 cabling (e.g., category 5 or 6 patch cabling) is used.

Serial RJ45 device ports for the EMG are reversed by default so that straight-through RJ45 patch cables may be used to connect to Cisco and Sun RJ45 serial console ports. See [Figure 2-7](#) and [Table 2-8](#). The RJ45 ports have software reversible pinouts to switch between DTE and DCE applications.

Note: *RJ45 to DB9/DB25 adapters are available from Lantronix. For serial pinout information, see the [Appendix C: Adapters and Pinouts on page 409](#).*

Additional device port features:

- ◆ RAW TCP, Telnet or SSH to a serial port by IP address per port or by IP address and TCP port number
- ◆ Simultaneous access on the same port - “listen” and “direct” connect mode
- ◆ Device ports support the following baud rate options: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, and 921600 baud.

USB Interface

The USB device ports are located on the front of the EMG unit in the I/O module device port bays (see [Figure 2-3](#)). USB device ports can be used with a USB type A connector to serial adapter, if needed.

I/O Modules

EMG provides two I/O slots for user replaceable I/O modules to be installed on the front side of the EMG 8500 unit.

[Figure 2-7](#) shows a sample configuration of an EMG 8500 unit containing one 4 port USB I/O module in Bay 1 and one 4 port RJ45 I/O module in Bay 2 for a total of 8 device ports.

Note: When installing the I/O modules, they can be populated or swapped in any order. One but not both of the slots can be empty. The I/O modules must only be installed on the front of the unit, never in the connectivity slots on the back.

Figure 2-7 I/O Modules

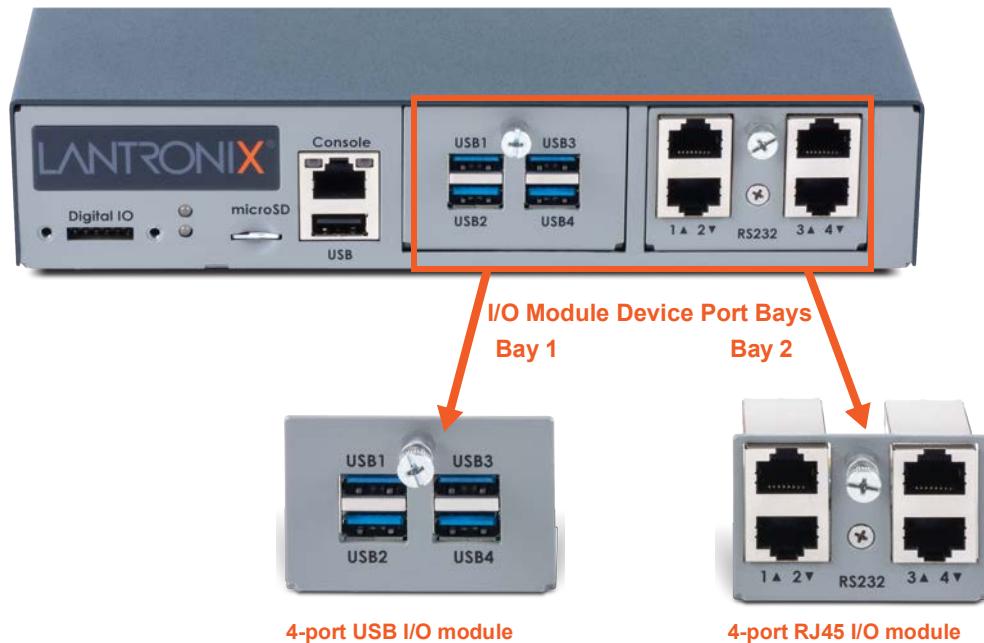


Table 2-8 Device (DCE Reversed & DTE) Port Pinout

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

Network Connections

Dual Ethernet Port and Dual SFP Port

The back side of the EMG unit is equipped with two Ethernet and two SFP ports. The EMG network interfaces are 10/100/1000 Base-T Ethernet for use with a conventional Ethernet network as shown in [Figure 2-9](#). Use standard RJ45-terminated cables, such as a Category 5 or 6 patch cable. CAT5E or better cables are recommended for 1000 Base Ethernet. Network parameters must be configured before the EMG can be accessed over the network.

The SFP interfaces support the use of single and multi-mode SFP transceivers. Fiber optic 1 Gigabit SFP transceiver modules may be used. See [Figure 2-10](#).

Note: EMG will recognize two network connections. Either Eth1 or SFP1 is active, but not both. Either Eth2 or SFP2 is active, but not both.

One possible use for the two Ethernet ports is to have one port on a private, secure network and the other on a public, unsecured network. The EMG can also be equipped with a factory-installed network interface card (NIC) (Ethernet RJ45 or SFP ports). The NIC with SFP ports can support single/multi-mode fiber optic SFP transceiver modules at 1 Gigabit speed.

Ethernet and SFP LEDs

The Ethernet ports and the SFP ports contain LEDs. The LED indicators are the following:

- ◆ Green LED - indicates link status
- ◆ Yellow LED - indicates activity status

Figure 2-9 Dual Ethernet Network Connection



Figure 2-10 Dual SFP Connection. Inserting the SFP transceiver



Connectivity Modules

EMG provides two connectivity slots for user replaceable connectivity modules on the back of the unit.

Note: When installing the connectivity modules, they can be populated or swapped in any order. One or both of the slots can be empty. The connectivity modules must only be installed on the back of the unit, never in the I/O slots on the front.

LTE Cellular Modem

One LTE/4G cellular modem may be installed in either connectivity slot. The LTE cellular modem may be configured to function as the failover interface with Eth1 as the primary link.

The LTE cellular modem module supports one main antenna, one AUX antenna, and one GPS antenna for geolocation. (The geolocation function is not active in the current release).

The LTE cellular modem module supports one external SIM card, provided by the user. The SIM card slot is located on the inside of the cellular modem module, as shown in [Figure 2-11](#). To install the SIM card, power off the EMG unit, unscrew the module faceplate and remove it from the EMG unit. Insert the SIM card into the slot and replace the cellular modem module in the EMG unit.

Figure 2-11 LTE Cellular Modem Module



Front Panel LEDs

The front panel LEDs provide quick visual troubleshooting. [Table 2-12](#) describes the front panel LED indicators.

Table 2-12 Front Panel LED Indicators

Indicator	LED 1 (Ethernet port)	LED 2 (Connectivity)
Solid Green	At least one of the Ethernet ports has a link, or both Ethernet ports are disabled.	Indicates one of the following conditions: <ul style="list-style-type: none"> ◆ There are no connectivity modules installed ◆ An LTE modem module is installed and is disabled ◆ An LTE modem module is installed and has a link
Solid Orange	Not applicable	An LTE modem module is installed but no SIM card is present
Blinking Red	None of the Ethernet ports has a link.	An LTE modem module is installed but does not have a link.

Digital IO Port

The terminal block digital input relay output is located on the front panel of the EMG unit. It provides two digital inputs and one relay output (terminal block) for use with sensors. The DIO port requires an adapter, which is available and sold separately. [Figure 2-13](#) shows the DIO adapter installed on the EMG 8500 with the DIO port pin order and pin definition.

Figure 2-13 Digital I/O Port



Pin Number	Pin Definition
1	Relay Out
2	Relay In
3	Input1+
4	Input1-
5	Input2+
6	Input2-

The DIO connector description is provided below.

Connector	Description
Relay Output	Output supports 1A 24V
Inputs	Inputs accept voltage 0 to 30 VDC. ON: Max 30 VDC Min 2 VDC OFF: Max 0.7 VDC Min 0 VDC

3: *Installation*

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

Caution: *To avoid physical and electrical hazards, please read [Appendix A: Security Considerations before installing the EMG.](#)*

Package Contents

The EMG 8500 package includes the following items. Verify and inspect the contents of the EMG package using the enclosed packing slip. If any item is missing or damaged, contact your place of purchase immediately.

Table 3-1 EMG 8500 Parts

Name
One EMG8500 EDGE MANAGEMENT GATEWAY
RJ45 to DB9F Adapter
RJ45 to RJ45 Cat5 Cable, 6.6 ft (2m) straight-through RJ45 patch
RJ45 Loopback Adapter
External Universal AC (90W, 100-240V, 50/60 Hz) power supply
North American Power cord - 110V AC power cord, 8 ft (2.43m), RoHS
<i>Note: Power cords for international regions are available and sold separately.</i>
<i>EMG Quick Start Guide</i>

The following user replaceable device modules are available and sold separately.

Table 3-2 EMG 8500 Device Modules

Name
User Replaceable Device Modules
I/O Modules
EMG 8500 FRU, RS232 SERIAL 4-PORT (UART)
EMG 8500 FRU, USB 4-PORT
Connectivity Modules
EMG 8500 FRU, LTE, US
EMG 8500 FRU, LTE, APAC

Additional parts and accessories are available and sold separately. For details and purchasing information, refer to the next section [Order Information](#).

- ◆ External DIO adapter
- ◆ Wall mount kit
- ◆ Rail mount kit

Order Information

To view order information, part numbers and extended support options, go to <https://www.lantronix.com/products/lantronix-emg/#tab-order-now>.

User Supplied Items

To complete your installation you will need the following items:

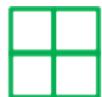
- ◆ Medium size Phillips screwdriver to install the mounting brackets to the EMG unit, if applicable
- ◆ One or more serial devices that require network connectivity
- ◆ A serial cable for each serial device.
 - For RJ45 ports, you may use a straight-through RJ45 patch cable to connect to Cisco and Sun RJ45 serial console ports.
 - For USB ports, use a cable with a USB Type A connector
 - For information about Lantronix adapters, see [Appendix C: Adapters and Pinouts](#).
- ◆ An available connection to your Ethernet network and an Ethernet cable CAT5E or better cables are recommended for 1000 Base Ethernet.
- ◆ A working AC power outlet to power the unit using the included AC (90W, 100-240V, 50/60 Hz) power supply.
- ◆ If the LTE cellular modem is installed, a network SIM card (and data services) from a service provider

Customize an EMG

Build any combination up to 8 managed console ports and up to two connectivity modules by following these steps:

1. Pick a baseline configuration:

- ◆ I/O: 4 port RS-232 or 4 port USB or two 4 port RS-232 modules



4 Port RS-232



or
4 Port USB



or
8 Ports RS-232



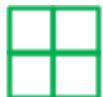
- ◆ Connectivity module: Zero or one LTE module



LTE/4G

2. Add up to one I/O module and up to two connectivity modules:

- ◆ I/O: 4 port RS-232 or 4 port USB



4 Port RS-232



or
4 Port USB

- ◆ Connectivity module: LTE or Wi-Fi module (coming soon)



3. Protect the investment with various extended warranty and service options. Go to <https://www.lantronix.com/products/lantronix-emg/#tab-order-now> to purchase extended support.

Hardware Specifications

Table 3-3 EMG Technical Specifications

Component	Description
Serial Interface (Device)	<ul style="list-style-type: none"> ◆ Up to 8 RJ45-type 8-conductor connectors as up to two 4 port RJ45 I/O modules can be installed. These connectors have individually configurable standard and reversible pinouts, 4 ports per I/O module. ◆ Speed software selectable (300 to 921600 baud) <p>Note: Serial RJ45 device ports for the EMG are reversed by default.</p>
USB 2.0 Interface (Device)	<ul style="list-style-type: none"> ◆ Up to 8 USB type A (Host) as up to two 4 port USB I/O modules can be installed. ◆ HS, FS, and LS ◆ Capable of providing VBUS 5V up to 100 mA per port, but not to exceed 400 mA total per 4 port USB I/O module. ◆ May be used with a USB-to-serial adapter to connect a serial device, if needed. Please contact Lantronix for the list of tested adapters. <p>Caution: <i>USB ports are designed for data traffic only. They are not designed for charging or powering devices. Over-current conditions on VBUS 5V may disrupt operations.</i></p>
Serial Interface (Console)	<ul style="list-style-type: none"> ◆ (1) RJ45-type 8-pin connector (DTE) ◆ Speed software selectable (300 to 921600 baud) ◆ LEDs: <ul style="list-style-type: none"> ➢ Green light ON indicates data transmission activity ➢ Yellow light ON indicates data receiving activity
Network Interface	<ul style="list-style-type: none"> ◆ (2) 10/100/1000 Base-T RJ45 Ethernet with LED indicators: <ul style="list-style-type: none"> ➢ Green light ON indicates a link at 1000 Base-T. ➢ Green light OFF indicates a link at other speeds or no link. ➢ Yellow light ON indicates a link is established. ➢ Yellow light blinking indicates activity. AND ◆ (2) SFP ports to support standard fiber SFP transceiver modules (single or multi-mode) at speed 1 Gigabit. with LED indicators: <ul style="list-style-type: none"> ➢ Green light ON indicates a link is established. ➢ Green light OFF indicates no link. ➢ Yellow light steady ON indicates no activity. ➢ Yellow light blinking indicates activity. <p>Note: Either Eth1 and Eth2 ports are active or SFP1 and SFP2 ports are active, but not both Eth and SFP.</p>

Component (continued)	Description
Connectivity Modules	<ul style="list-style-type: none"> ◆ (2) connectivity slots to support 2 connectivity modules. <ul style="list-style-type: none"> ➢ One LTE/4G cellular modem ➢ One Wi-Fi module (coming soon)
Power	<ul style="list-style-type: none"> ◆ Input: DC jack, 9-30 VDC (standard) ◆ External AC (90W, 100-240V, 50/60 Hz) power supply shipped with unit ◆
Dimensions (L x W x H)	212.6mm [8.37"] x 167.68mm [6.60"] x 43.21mm [1.70"], 1U
Weight	1.406 kg (3.10 lbs)
Temperature	<ul style="list-style-type: none"> ◆ Operating: 0 to 50°C (32 to 122°F) ◆ Storage: -20 to 80°C (-4 to 176°F) ◆ Heat flow rate: TBD BTU per hour
Relative Humidity	<ul style="list-style-type: none"> ◆ Operating: 10% to 90% non-condensing ◆ Storage: 10% to 90% non-condensing
Front USB Port	<ul style="list-style-type: none"> ◆ (1) port, type A, host USB 2.0 (HS, FS, LS)
Front Memory Card	(1) Secure Digital (micro SD) memory card slot supporting: <ul style="list-style-type: none"> ◆ SD ◆ SDHC
Internal Memory	Optional: 128 GB Flash internal storage
Front DIO Port	(1) Digital IO slot with two digital inputs and one relay output (terminal block)
LED Indicators	<ul style="list-style-type: none"> ◆ Ethernet port (upper LED on front panel) ◆ Connectivity (lower LED on front panel) ◆ RJ45 Ethernet (Activity/Link) ◆ SFP (Activity/Link) ◆ LTE Signal Strength
Operating Atmosphere	 For use at altitudes no more than 2000 meters above sea level only.  For use in non-tropical conditions only.
Caution: EQUIPMENT IS FOR INDOOR USE ONLY!	

Physical Installation

Install the EMG as a free-standing desktop unit, mounted on a wall, or mounted in an EIA-standard 19-inch rack (1U tall).

The EMG module uses convection cooling to dissipate excess heat.

To install the EMG unit:

1. If you have purchased additional I/O or Connectivity modules, install these modules.
 - ◆ For I/O modules, see [I/O Module Installation \(on page 47\)](#).
 - ◆ For Connectivity modules, see [Connectivity Module Installation \(on page 48\)](#).

Note: Always remove the power cord from the unit prior to installing or removing the I/O or Connectivity modules.

2. Prepare the EMG unit for installation:
 - ◆ If free-standing, attach the adhesive-backed rubber feet to the base of the EMG unit.
 - ◆ If rack-mounted or wall-mounted, attach the brackets on the sides of the EMG unit using a screw driver and the screws provided with the mounting kit.
3. Mount the EMG unit.
 - ◆ If free-standing, place the unit securely on a desktop or other flat horizontal surface.
 - ◆ If rack-mounted, mount the unit securely in a 19-inch rack. See [Rack Mount Installation \(on page 39\)](#).
 - ◆ If wall-mounted, mount the unit securely on a flat vertical surface. See [Wall Mounting Instructions \(on page 40\)](#).

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

4. Connect the serial device(s) to the EMG unit's device ports. See [Connecting to a Device Port \(on page 41\)](#).
5. Choose one of the following options:
 - ◆ To configure the EMG using the network, or to monitor serial devices on the network, connect at least one EMG network port to a network. See [Connecting to Network Ports \(on page 44\)](#).
 - ◆ To configure the EMG unit using a dumb terminal or a computer with terminal emulation, connect the terminal or PC to the front panel EMG console port. See [Connecting Terminals \(on page 45\)](#).
6. Connect the power cord to power on the unit. See [Power Input \(on page 46\)](#).
7. Wait approximately one minute for the boot process to complete.

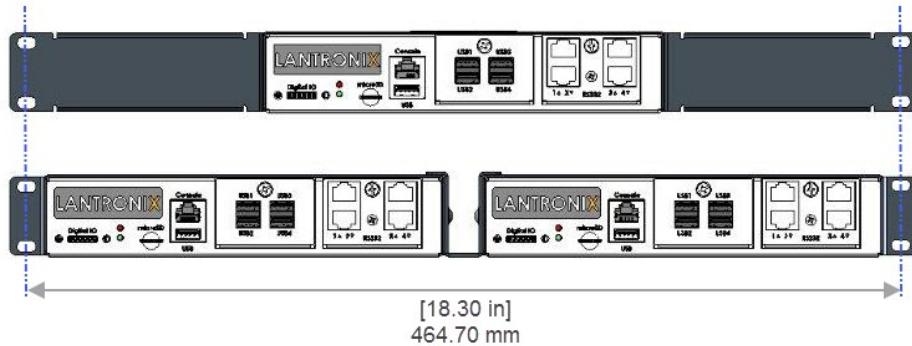
The first time the EMG boots, it attempts to get an IP address from DHCP. To configure the network settings, see [Chapter 4: Quick Setup](#).

Rack Mount Installation

Attach the brackets on the sides of the EMG unit using a screwdriver and the screws provided with the mounting kit.

Mount the unit securely in a 19-inch rack.

Figure 3-4 Rack Mount Dimensions



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

Wall Mounting Instructions

For installations to Walls Requiring Anchors

These instructions are for mounting the EMG to walls made of solid concrete, block, brick, or plasterboard.

(1) Wall mount:

1. Locate the place where you want to mount the unit and mark four holes using your EMG mount as a guide for the screws. See [Figure 3-5](#) for the location of the screw holes.
2. Drill four 3/16 inch (4.8 mm) diameter holes at a depth of 1.25 inches (32 mm).
3. Insert the anchors until they are flush with the surface.
4. Thread four pan head top mount screws through the unit mount hole and through the anchor, and tighten them.

(2) Keyhole mount:

1. Locate the place where you want to mount the unit and mark two holes using your EMG mount as a guide for the screws. See [Figure 3-5](#) for the location of the screw holes.
2. Drill two 3/16 inch (4.8 mm) diameter holes at a depth of 1.25 inches (32 mm).
3. Insert the anchors until they are flush with the surface.
4. Thread two pan head top mount screws through the unit mount hole and through the anchor, and reserve 0.08" to 0.12" (2-3 mm) clearance to the anchor surface.
5. Hang the EMG unit where both keyholes of wall mounts can go through the screw heads on the wall.

For installations to Walls Not Requiring Anchors

These instructions are for mounting the EMG to walls made of solid wood at least two (2) inches thick.

(1) Wall mount:

1. Locate the place where you want to mount the unit and mark four holes using your EMG mount as a guide for the screws. See [Figure 3-5](#) for the location of the screw holes.
2. Drill four 3/16 inch (4.8 mm) diameter holes at a depth of 1.25 inches (32 mm).
3. Thread four pan head top mount screws through the unit mount hole and tighten them.

(2) Keyhole mount:

1. Locate the place where you want to mount the unit and mark two holes using your EMG mount as a guide for the screws. See [Figure 3-5](#) for the location of the screw holes.
2. Drill two 3/16 inch (4.8 mm) diameter holes at a depth of 1.25 inches (32 mm).
3. Thread two pan head top mount screws through the unit mount hole and reserve 0.08" to 0.12" (2-3 mm) clearance to the wall surface.
4. Hang the EMG unit where both keyholes of wall mounts can go through the screw heads on the wall.

Figure 3-5 Wall Mount Dimensions



Connecting to a Device Port

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

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

To connect to a serial RJ45 device port:

1. Connect one end of the Cat 5 cable to the device port.
2. Connect the other end of the Cat 5 cable to an RJ45 serial console port on the serial device or use a Lantronix serial console adapter to connect it to other port types.

Notes:

- ◆ See [Device Port Commands](#) to enable or disable reverse pinouts through the CLI.
- ◆ [Table 3-6](#) and [Table 3-7](#) provide additional information on reverse pinouts.
- ◆ See [Appendix C: Adapters and Pinouts](#) for information about Lantronix adapters.

Table 3-6 Console Port and Device Port - Reverse Pinout Disabled

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

Table 3-7 Device Port - Reverse Pinout Enabled (Default)

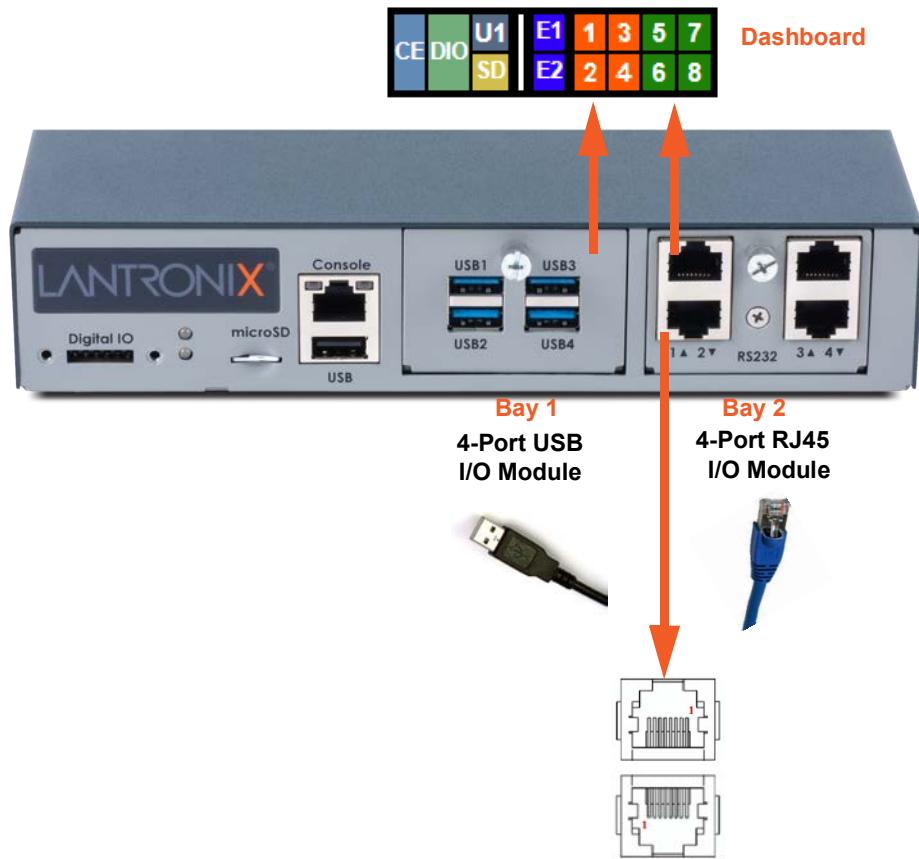
Pin Number	Description
1	CTS (input)
2	DSR (input)
3	RXD (input)
4	Ground
5	Ground
6	TXD (output)
7	DTR (output)
8	RTS (output)

To connect to a USB device port:

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

[Figure 3-8](#) shows a sample I/O module installation with one 4-port RJ45 I/O module and one 4-port USB I/O module, and how the device ports correspond to the buttons on the Web Manager [Dashboard](#).

Figure 3-8 Sample Device Port Connections (Front Side)



Modular Expansion for I/O Module Bays

The EMG module configuration can be changed by adding or replacing I/O modules in the I/O module bays. When populating the bays, Bay 1 and Bay 2 may be populated in any order and one module may be left empty. The bays are ordered from left to right: Bay 1 is the slot next to the console port and USB port and Bay 2 is the slot to the right of Bay 1. See [Figure 3-8](#).

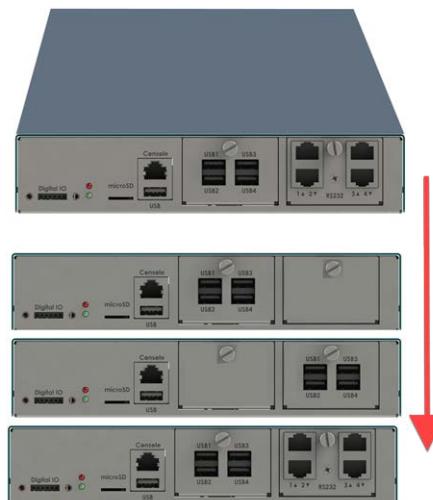
Any changes to the I/O modules must be done while the EMG unit is powered off. [Table 3-9](#) shows the available I/O module configurations. To install an I/O module, refer to [I/O Module Installation on page 47](#).

Warning: *The I/O module slots on the front of the EMG unit may only be used with the RJ45 or USB I/O modules. Do not insert the connectivity modules on the front of the EMG unit.*

Table 3-9 Available I/O Module Configurations

Examples of I/O Configurations		
Model	Ports	Final Configuration
		Bay 1 Bay2
Standard	4	[Green 2x2]
Customized	4	[Green 2x2]
Standard	8	[Green 2x2] [Green 2x2]
Customized	8	[Green 2x2] [Green 2x2]
Customized	8	[Green 2x2] [Red 2x2]
Standard	8	[Green 2x2] [Blue 2x2]
Customized	8	[Blue 2x2] [Green 2x2]

- [Green 2x2] Standard Model (RJ45 or USB)
- [Green 2x2] RJ45 I/O Module
- [Red 2x2] USB I/O Module
- [Blue 2x2] Ethernet Switch Module (coming soon)



Connecting to Network Ports

The EMG network ports, 10/100/1000 Base-T Ethernet, allow remote access to the attached devices and the system administrative functions. Use a standard RJ45-terminated Category 5 cable to connect to the network port. A CAT5e or better cable is recommended for use with a 1000 Base-T Ethernet connection.

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

Modular Expansion for Connectivity Module Bays

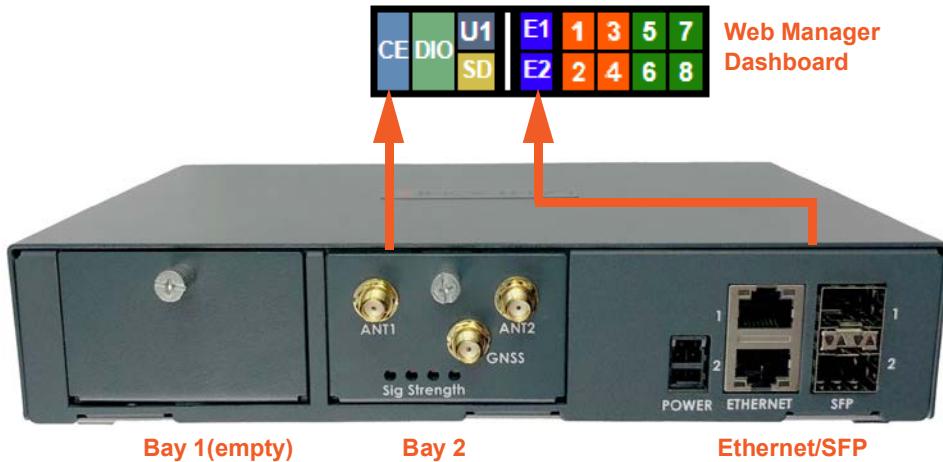
The EMG module configuration can be changed by adding or replacing connectivity modules in the Connectivity module bays. Bay 1 and Bay 2 may be populated in any order and one or both bays may be left empty. The bays are ordered from left to right: Bay 1 is the slot on the left side of the back panel and Bay 2 is the slot to the right of Bay 1. See [Figure 3-10](#).

Any changes to the connectivity modules must be done while the EMG unit is powered off. [Figure 3-10](#) shows a sample connectivity module installation with one LTE module, and how the connectivity interfaces correspond to the buttons on the [Dashboard](#), and how the device ports correspond to the buttons on the [Web Manager](#).

To install a connectivity module, refer to [Connectivity Module Installation on page 48](#).

Warning: The Connectivity module slots on the back of the EMG unit may only be used with the connectivity modules. Do not insert the I/O modules in the slots on the back of the EMG unit.

Figure 3-10 Sample Connectivity Module Configuration (Back Side)



Connecting Terminals

The console port is for local access to the EMG and the attached devices. You may attach a dumb terminal or a computer with terminal emulation to the console port. The EMG console port uses RS-232C protocol and supports VT100 emulation. The default serial settings are:

- ◆ 9600 baud
- ◆ 8 bit data
- ◆ No parity
- ◆ 1 stop bit
- ◆ No flow control

To connect the console port to a terminal or computer with terminal emulation, Lantronix offers optional adapters that provide a connection between an RJ45 jack and a DB9 or DB25 connector. The console port is configured as DTE (non-reversed RJ45). See [Appendix C: Adapters and Pinouts](#) for more information.

To connect a terminal:

1. Attach the Lantronix adapter to your terminal (typically a PN 200.2066A adapter - see [Figure C-1](#)) or your PC's serial port (use PN 200. adapter - see [Figure C-4](#)).
2. Connect the Cat 5 cable to the adapter, and connect the other end to the EMG console port.
3. Turn on the terminal or start your computer's communication program (e.g., PuTTY or TeraTerm Pro).
4. Once the EMG is running, press **Enter** to establish connection. You should see the model name and a login prompt on your terminal. On a factory default EMG you may log in with the default user name **sysadmin** and the password **PASS**.

Note: For security purposes, we recommend that you change the default password and choose a strong password.

Power Input

The EMG has a DC input jack connector for applying 9 to 30V DC. The EMG ships with an external 100 to 200VAC 50/60Hz to 12V DC power supply brick for supplying power to the DC input jack. (See [Package Contents on page 35](#).)

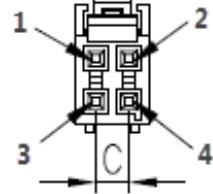
Warning: *Risk of serious electric shock! Disconnect the power cord before servicing the EMG.*

Figure 3-11 Power Input



Pin assignments

- Pin 1: Input voltage 9-30 VDC
- Pin 2: Power supply fault/power fail (active low)
- Pin 3: Ground
- Pin 4: Earth Ground



I/O Module Installation

The EMG module port configuration can be changed by adding or replacing I/O modules in the I/O module bays.

Warning: *Install the I/O module on the front only of the EMG unit. Do not insert any other module on the front of the EMG unit. Doing so may damage the EMG unit and will void the warranty.*

To install an I/O module:

1. Disconnect the power cord from the EMG unit and from the wall outlet. The EMG must be powered off when installing or replacing the modules.
2. On the front of the EMG unit, locate the module bay where the module will be inserted.
3. Unscrew the existing module or faceplate from the module bay with your fingers and carefully remove it from the module bay.
4. Insert the module into the module bay making sure the module sits completely and securely in the housing.



5. The module will sit flush with the EMG chassis.



6. Tighten the screw on the module with your fingers. Be careful not to over tighten it.
7. To verify the new module is recognized, connect power to the EMG, wait for it to boot, and log

into the web manager. The new module will be displayed in the Dashboard.

Connectivity Module Installation

The EMG module port configuration can be changed by adding or replacing connectivity modules in the connectivity module bays.

Warning: *Install the connectivity module on the back only of the EMG unit. Do not insert any other module on the back of the EMG unit. Doing so may damage the EMG unit and will void the warranty.*

To install the connectivity module:

1. Disconnect the power cord from the EMG unit and from the wall outlet. The EMG must be powered off when installing or replacing the modules.
2. On the back of the EMG unit, locate the module bay where the module will be inserted.
3. Unscrew the existing module or faceplate from the module bay with your fingers and carefully remove it from the module bay.
4. Insert the module into the module bay making sure the module sits completely and securely in the housing.



5. The module will sit flush with the EMG chassis.



6. Tighten the screw on the module with your fingers. Be careful not to over tighten it.
7. Insert and screw in the antennas to the module with your fingers.

8. To verify the new module is recognized, connect power to the EMG, wait for it to boot, and log into the web manager. The new module will be displayed in the Dashboard.

4: Quick Setup

This chapter helps get the IP network port up and running, so you can administer the EMG using your network.

Recommendations

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

- ◆ Complete the Quick Setup (see [Figure 4-2](#)) on the web interface.
- ◆ SSH to the command line interface and follow the Quick Setup script on the command line interface.
- ◆ Connect to the console port and follow the Quick Setup script on the command line interface.

Note: *The first time you power up the EMG unit, Eth1 tries to obtain its IP address via DHCP. If you have connected Eth1 to the network, and Eth1 is able to acquire an IP address, you can view this IP address by running the [Lantronix Provisioning Manager](#) application. If Eth1 cannot acquire an IP address, you cannot use Telnet, SSH, or the web interface to run Quick Setup.*

IP Address

Your EMG must have a unique IP address on your network. The system administrator generally provides the IP address and corresponding subnet mask and gateway. The IP address must be within a valid range and unique to your network. If a valid gateway address has not been assigned the IP address must be on the same subnet as workstations connecting to the EMG over the network.

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

Table 4-1 Methods of Assigning an IP Address

Method	Description
DHCP	A DHCP server automatically assigns the IP address and network settings. The EMG is DHCP-enabled by default. With the Eth1 network port connected to the network, and the EMG unit powered up, Eth1 acquires an IP address. At this point, you can use SSH or use the web interface to connect to the EMG.
BOOTP	Non-dynamic predecessor to DHCP.
Serial port login to command line interface	You assign an IP address and configure the EMG unit using a terminal or a PC running a terminal emulation program to the EMG serial console port connection.

Lantronix Provisioning Manager

You may use the Lantronix Provisioning Manager application to locate a device and view its properties and details such as its IP address. Lantronix Provisioning Manager is a free utility program provided by Lantronix that discovers, configures, upgrades, and manages Lantronix devices. It can be downloaded from the Lantronix website at <https://www.lantronix.com/products/lantronix-provisioning-manager/>. For instructions on using the application, see the Lantronix Provisioning Manager online help.

To install Lantronix Provisioning Manager:

1. Download the latest version of Lantronix Provisioning Manager from <https://www.lantronix.com/products/lantronix-provisioning-manager/>.
2. In most cases, you can simply extract the application from the archive and run the executable.

To access EMG using Lantronix Provisioning Manager:

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

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

Method #1 Quick Setup on the Web Page

After the unit has an IP address, you can use the [Quick Setup](#) page to configure the remaining network settings. This page displays the first time you log into the EMG only. Otherwise, the EMG [Home](#) page displays.

To complete the Quick Setup page:

1. Open a web browser (Firefox, Chrome or Internet Explorer web browsers with the latest browser updates).
2. In the URL field, type `https://` followed by the IP address of your EMG.

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

3. Log in using `sysadmin` as the user name and `PASS` as the password. The first time you log in to the EMG unit, the [Quick Setup](#) page automatically displays.

Note: To open the Quick Setup page at another time, click the [Quick Setup](#) tab.

Figure 4-2 Quick Setup

The screenshot shows the Lantronix EMG851000 web interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The Quick Setup tab is selected. On the right, there is a port status indicator showing U1, E1, 1, 3, SD, E2, 2, 4. Below the navigation bar, there is a sub-navigation bar with tabs for Quick Setup, Home, Help, and other icons. The main content area is titled "Quick Setup" and "Welcome to the Lantronix Edge Management Gateway". It contains sections for Network Settings, Date & Time Settings, and Administrator Settings. In the Network Settings section, there are fields for IP Address and Subnet Mask. In the Date & Time Settings section, there are fields for Date, Time, and Time Zone. In the Administrator Settings section, there are fields for Sysadmin Password and Retype Password. At the bottom of the page is an "Apply" button.

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

Note: Once you click the **Apply** button on the **Quick Setup** page, you can continue using the web interface to configure the EMG further.

5. Enter the following settings:

Network Settings

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

Network Setting	Description
Eth 1 Settings	<ul style="list-style-type: none"> ◆ Obtain from DHCP: Acquires IP address, subnet mask, hostname and gateway from the DHCP server. (The DHCP server may not provide the hostname gateway, depending on its setup.) This is the default setting. If you select this option, skip to Gateway. ◆ Obtain from BOOTP: Lets a network node request configuration information from a BOOTP "server" node. If you select this option, skip to Gateway. ◆ Specify: Lets you manually assign a static IP address, generally provided by the system administrator.
IP Address (if specifying)	<ul style="list-style-type: none"> ◆ Enter an IP address that is unique and valid on your network. There is no default. ◆ Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last segment octet. <p>Note: Currently, the EMG does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).</p>
Subnet Mask	If specifying an IP address, enter the subnet mask for the network on which the EMG unit resides. There is no default.
Default Gateway	The IP address of the router for this network. There is no default.
Hostname	The default host name is emgXXXX, where XXXX is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). Note: The host name becomes the prompt in the command line interface.
Domain	If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the EMG. For example, if abcd is specified for the SMTP server, and mydomain.com is specified for the domain, if abcd cannot be resolved, the EMG unit attempts to resolve abcd.mydomain.com for the SMTP server.

Date & Time Settings

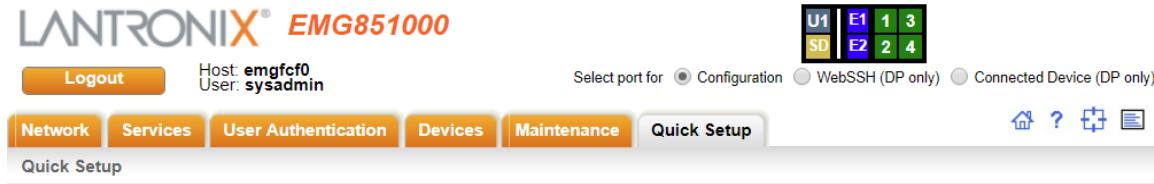
Date & Time Setting	Description
Change Date/Time	Select the checkbox to manually enter the date and time at the EMG unit's location.
Date	From the drop-down lists, select the current month, day, and year.
Time	From the drop-down lists, select the current hour and minute.
Time Zone	From the drop-down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

Administrator Settings

Administrator Setting	Description
Sysadmin Password	To change the password (e.g., from the default) enter a Sysadmin Password of up to 64 characters. <i>Note: As a security measure, we recommend that you change the default sysadmin password initially and then change the password periodically.</i>
Retype Password	Re-enter the Sysadmin Password above in this field as a confirmation.

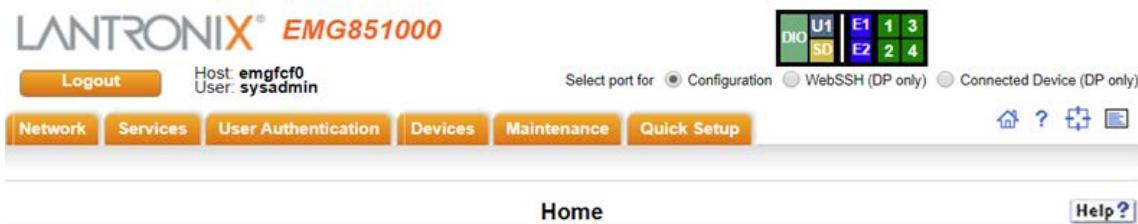
6. Click the **Apply** button to save your entries.

Figure 4-3 Quick Setup Completed in Web Manager



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

Figure 4-4 Home



Welcome to the Lantronix Edge Management Gateway



Method #2 Quick Setup on the Command Line Interface

If the EMG does not have an IP address, you can connect a dumb terminal or a PC running a terminal emulation program (VT100) to access the command line interface. (See [Connecting Terminals on page 45](#).) If the unit has an IP address, you can use SSH or Telnet to connect to the EMG unit.

By default, Telnet is disabled and SSH is enabled. To enable Telnet, use the [Services > SSH/Telnet/Logging \(on page 115\)](#).

To complete the command line interface Quick Setup script:

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

Figure 4-5 Beginning of Quick Setup Script

Welcome to the Lantronix Edge Management Gateway
Model Number: EMG851000

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

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

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

4. Enter the following information at the prompts:

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

CLI Quick Setup Settings	Description
Configure Eth1	Select one of the following: <ul style="list-style-type: none"> ◆ (1) obtain IP Address from DHCP: The unit will acquire the IP address, subnet mask, hostname, and gateway from the DHCP server. (The DHCP server may or may not provide the gateway and hostname, depending on its setup.) This is the default setting. ◆ (2) obtain IP Address from BOOTP: Permits a network node to request configuration information from a BOOTP "server" node. ◆ (3) static IP Address: Allows you to assign a static IP address manually. The IP address is generally provided by the system administrator.
IP Address (if specifying)	An IP address that is unique and valid on your network and in the same subnet as your PC. There is no default. If you selected DHCP or BOOTP , this prompt does not display. Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last octet. Note: Configurations with the same IP subnet on multiple interfaces (Ethernet or PPP) are not currently supported.
Subnet Mask	The subnet mask specifies the network segment on which the EMG resides. There is no default. If you selected DHCP or BOOTP , this prompt does not display.
Default Gateway	IP address of the router for this network. There is no default.
Hostname	The default host name is emgXXXX, where XXXX is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). Note: The host name becomes the prompt in the command line interface.
Domain	If desired, specify a domain name (for example, support.iantronix.com). The domain name is used for host name resolution within the EMG unit. For example, if abcd is specified for the SMTP server, and mydomain.com is specified for the domain, if abcd cannot be resolved, the EMG attempts to resolve abcd.mydomain.com for the SMTP server.
Time Zone	If the time zone displayed is incorrect, enter the correct time zone and press Enter . If the entry is not a valid time zone, the system guides you through selecting a time zone. A list of valid regions and countries displays. At the prompts, enter the correct region and country.
Date/Time	If the date and time displayed are correct, type n and continue. If the date and time are incorrect, type y and enter the correct date and time in the formats shown at the prompts.

CLI Quick Setup Settings	Description
Sysadmin password	<p>Enter a new sysadmin password.</p> <p>Note: As a security measure, we recommend that you change the default sysadmin password initially and then change the password periodically.</p>

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

Figure 4-6 Quick Setup Completed in CLI

Welcome to the Lantronix Edge Management Gateway
Model Number: EMG851000

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>.

The EMG851000 can be configured to use a default gateway.
Enter gateway IP Address: [none]

```
____ Hostname _____
The current hostname is 'emgfcf0', and the current domain is
'<undefined>'.
The hostname will be shown in the CLI prompt.
Specify a hostname: [emgfcf0]
Specify a domain: [<undefined>]
```

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

____ Date/Time _____
The current time is Wed Jul 3 14:23:24 2019
Change the current time? [n]

____ Sysadmin Password ____
The default sysadmin (administrator user) password is 'PASS'.
Enter new password: [PASS]

Quick setup is now complete.

For a list of commands, type 'help'.

Next Step

After completing quick setup on the EMG, you may want to configure other settings. You can use the web page or the command line interface for configuration.

- ◆ For information about the web and the command line interfaces, go to [Chapter 5: Web and Command Line Interfaces](#).
- ◆ To continue configuring the EMG unit, go to [Chapter 6: Networking](#).

Limiting Sysadmin User Access

For security purposes, full administrative access to the EMG via the default sysadmin local user account can be limited to only the front console port of the EMG device.

These steps will prevent any local users from logging in, restrict the default sysadmin local user to the front console port, and allow a user with administrative rights to login, as long as remote authentication is working.

To configure limited sysadmin user access:

1. Enable the Sysadmin access limited to Console Port option on the Local/Remote Users web page.
2. Enable a remote authentication method (such as TACACS+ or LDAP) and configure the remote authentication method to be first in the order of methods used.
3. Create a remote user account with full administrative rights.
4. Uncheck the **Attempt next method on authentication rejection** checkbox on the Authentication Methods web page.

5: Web and Command Line Interfaces

The EMG offers a web interface (Web Manager) and a command line interface (CLI) for configuring the EMG unit.

Note: See [Chapter 4: Quick Setup](#) for instructions on configuring basic network settings using the Web Manager and CLI quick setup.

Web Manager

A Web Manager allows the system administrator and other authorized users to configure and manage the EMG using most web browsers (Firefox, Chrome, Safari or Internet Explorer web applications with the latest browser updates). The EMG unit provides a secure, encrypted web interface over SSL (secure sockets layer).

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

The following figure shows a typical web page:

Figure 5-1 Web Page Layout

The figure shows a screenshot of the LANTRONIX EMG851000 Web Manager. The interface is titled 'LANTRONIX® EMG851000'. At the top, there is a 'Logout' button, a user session indicator ('Host: emgfcf0 User: sysadmin'), and a 'Dashboard' section showing port status (U1, E1, 1, 3, SD, F2, 2, 4). Below the dashboard are tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The 'Network' tab is selected, showing 'Network Settings'. The 'Network Settings' section contains 'Ethernet Interfaces' for Eth1 and Eth2, 'Hostname & Name Servers', 'DNS Servers', 'DHCP-Acquired DNS Servers', 'TCP Keepalive Parameters', and a summary table of Rx/Tx statistics for Eth1 and Eth2. The 'Ethernet Interfaces' section includes fields for IP Address, Subnet Mask, and MTU, as well as options for IPv4 and IPv6 settings. The 'Hostname & Name Servers' section includes fields for Hostname and Domain. The 'DNS Servers' section includes fields for #1, #2, and #3. The 'DHCP-Acquired DNS Servers' section lists #1: 172.19.1.1, #2: 172.19.1.2, and #3: None. The 'TCP Keepalive Parameters' section includes fields for Start Probes, Number of Probes, and Interval. The 'Rx/Tx' statistics table shows the following data:

	Rx			Tx			
	Bytes	Packets	Errors	Multicast	Bytes	Packets	Errors
Eth1	1401703	13091	0	0	196816	464	0
Eth2	0	0	0	0	0	0	0

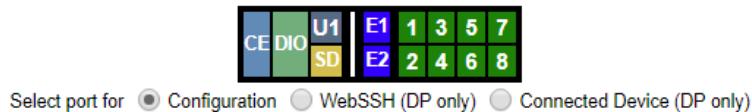
The web page has the following components:

- ◆ **Tabs:** Groups of settings to configure.

- ◆ **Options:** Below each tab are options for specific types of settings.

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

Figure 5-2 Sample Dashboard



- ◆ **Dashboard**

The Dashboard buttons allow you to view and configure EMG ports and interfaces. The appearance of the dashboard will differ according to the I/O and connectivity modules installed in the EMG and the type of network interface installed. See [System Features on page 28](#). The dashboard buttons are defined below:

CE	Cellular connectivity settings for the LTE cellular module (if installed). See Chapter 6: Cellular Modem Settings .
DIO	DIO port settings. See DIO Port on page 175 .
U1	USB device (flash drive or modem) plugged into the front panel USB connector. See Chapter 8: USB/SD Card Port .
SD	SD card settings. See Chapter 8: USB/SD Card Port .
E1 E2	Network settings for the Ethernet port. See Network Port Settings on page 67 .
F1 F2	Network settings for the SFP transceiver port. See Network Port Settings on page 67 .
1 3 2 4	Device port settings for the device ports. Only ports to which the currently logged-in user has rights are enabled. See Device Ports - Settings on page 152 .

- ◆ **Dashboard Options:** Options for use with the port buttons.

- Select a port and the **Configuration** option: displays the [Device Ports > Settings \(1 of 2\) page](#).
- Select a port and the **WebSSH** option: displays the WebSSH window for the device port - if Web SSH is enabled, and if SSH is enabled for the device port.
- Select a port and the **Connected Device** option: allows access to supported devices such as remote power managers (RPMs) and/or SensorSoft temperature and humidity probes connected to the device port.

- ◆ **Entry Fields and Options:** Allow you to enter data and select options for the settings.

Note: For specific instructions on completing the fields on the web pages, see Chapters 6 through 14.

- ◆ **Apply Button:** The Apply button (not shown in *Figure 5-1 Web Page Layout*) on each web page makes the changes immediately and saves them so they will be there when the EMG is rebooted.
- ◆ **Icons:** The icon bar above the Main Menu has icons that display the following:
 -  Home page.
 -  Information about the EMG unit and Lantronix contact information.
 -  Configuration site map.
 -  Status of the EMG.
- ◆ **Help Button:** Provides online Help for the specific web page.

Logging in

Only the system administrator or users with web access rights can log into the Web Manager. More than one user at a time can log in, but the same user cannot log in more than once.

To log in to the Web Manager:

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

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

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

Logging Out

To log off the EMG web interface:

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

Web Page Help

To view detailed information about an EMG web page:

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

Command Line Interface

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

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

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

Logging In

To log in to the EMG command line interface:

1. Do one of the following:
 - With a serial terminal connection, power up, and when the command line displays, press **Enter**.
 - If the EMG already has an IP address (assigned previously or assigned by DHCP), Telnet (if Telnet has been enabled) or SSH to `xx.xx.xx.xx` (the IP address in dot quad notation) and press **Enter**. The login prompt displays.
2. To log in as the system administrator for setup and configuration, enter `sysadmin` as the user name and press **Enter**.
3. Enter `PASS` as the password and press **Enter**. The first time you log in, the Quick Setup script runs automatically. Normally, the command prompt displays. (To display the Quick Setup script again, use the `admin quicksetup` command.)

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

To log in any other user:

1. Enter your EMG user name and press **Enter**.
2. Enter your EMG password and press **Enter**.

Logging Out

To log out of the EMG command line interface, type `logout` and press **Enter**.

Command Syntax

Commands have the following format:

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

where

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

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

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

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

Command Line Help

- ◆ For general Help and to display the commands to which you have rights, type: `help`
- ◆ For general command line Help, type: `help command line`
- ◆ For release notes for the current firmware release, type: `help release`
- ◆ For more information about a specific command, type `help` followed by the command. For example: `help set network` or `help admin firmware`

Tips

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


```
set network port 1 state static ipaddr 122.3.10.1 mask 255.255.0.0
      to
      se net po 1 st static ip 122.3.10.1 ma 255.255.0.0
```
- ◆ Use the Tab key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** either to complete the name if only one is possible, or to display the possible names if more than one is possible. Following a space after the preceding name, Tab displays all possible names.
- ◆ Should you make a mistake while typing, backspace by pressing the Backspace key and/or the Delete key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the left and right arrow keys to move within a command.
- ◆ Use the up and down arrows to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.
- ◆ To clear an IP address, type `0.0.0.0`, or to clear a non-IP address value, type `CLEAR`.
- ◆ When the number of lines displayed by a command exceeds the size of the window (the default is 25), the command output is halted until the user is ready to continue. To display the next line, press **Enter**, and to display the page, press the space bar. You can override the number of lines (or disable the feature altogether) with the `set cli` command.

General CLI Commands

The following commands relate to the CLI itself.

To configure the current command line session:

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

Allows you to use [Lantronix Secure Console Server](#) (SCS)-compatible commands as shortcuts for executing commands:

Note: *Settings are retained between CLI sessions for local users and users listed in the remote users list.*

Table 5-3 SCS Commands

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

To set the number of lines displayed by a command:

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

Sets the number of lines in the terminal emulation (screen) for paging through text one screenful at a time, if the EMG unit cannot detect the size of the terminal automatically.

To show current CLI settings:

```
show cli
```

To view the last 100 commands entered in the session:

```
show history
```

To clear the command history:

```
set history clear
```

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

```
show user
```

Note: For information about user rights, see [Chapter 13: User Authentication](#).

Table 5-4 CLI Keyboard Shortcuts

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

6: Networking

This chapter explains how to set the following network settings for the EMG using the web interface or the CLI:

- ◆ [*Network Port Settings*](#)
- ◆ [*Cellular Modem Settings*](#)
- ◆ [*IP Filter* and *Routing*](#)
- ◆ [*VPN Settings*](#)
- ◆ [*Security*](#)
- ◆ [*Performance Monitoring*](#)
- ◆ [*FQDN List*](#)

Requirements

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

To configure the unit, you need the following information:

Eth1 IP address: _____ - _____ - _____ - _____

 Subnet mask: _____ - _____ - _____ - _____

Eth2 IP address (optional): _____ - _____ - _____ - _____

 Subnet mask (optional): _____ - _____ - _____ - _____

Gateway: _____ - _____ - _____ - _____

DNS: _____ - _____ - _____ - _____

Network Port Settings

Network parameters determine how the EMG unit interacts with the attached network. Use this page to set the following basic configuration settings for the network ports (Eth1 and Eth2).

The EMG supports the following types of network interfaces:

- ◆ RJ-45 ports, as one of the user-selectable active ports on the EMG. In the web UI port banner bar, these are represented as **E1** and **E2**. These ports can be configured for speeds of 10Mbit, 100 Mbit or 1000 Mbit, at half-duplex or full-duplex. The RJ45 Ethernet LEDs display the following states:
 - **Green Light On:** indicates a link at 1000 BASE-T
 - **Green Light Off:** indicates a link at other speeds, or no link
 - **Yellow Light On:** indicates a link is established
 - **Yellow Light Blinking:** indicates link activity
- ◆ A variety of SFP modules, as one of the user-selectable active ports on the EMG. In the web UI port banner bar, these are represented as **F1** and **F2**, in a variety of colors.
 - **F1:** Single mode 1000 BASE-LX optical SFPs
 - **F1:** Multi mode 1000 BASE-SX optical SFPs
 - **F1:** RJ45 1000 BASE-T SFPs
 - **F1:** A port with no SFP module is shown in white.
 - **F1:** A port with an unknown SFP module

The SFP Ethernet LEDs are located between the two SFP module slots; the LEDs for Ethernet 1 are on the left, and the LEDs for Ethernet 2 are on the right. They display the following states:

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

These ports are fixed at 1000 Mbit full-duplex. Note that in some vendor's RJ45 1000 BASE-T transceivers, the RX LOS is internally ground, so the link status feature may fail.

To enter settings for one or both network ports:

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

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



Logout Host: emgeecc User: sysadmin

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

Network Services User Authentication Devices Maintenance Quick Setup

Network Settings Cellular Modem IP Filter Routing VPN Security Perf Monitoring FQDN List



Network Settings

Ethernet Interfaces

Eth1 Settings: Disabled Obtain from DHCP Obtain from BOOTP Specify

IP Address: 172.172.100.100

Subnet Mask: 255.255.0.0

IPv6 Address: (Static)

IPv6 Address: (Link Local) fe80::280:a3ff:feff:eecc/64

Mode: Auto

MTU: 1500

Active Port: RJ45

HW Address: 00:80:a3:ff:ee:cc

Multicast: 224.0.0.1

Eth1 Link: Up

Enable IPv6: (Requires reboot)

IP Forwarding:

IPv6 Forwarding:

Eth2 Settings: Disabled Obtain from DHCP Obtain from BOOTP Specify

IP Address: 172.19.100.212

Subnet Mask: 255.255.0.0

IPv6 Address: (Static)

IPv6 Address: (Global) 2001:db80:ac13:d91e:280:

IPv6 Address: (Link Local) fe80::280:a3ff:feff:ddbb/64

Mode: Auto

MTU: 1500

Active Port: SFP

HW Address: 00:80:a3:ff:dd:bb

Multicast: 239.255.255.251
224.0.0.1

Eth2 Link: Up

Ethernet Bonding: Disable

Hostname & Name Servers

Hostname: emgeecc

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

Domain:

DNS Servers

#1: 172.19.1.1

#2: 172.19.1.2

#3:

DHCP-Acquired DNS Servers

#1: None

#2: None

#3: None

Prefer IPv4

DNS Records:

TCP Keepalive Parameters

Start Probes: 185 secs

Number of Probes: 6

Interval: 20 secs

Rx				Tx			
	Bytes	Packets	Errors		Bytes	Packets	Errors
Eth1	132748	567	0	Eth1	137442	620	0
Eth2	3334348	25033	0	Eth2	2620950	20889	0

Gateway

Default: 172.19.0.1

DHCP-Acquired: none

Precedence: DHCP-Acquired Default

IPv6 Default:

Fail-Over Settings

Fail-over Gateway IP Address: 172.19.100.158

IP Address to Ping to Trigger Fail-Over: 172.19.39.22

Ethernet Port for Ping: Eth1 Eth2 Cell

Delay between Pings: 3 seconds

Number of Failed Pings: 3

Fail-over Port: Eth2 Cellular

The **SFP NIC Info & Diagnostics** link brings you to the *Network Settings > SFP NIC Information & Diagnostics* page.

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

Fail-Over Cellular Gateway Configuration

Fail-over Device:

APN of Mobile Carrier:

Admin Login:

Admin Password:

Change Admin Password:

New Admin Password: Retype:

Reboot Gateway When Making Changes:

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

[Fail-Over Cellular Gateway Status](#) >

Advanced Cellular Gateway Configuration

SIM Card PIN Lock:

PIN # for SIM Card: Retype:

SIM PUK: Retype:

SIM Username:

SIM Password:

Dial-Up String:

Roaming:

Load Cellular Gateway Firmware Options

Update Firmware:

Functional Firmware
Filename: [Upload File](#) >

Radio Firmware Filename: [Upload File](#) >

Load Firmware via:

USB Port: Port U1

FTP/SFTP/SCP Server:

Path:

Login:

Password:

Retype Password:

Figure 6-3 Network Settings > SFP NIC Information & Diagnostics

LANTRONIX® EMG851000

Logout Host: emgfco0 User: sysadmin

Network Services User Authentication Devices Maintenance Quick Setup

Network Settings IP Filter Routing VPN Security Perf Monitoring FQDN List

Network - SFP NIC Information & Diagnostics

Eth1 SFP Module: 1000BASE-LX Single Mode (Vendor: Fiberstore PN: SFP1G-EX-55 Rev: A0)
 Eth2 SFP Module: 1000BASE-LX Single Mode (Vendor: FiberStore PN: SFP1G-ZX-55 Rev: A)

SFP Diagnostic Information							
Port	Temp	Voltage	Current	Output Power	Input Power	LOS	TX Fault
Eth1	36.53 degC/97.76 degF	3.2058V	23.800mA	0.5475mW	0.5622mW	No	No
Eth2	48.42 degC/119.15 degF	3.1902V	20.000mA	1.0741mW	0.0000mW	Yes	No

[Back to Network Settings](#)

2. Enter the following information:

Ethernet Interfaces (Eth1 and Eth2)

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

Eth 1 Settings or Eth 2 Settings	<ul style="list-style-type: none"> ◆ Disabled: If selected, disables the network port. ◆ Obtain from DHCP: Acquires IP address, subnet mask, hostname and gateway from the DHCP server. (The DHCP server may not provide the hostname/gateway, depending on its setup.) This is the default setting. If you select this option, skip to Gateway. ◆ Obtain from BOOTP: Lets a network node request configuration information from a BOOTP "server" node. If you select this option, skip to Gateway. ◆ Specify: Lets you manually assign a static IP address, generally provided by the system administrator.
IP Address (if specifying)	<ul style="list-style-type: none"> ◆ Enter an IP address that will be unique and valid on your network. There is no default. ◆ Enter all IP addresses in dot-quad notation. Do not use leading zeros in the fields for dot-quad numbers less than 100. For example, if your IP address is 172.19.201.28, do not enter 028 for the last segment octet. <p>Note: Currently, the EMG unit does not support configurations with the same IP subnet on multiple interfaces (Ethernet or PPP).</p>
Subnet Mask	If specifying an IP address, enter the network segment on which the EMG unit resides. There is no default.

IPv6 Address (Static)	<p>Address of the port in IPv6 format.</p> <p>Note: The EMG supports IPv6 connections for the following services: the web, SSH, Telnet, remote syslog, SNMP, NTP, LDAP, Kerberos, RADIUS, TACACS+, connections to device ports, and diagnostic ping.</p> <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:</p> <p>1234 : 0BCD : 1D67 : 0000 : 0000 : 8375 : BADD : 0057 may be shortened to 1234 : BCD : 1D67 : : 8375 : BADD : 57.</p>
IPv6 Address (Global)	<p>IPv6 address with global scope that is generated by address auto configuration. The address is generated from a combination of router advertisements and MAC address to create a unique IPv6 address. This field is read only.</p> <p>Note: This field will not appear in the absence of an IPv6 global address.</p>
IPv6 Address (Link Local)	<p>An IPv6 address that is intended only for communications within the segment of a local network. This field is read only.</p>
Mode	<p>Select the direction, duplex mode (full duplex or half-duplex), and speed (10, 100, or 1000 Mbit) of data transmission. The default is Auto, which allows the Ethernet port to auto-negotiate the speed and duplex with the hardware endpoint to which it is connected.</p>
MTU	<p>Specifies the maximum transmission unit (MTU) or maximum packet size of packets at the IP layer (OSI layer 3) for the Ethernet port. When fragmenting a datagram, this is the largest number of bytes that can be used in a packet. The minimum MTU size is 108 bytes (to conform with RFC 2460) and the maximum size is 1500 bytes.</p>
Active Port	<p>Selects either the RJ45 port or the SFP port as the active Ethernet port. Selecting SFP requires that a SFP transceiver module be inserted into the appropriate SFP slot.</p> <p>When switching from RJ45 to SFP or vice versa, any active network connections may be disrupted or broken.</p>
HW Address	<p>Displays the hardware address of the Ethernet port.</p>
Multicast	<p>Displays the multicast address of the Ethernet port.</p>
Enable IPv6	<p>Select this box to enable the IPv6 protocol. If changed, the EMG unit will need to reboot. Enabled by default.</p>
IP Forwarding	<p>If enabled, IP forwarding enables IPv4 network traffic received on one interface (Eth1, Eth2, or an external/USB modem attached to the EMG unit with an active PPP connection) to be transferred out another interface (any of the above). The default behavior (if IP forwarding is disabled) is for network traffic to be received but not routed to another destination.</p> <p>Enabling IP forwarding is required if you enable Network Address Translation (NAT) for any device port modem or USB/ISDN modem. IP forwarding allows a user accessing the EMG over a modem to access the network connected to Eth1 or Eth2.</p>
IPv6 Forwarding	<p>If enabled, IPv6 forwarding enables IPv6 network traffic received on one interface (Eth1, Eth2, or an external/USB modem attached to the EMG unit with an active PPP connection) to be transferred out another interface (any of the above). The default behavior (if IP forwarding is disabled) is for network traffic to be received but not routed to another destination.</p>

SFP NIC Info & Diagnostics (Link)	Clicking the link brings you to the Network Settings > SFP NIC Information & Diagnostics page showing information and diagnostics about the SFP connection port, temperature, voltage, current, output power, input power, LOS, and TX fault. Click Back to Network Settings to return to the Network Settings page. Note:
Ethernet Bonding	Ethernet 1 and Ethernet 2 can be bonded to support redundancy (Active Backup), aggregation (802.3ad), and load balancing. Disabled by default. Ethernet Bonding requires that Eth1 and Eth2 must be set to Static IP. Note: <i>If Ethernet Bonding is enabled, assigning individual IP Addresses to Device Ports is not supported.</i>
Ethernet Bonding Status (Link)	Click the link to access Ethernet bonding status information. Ethernet 1 and Ethernet 2 can be bonded to support redundancy (Active Backup), aggregation (802.3ad), and load balancing. Disabled by default. Ethernet Bonding requires that Eth1 and Eth2 must be set to Static IP. Note: <i>If Ethernet Bonding is enabled, assigning individual IP Addresses to Device Ports is not supported.</i> Click Back to Network Settings link to return to the Network Settings page.

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

Hostname & Name Servers

Hostname	The default host name is emgXXXX, where XXXX is the last 4 characters of the hardware address of Ethernet Port 1. There is a 64-character limit (contiguous characters, no spaces). The host name becomes the prompt in the command line interface.
Domain	If desired, specify a domain name (for example, support.lantronix.com). The domain name is used for host name resolution within the EMG unit. For example, if abcd is specified for the SMTP server, and mydomain.com is specified for the domain, if abcd cannot be resolved, the EMG attempts to resolve abcd.mydomain.com for the SMTP server.

DNS Servers

#1 - #3	Configure up to three name servers with an IPv4 or IPv6 address. #1 is required if you choose to configure DNS (Domain Name Server) servers. The EMG will attempt to contact each DNS server in the order that they are given. If a DNS server cannot be reached, the next DNS server will be tried. If a DNS server is reachable, but does not resolve a hostname, no other attempts will be made to resolve the hostname using the remaining DNS servers. The first three DNS servers acquired via DHCP through Eth1 and/or Eth2 display automatically.
----------------	--

DHCP-Acquired DNS Servers

#1 - #3	Displays the IP address of the name servers if automatically assigned by DHCP.
Prefer IPv4 DNS Records	If enabled, IPv4 DNS records will be preferred when DNS hostname lookups are performed. Otherwise IPv6 records will be preferred (when IPv6 is enabled). Enabled by default.

TCP Keepalive Parameters

Start Probes	Number of seconds the EMG unit waits after the last transmission before sending the first probe to determine whether a TCP session is still alive. The default is 600 seconds (10 minutes).
Number of Probes	Number of probes the EMG sends before closing a session. The default is 5.
Interval	The number of seconds the EMG unit waits between probes. The default is 60 seconds.

Gateway

Default	IP address of the IPv4 router for this network. If this has not been set manually, any gateway acquired by DHCP for Eth1 or Eth2 displays. All network traffic that matches the Eth1 IP address and subnet mask is sent out Eth1. All network traffic that matches the Eth2 IP address and subnet mask is sent out Eth 2. If you set a default gateway, any network traffic that does not match Eth1 or Eth2 is sent to the default gateway for routing.
DHCP-Acquired	Gateway acquired by DHCP for Eth1 or Eth2. View only.
Precedence	Indicates whether the gateway acquired by DHCP or the default gateway takes precedence. The default is DHCP Gateway. If the DHCP Gateway is selected and both Eth1 and Eth2 are configured for DHCP, the EMG unit gives precedence to the Eth1 gateway.
IPv6 Default	Indicates the IP address of the IPv6 router for this network.

Fail-Over Settings

Fail-over Gateway IP Address	The fail-over gateway is a backup default gateway, used when it is determined through a fail-over trigger that the primary default gateway is no longer a viable route. A fail-over event happens when a Ping device reachable via an Ethernet interface and the default gateway becomes unreachable. Fail-back occurs when the Ping device becomes reachable again, causing the primary default route to be restored. <i>Note: The fail-over gateway is not supported when DHCP is used.</i>
IP Address to Ping to Trigger Fail-over	IP address to ping to determine whether to use the fail-over gateway.
Ethernet Port for Ping	Ethernet port to use for the ping. The options are Eth1, Eth2, and Cell (cellular).
Delay between Pings	Number of seconds between pings. The default is 3.
Number of Failed Pings	Number of pings that fail before the EMG uses the fail-over gateway. The default is 10.
Fail-over Port	The network interface to use for fail-over. The Fail-over Gateway IP address should either be accessible via this interface or assigned directly to this interface. Select Eth2 or Cellular if a cellular modem module is installed.

Fail-Over Cellular Gateway Configuration

Fail-over Device	<p>Note: The external gateways, Lantronix PremierWave XC HSPA+ Cellular Gateway and the Sierra Wireless AirLink ES450, are not supported in the current release.</p> <p>Select an integrated external device to be used as the fail-over gateway. Currently the Lantronix PremierWave XC HSPA+ Cellular Gateway and the Sierra Wireless AirLink ES450 are supported. When using an internal cellular modem as the fail-over gateway, the Fail-over Device should be set to None.</p> <p>The HSPA+ gateway must be configured in gateway mode before it can be used as the fail-over gateway. It is recommended that the HSPA+ Cellular Connection Mode be set to On Demand, which will leave the link quiescent until an application attempts to make use of the cellular network connection. It is also recommended that the SNTP protocol be disabled, as On Demand mode uses the egress traffic as a trigger. The console manager automatically disables UPnP on the HSPA+ gateway. If PIN or PUK is required by HSPA but not supplied by console manager then a syslog message and a non fatal error message will be generated.</p> <p>The Sierra gateway must be properly provisioned before first use by initializing the access point name (APN) of the installed SIM card. This is done by connecting the Sierra gateway to the second ethernet port of the EMG, and assigning a static IP address to the EMG port so that it is in the same subnet as the IP address of the Sierra gateway. Use the console CLI or web graphical user interface (GUI) to set the APN of the SIM card. After setting the APN, power cycle the Sierra gateway and allow it to reboot completely.</p> <p>The failover feature requires that both Ethernet ports be configured with a static IP address. Using DHCP on one of the Ethernet ports may overwrite the default route, interfering with fail-over and fail-back.</p> <p>Note: <i>The commands sent to the fail-over device to retrieve status and update the configuration are shown in the syslog (messages may be displayed under Network syslog; at the Debug level). If there are errors retrieving status or updating the configuration, check messages in the Network syslog, the device administrator login/password, connectivity to the device and the firmware version of the fail-over device (the minimum required firmware version for HSPA+ is 8.1.0.0 and for Sierra Wireless ES450, it is 4.9.2). For the HSPA+ gateway, if the firmware is updated and new items are added to the status output by the gateway, the new items will automatically be displayed on the EMG.</i></p> <p>When the EMG sends an updated configuration to the fail-over device, it is recommended to check the EMG syslog, even if the EMG indicates that the update was successful. Responses from the fail-over device indicating that the device needs to be rebooted for configuration changes to take affect may also be in the syslog. The configuration will be re-sent to the device if any of the fail-over device settings are changed, or the selected fail-over device is changed from None to one of the supported fail-over device types.</p> <p>When a fail-over or fail-back occurs, running applications such as VPN tunnel and ConsoleFlow will be restarted.</p>
APN of Mobile Carrier	For the HSPA+ and Sierra gateways, configure the Access Point Name for the mobile carrier. May have up to 256 characters.
Admin Login and Password/Retype	For the selected Fail-over Device , the administrator login and password used to retrieve status from the device and send configuration updates to the device. The login may have up to 32 characters, and the password may have up to 64 characters. The Admin Password displays the current password masked.
Change Admin Password (check box)	Select this check box if you wish to update the admin password for the selected gateway Fail-over Device .

New Admin Password/Retype	For the selected Fail-over Device , the administrator password can be changed on the gateway. The password may have up to 64 characters. To change the Admin Password, click the Change Admin Password checkbox and enter the new password in the New Admin Password and Retype fields. Changing the HSPA+ Admin password will save the password on the EMG for status and configuration queries to the HSPA+ gateway. The password must match what is stored on the HSPA+ gateway. Changing the Sierra Admin password will save the password on the EMG for status and configuration queries to the Sierra gateway. The new password will also be configured on the Sierra gateway. The Sierra gateway login must be set as 'user'.
Reboot Gateway When Making Changes (checkbox)	Select this check box if you wish to reboot the selected fail-over device when making changes.
Fail-Over Cellular Gateway Status (link)	Clicking the link opens the Fail-Over Cellular Gateway status window, showing status and statistics about the fail-over gateway. Click Back to Network Settings to return to the Network Settings page.

Advanced Cellular Gateway Configuration

SIM Card PIN Lock (checkbox)	For the HSPA+ and Sierra gateways, enable a lock so that the SIM card used by the gateway cannot be used by anyone who does not have the PIN.
Pin # for SIM Card/Retype	For the HSPA+ and Sierra gateways, the PIN number for the SIM card used by the gateway. May have up to 8 characters.
SIM PUK/Retype	For the HSPA+ gateway, the SIM Personal Unblocking Key (PUK). May have up to 16 characters. The Sierra gateway does not have this feature.
SIM Username	For the HSPA+ gateway, enter the username for dial up to the cellular carrier, if required. May have up to 64 characters. The Sierra gateway does not have this feature.
SIM Password	For the HSPA+ gateway, enter the password for dial up to the cellular carrier, if required. May have up to 64 characters. The Sierra gateway does not have this feature.
Dial-up String	For the HSPA+ gateway, enter the modem string used for making a connection to the carrier. May have up to 64 characters. The Sierra gateway does not have this feature.
Roaming	For the HSPA+ gateway, enable or disable network roaming. The Sierra gateway does not have this feature.

Fail-Over Cellular Gateway Firmware

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

Update Firmware (checkbox)	Select this option to update firmware on the HSPA+ gateway or the Sierra gateway. The Functional Firmware file and the Radio Firmware file (required for the Sierra gateway only) will be transferred to the EMG using the method selected by the Load Firmware via option. Once the file(s) have been transferred to the EMG, the EMG will initiate the firmware update on the gateway.
Functional Firmware Filename	Enter the name of the firmware filename exactly as it is represented.

Radio Firmware Filename	Enter the name of the radio firmware filename exactly as it is represented.
Load Firmware via	<p>Select the method to load the firmware from the options in the drop-down menu. Options are: FTP, SFTP, SCP, USB, SD Card, and HTTPS. FTP is the default.</p> <ul style="list-style-type: none"> ◆ If you select HTTPS, the Upload File link becomes active. Select the link to open a popup window that allows you to browse to a firmware update file to upload. ◆ If you select NFS, the mount directory must be specified. <p>Note: Connections available depend on the model of the EMG unit.</p>

Load Cellular Gateway Firmware Options

USB Port	The USB Port selection becomes active when you choose to Load Firmware via USB. EMG provides one USB port called U1 in the interface. The firmware files must be stored in the top level directory of the USB flash drive.
FTP/SFTP/SCP Server	Enter the IP address or host name of the server used for obtaining the firmware files. May have up to 64 alphanumeric characters; may include hyphens and underscore characters.
Path	Enter the path on the server for obtaining firmware update files.
Login	Enter the user login for the FTP/SFTP/SCP server to verify access. May be blank.
Password/ Retype Password	Enter the FTP/SFTP/SCP user password. Retype the password in the Retype Password field.

3. To save your entries, click the **Apply** button. **Apply** makes the changes immediately and saves them so they will persist when the EMG is rebooted.

Ethernet Counters

The [Network > Network Settings \(1 of 2\)](#) page displays statistics for each of the EMG Ethernet ports since boot-up. The system automatically updates them.

	Rx				Tx		
	Bytes	packets	Errors	Multicast	Bytes	packets	Errors
Eth1	62165901	546159	0	0	20230163	84196	0
Eth2	1850	20	0	0	106774	411	0

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

Network Commands

Go to [Network Commands](#) to view CLI commands which correspond to the web page entries described above.

Cellular Modem Settings

The EMG supports the use of one internal LTE cellular modem installed in the EMG unit. The Cellular Settings web page allows the user to configure parameters that determine how the EMG cellular modem network behaves, and to update the cellular modem firmware.

To complete the Cellular Settings page:

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

Figure 6-4 Network > Cellular Modem Settings Page

LANTRONIX® EMG852201

Logout Host: emgeecc User: sysadmin

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

Network Services User Authentication Devices Maintenance Quick Setup

Network Settings Cellular Modem IP Filter Routing VPN Security Perf Monitoring FQDN List

Cellular Settings Help ?

Cellular Interface

Cell Settings: Disabled Obtain from DHCP

IP Address: 10.38.105.23

Subnet Mask: 255.255.255.240

Rx				Tx			
	Bytes	Packets	Errors	Multicast	Bytes	Packets	Errors
Cell	1224	4	0	0	1847	9	0

Cellular Modem Configuration [Cellular Status](#)

APN of Cellular Carrier:

Reboot Modem

Cell Network Username:

Cell Network Password:

Cell Network Auth:

Roaming

SIM Card PIN Lock:

PIN # for SIM Card: Retype:

Cellular Modem Firmware

Update Firmware:

Modem Firmware Filename: [Upload File](#)

PRI Carrier Filename: [Upload File](#)

Load Firmware via:

Load Cellular Modem Firmware Options

FTP/SFTP/SCP Server:

Path:

Login:

Password:

Retype Password:

Apply

2. Enter the following information:

Cellular Interface

Cell Settings	Disabled: If selected, disables the cellular interface. Default is enabled for DHCP. Obtain from DHCP: Acquires IP address and subnet mask from DHCP.
IP Address	(view only) An IP address acquired via DHCP.
Subnet Mask	(view only) The network segment acquired via DHCP.

Cellular Modem Configuration

APN of Cellular Carrier	Configure the Access Point Name for the cellular carrier. May have up to 256 characters.
Reboot Modem	Select this option to restart the cellular modem. It is recommended that the modem be restarted after firmware update, after changing the state of the SIM Card PIN Lock, and after changing the PIN # for SIM Card.
Cellular Network Username and Password	The login and password for connecting to the cellular carrier, if required. The login may have up to 32 characters, and the password may have up to 64 characters. The Cellular Network Password displays the current password masked.
Cell Network Auth	Specify the type of authentication to be used for connecting to the cellular carrier. This is to be configured only if your carrier has setup the APN with a user name and password. The authentication type specifies the security protocol to be used for sending your user name and password to the server to establish a connection. The supported protocols are PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol), with CHAP considered to be more secure.
Roaming	Enable or disable network roaming. Disabled by default.
SIM Card PIN Lock	Enable a lock so that the SIM card used by the cellular gateway cannot be used by anyone who does not have the PIN.
PIN # for SIM Card	The PIN number for the SIM card used by the gateway. May have up to 8 characters.

Cellular Modem Firmware

Update Firmware	Select this option to update firmware on the cellular modem. The Modem Firmware file and the PRI Carrier file will be transferred to the console manager using the method selected by the Load Firmware via option. Once the file have been transferred to the console manager, the console manager will initiate the firmware update on the gateway.
------------------------	---

3. To save your entries, click the **Apply** button. **Apply** makes the changes immediately and saves them so they will persist when the EMG is rebooted.

Cellular Modem Commands

Go to [Cellular Modem Commands](#) to view CLI commands which correspond to the web page entries described above.

IP Filter

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

The administrator uses the [Network > IP Filter](#) page to view, add, edit, delete, and map IP filters.

Warning: *IP filters configuration is a feature for advanced users. Adding and enabling IP filter sets incorrectly can disable access to your EMG unit.*

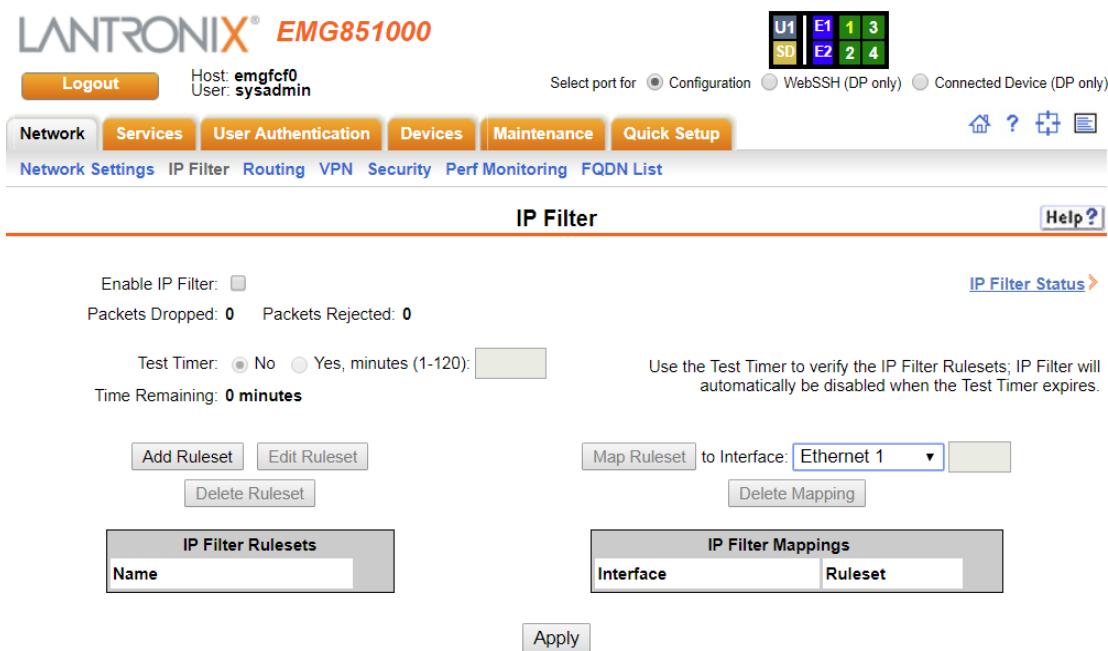
Viewing IP Filters

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

To view a list of IP filters:

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

Figure 6-5 Network > IP Filter



Mapping Rulesets

The administrator can assign an IP Filter Rule set to a network interface (Eth1 or Eth2), a modem connected to a device port, a USB modem, or an LTE modem, dialup modem, or Wi-Fi interface, if any of those connectivity modules are installed.

To map a ruleset to a network interface:

1. Click the **Network** tab and select the **IP Filter** option. The [Network > IP Filter](#) page displays.
2. Select the IP filter rule set to be mapped.

3. From the **Interface** drop-down list, select the desired network interface and click the **Map Ruleset** button. The Interface and rule set display in the IP Filter Mappings table.

To delete a mapping:

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

Enabling IP Filters

On the [Network > IP Filter](#) page, you can enable all filters or disable all filters.

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

To enable IP filters:

1. Enter the following:

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

Configuring IP Filters

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

Note: A configured filter has no effect until it is mapped to a network interface. See [Mapping Rulesets on page 79](#).

To add an IP filter:

1. On the [Network > IP Filter](#) page, click the **Add Ruleset** button. The following page displays:

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

LANTRONIX® EMG851000

Logout Host: emgcfc0 User: sysadmin Select port for Configuration WebSSH (DP only) Connected Device (DP only)

Network Services User Authentication Devices Maintenance Quick Setup

Network Settings IP Filter Routing VPN Security Perf Monitoring FQDN List

Help ?

Network - IP Filter Ruleset

Ruleset Name: Number of Rules: 1

Rule Parameters

IP Address(es): Subnet Mask: **Rules (in order of precedence)**

MAC Address: 0.0.0.0/0;All;;Drop

Protocol:

(or)

Port Range: Action: Drop Reject Accept

Generate rule to allow service:

DNS Telnet HTTP FTP
 RIP SNMP NIS SFTP
 NTP SMTP LDAP TFTP
 Syslog NFS RADIUS VPN
 SSH SMB/CIFS Kerberos LDP
 TACACS+ EMG Logging

[Back to IP Filter](#)

Rulesets can be added or updated on this page.

2. Enter the following:

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

Rule Parameters

IP Address(es)	Specify a single IP address to act as a filter. Example: 172.19.220.64 – this specific IP address only
Subnet Mask	Specify a subnet mask to determine how much of the address should apply to the filter. Example: 255.255.255.255 to specify the whole address should apply.
MAC Address	Specify a single MAC address to act as a filter. Example: 10:7d:1a:33:5c:e1
Protocol	From the drop-down list, select the type of protocol through which the filter will operate. The default setting is All .
Port Range	Enter a range of destination TCP or UDP port numbers to be tested. An entry is required for TCP, TCP New, TCP Established, and UDP, and is not allowed for other protocols. Separate multiple ports with commas. Separate ranges of ports by colons. Examples: <ul style="list-style-type: none">◆ 22 – filter on port 22 only◆ 23,64,80 – filter on ports 23, 64 and 80◆ 23:64,80,143:150 – filter on ports 23 through 64, port 80 and ports 143 through 150
Action	Select whether to Drop , Reject , or Allow communications for the specified IP address, subnet mask, protocol, and port range. Drop ignores the packet with no notification. Reject ignores the packet and sends back an error message. Allow permits the packet through the filter.
Clear	Click the Clear button to clear any Rule Parameter information set above.
Generate rule to allow service	You may wish to “punch holes” in your filter set for a particular protocol or service. For instance, if you have configured your NIS server and wish to create an opening in your filter set, select the NIS option and click the Add Rule button. This entry adds a new rule to your filter set using the NIS -configured IP address. Other services and protocols added automatically generate the necessary rule to allow their use.

3. Click the right arrow  button to add the new rule to the bottom of the Rules list box on the right. A maximum of 64 rules can be created for each ruleset.
4. To remove a rule from the filter set, highlight that line and click the left  arrow. The rule populates the rule definition fields, allowing you to make minor changes before reinserting the rule. To clear the definition fields, click the **Clear** button.
5. To change the order of priority of the rules in the list box, select the rule to move and use the up  or down  arrow buttons on the right side of the filter list box.
6. To save, click the **Apply** button. The new filter displays in the menu tree.

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

Updating an IP Filter

To update an IP filter rule set:

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

Deleting an IP Filter

To delete an IP filter rule set:

1. On the [Network > IP Filter](#) page, the administrator selects the IP filter rule set to be deleted and clicks the **Delete Ruleset** button.

IP Filter Commands

Go to [IP Filter Commands](#) to view CLI commands which correspond to the web page entries described above.

Routing

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

To configure routing settings:

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

Figure 6-7 Network > Routing

The screenshot shows the LANTRONIX EMG851000 web interface. The top navigation bar includes links for Logout, Host: emgfclf0, User: sysadmin, and tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The Network tab is selected, and the sub-tab Routing is active. The main content area is titled "Routing". It contains fields for "Enable RIP" (unchecked), "RIP Version" (radio buttons for 1, 2, and 1 and 2), and "Enable Static Routing" (unchecked). Below these are input fields for "IP Address", "Subnet Mask", and "Gateway". There are "Add/Edit Route" and "Delete Route" buttons. To the right, a note says "The Routing Table can be viewed with the [IP Routes Report](#)". A "Static Routes" table is shown with columns for No, IP Address, Subnet Mask, and Gateway. The table currently has four entries: U1 (IP 1.1.1.1, Mask 255.255.255.0, Gateway 1.1.1.2), E1 (IP 1.1.1.2, Mask 255.255.255.0, Gateway 1.1.1.1), E2 (IP 1.1.1.3, Mask 255.255.255.0, Gateway 1.1.1.1), and SD (IP 1.1.1.4, Mask 255.255.255.0, Gateway 1.1.1.1). The table has a header row with these column names.

2. Enter the following:

Dynamic Routing

Enable RIP	Select to enable Dynamic Routing Information Protocol (RIP) to assign routes automatically. Disabled by default.
RIP Version	Select the RIP version. The default is 2.

Static Routing

Enable Static Routing	Select to assign the routes manually. The system administrator usually provides the routes. Disabled by default. <ul style="list-style-type: none"> ◆ To add a static route, enter the IP Address, Subnet Mask, and Gateway for the route and click the Add/Edit Route button. The route displays in the Static Routes table. You can add up to 64 static routes. ◆ To edit a static route, select the radio button to the right of the route, change the IP Address, Subnet Mask, and Gateway fields as desired, and click the Add/Edit Route button. ◆ To delete a static route, select the radio button to the right of the route and click the Delete Route button.
-----------------------	---

3. Click the **Apply** button.

Note: *To display the routing table, status or specific report, see the section, [Status/Reports on page 298](#).*

Routing Commands

Go to [Routing Commands](#) to view CLI commands which correspond to the web page entries described above.

VPN Settings

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

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

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

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

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

Connections:

```

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

```

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

Sample ipsec.conf files are provided in the EMG online help files for a variety of tunnel configurations and peers. The strongSwan Wiki also provides a variety of [usable examples](#) and [sample configurations](#), in addition to interoperability recommendations.

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

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

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

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

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

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

To set up a VPN connection:

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

Figure 6-8 Network > VPN (1 of 2)

The screenshot shows the LANTRONIX EMG851000 web interface. The top navigation bar includes 'Logout', 'Host: emgfcf0', 'User: sysadmin', and tabs for 'Network', 'Services', 'User Authentication', 'Devices', 'Maintenance', and 'Quick Setup'. A 'VPN' tab is selected. The main content area is titled 'VPN' and contains the following fields:

- Enable VPN Tunnel:**
- Current Tunnel Status:** **Down**
- Name:**
- Remote Peer:**
- Remote Id:**
- Remote Subnet(s):**
- Remote Source IP:**
- Local IP Address:** [View Detailed Status](#)
- Local Id:** [View VPN Logs](#)
- Local Subnet(s):** [View EMG and Remote Peer RSA Public Key](#)
- Local Source IP:** [View X.509 Certificates](#)
- IKE Negotiation:** Main Mode Aggressive Mode
- IKE Version:**
- IKE Encryption:** **Authentication:** **DH Group:**
- ESP Encryption:** **Authentication:** **DH Group:**
- Authentication:** RSA Public Key
- RSA Public Key for Remote Peer:** [Upload File](#)

Figure 6-9 Network > VPN (2 of 2)

Pre-Shared Key: Retype Pre-Shared Key:

Certificate Authority for Remote Peer: [Upload File](#)

Certificate File for Remote Peer: [Upload File](#)

Certificate Authority for Local Peer: [Upload File](#)

Certificate File for Local Peer: [Upload File](#)

Key File for Local Peer: [Upload File](#)

SA Lifetime: 28800

XAUTH Client:

XAUTH Login:

XAUTH Password: Retype Password:

Cisco Unity:

Mode Config: Pull Push

Force Encapsulation:

Dead Peer Detection: No Yes, Delay: 30 seconds

Dead Peer Detection Timeout: 120

Dead Peer Detection Action: Hold ▾

Custom_ipsec.conf

Uploaded Configuration: [Upload File](#) [View Configuration](#)

[Download Configuration](#)

Apply

2. Enter the following:

Enable VPN Tunnel	Select to create a tunnel. Disabling this option will terminate any currently running tunnel. Note: The VPN peer that sends the first packet in tunnel bringup is the initiator or client; the VPN peer that listens for and responds to the first packet is the responder or server. In general, the responder / server side should be started before the initiator / client side. If it is desired to have the console manager VPN tunnel automatically reconnect when the remote peer disconnects and then reconnects, the console manager side of the tunnel should be started first so that it will act as a responder or server. If the console manager side of the tunnel is started after the remote peer, the console manager will act as a initiator / client, and may not automatically reconnect when the remote peer disconnects and is brought back up.
Name	The name assigned to the tunnel. Required to create a tunnel.
Remote Peer	The IP address or FQDN of the remote host's public network interface. The special value of any can be entered to signify an address to be filled in by automatic keying during negotiation. The console manager will act as a responder/server.
Remote Id	How the remote host should be identified for authentication. The Id is used to select the proper credentials for communicating with the remote host.

Remote Subnet(s)	<p>One or more allowed subnets behind the remote host, expressed in CIDR notation (IP address/mask bits). If multiple subnets are specified, the subnets should be separated by a comma. Up to 10 local subnets supported.</p> <p>Configured subnets of the peers may differ, the protocol narrows it to the greatest common subnet. In IKEv1, this may lead to problems with other implementations. Make sure to configure identical subnets in such configurations.</p> <p>If the remote subnet is not defined, it will be assumed that the remote end of the connection goes to the remote peer only.</p>
Remote Source IP	The internal source IP to use in a tunnel(Virtual IP). Currently the accepted values are config , CIDR Notation , IP Address Range or poolname . If the value is config on the responder side, the initiator must propose an address which is then echoed back. The supported address pools are expressed as CIDR notation and IP Address range as - or the use of an external IP address pool using poolname is the name of the IP address pool used for the lookup.
Local IP Address	The IP address of the EMG (local) side of the tunnel, specifically the public-network interface. If no IP address is given, the value %any will be used in ipsec.conf (this is the default), signifying an address to be filled in (by automatic keying) during negotiation. If the EMG initiates the connection setup the routing table will be queried to determine the correct local IP address. In case the EMG is responding to a connection setup then any IP address that is assigned to a local interface will be accepted.
Local Id	How the EMG should be identified for authentication. The Id is used by the remote host to select the proper credentials for communicating with the EMG.
Local Subnet(s)	<p>One or more subnets behind the EMG, expressed in CIDR notation (IP address/mask bits). If multiple subnets are specified, the subnets should be separated by a comma. Up to 10 local subnets supported.</p> <p>Configured subnets of the peers may differ, the protocol narrows it to the greatest common subnet. In IKEv1, this may lead to problems with other implementations. Make sure to configure identical subnets in such configurations.</p> <p>If the local subnet is not defined, it will be assumed that the local end of the connection goes to the console manager only.</p>
Local Source IP	The internal source IP to use in a tunnel (Virtual IP). Currently the accepted values are config4 , config6 or Valid IP Address . With config4 and config6 an address of the given address family will be requested explicitly. If an IP address is configured, it will be requested from the responder, which is free to respond with a different address.

IKE Negotiation	<p>The Internet Key Exchange (IKE) protocol is used to exchange security options between two hosts who want to communicate via IPSec. The first phase of the protocol authenticates the two hosts to each other and establishes the Internet Security Association Key Management Protocol Security Association (ISAKMP SA). The second phase of the protocol establishes the cryptographic parameters for protecting the data passed through the tunnel, which is the IPSec Security Association (IPSec SA). The IPSec SA can periodically be renegotiated to ensure security.</p> <p>The IKE protocol can use one of two modes: Main Mode, which provides identity protection and takes longer, or Aggressive Mode, which provides no identity protection but is quicker. With Aggressive Mode, there is no negotiation of which cryptographic parameters will be used; each side must give the correct cryptographic parameters in the initial package of the exchange, otherwise the exchange will fail. If Aggressive Mode is used, the IKE Encryption, IKE Authentication, and IKE DH Group must be specified.</p>
IKE Version	<p>IKE Version settings to be used. Currently the accepted values are IKEv1, IKEv2 and Any. Default is IKEv2. Any uses IKEv2 when initiating but will accept any protocol version while responding.</p> <p>It is recommended that any IKE Encryption or ESP Encryption parameters that are selected be supported by the IKE Version that is used. Refer to the list of IKEv1 and IKEv2 cipher suites for more information.</p>
IKE Encryption	<p>The type of encryption, 3DES, AES, AES192 or AES256, used for IKE negotiation. Any can be selected if the two sides can negotiate which type of encryption to use.</p> <p>Note: If IKE Encryption, Authentication and DH Group are set to Any, default cipher suite(s) will be used. If the console manager acts as an initiator, the tunnel will use a default IKE cipher of aes128-sha256-ecp256 (for IKEv1). For IKEv2 or when the console manager is the responder in tunnel initiation, it will propose a set of cipher suites and will accept the first supported proposal received from the peer.</p>
IKE Authentication	<p>The type of authentication, SHA2_256, SHA2_384, SHA2_512, SHA1, or MD5, used for IKE negotiation. Any can be selected if the two sides can negotiate which type of authentication to use.</p>
IKE DH Group	<p>The Diffie-Hellman Group, 2 (modp1024), 5 (modp1536), 14 (modp2048), 15 (modp3072), 16 (modp4096), 17 (modp6144), 18 (modp8192) or 19 (ecp256) can be used for IKE negotiation. Any can be selected if the two sides can negotiate which Diffie-Hellman Group to use.</p>

ESP Encryption	<p>The type of encryption, 3DES, AES, AES192 or AES256, used for encrypting the data sent through the tunnel. Any can be selected if the two sides can negotiate which type of encryption to use.</p> <p>Note: If <i>ESP Encryption, Authentication and DH Group</i> are set to Any, default cipher suite(s) will be used. If the console manager acts as an initiator, the tunnel will use a default ESP cipher of <code>aes128-sha256</code> (for IKEv1). For IKEv2 or when the console manager is the responder in tunnel initiation, it will propose a set of cipher suites and will accept the first supported proposal received from the peer. The proposal sent from the remote peer and the proposal used by the console manager can be viewed in the VPN logs. If there is no match between the two sets of proposals, the tunnel will fail with the message <code>no matching proposal found</code>, sending <code>NO_PROPOSAL_CHOSEN</code>. If a matching proposal is found, tunnel negotiation will proceed. Below is an example of no matching proposal in the log messages:</p> <pre>charon: 04 [CFG] received proposals: ESP:AES_CBC_128/HMAC_SHA2_256_128/ECP_256/ NO_EXT_SEQ charon: 04 [CFG] configured proposals: ESP:AES_CBC_128/AES_CBC_192/ AES_CBC_256/ HMAC_SHA2_256_128/ HMAC_SHA2_384_192/ HMAC_SHA2_512_256/ HMAC_SHA1_96/AES_XCBC_96/ NO_EXT_SE charon: 04 [IKE] no matching proposal found, sending NO_PROPOSAL_CHOSEN</pre>
ESP Authentication	<p>The type of authentication, SHA2_256, SHA2_384, SHA2_512, SHA2_256_96, SHA1, or MD5, used for authenticating data sent through the tunnel. Any can be selected if the two sides can negotiate which type of authentication to use.</p>
ESP DH Group	<p>The Diffie-Hellman Group, 2 (modp1024), 5 (modp1536), 14 (modp2048), 15 (modp3072), 16 (modp4096), 17 (modp6144), 18 (modp8192) or 19 (ecp256) can be used for the key exchange for data sent through the tunnel. Any can be selected if the two sides can negotiate which Diffie-Hellman Group to use.</p> <p>Note: PFS is automatically enabled by configuring <i>ESP Encryption</i> to use a <i>DH Group</i> (ESP Encryption without a DH Group will disable PFS); see <i>Perfect Forward Secrecy</i> below.</p>

Authentication	<p>The type of authentication used by the host on each side of the VPN tunnel to verify the identity of the other host.</p> <ul style="list-style-type: none"> ◆ For RSA Public Key, each host generates a RSA public-private key pair, and shares its public key with the remote host. The RSA Public Key for the EMG (which has 4096 bits) can be viewed at either the web or CLI. ◆ For Pre-Shared Key, each host enters the same passphrase to be used for authentication. ◆ For X.509 Certificate, each host is configured with a Certificate Authority certificate along with a X.509 certificate with a corresponding private key, and shares the X.509 certificate with the remote host. <p>Before using RSA Public Key authentication, select Generate EMG RSA Key to generate the EMG's RSA public/private key pair. This RSA key can be regenerated at any time.</p> <p>Note: <i>strongSwan does not support IKEv1 aggressive mode with Pre-Shared Key authorization without XAUTH enabled. If a tunnel is initiated with this configuration the log message Aggressive Mode PSK disabled for security reasons will be displayed, and a tunnel will not be initiated. It is possible to override this behavior, but it is not recommended.</i></p>
RSA Public Key for Remote Peer	<p>If RSA Public Key is selected for authentication, the remote peer's public key can be uploaded or deleted. If a public key has been uploaded this field will display key installed. The peer RSA public key must be in Privacy Enhanced Mail (PEM) format, e.g.:</p> <pre>-----BEGIN PUBLIC KEY----- (certificate in base64 encoding) -----END PUBLIC KEY-----</pre>
Pre-Shared Key	<p>If Pre-Shared Key is selected for authentication, enter the key.</p>
Retype Pre-Shared Key	<p>If Pre-Shared Key is selected for authentication, re-enter the key.</p>
Certificate Authority for Remote Peer	<p>A certificate can be uploaded to the EMG unit for peer authentication. The certificate for the remote peer is used to authenticate the EMG to the remote peer, and at a minimum contains the public certificate file of the remote peer. The certificate may also contain a Certificate Authority file; if the Certificate Authority file is omitted, the EMG may display "issuer cacert not found" and "X.509 certificate rejected" messages, but still authenticate. The Certificate Authority file and public certificate File must be in PEM format, e.g.:</p>
Certificate File for Remote Peer	<pre>-----BEGIN CERTIFICATE----- (certificate in base64 encoding) -----END CERTIFICATE-----</pre>

Certificate Authority for Local Peer	A certificate can be uploaded to the EMG unit for peer authentication. The certificate for the local peer is used to authenticate any remote peer to the EMG, and contains a Certificate Authority file, a public certificate file, and a private key file. The public certificate file can be shared with any remote peer for authentication. The Certificate Authority and public certificate file must be in PEM format, e.g.:
Certificate File for Local Peer	-----BEGIN CERTIFICATE----- (certificate in base64 encoding) -----END CERTIFICATE-----
Key File for Local Peer	The key file must be in RSA private key file (PKCS#1) format, eg: -----BEGIN RSA PRIVATE KEY----- (private key in base64 encoding) -----END RSA PRIVATE KEY-----
SA Lifetime	How long a particular instance of a connection should last, from successful negotiation to expiry, in seconds. Normally, the connection is renegotiated (via the keying channel) before it expires. The formula for how frequently rekeying (renegotiation) is done is: $\text{rekeytime} = \text{lifetime} - (\text{margintime} + \text{random}(0, \text{margintime} * \text{rekeyfuzz}))$ where the default margintime is 9m (or 540 seconds) and the default rekeyfuzz is 100%. For example, if the SA Lifetime is set to 3600 seconds (1 hour), how often the tunnel is rekeyed is calculated as: $\text{rekeytime minimum} = 1\text{h} - (9\text{m} + 9\text{m}) = 42\text{m}$ $\text{rekeytime maximum} = 1\text{h} - (9\text{m} + 0\text{m}) = 51\text{m}$ So the rekeying time will vary between 42 minutes and 51 minutes. It is recommended that the SA Lifetime be set greater than 540 seconds; any values less than 540 seconds may require adjustments to the margintime and rekeyfuzz values (which can be set with a custom ipsec.conf file). Some peer devices (Cisco, etc) may require that the SA Lifetime be set to a minimum of 3600 seconds in order for the VPN tunnel to come up and rekeying to function properly. For more information see the strongSwan Expiry documentation.
XAUTH Client	If this is enabled, the EMG will send authentication credentials to the remote host if they are requested. XAUTH, or Extended Authentication, can be used as an additional security measure on top of the Pre-Shared Key or RSA Public Key. This is typically used with Cisco peers, where the Cisco peer is acting as an XAUTH server.
XAUTH Login (Client)	If XAUTH Client is enabled, this is the login used for authentication.
XAUTH Password/Retype Password	If XAUTH Client is enabled, this is the password used for authentication.
Cisco Unity	If enabled, sends the Cisco Unity vendor ID payload (IKEv1 only), indicating that the EMG is acting as a Cisco Unity compliant peer. This indicates to the remote peer that Mode Config is supported (an IKE configuration method that is widely adopted, documented here).

Mode Config	In remote access scenarios, it is highly desirable to be able to push configuration information such as the private IP address, a DNS server's IP address, and so forth, to the client. This option defines which mode is used: pull where the config is pulled from the peer (the default), or push where the config is pushed to the peer. Push mode is not supported with IKEv2.
Force Encapsulation	In some cases, for example when ESP packets are filtered or when a broken IPsec peer does not properly recognise NAT, it can be useful to force RFC-3948 encapsulation.
Dead Peer Detection	Sets the delay (in seconds) between Dead Peer Detection (RFC 3706) keepalives (R_U_THERE, R_U_THERE_ACK) that are sent for the tunnel (default 30 seconds). Dead Peer Detection can also be disabled.
Dead Peer Detection Timeout	Sets the length of time (in seconds) the EMG will idle without hearing either an R_U_THERE poll from the peer, or an R_U_THERE_ACK reply. The default is 120 seconds. After this period has elapsed with no response and no traffic, the EMG will declare the peer dead, remove the Security Association (SA), and perform the action defined by Dead Peer Detection Action .
Dead Peer Detection Action	When a Dead Peer Detection enabled peer is declared dead, the action that should be taken. Hold (the default) means the tunnel will be put into a hold status. Clear means the Security Association (SA) will be cleared. Restart means the SA will immediately be renegotiated.

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

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

More Actions on the VPN page:

- ◆ To see details of the VPN tunnel connection, including the cryptographic algorithms used, select the **View Detailed Status** link.
- ◆ To see the last 200 lines of the logs associated with the VPN tunnel, select the **View VPN Logs** link.
- ◆ To see the RSA public key for the EMG (required for configuring the remote host if RSA Public Keys are being used), and the RSA public key for the remote peer, select the **View console manager and Remote Peer RSA Public Key** link.
- ◆ To see the X.509 Certificates for the local peer and the remote peer, select the **View X.509 Certificates** link.

Sample ipsec.conf Files

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

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

Cisco Pre-Shared Key / XAUTH / MODECFG / IKEv1

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

Console manager configuration

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

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

Cisco ASA5525x Pre-Shared Key / IKEv1

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

EMG configuration

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

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

Cisco configuration

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

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

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

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

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

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

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

```

crypto ipsec security-association pmtu-aging infinite

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

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

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

```

Cisco ASA5525x Pre-Shared Key / IKEv2

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

Console manager configuration

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

```

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

```

Cisco configuration

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

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

object-group network local-network
    network-object 192.168.3.0 255.255.255.0
    network-object 192.168.3.250 255.255.255.255
object-group network remote-network
    network-object 192.168.0.0 255.255.255.0
    network-object 192.168.0.222 255.255.255.255

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

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

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

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

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

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

Cisco ISR 2921 Pre-Shared Key / XAUTH / IKEv2

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

Console manager configuration

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

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

Cisco configuration

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

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

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

```
group 2

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

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

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

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

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

VPN Commands

Go to [VPN Commands](#) to view CLI commands which correspond to the web page entries described above.

Security

Note: FIPS 140-2 standard is not supported in the current release.

The EMG supports a security mode that complies with the FIPS 140-2 standard. FIPS (Federal Information Processing Standard) 140-2 is a security standard developed by the United States federal government that defines rules, regulations and standards for the use of encryption and cryptographic services. The National Institute of Standards and Technology (NIST) maintains the documents related to FIPS at: <http://csrc.nist.gov/publications/PubsFIPS.html>

FIPS 140-2 defines four security levels, Level 1 through Level 4. The EMG unit is FIPS certified at Level 1.

To enable FIPS mode, the **Network -> Security -> FIPS Mode** flag needs to be enabled and the EMG unit rebooted. Each time the EMG unit is booted in FIPS mode, it will perform a power up self test to verify the integrity of the EMG unit's cryptographic module. If there are any issues with the integrity of the cryptographic module, FIPS mode will be disabled and the EMG unit will be rebooted into non-FIPS mode.

When the EMG unit is running in FIPS mode, the following protocols are supported: TLS 1.0, TLS 1.1, TLS 1.2, and SSH v2. TLS 1.0 and TLS 1.1 are disabled by default for security reasons.

For SSL, the EMG unit will support the following cipher suites:

- ◆ AES128-SHA
- ◆ AES128-SHA256
- ◆ AES128-GCM-SHA256
- ◆ AES256-SHA
- ◆ AES256-SHA256
- ◆ AES256-GCM-SHA384

* AES signifies Advanced Encryption Scheme

SSL/secure certificates imported for use with the web server or LDAP authentication must use either the SHA1 or SHA2 hash with a RSA public key of 1024, 2048 or 3072 bits.

For SSH, the EMG unit will support the following cipher suites:

- ◆ AEAD-AES-128-GCM-SSH
- ◆ AEAD-AES-256-GCM-SSH
- ◆ AES128-CTR
- ◆ AES256-CTR
- ◆ AES192-CTR

* AEAD signifies Authenticated Encryption with Additional Data

SSH Keys imported for use with SSH authentication must use a RSA public key of 1024, 2048 or 3072 bits. SSH Keys exported by the EMG must use a RSA public key of 2048 or 3072 bits.

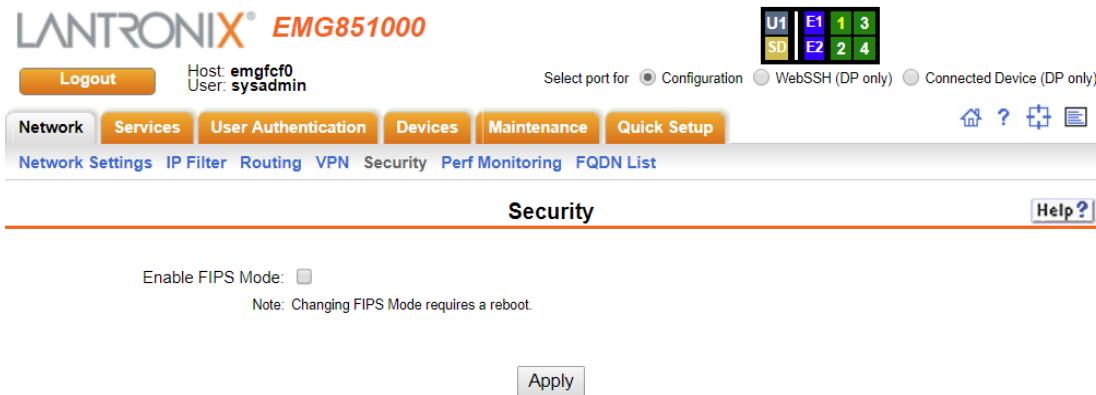
When the EMG unit is running in FIPS mode, the following protocols/functions will not be supported: NIS, Kerberos, RADIUS, TACACS+, Telnet/WebTelnet, WebSSH, IPSec/VPN, SSH v1, FTP, PPP, CIFS/Samba, TCP, UDP, unencrypted LDAP, and SNMP. If any of these protocols/functions are enabled prior to enabling FIPS mode, they will be automatically disabled.

LDAP authentication must be configured with the following:

- ◆ StartTLS encryption (SSL encryption over port 636 is not supported)
- ◆ A SSL/secure certificate
- ◆ Either Bind with Login or a Bind Name and Password

Note: In FIPS mode, passphrases are not supported for SSH keys and SSL certificates.

Figure 6-10 Network > Security



To enable FIPS:

Note: The SSH client keyboard-interactive authentication type is not supported while the EMG unit is in FIPS mode.

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

To disable FIPS:

1. Uncheck the **Enable FIPS Mode** check box on the **Networks > Security** page.
2. Click **Apply**. The EMG unit will need to be rebooted for this change to take effect. When rebooted after disabling FIPS mode, information about processes running in FIPS mode will no longer display on the Security page.

Performance Monitoring

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

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

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

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

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

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

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

To manage or view status for a Performance Monitoring probe:

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

Figure 6-11 Network > Perf Monitoring

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

U1 E1 1 3
SD E2 2 4

Network Services User Authentication Devices Maintenance Quick Setup

Network Settings IP Filter Routing VPN Security Perf Monitoring FQDN List

Performance Monitoring Help ?

Number of operations kept for each probe: 50

Repository for operations: Local

UDP Jitter Responder: UDP Echo Responder: UDP Port:

TCP Connect Responder: TCP Port:

Apply

Warning: high resolution timers are disabled; high resolution timers are required for accurate Performance Monitoring results.

Refresh > Add Probe > Operations > Latest RTT Results > Latest Accumulated Statistics >

0 probe(s)							State: <input type="button" value="Restart"/>	<input type="button" value="Edit Probe"/>	<input type="button" value="Delete Probe"/>
Id	Name	State	Start Time First Op	Finish Time Last Op	Error	Operations Comp/Total			

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

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

UDP Echo Responder	Starts the UDP Echo responder on the port configured in UDP Port to reply to UDP echo packets. The EMG UDP Echo responder supports one UDP echo sender. When the UDP Echo responder is enabled, the EMG will verify that the responder UDP port is not being used by any other EMG processes, including port 1967 which is reserved for the UDP Jitter responder.
TCP Connect Responder	Starts the TCP Connect responder on the port configured in TCP Port to reply to TCP connect requests. The EMG TCP Connect responder supports one TCP connect sender. When the TCP Connect responder is enabled, the EMG will verify that the responder TCP port is not being used by any other EMG processes.

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

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

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

Id	Unique identifier for the probe.
Name	Name assigned to the probe.
State	The current state of the probe: Complete if all operations have been run, or Running if there are still operations that need to be run.
Start Time First Op	The date and time that the first operation started.
Finish Time Last Op	The date time that the most recently completed operation finished.
Error	Any errors reported by the probe: <ul style="list-style-type: none"> ◆ NMT: the current repository is an external source, but the USB thumb drive or SD card is not mounted ◆ NDR: the repository directory for the probe does not exist ◆ OPF: failed to open an operation data file ◆ SCT: error initializing a socket ◆ CFG: error retrieving probe configuration ◆ EXP: probe start time has expired
Operations Comp/ Total	The number of operations that have been completed and the total number of operations that will be run.

Performance Monitoring - Add/Edit Probe

The [Performance Monitoring - Add/Edit Probe](#) web page allows a user to add a new Performance Monitoring probe or edit an existing Performance Monitoring probe.

To add a new probe or edit an existing probe:

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

Figure 6-12 Performance Monitoring - Add/Edit Probe

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The Network tab is selected. Below the navigation bar, there is a sub-navigation bar with links for Network Settings, IP Filter, Routing, VPN, Security, Perf Monitoring, and FQDN List. The Perf Monitoring link is selected. The main content area is titled "Performance Monitoring - Add/Edit Probe". It contains fields for "Probe Type" (dropdown menu), "Name" (text input), "Number of Operations" (text input), "Frequency between Operations" (text input), "Number of Packets" (text input), "Interval between Packets" (text input), "Timeout" (text input), "UDP Jitter VoIP Codec" (dropdown menu), and "ICMP Ethernet Interface" (dropdown menu). There are also fields for "Start Time" (radio buttons for "Now", "At date/time", or "After waiting", with date and time dropdowns), "Destination Host" (text input), "Destination Port" (text input), "Precision" (radio buttons for "milliseconds" or "microseconds"), "Data Size" (text input), "Verify Data" (checkbox), "Type of Service (TOS)" (text input), and "DNS Name Server IP Address" (text input). At the bottom of the form are "Apply" and "Help?" buttons.

3. Modify the probe settings:

Probe Type	Select from one of the available probe types: <ul style="list-style-type: none"> ◆ DNS Lookup - Performs a DNS lookup on the hostname specified in the Destination Host using the Name Server. By default port 53 is always used as the Destination Port. ◆ HTTP Get - Performs an HTTP Get to the home (root) of the web server at the Destination Host and Destination Port. ◆ ICMP Echo - Sends ICMP Echo (ping) packets to the Destination Host. ◆ TCP Connect - Performs a TCP Connection to the Destination Host and Destination Port. ◆ UDP Echo - Sends UDP Echo packets to the Destination Host and Destination Port. ◆ UDP Jitter - Sends UDP jitter packets using a simplified version of the Cisco IP SLA v2 (Engine II) protocol to the Destination Host and Destination Port. ◆ UDP Jitter VoIP - Sends UDP jitter packets configured to simulate Voice over IP network traffic (VoIP) using a simplified version of the Cisco IP SLA v2 (Engine II) protocol to the Destination Host and Destination Port.
Name	Probe name, up to 40 characters long. Valid characters are letters, numbers, dashes (-), periods and underscores (_).
Number of Operations	Number of operations to perform for the probe. Probes can perform a specific number of operations. The valid range is 1 - 1000, and the default is 100.
Frequency between Operations	Time between probe operations, in seconds. The valid range is 5 - 3600 seconds, and the default is 60 seconds.
Number of Packets	Number of packets to send for each probe. For DNS Lookup probes, this is the number of lookups to perform. For HTTP Get probes, this is the number of HTTP Gets to perform. For TCP Connect probes, this is the number of TCP connections to perform. The valid range is 1 - 1000 for the Local repository and 1 - 2000 for a USB or SD card repository. The default is 10 packets.
Interval between Packets	Interval between packets in milliseconds. The valid range is 10 - 5000 milliseconds, and the default is 500 milliseconds. For HTTP Get, DNS Lookup and TCP Connect probes, the timeout must be less than the interval due to a new socket being created and destroyed for each packet.
Start Time	Time to start the probe: Now starts the probe immediately; At date/time will start the probe at the specified date and time in the future; After waiting will start the probe after waiting a period of time that is less than 24 hours. When the EMG is rebooted, the probe will start according to the Start Time settings: (a) immediately if it is set to Now , (b) at a date and time in the future if it is set to At date/time and the date and time is in the future, (c) after waiting a period of time if it is set to After waiting .
Destination Host	The hostname or IP address to send packets to. For DNS Lookup probes this is the hostname to lookup.
Destination Port	The TCP or UDP port to send packets to. For ICMP probes, the port setting is not used. For DNS Lookup probes, the destination port is always port 53. Port 1967 is reserved for the UDP jitter responder. The valid range is 1 - 65535.
Precision	The precision to view results in - milliseconds (the default) or microseconds. Jitter results are always displayed in milliseconds.

Data Size	<p>The size in bytes to use for the payload portion of the packet - this size is in addition to the IPv4 header and the TCP, UDP or ICMP header. Any additional space in the packet that is not used by the protocol will be padded with random data that can be used for data verification (see below).</p> <p>This parameter is only supported for ICMP Echo, TCP Connect, UDP Echo, UDP Jitter, and UDP Jitter VoIP probes. The maximum payload for any probe is 1460 bytes. The minimum payload size for probes is: UDP Jitter VoIP G.729a codec probes - 32 bytes; all other UDP Jitter probes - 64 bytes; ICMP Echo probes - 18 bytes; TCP Connect probes - 1 bytes; UDP Echo probes - 4 bytes.</p> <p>If no data size is specified (e.g., it is set to zero), a default payload size will be used for the probes as follows:</p> <ul style="list-style-type: none"> ◆ ICMP Echo - 56 bytes ◆ UDP Jitter VoIP G.729A - 32 bytes ◆ UDP Jitter (all others) - 64 bytes ◆ TCP Connect and UDP Echo - 256 bytes
Verify Data	If enabled, indicates that the EMG should verify if there is data corruption in the reply packets. This parameter is only supported for ICMP Echo, UDP Echo, UDP Jitter, and UDP Jitter VoIP probes.
Timeout	How long the EMG will wait for a packet to arrive, in milliseconds. If the packet arrives after the timeout it will be considered a Late Arrival error (see Error Conditions Detected by Probes). The valid range is 10 - 1000, and the default is 200 msec.
UDP Jitter VoIP Codec	<p>For UDP Jitter VoIP probes, the codec to simulate. The following codecs are available:</p> <ul style="list-style-type: none"> ◆ G.729A - 32 byte packets sent 20 msec apart, 1000 packets per operation, 60 seconds between operations ◆ G.711 A-law - 172 byte packets sent 20 msec apart, 1000 packets per operation, 60 seconds between operations ◆ G.711 mu-law - 172 byte packets sent 20 msec apart, 1000 packets per operation, 60 seconds between operations <p>The default values for the VoIP probes can be overridden to use different packet sizes, intervals, etc.</p>
ICMP Ethernet Interface	For ICMP Echo probes, which Ethernet interface can be used for the probe: both interfaces, Ethernet Port 1, or Ethernet Port 2.
TOS (Type of Service)	Sets the IPv4 Type of Service field in the IPv4 header. This is available for UDP Jitter and UDP Jitter VoIP probes only. The range is 0 - 255, and the default value is 0.
DNS Name Server IP Address	For DNS Lookup probes, the IP address of the DNS name server to use for lookups.

4. Click the **Apply** button.

Performance Monitoring - Results

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

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

Round Trip Times

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

```
Round Trip Times (RTT)
Probe 1/ICMP, operation icmp_190709_154146.dat:
Pkt  Time          RT Time      Result
===
1  19/07/09 15:41:46.469  0.717 msec  OK
2  19/07/09 15:41:46.972  0.556 msec  OK
3  19/07/09 15:41:47.482  0.443 msec  OK
4  19/07/09 15:41:47.992  0.423 msec  OK
5  19/07/09 15:41:48.501  0.472 msec  OK
6  19/07/09 15:41:49.011  0.439 msec  OK
7  19/07/09 15:41:49.521  0.444 msec  OK
8  19/07/09 15:41:50.031  0.375 msec  OK
9  19/07/09 15:41:50.541  0.427 msec  OK
10 19/07/09 15:41:51.051  0.442 msec  OK
```

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

```
Round Trip Times (RTT)
Probe 4/test2-udp-jitter, operation udpjitter_190730_231540.dat:
Pkt  Time          Src To Dst Time  Dst To Src Time  Result
1  19/07/30 23:15:41.707  0.347 msec  0.043 msec  OK
2  19/07/30 23:15:42.208  0.327 msec  0.046 msec  OK
3  19/07/30 23:15:42.708  0.318 msec  0.041 msec  OK
4  19/07/30 23:15:43.209  0.313 msec  0.037 msec  OK
5  19/07/30 23:15:43.710  0.312 msec  0.043 msec  OK
6  19/07/30 23:15:44.210  0.350 msec  0.042 msec  OK
7  19/07/30 23:15:44.711  0.342 msec  0.075 msec  OK
8  19/07/30 23:15:45.212  0.342 msec  0.035 msec  OK
9  19/07/30 23:15:45.712  0.339 msec  0.069 msec  Late Arrival
10 19/07/30 23:15:46.213  0.327 msec  0.028 msec  OK
```

Accumulated Statistics

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

```
Latest Accumulated Statistics
Probe 1/ICMP, operation icmp_190709_154501.dat:
Operation Type:
    ICMP Echo to 172.19.100.17, Ethernet Port: both
    10 packets sent 500 ms apart, timeout 200 ms
Operation Start Time: 19/07/09 15:45:01.579
Last Packet RTT: 0.560 msec
Round Trip Time Results:
    Number of RTT: 10
    RTT Min/Avg/Max: 0.426/0.460/0.560 msec
Number of Successes: 10
Number of Errors: 0
    Lost Packet: 0 (0%)
    Out of Sequence: 0
    Late Arrival: 0
    Miscellaneous Error: 0
```

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

```
Latest Accumulated Statistics
Probe 2/UDP-Jitter, operation udpjitter_190709_154422.dat:
Operation Type:
    UDP Jitter to 172.19.100.17:60606
    10 packets sent 500 ms apart, timeout 200 ms
Operation Start Time: 19/07/09 15:44:22.480
Last Packet RTT: 3249468.402 msec
Round Trip Time Results:
    Number of RTT: 10
    RTT Min/Avg/Max: 3249468.251/3249468.304/3249468.402 msec
One-way Latency Results:
    Number of samples: 10
    Source to Destination Min/Avg/Max: 3772218.020/3772218.074/
    3772218.122 msec
    Destination to Source Min/Avg/Max: 3772217.466/3772217.526/
    3772217.578 msec
Jitter, Source to Destination:
    Number of Samples: 9
    Positive and Negative Min/Avg/Max: 0/0/0 msec
    Positive Min/Avg/Max: 0/0/0 msec
    Positive Number Of/Sum of All/Sum of All Squared: 0/0/0 msec
    Negative Min/Avg/Max: 0/0/0 msec
    Negative Number Of/Sum of All/Sum of All Squared: 0/0/0 msec
Jitter, Destination to Source:
    Number of Samples: 9
    Positive and Negative Min/Avg/Max: 0/0/0 msec
```

```

Positive Min/Avg/Max: 0/0/0 msec
Positive Number Of/Sum of All/Sum of All Squared: 0/0/0 msec
Negative Min/Avg/Max: 0/0/0 msec
Negative Number Of/Sum of All/Sum of All Squared: 0/0/0 msec
Number of Successes: 10
Number of Errors: 0
  Lost Packet: 0 (0%)
  Out of Sequence: 0
  Late Arrival: 0
  Miscellaneous Error: 0

```

Table 6-13 Error Conditions Detected by Probes

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

Error Condition	Description
Timeout	A response was never received for the packet. These packets are listed as Lost Packets under the accumulated statistics.
Late Arrival	A response was received for a packet, but the response was received after the timeout configured for the probe. The EMG will wait at most 2 times the probe's timeout for late arrival packets. The RTT results will be included in the accumulated statistics.
Not Connected	A packet could not be sent because the connection to the destination host could not be established, or because the attempt to send the packet failed.
Sequence Error	A packet response was received with an unexpected sequence number. Possible reasons are: a duplicate packet was received, a response was received after it timed out, a corrupted packet was received and was not detected.
Verify Data Error	A response was received for a packet with payload data that does not match the expected data.
DNS Server Timeout	A DNS lookup could not be completed because the EMG could not connect to the DNS name server.
DNS Lookup Error	A DNS lookup failed - the requested hostname could not be resolved. This is not considered a protocol error, but rather an expected result, depending on the hostname being resolved. The RTT results will be included in the accumulated statistics.
TCP Connect Timeout	A TCP connect could not be completed because a connection to the TCP server could not be established.
HTTP Transaction Timeout	An HTTP Get that failed because no response was received from the HTTP server before the timeout expired.
HTTP Error	An HTTP Get succeeded, but the HTTP content (base page) that was downloaded had errors: missing "HTTP/" header string, missing "Connection: close" string, or response has an HTTP error code (the code was not 200/OK). This is not considered a protocol error. The RTT results will be included in the accumulated statistics.
Generic Error	Any error that does fall into any of the above error conditions.

To view results for a Performance Monitoring probe:

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

Figure 6-14 Performance Monitoring - Operations

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. Below the navigation bar, there are links for Network Settings, IP Filter, Routing, VPN, Security, Perf Monitoring, and FQDN List. The main content area is titled "Performance Monitoring - Operations". A table shows "1 operation(s)" with a single row: Set Number 4115 and Set Name icmp_190709_154146. Navigation links at the top of the content area include Refresh, RTT Results, and Accumulated Statistics.

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

Refresh	Refreshes the information on the Performance Monitoring - Operations page.
RTT Results	Displays the round trip time (RTT) results for the selected operation in a separate window. The results show: <ul style="list-style-type: none"> the time that the packet was sent, the total round trip time for non-jitter probes or the source to destination time and destination to source time for jitter probes, and the status for the packet - OK/successful or an error condition. For more information, see Round Trip Times or Error Conditions Detected by Probes .
Accumulated Results	Displays the accumulated statistics for the selected operation in a separate window. The results show parameters used for the selected operation, and the minimum, average and maximum round trip times for all probes. For jitter probes, the results show minimum, average and maximum one way latency times, as well as jitter results for source to destination and destination to source. For a probes, a summary of lost packets and error conditions is displayed.

Performance Monitoring Commands

Go to [Performance Monitoring Commands](#) to view CLI commands which correspond to the web page entries described above.

FQDN List

Use the FQDN List (FQDN stands for fully qualified domain name) to add static hostname entries to the local hosts table so that the EMG can resolve hostnames that are not resolved via DNS.

To add/edit/delete hosts:

1. Click the **Network** tab and select **FQDN List**. The following page appears:

Figure 6-15 FQDN List

The screenshot shows the LANTRONIX EMG85100 web interface. At the top, it displays 'LANTRONIX® EMG85100' and the host information 'Host: emgfcf0 User: sysadmin'. Below the host information, there are tabs for Network, Services, User Authentication, Devices, Maintenance, and Quick Setup. The 'Network' tab is selected. Under the Network tab, there are sub-links: Network Settings, IP Filter, Routing, VPN, Security, Perf Monitoring, and FQDN List. The 'FQDN List' link is highlighted. The main content area is titled 'FQDN List'. It contains two input fields: 'IP Address:' and 'FQDN:', both with empty text boxes. Below these fields are two buttons: 'Add/Edit Hosts' and 'Delete Host'. To the right of these buttons is a table titled 'Hosts/FQDN List' with three columns: 'No', 'IP Address', and 'FQDN'. The table currently has no data. At the bottom of the form is an 'Apply' button.

2. Enter the following information:

- To add a Host, enter the **IP address**, **FQDN**, and click **Add/Edit Hosts**. The IP address and hostname displays in the Hosts/FQDN List. You may add up to 15 hosts.
- To edit a Host entry, select the radio button next to the host in the Hosts/FQDN List, change the IP address or FQDN fields as desired, and click **Add/Edit Hosts**.
- To delete a Host, select the radio button next to the host in the Hosts/FQDN List and click **Delete Host**.

3. Click **Apply**.

7: Services

System Logging and Other Services

Use the **Services** tab to:

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

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

- ◆ Identify a Simple Mail Transfer Protocol (SMTP) server.
- ◆ Configure an audit log.
- ◆ View the status of and manage the EMGs on the Secure Lantronix network.
- ◆ Set the date and time.
- ◆ Configure NFS and CIFS shares.
- ◆ Configure the web server.

SSH/Telnet/Logging

To configure SSH, Telnet, and Logging settings:

1. Click the **Services** tab and select the **SSH/Telnet/Logging** option. The following page displays.

Figure 7-1 Services > SSH/Telnet/Logging

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

Network Services User Authentication Devices Maintenance Quick Setup

SSH/Telnet/Logging SNMP NFS/CIFS Secure Lantronix Network Date & Time Web Server ConsoleFlow

SSH/Telnet/Logging

System Logging

Network Level: Warning
 Services: Warning
 Authentication: Warning
 Device Ports: Warning
 Diagnostics: Warning
 General: Warning

Remote Server #1:
 #2:
 RPM Log Size: 20 Kbytes
 Other Log Size: 200 Kbytes

Audit Log

Enable Log:
 Size: 50 Kbytes
 Include CLI Commands:
 Include in System Log:

SMTP

Server:
 Sender: donotreply@\$host.\$domain
 Note: '\$host' and '\$domain' will be substituted with hostname and domain.

SSH

Enable Logins: Web SSH:
 Timeout: No Yes: 0 minutes
 Timeout Data Direction: Both Directions
 SSH Port: 22
 DSA Keys:
 Use only SHA2 and Higher:

Telnet

Enable Logins: Web Telnet:
 Timeout: No Yes: 0 minutes
 Timeout Data Direction: Both Directions
 Escape Sequence: \x1bT
 Outgoing Telnet:

Web SSH/Web Telnet Settings

Terminal Buffer Size: 250

Apply

2. Enter the following settings:

System Logging

Alert Levels	Select one of the following alert levels from the drop-down list for each message category: <ul style="list-style-type: none"> ◆ Off: Disables this type of logging. ◆ Error: Saves messages that are output because of an error. ◆ Warning: Saves message output from a condition that may be cause for concern, in addition to error messages. This is the default for all message types. ◆ Info: Saves informative message, in addition to warning and error messages. ◆ Debug: Saves extraneous detail that may be helpful in tracking down a problem, in addition to information, warning, and error messages.
Network Level	Messages concerning the network activity, for example about Ethernet and routing.
Services	Messages concerning services such as SNMP and SMTP.
Authentication	Messages concerning user authentication.
Device Ports	Messages concerning device ports and connections.

Diagnostics	Messages concerning system status and problems.
General	Any message not in the categories above.
Remote Servers (#1 and #2)	<p>The IPv4 or IPv6 address of the remote server(s) where system logs are stored. The system log is always saved to local EMG storage. It is retained through EMG unit reboots for files up to Other Log Size (see below). Saving the system log to a server that supports remote logging services (see RFC 3164) allows the administrator to save the complete system log history.</p> <p>Note: If the EMG is unable resolve the Remote Server hostnames or contact the Remote Servers to send syslog messages, the syslog messages that cannot be sent to a Remote Server may appear on the EMG console port.</p>
RPM Log Size	The maximum size in Kbytes that RPM logs can grow to before they are pruned. When the file is pruned, it will be pruned to 50% of the RPM Log Size.
Other Log Size	The maximum size in Kbytes that all logs other than the RPM logs can grow to before they are pruned. When the file is pruned, it will be pruned to 50% of the Other Log Size.

Audit Log

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

SMTP

Server	IP address of your network's Simple Mail Transfer Protocol (SMTP) relay server. If an SMTP server is not specified, the EMG module will attempt to look up the MX record for the domain in the destination email addresses of outgoing emails.
Sender	The email address of the sender of outgoing emails. The strings "\$host" and "\$domain" can be part of the email address - they will be substituted with the actual hostname and domain. The default is donotreply@\$host.\$domain.

SSH

Enable Logins	<p>Enables or disables SSH logins to the EMG unit to allow users to access the CLI using SSH. Enabled by default.</p> <p>This setting does not control SSH access to individual device ports. (See Device Ports - Settings (on page 152) for information on enabling SSH access to individual ports.)</p> <p>Most system administrators enable SSH logins, which is the preferred method of accessing the system.</p>
Web SSH	Enables or disables the ability to access the EMG command line interface or device ports (connect direct) through the Web SSH window. Disabled by default.
Timeout	If you enable SSH logins, you can cause an idle connection to disconnect after a specified number of minutes. Select Yes and enter a value of from 1 to 30 minutes.

Timeout Data Direction	If idle connection timeouts are enabled, this setting indicates the direction of data used to determine if the connection has timed out. Select the type of data direction: <ul style="list-style-type: none"> ◆ Both Directions ◆ Incoming Network ◆ Outgoing Network
SSH Port	Allows you to change the SSH login port to a different value in the range of 1 - 65535. The default is 22. Use of ports other than 22 that are less than 1025 is not recommended.
DSA Keys	Enables or disables support for DSA keys for incoming and outgoing connections for the EMG unit. Any imported or exported DSA keys will be retained but will not be visible on the web or the CLI. Enabled by default.
Use only SHA2 and Higher	Enables or disables support for only Secure Hash Algorithm (SHA2) and higher ciphers for incoming connections for the EMG unit. Disabled by default. Enabling this option will also disable MACs with tag sizes lower than 128 bits (e.g. umac-64-etm@openssh.com and umac-64@openssh.com).

Telnet

Enable Logins	Enables or disables Telnet logins to the EMG unit to allow users to access the CLI using Telnet. Disabled by default. This setting does not control Telnet access to individual device ports. (See Device Ports > Settings (1 of 2) (on page 154) for information on enabling Telnet access to individual ports.) You may want to keep this option disabled for security reasons.
Web Telnet	Enables or disables the ability to access the EMG command line interface or device ports (connect direct) through the Web Telnet window. Disabled by default.
Timeout	If you enable Telnet logins, you can cause an idle connection to disconnect after a specified number of minutes. Select Yes and enter a value of from 1 to 30 minutes.
Timeout Data Direction	If idle connection timeouts are enabled, this setting indicates the direction of data used to determine if the connection has timed out. Select the type of data direction: <ul style="list-style-type: none"> ◆ Both Directions ◆ Incoming Network ◆ Outgoing Network
Escape Sequence	A single character or a two-character sequence that causes the EMG unit to terminate a Telnet client. Currently the Escape Sequence is only used for Web Telnet sessions. The default value is Esc+T (escape key, then uppercase "T" performed quickly but not simultaneously). You would specify this value as \x1bT , which is hexadecimal (x) character 27 (1B) followed by a T . A control character can be specified with the hexadecimal number for the control character; for example, Control-E can be specified as \x05 . Note that some browsers do not report key press events if Control is pressed for non-alphanumeric keys, so it is recommended to only use letters with Control character sequences.
Outgoing Telnet	Enables or disables the ability to create Telnet out connections.

Web SSH/Web Telnet Settings

Terminal Buffer Size	Number of lines in the Web SSH or Web Telnet terminal window that are available for scrolling back through output. Note: For tips on browser issues with Web SSH or Web Telnet, see Browser Issues on page 127 .
-----------------------------	--

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

SSH Commands

Go to [SSH Key Commands](#) to view CLI commands which correspond to the web page entries described above.

Logging Commands

Go to [Logging Commands](#) to view CLI commands which correspond to the web page entries described above.

SNMP

Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks. The Management Information Base (MIB) defines the set of manageable objects in the device. The EMG unit supports both MIB-II (as defined by [RFC 1213](#)) and a private enterprise MIB. The private enterprise MIB provides read-only access to all statistics and configurable items provided by the EMG unit. It provides read-write access to a select set of functions for controlling the EMG unit and device ports. See the MIB definition file for details. The EMG MIB definition file and the top level MIB file for all Lantronix products are accessible from the SNMP web page.

To configure SNMP:

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

Figure 7-2 Services > SNMP

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

Network Services User Authentication Devices Maintenance Quick Setup

SSH/Telnet/Logging SNMP NFS/CIFS Secure Lantronix Network Date & Time Web Server ConsoleFlow

SNMP Help?

<p>Enable Agent: <input type="checkbox"/></p> <p>Enable v1: <input type="checkbox"/></p> <p>Enable v2c: <input checked="" type="checkbox"/></p> <p>Enable Traps: <input type="checkbox"/></p> <p>Trap Version: 2c <input type="button" value="▼"/></p> <p>NMS #1: <input type="text"/></p> <p>NMS #2: <input type="text"/></p> <p>Alarm Delay: 60 seconds</p> <p>Engine ID: 800000F4030080A38BFCF0</p> <p>Location: <input type="text"/> location</p> <p>Contact: <input type="text"/> contact</p> <p>v1/v2c Communities</p> <p>Read-Only: <input type="text"/> public</p> <p>Read-Write: <input type="text"/> private</p> <p>Trap: <input type="text"/> public</p> <p>Version 3</p> <p>Security: <input checked="" type="radio"/> No Auth/No Encrypt <input type="radio"/> Auth/No Encrypt <input type="radio"/> Auth/Encrypt</p> <p>Auth with: MD5 <input type="button" value="▼"/></p> <p>Encrypt with: <input checked="" type="radio"/> DES <input type="radio"/> AES</p>	<p>Traps Enabled for Sending</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 10%;">coldStart (1.3.6.1.6.3.1.1.5.1)</td><td style="width: 10%; text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>linkDown (1.3.6.1.6.3.1.1.5.3)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>linkUp (1.3.6.1.6.3.1.1.5.4)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>authenticationFailure (1.3.6.1.6.3.1.1.5.5)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventPowerSupply (1.3.6.1.4.1.244.1.1.0.1)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventSysadminPassword (1.3.6.1.4.1.244.1.1.0.2)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventSLCShutdown (1.3.6.1.4.1.244.1.1.0.3)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortData (1.3.6.1.4.1.244.1.1.0.4)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortSLMData (1.3.6.1.4.1.244.1.1.0.5)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortSLMConfig (1.3.6.1.4.1.244.1.1.0.6)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortDeviceLowTemp (1.3.6.1.4.1.244.1.1.0.7)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortDeviceHighTemp (1.3.6.1.4.1.244.1.1.0.8)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortDeviceLowHumidity (1.3.6.1.4.1.244.1.1.0.9)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortDeviceHighHumidity (1.3.6.1.4.1.244.1.1.0.10)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortDeviceError (1.3.6.1.4.1.244.1.1.0.11)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventUSBAction (1.3.6.1.4.1.244.1.1.0.14)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventInternalTemp (1.3.6.1.4.1.244.1.1.0.13)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortError (1.3.6.1.4.1.244.1.1.0.15)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventSDCardAction (1.3.6.1.4.1.244.1.1.0.16)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventNoDialToneAlarm (1.3.6.1.4.1.244.1.1.0.17)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventRPMAction (1.3.6.1.4.1.244.1.1.0.18)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventPingHostFails (1.3.6.1.4.1.244.1.1.0.19)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortDeviceContactChanged (1.3.6.1.4.1.244.1.1.0.20)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventSFPAction (1.3.6.1.4.1.244.1.1.0.21)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventDevicePortAction (1.3.6.1.4.1.244.1.1.0.22)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> <tr><td>slcEventNetworkFailover (1.3.6.1.4.1.244.1.1.0.23)</td><td style="text-align: right;"><input checked="" type="checkbox"/></td></tr> </table>	coldStart (1.3.6.1.6.3.1.1.5.1)	<input checked="" type="checkbox"/>	linkDown (1.3.6.1.6.3.1.1.5.3)	<input checked="" type="checkbox"/>	linkUp (1.3.6.1.6.3.1.1.5.4)	<input checked="" type="checkbox"/>	authenticationFailure (1.3.6.1.6.3.1.1.5.5)	<input checked="" type="checkbox"/>	slcEventPowerSupply (1.3.6.1.4.1.244.1.1.0.1)	<input checked="" type="checkbox"/>	slcEventSysadminPassword (1.3.6.1.4.1.244.1.1.0.2)	<input checked="" type="checkbox"/>	slcEventSLCShutdown (1.3.6.1.4.1.244.1.1.0.3)	<input checked="" type="checkbox"/>	slcEventDevicePortData (1.3.6.1.4.1.244.1.1.0.4)	<input checked="" type="checkbox"/>	slcEventDevicePortSLMData (1.3.6.1.4.1.244.1.1.0.5)	<input checked="" type="checkbox"/>	slcEventDevicePortSLMConfig (1.3.6.1.4.1.244.1.1.0.6)	<input checked="" type="checkbox"/>	slcEventDevicePortDeviceLowTemp (1.3.6.1.4.1.244.1.1.0.7)	<input checked="" type="checkbox"/>	slcEventDevicePortDeviceHighTemp (1.3.6.1.4.1.244.1.1.0.8)	<input checked="" type="checkbox"/>	slcEventDevicePortDeviceLowHumidity (1.3.6.1.4.1.244.1.1.0.9)	<input checked="" type="checkbox"/>	slcEventDevicePortDeviceHighHumidity (1.3.6.1.4.1.244.1.1.0.10)	<input checked="" type="checkbox"/>	slcEventDevicePortDeviceError (1.3.6.1.4.1.244.1.1.0.11)	<input checked="" type="checkbox"/>	slcEventUSBAction (1.3.6.1.4.1.244.1.1.0.14)	<input checked="" type="checkbox"/>	slcEventInternalTemp (1.3.6.1.4.1.244.1.1.0.13)	<input checked="" type="checkbox"/>	slcEventDevicePortError (1.3.6.1.4.1.244.1.1.0.15)	<input checked="" type="checkbox"/>	slcEventSDCardAction (1.3.6.1.4.1.244.1.1.0.16)	<input checked="" type="checkbox"/>	slcEventNoDialToneAlarm (1.3.6.1.4.1.244.1.1.0.17)	<input checked="" type="checkbox"/>	slcEventRPMAction (1.3.6.1.4.1.244.1.1.0.18)	<input checked="" type="checkbox"/>	slcEventPingHostFails (1.3.6.1.4.1.244.1.1.0.19)	<input checked="" type="checkbox"/>	slcEventDevicePortDeviceContactChanged (1.3.6.1.4.1.244.1.1.0.20)	<input checked="" type="checkbox"/>	slcEventSFPAction (1.3.6.1.4.1.244.1.1.0.21)	<input checked="" type="checkbox"/>	slcEventDevicePortAction (1.3.6.1.4.1.244.1.1.0.22)	<input checked="" type="checkbox"/>	slcEventNetworkFailover (1.3.6.1.4.1.244.1.1.0.23)	<input checked="" type="checkbox"/>
coldStart (1.3.6.1.6.3.1.1.5.1)	<input checked="" type="checkbox"/>																																																				
linkDown (1.3.6.1.6.3.1.1.5.3)	<input checked="" type="checkbox"/>																																																				
linkUp (1.3.6.1.6.3.1.1.5.4)	<input checked="" type="checkbox"/>																																																				
authenticationFailure (1.3.6.1.6.3.1.1.5.5)	<input checked="" type="checkbox"/>																																																				
slcEventPowerSupply (1.3.6.1.4.1.244.1.1.0.1)	<input checked="" type="checkbox"/>																																																				
slcEventSysadminPassword (1.3.6.1.4.1.244.1.1.0.2)	<input checked="" type="checkbox"/>																																																				
slcEventSLCShutdown (1.3.6.1.4.1.244.1.1.0.3)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortData (1.3.6.1.4.1.244.1.1.0.4)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortSLMData (1.3.6.1.4.1.244.1.1.0.5)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortSLMConfig (1.3.6.1.4.1.244.1.1.0.6)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortDeviceLowTemp (1.3.6.1.4.1.244.1.1.0.7)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortDeviceHighTemp (1.3.6.1.4.1.244.1.1.0.8)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortDeviceLowHumidity (1.3.6.1.4.1.244.1.1.0.9)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortDeviceHighHumidity (1.3.6.1.4.1.244.1.1.0.10)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortDeviceError (1.3.6.1.4.1.244.1.1.0.11)	<input checked="" type="checkbox"/>																																																				
slcEventUSBAction (1.3.6.1.4.1.244.1.1.0.14)	<input checked="" type="checkbox"/>																																																				
slcEventInternalTemp (1.3.6.1.4.1.244.1.1.0.13)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortError (1.3.6.1.4.1.244.1.1.0.15)	<input checked="" type="checkbox"/>																																																				
slcEventSDCardAction (1.3.6.1.4.1.244.1.1.0.16)	<input checked="" type="checkbox"/>																																																				
slcEventNoDialToneAlarm (1.3.6.1.4.1.244.1.1.0.17)	<input checked="" type="checkbox"/>																																																				
slcEventRPMAction (1.3.6.1.4.1.244.1.1.0.18)	<input checked="" type="checkbox"/>																																																				
slcEventPingHostFails (1.3.6.1.4.1.244.1.1.0.19)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortDeviceContactChanged (1.3.6.1.4.1.244.1.1.0.20)	<input checked="" type="checkbox"/>																																																				
slcEventSFPAction (1.3.6.1.4.1.244.1.1.0.21)	<input checked="" type="checkbox"/>																																																				
slcEventDevicePortAction (1.3.6.1.4.1.244.1.1.0.22)	<input checked="" type="checkbox"/>																																																				
slcEventNetworkFailover (1.3.6.1.4.1.244.1.1.0.23)	<input checked="" type="checkbox"/>																																																				

SNMP Traps Sent/Fail: 0/0

v3 Users	Read-Only	Trap
User Name: <input type="text"/> snmpuser	Read-Write	Trap
Password: <input type="text"/> *****	<input type="text"/> snmpwuser	<input type="text"/> snmptrapuser
Retype Password: <input type="text"/> *****	<input type="text"/> *****	<input type="text"/> *****
Passphrase: <input type="text"/>	<input type="text"/> *****	<input type="text"/> *****
Retype Passphrase: <input type="text"/>	<input type="text"/>	<input type="text"/>

Apply

2. Enter the following:

Enable Agent	Enables or disables the Simple Network Management Protocol (SNMP) agent, which allows read-only access to the system. Disabled by default.
---------------------	--

Top Level MIB (link)	Click the link to access the top level MIB file for all Lantronix products.
EMG MIB (link)	Click the link to access the EMG MIB definition file for EMGs.
EMG MON MIB (link)	Click the link to access the EMG monitor MIB definition file for EMGs.
Enable v1	If checked, SNMP version 1 (which uses the Read-Only and Read-Write Communities) is enabled. The default is disabled.
Enable v2c	If checked, SNMP version 2c (which uses the Read-Only and Read-Write Communities) is enabled. The default is enabled.
Enable Traps	<p>Traps are notifications of certain critical events. Disabled by default. This feature is applicable when SNMP is enabled.</p> <p>Traps that the EMG unit sends include:</p> <ul style="list-style-type: none"> ?coldStart (generic trap 0, OID 1.3.6.1.6.3.1.1.5.1) ?linkDown (generic trap 2, OID 1.3.6.1.6.3.1.1.5.3) ?linkUp (generic trap 3, OID 1.3.6.1.6.3.1.1.5.4) ?authenticationFailure (generic trap 4, OID 1.3.6.1.6.3.1.1.5.5) ?slcEventPowerSupply (1.3.6.1.4.1.244.1.1.0.1) ?slcEventSysadminPassword (1.3.6.1.4.1.244.1.1.0.2) ?slcEventSLCShutdown (1.3.6.1.4.1.244.1.1.0.3) ?slcEventDevicePortData (1.3.6.1.4.1.244.1.1.0.4) ?slcEventDevicePortSLMData (1.3.6.1.4.1.244.1.1.0.5) ?slcEventDevicePortSLMConfig (1.3.6.1.4.1.244.1.1.0.6) ?slcEventDevicePortDeviceLowTemp (1.3.6.1.4.1.244.1.1.0.7) ?slcEventDevicePortDeviceHighTemp (1.3.6.1.4.1.244.1.1.0.8) ?slcEventDevicePortDeviceLowHumidity (1.3.6.1.4.1.244.1.1.0.9) ?slcEventDevicePortDeviceHighHumidity (1.3.6.1.4.1.244.1.1.0.10) ?slcEventDevicePortDeviceError (1.3.6.1.4.1.244.1.1.0.11) ?slcEventUSBAction (1.3.6.1.4.1.244.1.1.0.14) ?slcEventInternalTemp (1.3.6.1.4.1.244.1.1.0.13) ?slcEventDevicePortError (1.3.6.1.4.1.244.1.1.0.15) ?slcEventSDCardAction (1.3.6.1.4.1.244.1.1.0.16) ?slcEventNoDialToneAlarm (1.3.6.1.4.1.244.1.1.0.17) ?slcEventDevicePortDeviceContactChanged (1.3.6.1.4.1.244.1.1.0.20) ?slcEventSFPAction (1.3.6.1.4.1.244.1.1.0.21) ?slcEventNoDialToneAlarm (1.3.6.1.4.1.244.1.1.0.17) ?slcEventRPMAction (1.3.6.1.4.1.244.1.1.0.18) ?slcEventPingHostFails (1.3.6.1.4.1.244.1.1.0.19) ?slcEventDevicePortDeviceContactChanged (1.3.6.1.4.1.244.1.1.0.20) ?slcEventSFPAction (1.3.6.1.4.1.244.1.1.0.21) ?slcEventDevicePortAction (1.3.6.1.4.1.244.1.1.0.22) ?slcEventNetworkFailover (1.3.6.1.4.1.244.1.1.0.23) <p>The EMG unit sends the traps to the host identified in the NMS #1 and NMS #2 field using the selected Trap Version.</p> <p>For information on these traps, view the EMG enterprise MIB, which is available on the SNMP web page.</p> <p>Note: When the DSR signal drops on a device port, indicating that the attached cable has been disconnected or the attached device has been powered off, the EMG will log the event in the Device Ports system log and send a slcEventDevicePortAction SNMP trap. The log message and SNMP trap only occur if there is an active (connect direct or network connection) to the device port.</p>
Trap Version	When traps are sent, which SNMP version to use when sending the trap: v1, v2c or v3. The default is v2c.

NMS #1 (or #2)	When SNMP is enabled, an NMS (Network Management System) acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP. The NMS can request information from the EMG and receive traps from the EMG unit. Enter the IPv4 or IPv6 address of the NMS server. At least NMS #1 is required if you selected Enable Traps .
Alarm Delay	Number of seconds delay between outgoing SNMP traps.
Engine ID	The unique SNMP engine identifier for the EMG. This identifier may be required by the NMS in order to receive v3 traps.
Location	Physical location of the EMG (optional). Useful for managing the EMG unit using SNMP. Up to 20 characters.
Contact	Description of the person responsible for maintaining the EMG, for example, a name (optional). Up to 20 characters.

v1/v2c Communities

Read-Only	A string that SNMP agent provides. The Read-Only Community is used for SNMP v1 and v2c. The default is public .
Read-Write	A string that acts like a password for an SNMP manager to access the read-only data from the EMG unit SNMP, like a password for an SNMP manager to access the read-only data the EMG SNMP agent provides, and to modify data where permitted. The Read-Write Community is used for SNMP v1 and v2c. The default is private .
Trap	The trap used for outgoing generic and enterprise traps. Traps sent with the Event trigger mechanism still use the trap community specified with the Event action. The default is public .

Version 3

Security	Levels of security available with SNMP v. 3. <ul style="list-style-type: none"> ◆ No Auth/No Encrypt: No authentication or encryption. ◆ Auth/No Encrypt: Authentication but no encryption. (default) ◆ Auth/Encrypt: Authentication and encryption.
Auth with	For Auth/No Encrypt or Auth/Encrypt , the authentication method: <ul style="list-style-type: none"> ◆ MD5: Message-Digest algorithm 5 (default) ◆ SHA: Secure Hash Algorithm ◆ SHA2: Secure Hash Algorithm 2: SHA2_224, SHA2_256, SHA2_384, and SHA2_512
Encrypt with	Encryption standard to use: <ul style="list-style-type: none"> ◆ DES: Data Encryption Standard (default) ◆ AES: Advanced Encryption Standard

V3 User Read-Only

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

V3 User Read-Write

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

V3 User Trap

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

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

Services Commands

Go to [Services Commands](#) to view CLI commands which correspond to the web page entries described above.

NFS and SMB/CIFS

Use the [Services > NFS & SMB/CIFS](#) page if you want to save configuration and logging data onto a remote NFS server, or export configurations by means of an exported CIFS share.

Mounting an NFS shared directory on a remote network server onto a local EMG directory enables the EMG to store device port logging data on that network server. This configuration avoids possible limitations in the amount of disk space on the EMG unit available for the logging file(s). You may also save EMG configurations on the network server.

Similarly, use SMB/CIFS (Server Message Block/Common Internet File System), Microsoft's file-sharing protocol, to export a directory on the EMG as an SMB/CIFS share. The EMG unit exports a single read-write CIFS share called "public," with a subdirectory called config, which contains saved configurations and is read-write.

The share allows users to access the contents of the directory or map the directory onto a Windows computer. Users can also access the device port local buffers from the CIFS share.

To configure NFS and SMB/CIFS:

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

Figure 7-3 Services > NFS & SMB/CIFS

The screenshot shows the Lantronix EMG85100 web interface. At the top, the device name 'EMG85100' is displayed, along with the host 'emgfcf0' and user 'sysadmin'. A navigation bar includes links for Network, Services (which is selected), User Authentication, Devices, Maintenance, and Quick Setup. Below the navigation bar, there are links for SSH/Telnet/Logging, SNMP, NFS/CIFS, Secure Lantronix Network, Date & Time, Web Server, and ConsoleFlow. The main content area is titled 'NFS & SMB/CIFS'. The 'NFS Mounts' section contains three rows for mapping remote directories to local ones. The 'SMB/CIFS Share' section includes fields for sharing a directory, selecting network interfaces (Eth1 and Eth2), entering a CIFS user password, retying the password, and specifying a workgroup. An 'Apply' button is located at the bottom of this section.

2. Enter the following for up to three directories:

NFS Mounts

Remote Directory	The remote NFS share directory in the format: nfs_server_hostname or ipaddr:/exported/path
Local Directory	The local directory on the EMG on which to mount the remote directory. The EMG unit creates the local directory automatically.
Read-Write	If enabled, indicates that the EMG can write files to the remote directory. If you plan to log port data or save configurations to this directory, you must enable this option.
Mount	Select the checkbox to enable the EMG unit to mount the file to the NFS server. Disabled by default.
Mounted	Indicates if the EMG was able to successfully mount the NFS share directory.

3. Enter the following:

SMB/CIFS Share

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

4. To save, click the **Apply** button.
5. Click the Firmware & Configurations link to access the [Firmware & Configurations \(on page 283\)](#) to save EMG configuration, as desired.

NFS and SMB/CIFS Commands

Go to [NFS and SMB/CIFS Commands](#) to view CLI commands which correspond to the web page entries described above.

Secure Lantronix Network

Use the **Secure Lantronix Network** option to view and manage Lantronix IT management (ITM) devices on the local subnet.

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

To access Lantronix ITM devices on the local network:

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

Figure 7-4 Services > Secure Lantronix Network

LANTRONIX® EMG85100

Logout Host: emgfcf0 User: sysadmin Select port for Configuration WebSSH (DP only) Connected Device (DP only)

Network Services User Authentication Devices Maintenance Quick Setup

SSH/Telnet/Logging SNMP NFS/CIFS Secure Lantronix Network Date & Time Web Server ConsoleFlow

Secure Lantronix Network

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

45 Device(s) found.

Hostname	Model	IP Address/ Web Interface	FW Ver	SSH/ Telnet to CLI	Ports								
emgfcf0	EMG851000	172.19.100.153	8.2.0.0R4	N/A	<table border="1"><tr><td>1</td><td>3</td></tr><tr><td>2</td><td>4</td></tr></table>	1	3	2	4				
1	3												
2	4												
emgfcfdc	EMG851000	172.19.100.208	8.2.0.0R4	N/A	<table border="1"><tr><td>1</td><td>3</td></tr><tr><td>2</td><td>4</td></tr></table>	1	3	2	4				
1	3												
2	4												
emgfcb5	EMG851201	172.19.100.223	8.2.0.0R5	N/A	<table border="1"><tr><td>1</td><td>3</td><td>5</td><td>7</td></tr><tr><td>2</td><td>4</td><td>6</td><td>8</td></tr></table>	1	3	5	7	2	4	6	8
1	3	5	7										
2	4	6	8										
Emg8200R5	EMG851213	172.19.100.69	8.2.0.0R5	SSH Telnet	<table border="1"><tr><td>1</td><td>3</td><td>5</td><td>7</td></tr><tr><td>2</td><td>4</td><td>6</td><td>8</td></tr></table>	1	3	5	7	2	4	6	8
1	3	5	7										
2	4	6	8										
slb7941	SLB882	172.19.100.232	6.9.0.0RC3	N/A	<table border="1"><tr><td>1</td><td>3</td><td>5</td><td>7</td></tr><tr><td>2</td><td>4</td><td>6</td><td>8</td></tr></table>	1	3	5	7	2	4	6	8
1	3	5	7										
2	4	6	8										
slb2a6c	SLB882	172.19.100.82	6.8.0.0RC8	N/A	<table border="1"><tr><td>1</td><td>3</td><td>5</td><td>7</td></tr><tr><td>2</td><td>4</td><td>6</td><td>8</td></tr></table>	1	3	5	7	2	4	6	8
1	3	5	7										
2	4	6	8										
slb1c22	SLB882	172.19.205.52	6.6.0.0RC3	SSH Telnet	<table border="1"><tr><td>1</td><td>3</td><td>5</td><td>7</td></tr><tr><td>2</td><td>4</td><td>6</td><td>8</td></tr></table>	1	3	5	7	2	4	6	8
1	3	5	7										
2	4	6	8										

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

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

3. On the Secure Lantronix Network page, click the IP address of a specific secure Lantronix device to open a new browser page with the web interface for the selected device.
4. Log in as usual.

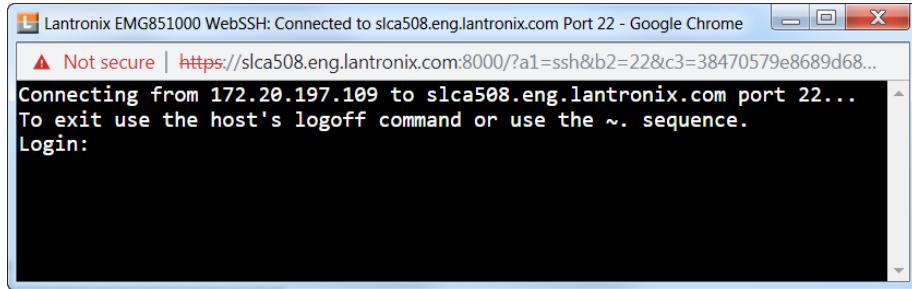
Figure 7-5 IP Address Login Page



To directly access the CLI interface for a device:

1. Make sure that Web Telnet or Web SSH is enabled for the specific device.
2. On the Secure Lantronix Network page, click the **SSH** or **Telnet** link in the SSH/Telnet to CLI column directly beside the device you would like to access.
3. Click your mouse into the CLI login interface that appears and login. The CLI interface will indicate when your connection is established.
4. To terminate the session, use either the host's logoff command or use `^]` to terminate a Telnet session or `~.` to terminate an SSH session.

Figure 7-6 SSH or Telnet CLI Session



To directly access a specific port on a particular device:

1. You have two options:
 - **Dashboard**
Make sure the **WebSSH (DP only)** radio button directly beneath the Dashboard is selected and click the desired port number. The Dashboard is located on the upper right corner of each Web Manager page (see *Figure 5-1.*) The CLI login interface appears.

Note: WebTelnet is not available from the Dashboard. See [Dashboard](#) as the dashboard may vary in appearance.



- **Secure Lantronix Page**

Click the **Services** tab, then click the **Secure Lantronix Network** link (see [Figure 7-4](#).) Select the port you want to configure. Enabled port numbers are in bright green boxes and will allow you to select either a **WebSSH** or a **WebTelnet** session. The SSH or Telnet popup window appears depending on what is clicked.

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

Figure 7-7 Disabled Port Number Popup Window

172.19.216.1 says
SSH In & Telnet In for this port are disabled.

OK

2. Click your mouse into the CLI login interface that appears (see [Figure 7-6](#)) and login. The CLI interface will indicate when your connection is established.
3. To terminate the session, use either the host's logoff command, or use ^] to terminate a Telnet session or ~. to terminate an SSH session.

Browser Issues

Please review the Lantronix Knowledge Base at <http://ltxfaq.custhelp.com/app/answers/list> to research any browser errors.

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

1. Click the **Search Options** link on the top right of the [Services > Secure Lantronix Network](#) page. The following web page displays:

Figure 7-8 Services > Secure Lantronix Network - Search Options



2. Enter the following:

Secure Lantronix Network Search	Select the type of search you want to conduct. <ul style="list-style-type: none"> ◆ Local Subnet performs a broadcast to detect secure Lantronix devices on the local subnet. ◆ Manually Entered IP Address List provides a list of IP addresses that may not respond to a broadcast because of how the network is configured. ◆ Both is the default selection.
IP Address	If you selected Manually Entered IP Address List or Both, enter the IP address of the secure Lantronix device you want to find and manage.

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

Troubleshooting Browser Issues

Depending on which browser you are using and what type of SSL certificate the EMG web server is configured with, there may be errors connecting to a Web SSH or Web Telnet session. These errors may be the standard browser error displayed for self-signed or untrusted certificates ("There is a problem with this website's security certificate." or "Your connection is not private.").

The SSL server that handles Web SSH and Web Telnet sessions is accessible on port 8000, instead of the standard port 443 for SSL connections. It is recommended that the EMG be configured to use a SSL certificate from a Certificate Authority to prevent issues accessing Web SSH and Web Telnet terminals. If your EMG web server is configured to use a self-signed or untrusted SSL certificate, refer to the notes below for how to work around this for various browsers.

When an EMG is configured with a SSL certificate that is either a wildcard certificate or associated with a specific name, in order to establish a Web SSH or Web Telnet session to the EMG unit, the unit must be able to successfully perform a reverse lookup on any IP address to which Web SSH or Web Telnet requests are sent. For example, if a unit is configured with a SSL certificate for the name "EMGXYZ.lantronix.com", and the unit website is being accessed in a browser with "https://EMGXYZ.lantronix.com", the unit needs to be configured with a name server that will allow the unit to perform a reverse lookup on the IP address associated with EMGXYZ.lantronix.com. Failure to perform a reverse lookup on a name may result in name mismatch errors in the browser when it attempts to open the Web SSH or Web Telnet window.

If you are unable to connect to a Web SSH or Web Telnet session for a reason other than a browser SSL certificate issue, restarting the SSL server on port 8000 may resolve the connection problem. This can be done by restarting the web server (with the CLI command "admin web restart") or by disabling both Web SSH and Web Telnet on the [SSH/Telnet/Logging](#) web page, and then re-enabling them.

- ◆ **Chrome** - For the greatest ease of use with Web SSH and Web Telnet, when the EMG web server is using a self-signed SSL certificate, use the Chrome browser. When the user accepts the self-signed SSL certificate in the browser for the primary EMG website, the self-signed SSL certificate is accepted for all ports - including port 8000 - for the EMG website.
- ◆ **Firefox** - When accessing the EMG website with Firefox, and when the EMG web server is using a self-signed SSL certificate, accepting the self-signed SSL certificate in the browser for the primary EMG website will only accept the certificate for port 443. It will not accept the certificate for port 8000. This may result in a popup being displayed in the Web SSH or Web Telnet window indicating that the browser needs to accept a certificate. To accept the self-signed certificate for port 8000, go to Firefox -> Options (or Preferences) -> Advanced -> Certificates -> View Certificates -> Servers, and add an exception for the EMG IP address or hostname, with port 8000.
- ◆ **Internet Explorer** - When accessing the EMG website with Internet Explorer, and when the EMG web server is using a self-signed SSL certificate, Explorer will grant access to the Web SSH and Web Telnet terminals if (a) the host name or common name in the self-signed certificate matches the name (or IP address) being used to access the EMG website, and (b) Explorer has imported and trusted the self-signed certificate. A custom self-signed certificate with the EMG name can be generated via the [Web Server - SSL Certificate](#) web page or the admin web certificate custom CLI command.

Once the EMG web server has been configured to use the custom self-signed certificate, follow these steps for Internet Explorer to trust the custom certificate:

- ◆ In Internet Explorer, browse to the EMG website whose certificate you want to trust.
- ◆ When you see the message "There is a problem with this website's security certificate.", choose **Continue to this website (not recommended)**.
- ◆ In Internet Explorer, select **Tools -> Internet Options**.
- ◆ Select **Security -> Trusted Sites -> Sites**.
- ◆ Verify or fill in the EMG website URL in the **Add this website** field, click **Add**, and then **Close**.
- ◆ Close the **Internet Options** dialog with either **OK** or **Cancel**.
- ◆ Refresh the Internet Explorer web page with the EMG website.
- ◆ When you see the message "There is a problem with this website's security certificate", choose **Continue to this website (not recommended)**.
- ◆ Click on the red **Certificate Error** at the right of the URL address bar and select **View certificates**.

- ◆ In the dialog that displays, click on **Install Certificate**, then in the **Certificate Import Wizard**, click **Next**.
- ◆ On the next page select **Place all certificates in the following store**.
- ◆ Click **Browse**, select **Trusted Root Certification Authorities**, and click **OK**.
- ◆ Back in the **Certificate Import Wizard**, click **Next**, then **Finish**.
- ◆ If you get a **Security Warning** message box, click **Yes**.
- ◆ Dismiss the **Import was successful** message box with **OK**.
- ◆ In Internet Explorer, select **Tools -> Internet Options**.
- ◆ Select **Security -> Trusted Sites -> Sites**.
- ◆ Select the EMG website URL you just added, click **Remove**, then **Close**.
- ◆ Now shut down all running instances of Internet Explorer, and restart Internet Explorer.
- ◆ The EMG website's certificate should now be trusted.

Web SSH/Telnet Copy and Paste

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

Support for copying and pasting content between the system clipboard and the Web SSH or Web Telnet window will vary from browser to browser. With the exception of Internet Explorer, most browsers will not allow highlighted content from the Web SSH or Web Telnet window to be copied to the system clipboard (Internet Explorer will display a prompt confirming the copy). Likewise, most browsers will not allow content from the system clipboard to be directly pasted into the Web SSH or Web Telnet window with the standard Control-V paste key sequence. With some browsers, the user will be able to use the **Paste from browser** option in the right-click menu to paste content from the system clipboard into a text field in a popup, and after hitting Enter, the content will be sent to the Web SSH or Web Telnet window.

Secure Lantronix Network Commands

Go to [SLC Network Commands \(on page 390\)](#) to view CLI commands which correspond to the web page entries described above.

Date and Time

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

The CLI `show ntp` command will display the current NTP status if NTP is enabled. The column headings are as follows: the host names or addresses shown in the remote column correspond to configured NTP server names; however, the DNS names might not agree if the names listed are not the canonical DNS names. The refid column shows the current source of synchronization, while the st column reveals the stratum, t the type (u = unicast, m = multicast, l = local, - = don't know), and poll the poll interval in seconds. The when column shows the time since the peer was last heard in seconds, while the reach column shows the status of the reachability register (see RFC-1305) in octal. The remaining entries show the latest delay, offset and jitter in milliseconds. The symbol at the left margin displays the synchronization status of each peer. The currently selected peer is marked *, while additional peers designated acceptable for synchronization, but not currently selected, are marked +. Peers marked * and + are included in the weighted average computation to set the local clock; the data produced by peers marked with other symbols are discarded.

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

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

Figure 7-9 Services > Date & Time

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, the title 'LANTRONIX® EMG851000' is displayed, along with the host 'emgfcf0' and user 'sysadmin'. The navigation bar includes tabs for Network, Services (which is selected), User Authentication, Devices, Maintenance, and Quick Setup. Below the navigation bar, there are links for SSH/Telnet/Logging, SNMP, NFS/CIFS, Secure Lantronix Network, Date & Time (which is selected), Web Server, and ConsoleFlow.

The main content area is titled 'Date & Time'. It contains the following fields:

- Change Date/Time:** A checkbox followed by date and time selection dropdowns (Date: July 10, 2019; Time: 09:56:26 am) and a Time Zone dropdown (GMT).
- Enable NTP:** A checkbox. To its right, a note states: 'The EMG can synchronize its clock with a remote time server using NTP.'
- Synchronize via:** A radio button group with two options: 'Broadcast from NTP Server' (selected) and 'Poll NTP Server(s)'.
- Local:** A radio button group with three options: '#1' (selected), '#2', and '#3'. Each option has an associated text input field.
- Public:** A radio button group with two options: 'Public' (selected) and 'NTP Pool: 0.pool.ntp.org (random)'.
- Apply:** A button at the bottom right of the form.

2. Enter the following:

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

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

To synchronize the EMG with a remote timeserver using NTP:

1. Enter the following:

Enable NTP	Select the checkbox to enable NTP synchronization. NTP is disabled by default.
Current NTP status	Displays the current NTP status if NTP is enabled above.
Synchronize via	Select one of the following: <ul style="list-style-type: none"> ◆ Broadcast from NTP Server: Enables the EMG unit to accept time information periodically transmitted by the NTP server. This is the default if you enable NTP. ◆ Poll NTP Server: Enables the EMG to query the NTP Server for the correct time. If you select this option, complete one of the following: <ul style="list-style-type: none"> ➢ Local: Select this option if the NTP servers are on a local network, and enter the IPv4 or IPv6 address of up to three NTP servers. This is the default, and it is highly recommended. ➢ Public: Select this option if you want to use a public NTP server, and select the address of the NTP server from the drop-down list. This is not recommended because of the high load on many public NTP servers. All servers in the drop-down list are stratum-2 servers. (See www.ntp.org for more information.) Each public NTP server has its own usage rules --please refer to the appropriate web site before using one. Our listing them here is to provide easy configuration but does not indicate any permission for use.

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

Date and Time Commands

Go to [Date and Time Commands \(on page 351\)](#) to view CLI commands which correspond to the web page entries described above.

Web Server

The Web Server supports all versions of the TLS protocol, but due to security concerns, does not support any versions of the SSL protocol. The Web Server page allows the system administrator to:

- ◆ Configure attributes of the web server.
- ◆ View and terminate current web sessions.
- ◆ Import a site-specific SSL certificate.

To configure the Web Server:

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

Figure 7-10 Services > Web Server

LANTRONIX® **EMG851000**

Logout Host: emgfcf0 User: sysadmin Select port for Configuration WebSSH (DP only) Connected Device (DP only)

Network Services User Authentication Devices Maintenance Quick Setup [Home](#) [?](#) [Help](#) [ConsoleFlow](#)

[SSH/Telnet/Logging](#) [SNMP](#) [NFS/CIFS](#) [Secure Lantronix Network](#) [Date & Time](#) [Web Server](#) [ConsoleFlow](#)

Web Server [Help ?](#)

Timeout: No [Web Sessions](#) Yes, minutes (5-120): [SSL Certificate](#)

Enable TLS v1.0 Protocol:
 Enable TLS v1.1 Protocol:

Cipher: High (256,168,128)
 High (256,168,128), Medium (128)
 FIPS Approved

Use only SHA2 and Higher Ciphers:
 Note: Changing TLS protocol or cipher requires a reboot or the CLI command "admin web restart".

Group Access:

Banner:
 Note: Line feeds can be included in the banner with the '\n' character sequence.

Network Interfaces: Eth1 Eth2 PPP

Run Web Server: Setting can be changed via the CLI.

Apply

2. Enter the following fields:

Timeout	<ul style="list-style-type: none"> ◆ Select No to disable Timeout. ◆ Select Yes, minutes (5-120) to enable timeout. Enter the number of minutes (must be between 30 and 120 minutes) after which the EMG web session times out. The default is 30. <p>Note: If a session times out, refresh the browser page and login to a new web session. If you close the browser without logging off the EMG unit first, you will have to wait for the timeout time to expire. You can also end a web session by using the admin web terminate command at the CLI or by asking your system administrator to terminate your active web session.</p> <ul style="list-style-type: none"> ◆ To view or terminate current web sessions, click the Web Sessions link. See Services - Web Sessions. ◆ To view, import, or reset the SSL Certificate, click the SSL Certificate link. See Services - SSL Certificate.
Enable TLS v1.0 Protocol	By default, the web supports the TLS v1.0 protocol. Uncheck this to disable the TLS v1.0 protocol. Changing this option requires a reboot or restarting the web server with the CLI command <code>admin web restart</code> for the change to take effect.
Enable TLS v1.1 Protocol	By default, the web supports the TLS v1.1 protocol. Uncheck this to disable the TLS v1.1 protocol. Changing this option requires a reboot or restarting the web server with the CLI command <code>admin web restart</code> for the change to take effect.
Cipher	By default, the web uses High/Medium security (128 bits or higher) for the cipher. This option can be used to configure the web to also support just High security ciphers (256 bit, 168 bit and some 128 bit). Changing this option requires a reboot or restarting the web server with the CLI command <code>admin web restart</code> for the change to take effect.
Use only SHA2 and Higher Ciphers	By default, the web supports SHA1 as well as SHA2 and higher ciphers. Check this option to support only SHA2 and higher ciphers. Changing this option requires a reboot or restarting the web server with the CLI command <code>admin web restart</code> for the change to take effect.
Group Access	Specify one or more groups to allow access to the Web Manager user interface. If undefined, any group can access the web. If one or more groups are specified (groups are delimited by the characters ',' (comma) or ';' (semicolon)), then any user who logs into the web must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the EMG. A group provided by a remote server must be either a single group or multiple groups delimited by the characters ',' (comma), ';' (semicolon), or '=' (equals) - for example "group=group1,group2;" or "group1,group2,group3".
Banner	Enter to replace default text displayed on the Web Manager home page after the user logs in. May contain up to 1024 characters. Blank by default. To create additional lines in the banner use the <code>\n</code> character sequence.
Network Interfaces	The interfaces that the web server is available on. By default, Eth1, Eth2 and PPP interfaces on modems are enabled.
Run Web Server	If enabled, the web server will run and listen on TCP ports 80 and 443 (all requests to port 80 are redirected to port 443). By default, the web server is enabled. The web server supports TLS 1.0, TLS 1.1, and TLS 1.2. Due to security vulnerabilities, SSL is not supported.
	Note: This option can only be changed at the CLI.

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

Admin Web Commands

Go to [Administrative Commands](#) to view CLI commands which correspond to the web page entries described above.

Services - SSL Certificate

The [Services > Web Server](#) page enables you to view and update SSL certificate information. The SSL certificate, consisting of a public/private key pair used to encrypt HTTP data, is associated with the web server. You can import a site-specific SSL certificate or generate a custom self-signed SSL certificate. The custom self-signed SSL certificates generated by the EMG use the SHA256 hash algorithm.

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

1. On the **Services** tab, click the **Web Server** page and click the **SSL Certificate** link. The following page displays the current SSL certificate.

Figure 7-11 Web Server - SSL Certificate

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin Select port for Configuration WebSSH (DP only) Connected Device (DP only)

Network Services User Authentication Devices Maintenance Quick Setup

SSH/Telnet/Logging SNMP NFS/CIFS Secure Lantronix Network Date & Time Web Server ConsoleFlow

Web Server - SSL Certificate

Current SSL Certificate (Default)

Current SSL Certificate:
Certificate:
Data:
Version: 1 (0x0)
Serial Number:
dd:2e:fe:b8:9f:06:0c:56
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, ST=California, L=Irvine, O=Lantronix, CN=SLC
Validity
Not Before: Jun 6 14:09:05 2016 GMT
Not After : Jun 4 14:09:05 2026 GMT
Subject: C=US, ST=California, L=Irvine, O=Lantronix, CN=SLC
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)

Reset to Default Certificate:

Note: changing the SSL Certificate requires a reboot or restarting the web server for the update to take effect.

Import SSL Certificate: via: **HTTPS**

Root Filename:

Certificate Filename:

Key Filename:

Passphrase:

Retype Passphrase:

Host:

Login:

Path:

Password:

Retype Password:

Generate custom self-signed SSL Certificate:

Number of Bits: **2048**

Number of Days:

Country Name:

State or Province Name:

Locality Name:

Organization Name:

Organization Unit Name:

Hostname or Common Name:

Email Address:

Optional Challenge Password:

Retype Password:

[Back to Web Server](#)

2. If desired, enter the following:

Reset to Default Certificate	To reset to the default certificate, select the checkbox to reset to the default certificate. Unselected by default.
Root Filename	Filename of the imported root or intermediate Certificate Authority. If HTTPS is selected as the method for import, the Upload File link will be selectable to upload a Certificate authority.
Import SSL Certificate	To import your own SSL Certificate, select the checkbox. Unselected by default.
Import via	From the drop-down list, select the method of importing the certificate (SCP , SFTP , or HTTPS). The default is HTTPS .

Certificate Filename	Filename of the certificate. If HTTPS is selected as the method for import, the Upload File link will be selectable to upload a certificate file.
Key Filename	Filename of the private key for the certificate. If HTTPS is selected as the method for import, the Upload File link will be selectable to upload a key file.
Passphrase / Retype Passphrase	Enter the passphrase associated with the SSL certificate if the private key is encrypted.
Host	Host name or IP address of the host from which to import the file.
Path	Path of the directory where the certificate will be stored.
Login	User ID to use to SCP or SFTP the file.
Password / Retype Password	Password to use to SCP or SFTP the file.
Generate custom self-signed SSL Certificate	To generate your own custom self-signed certificate with attributes specific to your site, select the checkbox. The SHA256 hashing algorithm will be used to generate the certificate. Unselected by default.
Number of Bits	The number of bits to use when generating the certificate: 2048, 3072 or 4096.
Number of Days	The number of days that the certificate can be used before it expires, up to 7500 days.
Country Name	The two letter country code for the custom certificate, e.g. "US" or "FR".
State or Province Name	The state or province for the custom certificate, e.g. "California". Must be at least 2 characters long.
Locality Name	The locality or city for the custom certificate, e.g. "Irvine". Must be at least 2 characters long.
Organization Name	The organization or company name for the custom certificate, e.g. "Lantronix". Must be at least 2 characters long.
Organization Unit Name	The unit name for the custom certificate, e.g. "Engineering" or "Sales". Must be at least 2 characters long.
Hostname or Common Name	The hostname or other name associated with the EMG the certificate is generated on, e.g., "emgxyz.engineering.lantronix.com". Must be at least 2 characters long.
Email Address	An optional email address to associate with the custom certificate.
Optional Challenge Password & Retype Password	An optional password use to encrypt the custom certificate.

3. Click the **Apply** button.

Note: You must reboot the EMG for the update to take effect.

4. To return to the [Services > Web Server](#) page, click the **Back to Web Server** link.

Services - Web Sessions

The [Services > Web Server](#) page enables you to view and terminate current web sessions.

To view or terminate current web sessions:

1. On the **Services** tab, click the **Web Server** page and click the **Web Sessions** link to the right. The following page displays:

Figure 7-12 Web Server - Web Sessions

Current Web Sessions					Terminate
Id	User	Login Time	Idle Time	Type	
1	sysadmin	07/10/19 09:45	0:00:00:00	Web	<input checked="" type="checkbox"/>

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

ConsoleFlow

ConsoleFlow is a cloud or on-premise portal for the centralized management of multiple Lantronix ITM devices. A browser based interface (including mobile phone app support) allows an administrator to view status, send commands, view logs and charts and update firmware. Each Lantronix device can communicate with the cloud server or on-premise server, sending status updates and responding to commands sent by the server.

An EMG gateway requires a unique Device ID to communicate with the ConsoleFlow portal. The ID is viewable in the ConsoleFlow settings. If a device is not already pre-configured with the ID, the ID must be provisioned using Lantronix Provisioning Manager (LPM). See the Lantronix *Provisioning Manager User Guide* at <https://www.lantronix.com/products/lantronix-provisioning-manager/>.

The ConsoleFlow client follows a sequence of steps to connect to the ConsoleFlow server, send status updates, check for firmware and configuration updates, and respond to commands from the server. This series of steps is the same each time the client starts - at EMG boot, or if the client is enabled. Any changes to the ConsoleFlow Device ID, Registration settings or Messaging settings require the ConsoleFlow client to be disabled and re-enabled for the changes to take effect.

1. Registration

The client will attempt to register to the **Registration Host** using the Project Tag and Device ID. If registration fails, the client will wait 30 seconds and retry. The client will retry until it is successful, or the client is disabled. Registration may fail if the Project Tag is invalid, the

Device ID is invalid, the Registration Host name cannot be resolved, or the Registration Host is not reachable. Once registration is successful, **Status of Client** will display **Registered** with the date and time of registration. Note that the Registered date/time displayed in the EMG status may be different from the registered date/time shown in the ConsoleFlow web UI. The EMG registered date/time is the most recent date and time that the EMG registered with the ConsoleFlow server. The registered date and time shown in the ConsoleFlow web UI is the first time that the EMG ever registered with the ConsoleFlow server.

2. Telemetry

After registration, the client will connect to the Telemetry Host (the hostname is provided during registration) and perform a telemetry handshake. This handshake may request that the client publish a set of statistics at regular intervals. If a telemetry handshake is successful, **Status of Client** will display **Telemetry Handshake** with the date and time of the handshake. Each time telemetry statistics are published, **Status of Client** will display **Telemetry Statistics** with the date and time the statistics were sent.

3. Messages and Status Updates

After the telemetry handshake, the client will connect to the **Messaging Host** to receive messages and publish status updates. If the connection fails, the client will wait 5 seconds and retry. The connection may fail if the Messaging Host name cannot be resolved, or the Messaging Host is not reachable. Once the connection is successful, Status of Client will display **Messaging connected** with the date and time the connection was established.

The client publishes status update messages (changes to device attributes) at the interval defined by **Interval between Status Updates**. Each time a status update is published, **Status of Client** will display **Status** with the date and time the status was sent. The client also accepts command messages from the ConsoleFlow server to perform actions, such as reboot or shutdown. Each time a message is received, **Status of Client** will display **Message received** with the date and time the message was received.

4. Firmware and Configuration Updates

The client checks for firmware and configuration updates at the interval defined by **Interval between FW and Config Checks**. When the client checks for firmware or configuration updates, **Status of Client** will display **Checked for Content** with the date and time the check was performed. If a firmware update is found, it will be applied to the alternate (non-active) boot bank, and **Status of Client** will display **Firmware updated** with the date and time the firmware was updated. If a configuration update is found, it will be applied to the current boot bank, and **Status of Client** will display **Configuration restored** with the date and time the configuration was restored.

To configure ConsoleFlow settings:

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

Figure 7-13 Services > ConsoleFlow

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin Select port for Configuration WebSSH (DP only) Connected Device (DP only)

Network Services User Authentication Devices Maintenance Quick Setup

SSH/Telnet/Logging SNMP NFS/CIFS Secure Lantronix Network Date & Time Web Server ConsoleFlow

ConsoleFlow

ConsoleFlow Client:

Interval between status updates: minutes

Interval between FW and Config checks: hours

Firmware Updates via ConsoleFlow:

Configuration Updates via ConsoleFlow:

Reboot after Firmware Update:

Connect to Cloud:

ConsoleFlow Cloud Settings

Registration Host:

Registration Port:

Use HTTPS for registration:

Validate certificates with HTTPS:

Messaging Services:

Messaging Host:

Messaging Port:

Messaging Services Security:

ConsoleFlow On-Premise Settings

Registration Host:

Registration Port:

Use HTTPS for registration:

Validate certificates with HTTPS:

Messaging Services:

Messaging Host:

Messaging Port:

Messaging Services Security:

Apply

ConsoleFlow Status:
Status of Client: not running

2. Enter the following:

ConsoleFlow Client	Enables or disables the ConsoleFlow client. This option is enabled by default, unless an EMG is not configured with a Device ID. When the client is enabled, it will attempt to register with the Registration Host . If this is successful, the client will attempt to establish a connection with the Messaging Host . The General log (see SSH/Telnet/Logging on page 114) will contain messages about connections made to the Registration Host and Messaging Host. Status of Client displays the last time of actions performed by the client. Note that when the client is disabled, it may take as long as 30 seconds for the client to terminate, depending on what actions the client was performing at the time it was disabled.
Interval between status updates	Number of minutes between status updates sent from the client to the server. Valid values are 1 - 60 minutes. The default is 2 minutes.
Interval between FW and Config Checks	Number of hours between checks for firmware and configuration updates initiated by the server. Valid values are 1 - 72 hours. The default is 24 hours.
Firmware Updates via ConsoleFlow	If enabled, firmware updates can be initiated by ConsoleFlow for the EMG. The device will check for updates per the frequency defined by Interval between FW and Config Checks, and if a firmware update is found, the update will be downloaded to the device and applied to the alternate boot bank. Enabled by default.
Configuration Updates via ConsoleFlow	If enabled, configuration updates can be initiated by ConsoleFlow for the EMG. The device will check for updates per the frequency defined by Interval between FW and Config Checks, and if a configuration update is found, the update will be downloaded to the device and applied to the current boot bank, and the EMG will be immediately rebooted. Enabled by default.
Reboot after Firmware Update	If enabled, the EMG will automatically reboot after a successful firmware update via ConsoleFlow. Disabled by default.
Connect to Cloud	If enabled, the ConsoleFlow client uses Cloud server settings for registration. Otherwise it uses On-Premise server settings. Enabled by default. i.e., By default, ConsoleFlow Active connection is to Cloud.

Device Attributes

Device Name	The device name displayed in the ConsoleFlow server UI. Valid characters are alphanumeric characters, dash "-", and underscore "_". The default is the device type (EMG) with the last 4 characters of the Eth1 MAC address appended.
Device Description	Long description that is displayed in the ConsoleFlow server UI.
Device ID	The unique device identifier. The ID is 32 alphanumeric characters. The ID may be provisioned using Lantronix Provisioning Manager (LPM). Contact Lantronix Tech Support for more information on LPM.
S/N	Displays the serial number.

Remote Access Idle Timeout

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

ConsoleFlow Cloud Settings and ConsoleFlow On-Premise Settings

Registration Host	Hostname of the server the client registers with. The Host Name should start with api.
Registration Port	The TCP port on the Registration Host. Defaults to 443.
Use HTTPS for registration	If enabled, HTTPS (instead of HTTP) is used for registration. Enabled by default.
Validate certificates with HTTPS	If enabled, use a certificate authority to validate the HTTPS certificate. A certificate authority file can be uploaded on the Web Server page. Disabled by default.
Messaging Services	If enabled, messaging services are used for status updates and commands. Enabled by default.
Messaging Host	Hostname of the server used for messaging services. The hostname should start with mqtt.
Messaging Port	The TCP port on the Messaging Host. Defaults to 443.
Messaging Services Security	If enabled, TLS is used for messaging. If Validate certificates with HTTPS is enabled for the Registration Host, a certificate authority will be used to validate the HTTPS certificates used for TLS. Enabled by default.

Messaging Host

Messaging Services	If enabled, messaging services are used for status updates and commands. Enabled by default.
Messaging Host	Hostname of the server used for messaging services. The hostname should start with mqtt.
Messaging Port	The TCP port on the Messaging Host. Defaults to 443.
Messaging Services Security	If enabled, TLS is used for messaging. If Validate certificates with HTTPS is enabled for the Registration Host, a certificate authority will be used to validate the HTTPS certificates used for TLS. Enabled by default.

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

ConsoleFlow Commands

Go to [ConsoleFlow Commands \(on page 342\)](#) to view CLI commands which correspond to the web page entries described above.

8: USB/SD Card Port

This chapter describes how to configure storage by using the [Devices > USB / SD Card](#) page and CLI. This page can be used to configure the micro SD card or the USB flash drive (thumb drive). The USB flash drive or micro SD card is useful for firmware updates, saving and restoring configurations and for device port logging. See [Firmware & Configurations \(on page 283\)](#).

The EMG supports a variety of USB flash drives (thumb drives).

Set up USB/SD Card Storage

The [Devices > USB / SD Card](#) page has a checkbox for both USB Access and SD card access. These checkboxes are a security feature to ensure that access to any USB device or the SD card is disabled if the box is unchecked. If unchecked, the EMG unit ignores any device plugged into the port.

To set up USB or SD card storage in the EMG:

1. Insert any of the supported storage devices into the USB port or the SD card slot on the front of the EMG unit. You can do this before or after powering up the EMG. If the first partition on the storage device is formatted with a file system supported by the EMG unit (ext2, FAT16 and FAT32), the card mounts automatically.
2. Log into the EMG unit and click **Devices**.
3. Click **USB / SD Card**. [Figure 8-1](#) shows the page that displays. Your storage device should display in the appropriate row of the USB ports / SD card table if you have inserted it. If it does not display and you have inserted it, refresh the web page.
4. View the USB/SD card information and options available on the page:

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

Figure 8-1 Devices > USB / SD Card

The screenshot shows the LANTRONIX EMG85100 web interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication, Devices (which is selected), Maintenance, and Quick Setup. Below the navigation bar, there is a sub-navigation bar with links for Device Status, Device Ports, Console Port, USB / SD Card (which is selected), RPMs, Connections, Xmodem, Host Lists, Scripts, and Sites. On the right side of the header, there is a port status indicator showing U1, E1, 1, 3, SD, E2, 2, 4. Below the header, there is a table titled "USB Ports / SD Card" with the following data:

Port	Device	Type	State
U1	storage	Lexar Media, Inc.	fat32, mounted, Size/Used/Avail 29.8G/22.2G/7.6G
SD	storage	Ultra HS-SD/MMC2	not mounted
Int SD	Storage	Internal SD Card	

On the right side of the table, there is a "Configure" button. Below the table, there are two checkboxes: "USB Access" (checked) and "SD Card Access" (checked). At the bottom right of the table area is an "Apply" button. To the right of the table, there is a sidebar with the following text:

USB Devices

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

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

To configure a USB/SD card storage port:

1. Insert any of the supported storage devices into the USB port or the SD card slot on the front of the EMG unit.
2. Click the **USB/SD Card** tab. *Figure 8-1* shows the page that displays.
3. Click the radio button (on the far right) of a USB or SD card device storage port.
4. Click **Configure**.
 - *Figure 8-2* shows the page that displays if a USB storage device is inserted.
 - *Figure 8-3* shows the page that displays if an SD Card is inserted.

Figure 8-2 Devices > USB > Configure

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

Network Services User Authentication Devices **Maintenance** Quick Setup

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

USB / SD Card - Storage [Help ?](#)

Port: U1 Mount:

Device: Storage Unmount:

Type: Lexar Media, Inc. Format:

State: fat32, mounted, Size/Used/Avail 29.8G/22.2G/7.6G Filesystem: Ext2 FAT16 FAT32 NTFS

Filesystem Check:

[Manage Files on Storage Device](#)

Apply

Figure 8-3 Devices > SD Card > Configure

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

Network Services User Authentication Devices **Maintenance** Quick Setup

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

USB / SD Card - Storage [Help ?](#)

Port: SD Mount:

Device: Storage Unmount:

Type: Ultra HS-SD/MMC2 Format:

State: not mounted Filesystem: Ext2 FAT16 FAT32 NTFS

Filesystem Check:

[Manage Files on Storage Device](#)

Apply

5. Enter the following fields.

Mount	Select the checkbox to mount the first partition of the storage device on the EMG unit (if not currently mounted). Once mounted, a USB thumb drive or SD card is used for firmware updates, device port logging and saving/restoring configurations.
--------------	--

Unmount	To eject the USB thumb drive or SD card from the EMG unit , first unmount the thumb drive or SD card . Select the checkbox to unmount it. Warning: <i>If you eject a thumb drive or SD card from the EMG unit without unmounting it, subsequent mounts of a USB thumb drive or SD card in may fail, and you will need to reboot the device to restore thumb drive or SD card functionality.</i>
Format	Format will do the following: <ul style="list-style-type: none">◆ Unmount the USB/SD card device (if it is mounted),◆ Remove all existing partitions,◆ Create one partition,◆ Format it with the selected filesystem◆ Mount the device
Filesystem	Select Ext2, FAT16, FAT32 or NTFS, the filesystems the EMG supports.
Filesystem Check	Select to run a filesystem integrity check on the thumb drive. This is recommended if the filesystem does not mount or if the filesystem has errors.

6. Click **Apply**.
7. Click the **Manage Files on Storage Device** link to view and manage files on the selected USB thumb drive or SD Card. Files on the storage device may then be deleted, downloaded or renamed. See [Manage Files on page 146](#) for more information.

Manage Files

To manage files, perform the following steps.

1. Click the **Manage Files on the Storage Device** link on the [Devices > SD Card > Configure](#) page.

Figure 8-4 Firmware and Configurations - Manage Files

LANTRONIX® **EMG851000**

Logout Host: emgfcf0 User: sysadmin

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

Devices **Maintenance** **Quick Setup**

File Manager

USB / SD Card

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

Firmware & Configurations - Manage Files

Help ?

Back to USB / SD Card - Storage

Files - USB Port U1

Name	Date/Time Saved	SSH Keys	SSL Certificate	Scripts	<input type="checkbox"/>
System Volume Information	05/09/16 15:36:28	N/A	N/A	N/A	<input type="checkbox"/>
.dropbox.device	03/07/17 12:57:04	N/A	N/A	N/A	<input type="checkbox"/>
archive	07/10/19 10:51:54	N/A	N/A	N/A	<input type="checkbox"/>
slcupdate-8.0.0.1R1.tgz	07/10/19 10:55:44	N/A	N/A	N/A	<input type="checkbox"/>
slcupdate-8.0.0.1R1.tgz.md5sum	07/10/19 10:55:34	N/A	N/A	N/A	<input type="checkbox"/>
slcupdate-8.1.0.0R6.tgz	07/10/19 10:55:24	N/A	N/A	N/A	<input type="checkbox"/>
slcupdate-8.1.0.0R6.tgz.md5sum	07/10/19 10:55:14	N/A	N/A	N/A	<input type="checkbox"/>

Actions:

New File Name:

Note: The **Delete**, **Download**, and **Rename** options are at the bottom of the page (Figure 8-4).

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

USB Commands

Go to [USB Access Commands](#), [USB Device Commands](#), [USB Storage Commands](#), and [Internal Modem Commands](#) to view CLI commands which correspond to the web page entries described above.

SD Card Commands

Go to [SD Card Commands](#) to view CLI commands which correspond to the web page entries described above.

9: Device Ports

This chapter describes how to configure and use an EMG port connected to an external device, such as a server or a modem. This chapter also describes how to configure the console port.

[Chapter 12: Connections](#) describes how to use the [Devices > Connections](#) web page to connect external devices and outbound network connections (such as Telnet or SSH) in various configurations.

For details on managing Remote Power Managers (RPMs), see [Chapter 10: Remote Power Managers](#).

For details on using scripts to automate tasks run on the CLI or device ports, see [Chapter 11: Scripts](#).

Connection Methods

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

1. Telnet or SSH to the Eth1 or Eth2 IP address, or connect to the console port, and log in to the command line interface. At the command line interface, issue the connect direct or connect listen commands.
2. If Telnet is enabled for a device port, Telnet to <Eth1 IP address>:< telnet port number> or <Eth2 IP address>:<telnet port number>, where telnet port number is uniquely assigned for each device port.
3. If SSH is enabled for a device port, SSH to <Eth1 IP address>:<ssh port number> or <Eth2 IP address>:<ssh port number>, where ssh port number is uniquely assigned for each device port.
4. If TCP is enabled for a device port, establish a raw TCP connection to <Eth1 IP address>:<tcp port number> or <Eth2 IP address>:<tcp port number>, where tcp port number is uniquely assigned for each device port.
5. If a device port has an IP address assigned to it, you can Telnet, SSH, or establish a raw TCP connection to the IP address. For Telnet and SSH, use the default TCP port number (23 and 22, respectively) to connect to the device port. For raw TCP, use the TCP port number defined for TCP In to the device port according to the [Device Ports - Settings \(on page 152\)](#) section.
6. Connect a terminal or a terminal emulation program directly to the device port. If logins are enabled, the user is prompted for a username/password and logs in to the command line interface.
For #2, #3, #4, #5, and #6, if logins or authentication are not enabled, the user is directly connected to the device port with no authentication.
For #1 and #6, if logins are enabled, the user is authenticated first, and then logged into the command line interface. The user login determines permissions for accessing device ports.

Permissions

There are three types of permissions:

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

3. **Clear mode:** The user can clear the contents of the device port buffer (set locallog <port> clear buffer command).

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

I/O Modules

The EMG module port configuration can be changed by adding or replacing I/O modules in the I/O module bays. Any changes to the I/O modules must be done while the unit is powered off. The following I/O module configurations are supported (Bay 1 is the leftmost bay when viewing the front of the EMG where the device ports are located):

Table 9-1 Supported I/O Module Configurations

Model	Bay 1	Bay 2
EMG 8510xx	4 port RJ45 module	Empty
EMG8501xx	Empty	4 port RJ45 module
EMG8520xx	4 port USB module	Empty
EMG8502xx	Empty	4 port USB module
EMG8511xx	4 port RJ45 module	4 port RJ45 module
EMG8512xx	4 port RJ45 module	4-port module
EMG8521xx	4 port USB module	4 port RJ45 module
EMG8522xx	4 port USB module	4 port USB module

The number of device ports in the EMG can be expanded by adding a 4-port I/O module in Bay 2. The configurations listed above are the only valid configurations; if any other configuration is detected at boot, the EMG unit will still boot, disable use of the device ports, and provide indications in the boot messages, in the CLI and in the web that the I/O configuration is invalid. When an invalid configuration is corrected by reconfiguring the I/O modules into a valid configuration, after the EMG module is powered up and booted, the valid configuration will be detected and the EMG module ports can be used again.

See [Figure 9-2 Devices > Device Status on page 150](#).

Device ports in slot 1 are numbered 1-4 and device ports in slot 2 are numbered 5-8, even if slot 1 is empty.

Restoring Configurations

Restoring a configuration to the EMG will automatically adjust the number of device ports to reflect the number of ports in the EMG unit the configuration is being restored to.

Device Status

The [Devices > Device Status](#) page displays the status of the EMG ports, the USB port and SD card port.

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

Figure 9-2 Devices > Device Status

Device Port Status and Counters					
No	Name	DSR	Bytes Input/Output	Errors	Connection Status
1	Port-1	No	0/0	0	Idle
2	Port-2	No	0/0	0	Idle
3	Port-3	No	0/0	0	Idle
4	Port-4	No	0/0	0	Idle

USB Ports / SD Card			
Port	Device	Type	State
U1	storage	Lexar Media, Inc.	fat32, mounted, Size/Used/Avail 29.8G/22.2G/7.6G
SD Card	storage	Ultra HS-SD/MMC2	not mounted

Device Ports

On the [Devices > Device Ports](#) page, you can set up the numbering of Telnet, SSH, and TCP ports, view a summary of current port modes, and select individual ports to configure.

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

Figure 9-3 Devices > Device Ports

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, there is a navigation bar with tabs: Network, Services, User Authentication, Devices (which is the active tab), Maintenance, and Quick Setup. Below the navigation bar, there are links for Device Status, Device Ports (which is the active tab), Console Port, USB / SD Card, RPMs, Connections, Xmodem, Host Lists, Scripts, and Sites. On the right side of the header, there is a port status indicator showing U1, E1, 1, 3, SD, E2, 2, 4. Below the header, there is a message: "Select port for Configuration WebSSH (DP only) Connected Device (DP only)". The main content area is titled "Device Ports". On the left, there is a section titled "Telnet/SSH/TCP In Port Numbers" with fields for "Starting Telnet Port" (2001), "Starting SSH Port" (3001), and "Starting TCP Port" (4001), followed by an "Apply" button. On the right, there is a table titled "Ports:" with columns: No, Name, Mode, and Select. The table lists 16 ports, numbered 1 to 16, all in "Idle" mode. Each row has a "Select" checkbox in the last column.

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

Note:

Icons that represent some of the possible modes include:

Idle	The port is not in use.
	The port is in data/text mode. <i>Note: You may set up ports to allow Telnet access using the IP Setting per Device Ports - Settings (on page 152).</i>
	An external modem is connected to the port. The user may dial into or out of the port.
	Telnet in or SSH in is enabled for the device port. The device port is either waiting for a Telnet or SSH login or has received a Telnet or SSH login (a user has logged in).

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

1. Enter the following:

Telnet/SSH/TCP in Port Numbers

Starting Telnet Port	Each port is assigned a number for connecting via Telnet. Enter a number (1025-65528) that represents the first port. The default is 2000 plus the port number. For example, if you enter 2001, port 1 will be 2001 and subsequent 2000 ports are automatically assigned numbers 2001, 2002, and so on.
Starting SSH Port	Each port is assigned a number for connecting via SSH. Enter a number (1025-65528) that represents the first port. The default is 3000 plus the port number. For example, if you enter 3001, port 1 will be 3001 and subsequent 3000 ports are automatically assigned numbers 3001, 3002, and so on.
Starting TCP Port	<p>Each port is assigned a number for connecting through a raw TCP connection. Enter a number (1025-65528) that represents the first port. The default is 4000 plus the port number. For example, if you enter 4001, port 1 will be 4001 and subsequent 4000 ports are automatically assigned numbers 4001, 4002, and so on.</p> <p>You can use a raw TCP connection in situations where a TCP/IP connection is to communicate with a serial device. For example, you can connect a serial printer to a device port and use a raw TCP connection to send print jobs to the printer over the network.</p> <p>Note: When using raw TCP connections to transmit binary data, or where the break command (escape sequence) is not required, set the Break Sequence of the respective device port to null (clear it).</p>

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

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

To configure a specific port:

1. You have two options:
 - Select the port from the ports list and click the **Configure** button. The [Device Ports > Settings \(1 of 2\)](#) page for the port displays.
 - Click the port number on the green bar at the top of each page.
2. Continue with directions in the section, [Device Ports - Settings \(on page 152\)](#).

Device Port Global Commands

Go to [Device Port Commands](#) to view CLI commands which correspond to the web page entries described above.

Device Ports - Settings

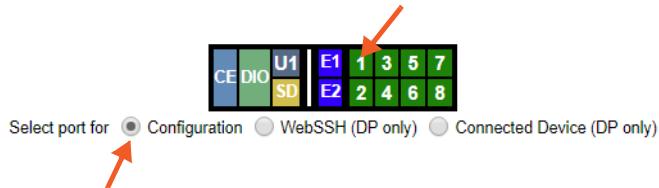
On the [Device Ports > Settings \(1 of 2\)](#) page, configure IP and data (serial) settings for individual ports, and if the port connects to an external modem, modem settings as well.

To open the Device Ports - Settings page:

1. You have two options:

- **Dashboard**

Make sure the **Configuration** radio button directly beneath the **Dashboard** is selected and click the desired port number in the **Dashboard**. The Dashboard is located on the upper right corner of each Web Manager page (see [Chapter 5: Web Manager](#).)



- **Device Ports Page**

Click the **Devices** tab and select the **Device Ports** option. Select the port you want to configure and then click the **Configure** button.

No	Name	Mode	Select
1	Port-1	Idle	<input type="radio"/>
2	Port-2	Idle	<input type="radio"/>
3	Port-3	Idle	<input type="radio"/>
4	Port-4	Idle	<input type="radio"/>
	Port-5		<input type="radio"/>
	Port-6		<input type="radio"/>
	Port-7		<input type="radio"/>
	Port-8		<input type="radio"/>
			<input type="radio"/>

The following page displays:

Figure 9-4 Device Ports > Settings (1 of 2)

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

Device Ports - Settings Help?

Port: 1 Mode: Idle Name: Port-1

Logging & Events: [Settings](#) Power Management: [Settings](#)

Connected to: undefined

IP Settings

Telnet In: Port: 2001 Authentication: Telnet Timeout: Seconds: 600 Data Direction: Both Directions

Telnet Soft IAC Mode:

SSH In: Port: 3001 Authentication: SSH Timeout: Seconds: 600 Data Direction: Both Directions

TCP In: Port: 4001 Authentication: TCP Timeout: Seconds: 600 Data Direction: Incoming Network

IP Address/Netmask Bits:

Send Term String: Term String:

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

Break Sequence: \x1bB

View Port Log Seq: \x1bV

View Port Log:

Zero Port Counters:

Data Settings

Baud: 9600 Data Bits: 8 Stop Bits: 1 Parity: none Flow Control: none

Modem Settings

State: Disabled Mode: Text PPP Use Sites: Initialization Script: PPP Logging: PPP Debug: Modem Timeout: No Yes, seconds (1-9999):

[View Modem Log](#)

Figure 9-5 Device Ports > Settings (2 of 2)

Enable Logins:

Max Direct Connects:

Show Lines On Connecting: No Yes, # of lines:

USB Channel:

Hardware Signals

Check DSR on Connect:

Disconnect on DSR:

Assert DTR:

DTR Control:

Reverse Pinout:

USB VBUS:

Caller ID Logging: Local User Number Fixed Number:

Dial-back Number: Local User Number Fixed Number:

Dial-back Delay: seconds

Dial-back Retries:

Text Mode

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

Dial-in Host List:

PPP Mode

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

Authentication: PAP CHAP Host/User Name:

CHAP Handshake: Secret/User Password: Retype Password:

CHAP Auth Uses: CHAP Host Local Users Same authentication for Dial-in & Dial-on-Demand (DOD):

DOD Authentication: PAP CHAP Host/User Name:

DOD CHAP Handshake: Secret/User Password: Retype Password:

Enable NAT: Note: Enabling NAT requires [IP Forwarding](#) to be enabled.

Dial-out Number:

Remote/Dial-out Login:

Remote/Dial-out Password: Retype:

Restart Delay: seconds

CBCP Server Allow No Callback:

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

[Back to Device Ports](#)

Apply Settings: to Device Ports:

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

2. Enter the following:

Device Port Settings

Port	Displays number of port; displays automatically.
Mode	The status of the port; displays automatically.
USB Device	This field is only displayed for USB ports. If a USB device is connected to the device port, this displays the USB version, speed, and a short type description for the USB device. The EMG supports up to 8 USB type A (Host) devices at data rates of HS (480 Mbit/s), FS (12 Mbit/s) or LS (1.5 Mbit/s). Each port has VBUS 5V support of up to 100mA (but not to exceed 600mA total per 4-port USB I/O module). Drawing more than 150 mA on a USB device port will shut down the VBUS 5V. USB ports are designed for data traffic only, and are not designed for charging or powering devices. Overcurrent conditions may disrupt operations.
Name	The name of the port. Valid characters are letters, numbers, dashes (-), periods, and underscores (_).

Detect Port Name	If enabled, the EMG will attempt to detect the hostname of the device connected to the device port, and set the device port name to the detected hostname. Many devices use their hostname or another identifier as the device prompt, and the EMG can extract this name from the prompt using the Detect Name Tokens . If the device port name is set to the default value, when a user interacts with a device connected to a device port, the EMG will look for the device prompt and set the device port name. The device prompt must be output at least 3 times in a single session for the prompt to be detected and the name extracted from the prompt. Any characters that are not part of the allowed characters for the device port Name will be removed. If the device name is automatically detected, the name will be logged in the Device Ports log.
Detect Name Tokens	If Detect Port Name is enabled, the EMG will attempt to extract a hostname or other identifier from the device prompt, to use as the device port name. The EMG will extract any name between either the start of a line sent from the device up until one of the tokens, or any part of a prompt that does not include the tokens, as the device port name. For example, if the device prompt is set to [EMG431d]>, and the Detect Name Tokens include "[" and "]", the EMG will extract the identifier EMG431d and set it as the device port name. If the device prompt is set to myrouter>, and the Detect Name Tokens include ">", the EMG will extract the identifier myrouter and set it as the device port name.
Group Access	If undefined, any group can access the device port. If one or more groups are specified (groups are delimited by the characters '' (space), ',' (comma), or ';' (semicolon)), then any user who logs into the device port must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the EMG unit. A group provided by a remote server must be either a single group or multiple groups delimited by the characters '' (space), ',' (comma), ';' (semicolon), or '=' (equals) - for example "group=group1,group2;" or "group1,group2,group3".
Banner	Text to display when a user connects to a device port by means of Telnet, SSH, or TCP. If authentication is enabled for the device port, the banner displays once the user successfully logs in. Blank is the default.
# of Sessions Msg	If enabled, a message will be displayed to a user when connecting to a device port that indicates how many users are currently connected to the device port. Disabled by default.
Idle Timeout Msg	If enabled, a message will be displayed to a user when their connection to a device port will be terminated soon due to the connection being idle. Disabled by default. <i>Note:</i> When the Idle Timeout Msg is enabled, the terminal application timeout values for Telnet, SSH and TCP should be set to a value greater than 15 seconds.
Connected Msg	If enabled, a message will be displayed to a user when they initially connect to a device port. Enabled by default.
New User Msg	If enabled, a message will be displayed to all the users connected to the device port when a new user connects to the same device port. Disabled by default.
Minimize Latency	Minimize device port latency by reducing read delays. This may improve communication efficiency in scenarios where a series of short messages are exchanged, but may increase central processing unit (CPU) utilization and decrease throughput in cases where large messages are transmitted. Disabled by default.

Break Sequence	A series of one to ten characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase “B” performed quickly but not simultaneously). You would specify this value as \x1bB , which is hexadecimal (\x) character 27 (1B) followed by a B . See Key Sequences on page 191 for notes on key sequence precedence and behavior.
View Port Log Seq	The key sequence used to view the Port Log while in Connect Direct mode. Non-printing characters can be specified by giving their hexadecimal code (see Break Sequence above). The default is Esc+V (\x1bV). See Key Sequences on page 191 for notes on key sequence precedence and behavior.
View Port Log	Select to allow the user to enter the View Port Log Sequence to view the Port Log during Connect Direct mode. The default is disabled.
Zero Port Counters	Resets all of the numerical values in the Port Counters table at the bottom of the page to zero (0).
Logging & Events	Click the Settings link to configure file logging (see Device Ports - Logging and Events on page 169), email logging, local logging, and USB logging.
Power Management	Click the Settings link to configure power supplies for the device connected to this device port on the Device Ports - Power Management page.
Connected to	The type of device connected to the device port. Currently, the EMG unit supports Remote Power Managers (PDUs and UPSes) from 140+ vendors, as well as Sensorsoft devices. If the connected device is an RPM, the user can assign an RPM to the device port by either select an existing RPM (via the Select dropdown) or clicking the Add RPM link to configure a new RPM for the EMG. If an RPM is already assigned to the device port, the user can click on the Selected RPM link to view status and configuration for the RPM. If the connected device is a Sensorsoft device, the user can click on Device Commands to manage the Sensorsoft device. If the type of device connected to the device port is not listed, select Undefined . Note: Sensorsoft temperature/humidity devices are supported with USB-to-serial adapters (ftdi/pl2303/cp210x) but are not supported for use with USB-to-Serial CDC_ACM devices.

IP Settings

Telnet In	Enables access to this port through Telnet. Disabled by default.
SSH In	Enables access to this port through SSH. Disabled by default.
TCP in	Enables access to this port through a raw TCP connection. Disabled by default: Note: When using raw TCP connections to transmit binary data, or where the break command (escape sequence) is not required, set the Break Sequence of the respective device port to null (clear it).
Port	Automatically assigned Telnet, SSH, and TCP port numbers. You may override this value, if desired. The value must be unique on the EMG; for example, you cannot have two or more ports numbered 10001.
Authentication	If selected, the EMG unit requires user authentication before granting access to the port. Authenticate is selected by default for Telnet in and SSH in , but not for TCP in .
Telnet/SSH/TCP Timeout	Select the checkbox to cause an idle Telnet, SSH or TCP connection to disconnect after a specified number of seconds as defined in the Seconds field to the right.

Seconds	Enter a value from 1 to 3600 seconds if selecting the Telnet, SSH or TCP Timeout checkbox to the left. The default is 600 seconds. Note: When the Idle Timeout Msg is enabled, the terminal application timeout values for Telnet, SSH and TCP should be set to a value greater than 15 seconds.
Data Direction	If a Telnet, SSH or TCP connection has the idle Timeout enabled, this setting indicates the direction of data use to determine if the connection has timed out: incoming network data, outgoing network data, or data from both directions. The default is Both Directions for Telnet and SSH , and Incoming Network data for TCP .
Telnet Soft IAC Mode	When Telnet Soft IAC mode is enabled, the Telnet server will not block waiting for the initial Telnet protocol IAC option responses. An abbreviated list of IAC options will be sent to the client, including a request for client side Echoing. Disabled by default.
IP Address/Netmask Bits	IP address used for this device port so a user can Telnet, SSH, or establish a raw TCP connection to this address and connect directly to the device port. The optional netmask bits specify the netmask to use for the IP address. For example, for a netmask of 255.255.255.0 specify 24 bits. If the netmask bits are not specified, a default netmask used for the class of network that the IP address falls in will be used. For Telnet and SSH, the default TCP port numbers (22 and 23, respectively) are used to connect to the device port. For raw TCP, the TCP port number defined for TCP In to the device port is used. Note: If Ethernet Bonding is enabled, assigning individual IP Addresses to Device Ports is not supported. Note that the IP address will be bound to Eth1 only, so if Eth2 is connected and configured, and Eth1 is not, this feature will not work.
Send Term String/Term String	If Send Term String is enabled and a Term String is defined, when a network connection to a device port is terminated, the termination string is sent to the device connected to the device port. The string should be defined so that it sends the appropriate command(s) to the device to terminate any active user sessions, e.g. "logout" or "exit". The string may contain multiple commands separated by a newline ("n") character. This is a security mechanism used to close sessions that are inadvertently left open by users.

Data Settings

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

Baud	The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate. The baud rate can also be set from the Power Management and Baud Rate menu. See the Device Ports - Power Management page.
Data Bits	Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is 8 data bits.
Stop Bits	The number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is 1 .

Parity	Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is none .
Flow Control	A method of preventing buffer overflow and loss of data. The available methods include none , xon/xoff (software), and rts/cts (hardware). The default is none .
Enable Logins	For serial devices connected to the device port, displays a login prompt and authenticates users. Successfully authenticated users are logged into the command line interface. The default is disabled. This is the correct setting if the device port is the endpoint for a network connection.
Max Direct Connects	Enter the maximum number (1-15) of simultaneous connections for the device port. The default is 1.
Show Lines on Connecting	If enabled, when the user either does a <code>connect direct</code> from the CLI or connects directly to the port using Telnet or SSH, the EMG outputs up to 24 lines of buffered data as soon as the serial port is connected. For example, an EMG user issues a <code>connect direct device 1</code> command to connect port 1 to a Linux server. For example, if the user issues the <code>ls</code> command to display a directory on a Linux server, then exits the connection, the results of the <code>ls</code> will be stored in the buffer. When the user then issues another <code>direct connect device 1</code> , the last 24 lines of the <code>ls</code> command is displayed so the user can see what state the server was left in.
USB Channel	Applies to USB device ports only. When a dual channel USB device is connected to the device port, this allows the user to select which of the channels is the active channel used for all connections. Only one channel can be active at any time. Enter the number 1 or 2 . The default is 1 .

Hardware Signal Triggers

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

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

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

Modem Settings (Device Ports)

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

State	Used if an external modem is attached to the device port. If enabling, set the modem to dial-out, dial-in, dial-back, dial-on-demand, dial-in/host list, dial-back & dial-on-demand, dial in & dial-on-demand, CBCP Server, and CBCP Client. Disabled by default. See Modem Dialing States (on page 186) for more information.
Mode	<p>The format in which the data flows back and forth:</p> <ul style="list-style-type: none"> ◆ Text: In this mode, the EMG assumes that the modem will be used for remotely logging into the command line. Text mode can only be used for dialing in or dialing back. Text is the default. ◆ PPP: This mode establishes an IP-based link over the modem. PPP connections can be used in dial-out mode (e.g., the EMG unit connects to an external network), dial-in mode (e.g., the external computer connects to the network that the EMG is part of), or dial-on-demand.

Use Sites	Enables the use of site-oriented modem parameters which can be activated by various modem-related events (authentication, outbound network traffic for dial-on-demand connections, etc.). Sites can be used with the following modem states: dial-in, dial-back, dial-on-demand, dial-in & dial-on-demand, dial-back & dial-on-demand, and CBCP server.
Initialization Script	Commands sent to configure the modem may have up to 100 characters. Consult your modem's documentation for recommended initialization options. If you do not specify an initialization script, the EMG unit uses a default initialization string of AT S7=45 SO=0 L1 V1 X4 &D2 &C1 E1 Q0. Note: We recommend that the modem initialization script always be preceded with AT and include E1 V1 x4 Q0 so that the EMG may properly control the modem. For information on AT commands, refer to the modem user guide, or do a web search for at command set. Serial modems may need to include &B1 in the modem initialization string to set the DTE rate to a fixed baud rate.
Modem Timeout	Timeout for all modem connections. Select Yes (default) for the EMG unit to terminate the connection if no traffic is received during the configured idle time. Enter a value of from 1 to 9999 seconds. The default is 30 seconds.
Caller ID Logging	Select to enable the EMG to log caller IDs on incoming calls. Disabled by default. Note: For the Caller ID AT command, refer to the modem user guide.
Modem Command	Modem AT command used to initiate caller ID logging by the modem. Note: For the AT command, refer to the modem user guide.
Dial-Back Number	Users with dial-back access can dial into the EMG gateway and enter their login and password. Once the EMG authenticates them, the modem hangs up and dials them back. Select the phone number the modem dials back on - a fixed number or a number associated with their login. If you select Fixed Number , enter the number (in the format 2123456789). The dial-back number is also used for CBCP client as the number for a user-defined number. See Device Ports - Settings (on page 152) for more information.
Dial-Back Delay	For dial-back and CBCP Server, the number of seconds between the dial-in and dial-out portions of the dialing sequence.
Dial-Back Retries	For dial-back and CBCP Server, the number of times the EMG unit will retry the dial-out portion of the dialing sequence if the first attempt to dial-out fails.

Modem Settings: Text Mode

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

Modem Settings: PPP Mode

Negotiate IP Address	If the EMG unit and/or the serial device have dynamic IP addresses (e.g., IP addresses assigned by a DHCP server), select Yes . Yes is the default. If the EMG or the modem have fixed IP addresses, select No , and enter the Local IP (IP address of the port) and Remote IP (IP address of the modem).
Authentication	Enables PAP or CHAP authentication for modem logins. PAP is the default. With PAP, users are authenticated by means of the Local Users and any of the remote authentication methods that are enabled. With CHAP, the CHAP Handshake fields authenticate the user.
CHAP Handshake	The Host/User Name (for UNIX systems) or Secret/User Password (for Windows systems) used for CHAP authentication. May have up to 128 characters.
CHAP Auth Uses	For CHAP authentication, determines what is used to validate the CHAP host/user sent by the remote peer: either the CHAP Host defined for the modem, or any of the users in the Local Users list.
Same authentication for Dial-in & Dial-on-Demand (DOD)	Select this option to let incoming connections (dial-in) use the same authentication settings as outgoing connections (dial-on-demand). If this option is not selected, then the dial-on-demand connections take their authentication settings from the DOD parameter settings. If DOD Authentication is PAP , then the DOD CHAP Handshake field is not used.
DOD Authentication	Enables PAP or CHAP authentication for dial-in & dial-on-demand. PAP is the default. With PAP, users are authenticated by means of the Local Users and any of the remote authentication methods that are enabled. With CHAP , the DOD CHAP Handshake fields authenticate the user.
DOD CHAP Handshake	For DOD Authentication , enter the Host/User Name for UNIX systems) or Secret/User Password (for Windows systems) used for CHAP authentication. May have up to 128 characters.
Enable NAT	Select to enable Network Address Translation (NAT) for dial-in and dial-out PPP connections on a per modem (device port or USB port) basis. Users dialing into the EMG access the network connected to Eth1 and/or Eth2. <i>Note: IP forwarding must be enabled on the Network > Network Settings (1 of 2) page for NAT to work. See Chapter 6: Networking on page 66.</i>
Dial-out Number	Phone number for dialing out to a remote system or serial device. May have up to 20 characters. Any format is acceptable.
Remote/Dial-out Login	User ID for dialing out to a remote system. May have up to 32 characters.
Remote/Dial-out Password	Password for dialing out to a remote system. May have up to 64 characters.
Retype	Re-enter remote/dial-out password for dialing out to a remote system. May have up to 64 characters.
Restart Delay	The number of seconds after the timeout and before the EMG unit attempts another connection. The default is 30 seconds.
CBCP Server Allow No Callback	For CBCP Server state, allows "No Callback" as an option in the CBCP handshake in addition to User-defined Number and Admin-defined Number.
CBCP Client Type	For CBCP Client, this selects the number that the client would like to use for callback - either a user-defined number passed to the server (specified by the Fixed Dial-back Number) or an administrator-defined number determined by the server based on the login that is PAP or CHAP authenticated.

3. To save settings for just this port, click the **Apply** button.
4. To save selected settings to ports other than the one you are configuring:

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

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

Port Status and Counters

Port Counters describe the status of signals and interfaces. EMG updates and increments the port counters as signals change and data flows in and out of the system. These counters help troubleshoot connections or diagnose problems because they give the user an overview of the state of various parameters. By setting them to zero and then re-checking them later, the user can view changes in status.

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

Note: *Status and statistics shown on the web interface represent a snapshot in time. To see the most recent data, you must reload the web page. Status may display "N/A" if EMG is unable to dynamically determine the connected/inserted device.*

Table 9-6 Port Status and Counters

Port Status and Counters	
DSR/CD	No
DTR	Yes
CTS	No
RTS	Yes
Bytes input	0
Bytes output	0
Framing errors	0
Parity errors	0
Overrun errors	0
Flow Control errors	0
Seconds since zeroed	11931

Device Ports - Power Management

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

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

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

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

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

To configure power management settings for a device port:

1. Connect to a specific port on the **Devices > Device Ports** page according to instructions in [To open the Device Ports - Settings page: \(on page 152\)](#).
2. Click the **Settings** link beside **Power Management** to access the [Device Ports - Power Management](#) page.

Figure 9-7 Device Ports - Power Management

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

U1 E1 1 3
SD E2 2 4

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

Device Ports - Power Management Help ?

Port: 1 Name: Port-1

Power Management Sequence: \x1bP

Managed Power Supplies

#1	RPM: select RPM	View Outlets >>
	Outlet: <input type="text"/>	<< Select Outlet
	Name: <input type="text"/>	
	State: <input type="text"/>	
	Action: None	
#2	RPM: select RPM	View Outlets >>
	Outlet: <input type="text"/>	<< Select Outlet
	Name: <input type="text"/>	
	State: <input type="text"/>	
	Action: None	
#3	RPM: select RPM	View Outlets >>
	Outlet: <input type="text"/>	<< Select Outlet
	Name: <input type="text"/>	
	State: <input type="text"/>	
	Action: None	
#4	RPM: select RPM	View Outlets >>
	Outlet: <input type="text"/>	<< Select Outlet
	Name: <input type="text"/>	
	State: <input type="text"/>	
	Action: None	

RPM Outlets

Back to Device Port Settings Apply

3. Enter the following:

Power Management Sequence	A series of one to ten characters that will display the Power Management menu when connected to the device port. The default value is Esc+P (escape key, then uppercase "P"). This value is specified as \x1bP , which is hexadecimal (\x) character 27 (1B) followed by a P. See Key Sequences on page 191 for notes on key sequence precedence and behavior.
RPM	For each managed power supply, select a RPM, most likely a PDU, which has outlets that can be individually controlled, and which provides power to the device connected to the device port. See Chapter 10: Remote Power Managers for details on managing Remote Power Managers with EMG.

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

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

Device Port - Sensorsoft Device

Devices made by Sensorsoft are used to monitor environmental conditions.

1. Connect to a specific port on the **Devices > Device Ports** page according to instructions in [To open the Device Ports - Settings page: \(on page 152\)](#).
2. In the **Connected to** drop-down menu above the IP Settings section of the [Device Ports > Settings \(1 of 2\)](#) page, select **Sensorsoft**.

Note: Sensorsoft temperature/humidity devices are supported with USB-to-serial adapters (ftdi/p12303/cp210x) but not supported for use with USB-to-Serial CDC_ACN devices.

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

Figure 9-8 Devices > Device Ports - Sensorsoft

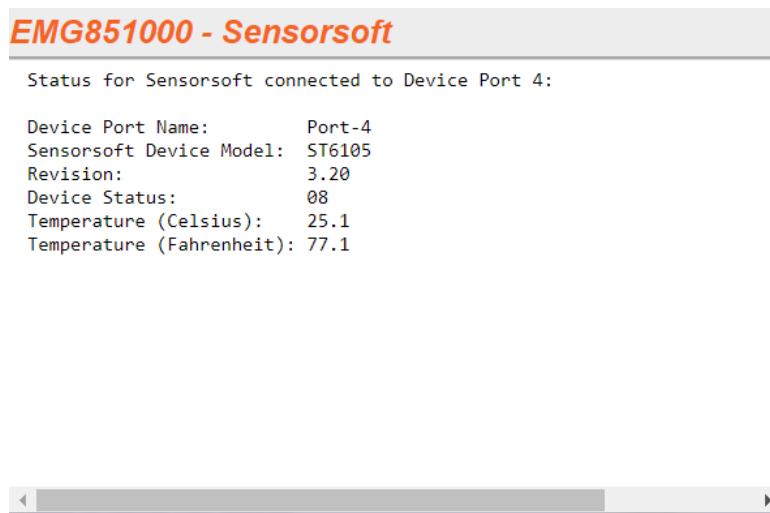
4. Select a port and enter or view the following information:

Dev Port	Displays the number of the EMG port.
Device Port Name	Displays the name of the EMG port.
Curr Temp	Current temperature (degrees Celsius) on the device the sensor is monitoring.
Low Temp	Enter the temperature (degrees Celsius) permitted on the monitored device below which the EMG sends a trap.
High Temp	Enter the temperature (degrees Celsius) permitted on the monitored device above which the EMG unit sends a trap.
Use °F	Display and set the temperature for this device in degrees Fahrenheit, instead of Celsius, which is the default.
Humidity (%)	Current relative humidity on the device the sensor is monitoring.
Low Humidity	Enter the relative humidity permitted on the device the sensor is monitoring below which the sensor sends a trap to the EMG.
High Humidity	Enter the highest relative acceptable humidity permitted on the device above which the sensor sends a trap to the EMG unit.
Contact	Displays the current contact closure status of the sensor, if supported by the connected Sensorsoft device. If the Sensorsoft device does not report a contact status, N/A will be displayed. If Traps are enabled for the Sensorsoft device, an <code>s1cEventDevicePortDeviceContactChanged</code> trap will be sent when the contact state changes from Open to Closed and from Closed to Open.
Traps	Select to indicate whether the EMG unit should send a trap or configured Event Alert when the sensor detects an out-of-range configured threshold.

5. Click the **Apply** button.

6. To view the status detected by the Sensorsoft, click the **Show Status** link in the far right column of the table.

Figure 9-9 Sensorsoft Status



Device Port Commands

Go to [Device Port Commands](#) to view CLI commands which correspond to the web page entries described above.

Device Commands

Go to [Device Commands](#) to view CLI commands which correspond to the web page entries described above.

Interacting with a Device Port

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

To connect to a device port to monitor it:

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

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

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

```
connect direct <endpoint>
```

endpoint is one of:

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

where:

<SSH flags> is one or more of:

```

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

```

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

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

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

Device Ports - Logging and Events

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

Local Logging

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

NFS File Logging

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

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

Examples:

02_Port-2_1.log

02_Port-2_2.log
02_Port-2_3.log
02_Port-2_4.log
02_Port-2_5.log

USB and SD Card Logging

Data can be logged to a USB flash drive or the SD card slot on the front of the EMG unit and properly mounted. Data logged locally to the EMG is limited to 256 Kbytes and may be lost in the event of a power loss. Data logged to a USB flash drive or SD card does not have these limitations. The system administrator can define the file size and number of files per port. For each logging file, once the file size reaches the maximum, a new file opens for logging. Once the number of files reaches the maximum, the oldest file is overwritten. The file naming convention is: <Device Port Number>_<Device Port Name>_<File number>.log

Examples:

02_Port-2_1.log
02_Port-2_2.log
02_Port-2_3.log
02_Port-2_4.log
02_Port-2_5.log

Token/Data Detection

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

Syslog Logging

Data can be logged to the system log. If this feature is enabled, the data will appear in the Device Ports log, under the Info level. The log level for the Device Ports log must be set to Info for the data to be saved to the system log. See [Device Ports - Logging and Events \(on page 169\)](#).

To set logging parameters:

1. In the top section of the [Device Port Settings](#) page, click the **Settings** link in the Logging field. The following page displays:

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

LANTRONIX® EMG851110

Logout Host: emgfcee User: sysadmin

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

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port USB / SD Card DIO Ports RPMs Connections Xmodem Host Lists Scripts Sites

Device Ports - Logging & Events

Port: 1 Name: Port-1

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

Token & Data Detection:

Trigger on: Data Byte Count Token/Character String

Byte Threshold: 100

Token:

Actions

Syslog:

SNMP Trap:

Email:

Email To:

Email Subject: Port %d Logging

Send String to Device:

String to Send:

Control Power Supply:

Power Supply:

Power Action: Cycle Power Turn On Turn Off

See online help for how Delay parameters affect Actions.

Action Delay: 60 seconds

Restart Delay: 60 seconds

[Back to Device Port Settings](#)

Local Logging:

Clear Local Log: [View Local Log](#)

Log Viewing Attributes

Display: Tail Head

Number of Lines: 40

NFS File Logging:

NFS Log to View: [View](#)

Directory to Log to:

Max Number of Files: 10

Max Size of Files: 2048 bytes

USB / SD Card Logging:

Log to View: [View](#)

Log to: Port U1 SD Card Int SD Card

Max Number of Files: 10

Max Size of Files: 2048 bytes

Syslog Logging:

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

Apply settings to Device Ports:

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

2. Enter the following:

Token & Data Detection

Token & Data Detection	Select to enable token and data detection on the selected device port, with a set of actions that can be enabled if a data trigger occurs. The default is disabled.
Trigger on	<p>Select the method of triggering an action:</p> <ul style="list-style-type: none"> ◆ Data Byte Count: A specific number of bytes of data. This is the default. ◆ Token/Character String: A specific pattern of characters, which you can define by a regular expression. <p>Note: Token/Character String recognition may negatively impact the EMG unit's performance, particularly when regular expressions are used.</p>

Byte Threshold	<p>The number of bytes of data the port will receive before the EMG unit will capture log data and initiate the selected actions. The default is 100 bytes.</p> <p>In most cases, the console port of your device does not send any data unless there is an alarm condition. After the EMG unit receives a small number of bytes, it perceives that your device needs some attention.</p> <p>A threshold set to 30 characters means that as soon as the unit receives 30 bytes of data, it performs the actions that are selected for this port.</p>
Token	<p>The specific pattern of characters the EMG unit must recognize before initiating the actions configured for this port. The maximum is 100 characters. You may use a regular expression to define the pattern. For example, the regular expression "abc[def]g" recognizes the strings abcdg, abceg, abcfg.</p> <p>The EMG supports GNU regular expressions. For more information see:</p> <ul style="list-style-type: none"> ◆ http://www.gnu.org/software/libc/manual/html_node/Regular-Expressions.html ◆ http://www.delorie.com/gnu/docs/regex/regex.html
Actions	<p>Select one or more actions to perform if there is a data trigger:</p> <ul style="list-style-type: none"> ◆ Syslog: A message is logged to the system log indicating what the data trigger was along with the initial portion of the data received. ◆ SNMP Trap: A slcEventDevicePortData trap will be sent to the NMS configured in the SNMP settings. ◆ Email: An email alert will be sent to the address configured for the device port. ◆ Send String to Device: A string will be sent to the device connected to the device port. ◆ Control Power Supply: The state of one or more of the device port power supplies can be changed.
Email to	<p>The email address of the message recipient(s) for an email alert. To enter more than one email address, separate the addresses with a single space. You can enter a total of 128 characters.</p>
Email Subject	<p>A subject text appropriate for your site. May have up to 128 characters.</p> <p>The email subject line is pre-defined for each port with its port number. You can use the email subject to inform the desired recipients of the problem on a certain server or location (e.g., server location or other classification of your equipment).</p> <p>Note: The character sequence %d anywhere in the email subject is automatically replaced with the device port number.</p>
String to Send	<p>The string to send to the device connected to the device port. The string supports the following special characters: newline (" \n "), double quote (" \ " "), single quote (" \ ' "), and escape (" \x1b "). You can enter a total of 128 characters.</p>
Power Supply	<p>The power supply that provides power to the device connected to the device port which to control. Select either all power supplies or an individual power supply.</p>
Power Action	<p>The action to perform on the selected power supply or power supplies - Cycle Power, Turn On or Turn Off.</p>
Action Delay	<p>A time limit of how long, in seconds, the device port will capture data after the data trigger is detected and before closing the log file (with a fixed internal buffer maximum capacity of 1500 bytes) and performing the selected actions. The default is 60 seconds.</p>
Restart Delay	<p>The number of seconds for the period of time, after performing the selected action, during which the device port will ignore additional characters received. The data will simply be ignored and not trigger additional actions until this time elapses. The default is 60 seconds.</p>

Local Logging

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

Log Viewing Attributes

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

NFS File Logging

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

USB / SD Card Logging

USB / SD Card Logging	Select to enable USB / SD card logging. A USB thumb drive or SD card must be loaded into one of the ports of the EMG and properly mounted. Disabled by default.
Log to View	Available log files in the selected USB / SD card slot to view.
Log To	Select the USB port, SD card, or internal SD card (if installed) to use for logging.
Max Number of Files	The maximum number of files to create to contain log data to the port. These files keep a history of the data received from the port. Once this limit is exceeded, the oldest file is overwritten. The default is 10.
Max Size of Files	The maximum allowable file size in bytes. The default is 2048 bytes. Once the maximum size of a file is reached, the EMG begins generating a new file. The default is 2048 bytes.

Syslog Logging

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

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

3. To apply settings to other device ports in addition to the currently selected port, select the **Apply** settings to Device Ports and enter port numbers separated by commas. Indicate a

range of port numbers with a hyphen (e.g., 2, 5, 7-10), and separate ranges with commas.

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

Logging Commands

Go to [Logging Commands](#) to view CLI commands which correspond to the web page entries described above.

Console Port

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

To set console port parameters:

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

Figure 9-11 Devices > Console Port

The screenshot shows the LANTRONIX EMG851000 web interface. The top navigation bar includes 'Logout', 'Host: emgfcf0', 'User: sysadmin', and a port selection dropdown ('Select port for Configuration', 'WebSSH (DP only)', 'Connected Device (DP only)'). The main menu tabs are 'Network', 'Services', 'User Authentication', 'Devices' (which is selected), 'Maintenance', and 'Quick Setup'. Below the menu is a sub-navigation bar with links for 'Device Status', 'Device Ports', 'Console Port' (which is selected and highlighted in blue), 'USB / SD Card', 'RPMs', 'Connections', 'Xmodem', 'Host Lists', 'Scripts', and 'Sites'. The main content area is titled 'Console Port'. It displays the following configuration settings:

- Status: Not Connected
- Baud: 9600
- Data Bits: 8
- Stop Bits: 1
- Parity: none
- Flow Control: none
- Timeout: No
- Show Lines On Connecting: No
- Group Access: (empty input field)

An 'Apply' button is located at the bottom right of the form.

2. Change the following as desired:

Baud	The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the console port defaults to this value.
Data Bits	Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is 8 data bits.
Stop Bits	The number of stop bits that indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is 1 .

Parity	Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is none .
Flow Control	A method of preventing buffer overflow and loss of data. The available methods include none , xon/xoff (software), and rts/cts (hardware). The default is none .
Timeout	The number of minutes (1-30) after which an idle session on the console is automatically logged out. Disabled by default.
Show Lines on Connecting	If selected, when you connect to the console port with a terminal emulator, you will see the last lines output to the console, for example, the EMG boot messages or the last lines output during a CLI session on the console.
Group Access	If undefined, any group can access the console port. If one or more groups are specified (groups are delimited by the characters '' (space), ',' (comma), or ';' (semicolon)), then any user who logs into the console port must be a member of one of the specified groups, otherwise access will be denied. Users authenticated via RADIUS may have a group (or groups) provided by the RADIUS server via the Filter-Id attribute that overrides the group defined for a user on the EMG. A group provided by a remote server must be either a single group or multiple groups delimited by the characters '' (space), ',' (comma), ';' (semicolon), or '=' (equals) - for example "group=group1,group2;" or "group1,group2,group3".

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

Console Port Commands

Go to [Console Port Commands](#) to view CLI commands which correspond to the web page entries described above.

DIO Port

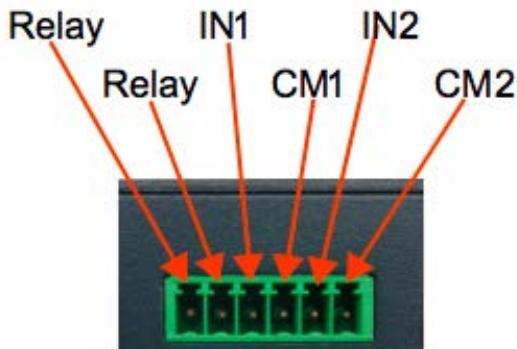
The front of the EMG unit has two Digital Inputs and one Relay Output. DIO ports can be used in Events as a trigger (inputs) or an action (relay output). Specifications for the DIO port:

- Two configurable inputs suitable for TTL input levels and tolerant up to 30VDC input voltage. The DIO inputs can be used to monitor the current status of any attached sensor.

On	Minimum: 2 VDC, Maximum: 30 VDC
Off	Minimum: 0 VDC, Maximum: 0.7 VDC

- One independently isolated mechanical form-C relay, supporting 1A 24V. When the relay is energized/turned on, the relay is closed, connecting both relay ports on the I/O connector through the relay. When the relay is turned off, the signal path is open, disconnecting the relay ports on the I/O connector.

DIO terminal block (in the UIs the ports are designated as Front #1, Front #2 and Front Relay):



To configure the DIO ports:

1. Change the following Front #1 and Front #2 Input port fields:

Name	The name of the port. Valid characters are letters, numbers, dashes (-), periods and underscores (_).
State	(view only) Displays the current state of the port: on or off.
Normal State	Defines the typical or normal state of the DIO Input port. This setting is used for Events.

2. Change the following Front Relay port fields:

Name	The name of the port. Valid characters are letters, numbers, dashes (-), periods and underscores (_).
State	(view only) Displays the current state of the port: on or off. The Change State check box and Off / On selection can be used to change the state of the port.
Normal State	Defines the typical or normal state of the Relay port. This setting is used for Events.
Wake State	The initial state of the relay port when the console manager boots.
Latch	Controls how a relay will be turned off if it is turned on as the result of an event trigger. If Latch is enabled, the user will need to explicitly turn off the relay when it is turned on as a result of an event. If Latch is disabled, the relay will automatically turn off after the trigger condition corrects itself and is no longer active.

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

See [Events on page 303](#) for information on configuring events for the DIO ports.

DIO Commands

Go to [DIO Commands](#) to view CLI commands which correspond to the web page entries described above.

Xmodem

The EMG supports using the Xmodem, Ymodem, or Zmodem protocols to send and receive files across serial ports. An Xmodem repository on the EMG holds files that can be sent or have been

received. In order to use one of the protocols, the device port that will be used must not be currently in use for any other purpose.

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

```
[emg431d]> set xmodem send 3 file update.bin protocol zmodem xfer binary
Starting Zmodem send of 117K file update.bin...
Sending: update.bin
Bytes Sent: 117988 BPS:919
```

Transfer complete

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

```
[emg431d]> se xmodem receive 4 protocol zmodem xfer binary
Starting Zmodem receive of file specified by protocol...
Receiving: update.bin.0
Bytes received: 117988/ 117988 BPS:937
```

Transfer complete

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

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

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

2. To upload a file to the repository, click the **Upload File** link and upload a file in the window that is displayed. Upload file size should not exceed 20 MB. The maximum length for the upload file name is 40 characters. The file name should not contain the following characters: forward slash ‘/’, backslash ‘\’, colon ‘:’, asterisk ‘*’, question mark ‘?’, double quotation mark (“), less than symbol ‘<’, greater than symbol ‘>’, or the vertical bar symbol ‘|’. After upload is complete, the filename will appear in the **File to Add** field. Click the **Add Uploaded File to Repo** button to add the file to the repository. The maximum repository size is 25 MB.
3. To rename a file, select the box to the right of the file in the **Xmodem Files Repository** list, enter the new file name in the **New File Name** field, and click the **Rename File** button.
4. To delete a file, select the box to the right of the file in the **Xmodem Files Repository** list, and click the **Delete** button.
5. To send a file, select the box to the right of the file in the **Xmodem Files Repository** list, and complete the following fields:

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

6. Click the **Send File to Device Port** button. The send will be initiated, and the **Status** window

can be opened to view the progress of the send. When the Xmodem protocol is used, the user will be prompted when to start the file receive with the message, “Give your local XMODEM receive command now.”

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

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

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

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

Xmodem Commands

Go to [Xmodem Commands](#) to view CLI commands which correspond to the web page entries described above.

Host Lists

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

To add a host list:

1. Click the **Devices** tab and select the **Host Lists** option. The following page displays:

Figure 9-12 Devices > Host Lists

The screenshot shows the LANTRONIX EMG85100 web interface. At the top, the device name 'EMG85100' is displayed. The 'Devices' tab is selected, and the 'Host Lists' option is chosen. The page title is 'Host Lists'. On the left, there is a table for 'Host Lists' with columns for 'Id' and 'Name'. On the right, there are buttons for 'View Host List' and 'Delete Host List'. Below this, there are fields for 'Host List Id' (0), 'Host List Name' (empty), 'Retry Count' (empty), and 'Authentication' (unchecked). To the right of these fields are buttons for 'Clear Host List', 'Add Host List', and 'Edit Host List'. Further down, there is a section for 'Host Parameters' with fields for 'Host', 'Protocol' (TCP), 'Port', and 'Escape Sequence', along with a 'Clear Host Parameters' button. To the right of this is a table titled 'Hosts (in order of precedence)' with an empty list. On the far right, there are up and down arrows for reordering the host list.

2. Enter the following:

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

Host List Id	Displays after a host list is saved.
Host List Name	Enter a name for the host list.
Retry Count	Enter the number of times the EMG should attempt to retry connecting to the host list.
Authentication	Select to require authentication when the EMG unit connects to a host.

3. To add hosts, enter the following:

Host Parameters

Host	Name or IP address of the host.
-------------	---------------------------------

Protocol	Protocol for connecting to the host (TCP, SSH, or Telnet).
Port	Port on the host to connect to.
Escape Sequence	<p>The escape character used to get the attention of the SSH or Telnet client. It is optional, and if not specified, Telnet and SSH use their default escape character.</p> <p>For Telnet, the escape character is either a single character or a two-character sequence consisting of '^' followed by one character. If the second character is '?', the DEL character is selected. Otherwise, the second character is converted to a control character and used as the escape character.</p> <p>For SSH, the escape character is a single character.</p> <p>Note: When the Device Port Esc Sequence/ViewLog/PowerMenu Escape Sequence is configured, the following escape sequence precedent behavior can be expected: 1) Escape 2) PowerMenu 3) ViewLogs</p> <p>A clear/restart of the remaining escape events occurs when there is a match in any configured sequence. All the sequences should have unique sequence defined and user should avoid overlapping sequence strings. When detecting key sequences, after receiving the first character(s) of a sequence, the EMG will wait 3 or more seconds for the remaining characters, before timing out and sending all characters to the device. For example, if the Escape Sequence is ABCD, and the user types "AB", the EMG will wait at least 3 seconds for the next character ("C") before timing out and sending the "AB" characters to the device.</p>

4. Click the right  arrow to add the host. The host displays in the Hosts box.
5. Repeat steps 3-4 to add more hosts to the host list.
6. Click the **Clear Host Parameters** button to clear fields before adding the next host.
7. You have the following options:
 - To remove a host from the host list, select the host in the Hosts box and click the left  arrow.
 - To give the host a higher precedence, select the host in the Hosts box and click the up  arrow.
 - To give the host a lower precedence, select the host in the Hosts box and click the down  arrow.
8. Click the **Add Host List** button. After the process completes, a confirmation message is displayed on the page.

To view or update a host list:

1. In the Host Lists table, select the host list and click the **View Host List** button. The list of hosts display in the Hosts box.

Figure 9-13 Devices >View Host Lists

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin Select port for Configuration WebSSH (DP only) Connected Device (DP only)

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

Host Lists Help ?

Host Lists	
Id	Name
1	test

View Host List Delete Host List

Host List Id: 1 Host List Name: test Host List Name: test

Host List Name: test

Retry Count: 2

Authentication:

Clear Host List Add Host List Edit Host List

Host Parameters

Host: Protocol: TCP Port: Escape Sequence: Clear Host Parameters

Hosts (in order of precedence)

172.19.100.17;tcp/389;

Up Arrow Down Arrow

2. View or update the following:

Host List Id	View only. Displays after a host list is saved.
Host List Name	Enter a name for the host list.
Retry Count	Enter the number of times the EMG should attempt to retry connecting to the host list.
Authentication	Select to require authentication when the EMG unit connects to a host.

3. View, add, or update the host parameters:

Host	Name or IP address of the host.
Protocol	Protocol for connecting to the host (TCP, SSH, or Telnet).
Port	Port on the host to connect to EMG

Escape Sequence	The escape character used to get the attention of the SSH or Telnet client. It is optional, and if not specified, Telnet and SSH use their default escape character. For Telnet, the escape character is either a single character or a two-character sequence consisting of '^' followed by one character. If the second character is '?', the DEL character is selected. Otherwise, the second character is converted to a control character and used as the escape character. For SSH, the escape character is a single character.
------------------------	---

4. You have the following options:
 - To add a host to the host list, click the right  arrow. The host displays in the Hosts box.
 - To remove a host from the host list, select the host in the Hosts box and click the left  arrow.
 - To give the host a higher precedence, select the host in the Hosts box and click the up  arrow.
 - To give the host a lower precedence, select the host in the Hosts box and click the down  arrow.
5. Click the **Edit Host List** button. After the process completes, a confirmation message is displayed on the page.

To delete a host list:

1. Select the host list in the Host Lists table.
2. Click the **Delete Host List** button. After the process completes, a confirmation message is displayed on the page.

Host List Commands

Go to [Host List Commands](#) to view CLI commands which correspond to the web page entries described above.

Sites

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

To use sites with a modem, create one or more sites (described below), then enable Use Sites for the modem. Sites can be used with the following modem states: dial-in, dial-back, CBCP Server, dial-on-demand, dial-in & dial-on-demand, and dial-back & dial-on-demand. For more information on how sites are used with each modem state, see [Modem Dialing States on page 186](#).

To add a site:

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

Figure 9-14 Devices > Sites

2. In the lower section of the page, enter the following:

Note: To clear fields in the lower part of the page, click the **Reset Site** button.

Site Id (view only)	Displays after a site is created.
Site Name	Enter a name for the site.
Port	Select the port: None , Internal Modem , Device Port , or USB Port U1 the site is assigned to. For dial-on-demand sites, a port must be selected. For any other sites, the port selection can be set to None . See Modem Dialing States on page 186 .

Login/CHAP Host	The login name (for PAP authentication) or CHAP host (for CHAP authentication) associated with this site. If a modem has sites enabled and the authentication is successful at dial-in (for modem states dial-in, dial-back, CBCP server, dial-in & dial-on-demand, or dial-back & dial-on-demand), and the name that was authenticated matches the Login/CHAP Host, the site parameters will be used for the remainder of the modem connection.
CHAP Secret/Retype	The CHAP secret associated with this site. If a modem has sites enabled and CHAP authentication enabled, then at dial-in, if the remote server sends a name in the CHAP challenge response that matches the CHAP host of a site, the CHAP secret for the site will be used to authenticate the CHAP challenge response sent by the remote server.
Authentication	The type of authentication, PAP or CHAP , for which this site is applicable. On dial-in authentication, only sites with the authentication type that matches the authentication type configured for the modem will be used to try to find a matching site.
Timeout Logins	For text dial-in connections, the connection can time out after the connection is inactive for a specified number of minutes.
Negotiate IP Address	If the EMG and the remote server should negotiate the IP addresses for each side of the PPP connection, select Yes. Select No if the address of the EMG unit (Local IP) and remote server (Remote IP) need to be specified.
Static Route IP Address	The Static Route IP Address, Subnet Mask and Gateway must be configured for dial-on-demand sites. The EMG will automatically dial-out and establish a PPP connection when IP traffic destined for the network specified by the static route needs to be sent. <i>Note: Static Routing must be enabled on the Network - Routing page for dial-on-demand connections.</i>
Static Route Subnet Mask	The subnet mask for a dial-on-demand connection.
Static Route Gateway	The gateway for a dial-on-demand connection.
Dial-out Number	The dial-out number must be specified for dial-on-demand sites. This indicates the phone number to dial when the EMG unit needs to send IP traffic for a dial-on-demand connection.
Dial-out Login	User ID for authentication when dialing out to a remote system, or when a remote system requests authentication from the EMG unit when it dials in. May have up to 32 characters. This ID is used for authenticating the EMG during the dial-out portion of a dial-back (including CBCP server) and dial-on-demand.
Dial-out Password	Password for authentication when dialing out to a remote system, or if a remote system requests authentication from the EMG unit when it dials in. May have up to 64 characters
Retype Password	Re-enter password for dialing out to a remote system. May have up to 64 characters.
Dial-back Number	The phone number to dial on callback for text or PPP dial-back connections. A site must successfully authenticate, have Allow Dial-back enabled and have a Dial-back Number defined in order for the site to be used for callback.
Allow Dial-back	If enabled, the site is allowed to be used for dial-back connections.
Dial-back Delay	For dial-back and CBCP Server, the number of seconds between the dial-in and dial-out portions of the dialing sequence.
Dial-back Retries	For dial-back and CBCP Server, the number of times the EMG unit will retry the dial-out portion of the dialing sequence if the first attempt to dial-out fails.

Modem Timeout	Timeout for dial-in and dial-on-demand PPP connections. Select Yes (default) for the EMG to terminate the connection if no traffic is received during the configured idle time. Enter a value of from 1 to 9999 seconds. The default is 30 seconds.
Restart Delay	The number of seconds after the modem timeout and before the EMG unit attempts another connection. The default is 30 seconds.
CBCP Server Allow No Callback	For a CBCP Server site, allows "No Callback" as an option in the CBCP handshake in addition to User-defined Number and Admin-defined Number.
Enable NAT	Select to enable Network Address Translation (NAT) for PPP connections. <i>Note: IP forwarding must be enabled on Network Port Settings (on page 67) for NAT to work.</i>

3. Click the **Add Site** button.

To view or update a site:

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

To delete a site:

1. Select the site in the **Sites** table.
2. Click the **Delete Site** button.

Site Commands

Go to [Site Commands](#) to view CLI commands which correspond to the web page entries described above.

Modem Dialing States

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

Dial In

The EMG waits for a peer to call the EMG unit to establish a text (command line) or PPP connection.

- ◆ For text connections, the user will be prompted for a login and password, and will be authenticated via the currently enabled authentication methods (Local Users, NIS, LDAP, etc). The site list will be searched for a site that (a) the **Login/CHAP Host** matches the name that was authenticated, (b) **Authentication** is set to PAP, and (c) the **Port** is set to **None** or matches the port the modem is on.

If a matching site is found, the **Timeout Logins** parameter configured for the site will be used for the rest of the dial-in connection instead of the **Timeout Logins** parameter configured for the modem. Once authenticated, a CLI session will be initiated, and the user will remain

connected to the EMG until they either logout of the CLI session, or (if **Timeout Logins** is enabled) the CLI session is terminated if it has been idle.

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

Dial-back

The EMG waits for a peer to call the EMG unit, establishes a text (command line) or PPP connection, authenticates the user, and if the EMG is able to determine a dial-back number to use, hangs up and calls the dial-back number to establish either a text or PPP connection.

- ◆ For text connections, the user will be prompted for a login and password, and will be authenticated via the currently enabled authentication methods (Local Users, NIS, LDAP, etc). The site list will be searched for a site that (a) the **Login/CHAP Host** matches the name that was authenticated, (b) **Authentication** is set to PAP, and (c) the **Port** is set to **None** or matches the port the modem is on. If a matching site is found, its **Timeout Logins**, **Dial-back Number**, **Allow Dial-back**, and **Dial-back Delay** parameters will be used for the rest of the dial-back connection instead of the parameters configured for the modem. Once the remote server is authenticated, if **Allow Dial-back** is enabled for the site and a **Dial-back Number** is defined, the EMG unit will hang up and wait **Dial-back Delay** seconds before initiating the dial-back. The EMG will dial, prompt the user again for a login and password, and a CLI session will be initiated. The user will remain connected to the EMG unit until they either logout of the CLI session, or (if **Timeout Logins** is enabled) the CLI session is terminated if it has been idle.
- ◆ For PPP connections, the user will be authenticated via PAP or CHAP (determined by the **Authentication** setting for the modem). For PAP, the Local/Remote User list will be used to authenticate the login and password sent by the PPP peer, and the site list will be searched for a site that (a) the **Login/CHAP Host** matches the name that was authenticated, (b) **Authentication** is set to PAP, and (c) the **Port** is set to **None** or matches the port the modem is on. For CHAP, the site list will be searched for a site that (a) the **Login/CHAP Host** and **CHAP Secret** match the name and secret sent in the CHAP Challenge response by the PPP peer, (b) **Authentication** is set to CHAP, and (c) the **Port** is set to **None** or matches the port the modem is on. If the remote peer requests PAP or CHAP authentication from the EMG, the **Remote/Dial-out Login** and **Remote/Dial-out Password** configured for the modem (not the site) will be provided as authentication tokens. If a matching site is found, its **Dial-back Number**, **Allow Dial-back**, **Dial-back Delay**, **Dial-out Login**, **Dial-out Password**, **Negotiate IP Address**, **NAT**, and **Modem Timeout** parameters will be used for the rest of the dial-back connection instead of the parameters configured for the modem. Once the remote server is authenticated, if **Allow Dial-back** is

enabled for the site and a **Dial-back Number** is defined, the EMG unit will hang up and wait **Dial-back Delay** seconds before initiating the dial-back. The EMG will dial, and if the remote peer requests PAP or CHAP authentication, provide the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting).

Dial-on-demand

The EMG unit automatically dial outs and establishes a PPP connection when IP traffic destined for a remote network needs to be sent. It will remain connected until no data packets have been sent to the peer for a specified amount of time.

When this modem state is initiated, the EMG searches the site list for all sites that (a) have a **Dial-out Number** defined, (b) have a **Static Route IP Address**, **Static Route Subnet Mask** and **Static Route Gateway** defined, and (c) the **Port** matches the port the modem is on. A dial-on-demand connection will be started for each, waiting for IP traffic destined for a remote network.

When IP traffic needs to be sent, the EMG unit dials the appropriate **Dial-out Number** for the site, and if the remote peer requests PAP or CHAP authentication, provides the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting). The PPP connection will stay active until no IP traffic is sent for **Modem Timeout** seconds. Once the timeout has expired, the PPP connection will be terminated and will not be reestablished for at least **Restart Delay** seconds.

Dial-in & Dial-on-demand

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

- ◆ For Dial-in, the user will be authenticated via PAP or CHAP (determined by the **Authentication** setting for the modem). For PAP, the Local/Remote User list will be used to authenticate the login and password sent by the PPP peer, and the site list will be searched for a site that (a) the **Login/CHAP Host** matches the name that was authenticated, (b)

Authentication is set to PAP, and (c) the **Port** is set to **None** or matches the port the modem is on. For CHAP, the site list will be searched for a site that (a) the **Login/CHAP Host** and **CHAP Secret** match the name and secret sent in the CHAP Challenge response by the PPP peer, (b) **Authentication** is set to CHAP, and (c) the **Port** is set to **None** or matches the port the modem is on. If the remote peer requests PAP or CHAP authentication from the EMG, the **Remote/Dial-out Login** and **Remote/Dial-out Password** configured for the modem (not the site) will be provided as authentication tokens.

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

- ◆ For Dial-on-Demand, the EMG unit searches the site list for all sites that (a) have a **Dial-out Number** defined, (b) have a **Static Route IP Address**, **Static Route Subnet Mask** and **Static Route Gateway** defined, and (c) the **Port** matches the port the modem is on. A dial-on-demand connection will be started for each, waiting for IP traffic destined for a remote network. When IP traffic needs to be sent, the EMG dials the appropriate **Dial-out Number** for the site, and if the remote peer requests PAP or CHAP authentication, provides the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session

will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting). The PPP connection will stay active until no IP traffic is sent for **Modem Timeout** seconds. Once the timeout has expired, the PPP connection will be terminated and will not be reestablished for at least **Restart Delay** seconds.

Dial-back & Dial-on-demand

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

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

If a matching site is found, its **Dial-back Number**, **Allow Dial-back**, **Dial-back Delay**, **Dial-out Login**, **Dial-out Password**, **Negotiate IP Address**, **NAT**, and **Modem Timeout** parameters will be used for the rest of the dial-back connection instead of the parameters configured for the modem. Once the remote server is authenticated, if **Allow Dial-back** is enabled for the site and a **Dial-back Number** is defined, the EMG will hang up and wait **Dial-back Delay** seconds before initiating the dial-back. The EMG unit will dial, and if the remote peer requests PAP or CHAP authentication, provide the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting).

- ◆ For Dial-on-Demand, the EMG searches the site list for all sites that (a) have a **Dial-out Number** defined, (b) have a **Static Route IP Address**, **Static Route Subnet Mask** and **Static Route Gateway** defined, and (c) the **Port** matches the port the modem is on. A dial-on-demand connection will be started for each, waiting for IP traffic destined for a remote network.

When IP traffic needs to be sent, the EMG unit dials the appropriate **Dial-out Number** for the site, and if the remote peer requests PAP or CHAP authentication, provides the **Dial-out Login** and **Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting). The PPP connection will stay active until no IP traffic is sent for **Modem Timeout** seconds. Once the timeout has expired, the PPP connection will be terminated and will not be reestablished for at least **Restart Delay** seconds.

CBCP Server and CBCP Client

Callback Control Protocol (CBCP) is a PPP option that negotiates the use of callback where the server, after authenticating the client, terminates the connection and calls the client back at a phone number that is determined by the CBCP handshake. For more information on CBCP, see <http://technet.microsoft.com/en-us/library/cc957979.aspx>. CBCP is used primarily by Microsoft PPP peers. CBCP supports two options for determining the number to dial on callback: the client can specify a user-defined number for the server to dial on callback, or the client can request the

server use an administrator-defined number to dial on callback. Optionally, some servers may also allow "no callback" as an option.

CBCP Server

The EMG waits for a client to call the EMG unit, establishes a PPP connection, authenticates the user, and negotiates a dial-back number with the client using CBCP. If the EMG is able to determine a dial-back number to use, it hangs up and calls the dial-back number.

When a call is received, a PPP connection is established, and the user will be authenticated via PAP or CHAP (configured with the **Authentication** setting). For PAP, the Local/Remote list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the **CHAP Handshake Host/User Name** and **Secret/User Password** will be used to authenticate CHAP Challenge response sent by the PPP peer. If the remote peer requests PAP or CHAP authentication from the EMG unit, the **Remote/Dial-out Login** and **Remote/Dial-out Password** will be provided as authentication tokens. Once authenticated, the CBCP handshake with the client determines the number to use for dial-back. The EMG unit will present the client with the available options: if the authenticated user is a Local/Remote User with **Allow Dial-back** enabled and a Dial-back Number defined, the administrator-defined option is allowed; if this is not the case, the user-defined number is allowed. Additionally, if **CBCP Server Allow No Callback** is enabled, the client can also select no callback (the PPP connection established at dial-in will remain up). The client will select from the available callback options. If the EMG unit can determine a dial-back number to use, it will hang up and wait **Dial-back Delay** seconds before initiating the dial-back (if the dial-back fails, the EMG will try **Dial-back Retries** times to dial-back). The EMG unit will call back the previously authenticated remote peer, and if the remote peer requests PAP or CHAP authentication, provide the **Remote/Dial-out Login** and **Remote/Dial-out Password** as authentication tokens. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting).

CBCP Client

The EMG unit will dial out to a CBCP server, establish a PPP connection, negotiate a callback number with the server using CBCP, terminate the connection, and wait for the server to call back. The EMG unit dials the **Dial-out Number**, and if the remote peer requests PAP or CHAP authentication, provides the **Remote/Dial-out Login** and **Remote/Dial-out Password** as authentication tokens. Once authenticated, the CBCP handshake with the server determines the number to use for dial-back. The EMG device will request the type of number defined by **CBCP Client Type** - either an Admin-defined Number (the CBCP server determines the number to call) or a User-defined Number (the EMG unit will provide the **Fixed Dial-back Number** as the number to call). If the CBCP handshake is successful, the EMG unit will terminate the PPP connection, hang up, and wait for the server to dial back. When the remote server calls back the EMG unit and the PPP connection is established, the user will be authenticated via PAP or CHAP (configured with the **Authentication** setting). For PAP, the Local/Remote list will be used to authenticate the login and password sent by the PPP peer. For CHAP, the **CHAP Handshake Host/User Name** and **Secret/User Password** will be used to authenticate CHAP Challenge response sent by the PPP peer. Once authenticated, a PPP session will be established using either negotiated IP addresses or specific IP addresses (determined by the **Negotiate IP Address** setting).

Notes:

- ◆ *In a state where the modem will be answering a call, the modem should always be configured for manual answer, not auto answer.*
- ◆ *When answering a call, the EMG unit answers after the 2nd ring.*
- ◆ *Any text or PPP connection can be terminated by setting the modem state to disabled.*

Key Sequences

The default values for the various key sequences (Escape Sequence, Break Sequence, View Port Log Sequence, Power Menu Sequence) are set to different key sequences, and it is recommended that they always be set to different key sequences so that the EMG can properly handle each of the functions accessed by the key sequence while connected to a device.

For example, if the View Port Log Sequence is set to the same sequence as the Power Menu Sequence, and this sequence is typed while connected to a device port, both the Power Menu and the option to display Port Log will be displayed, with the Power Menu taking precedence and processing user input.

If any of the key sequences are set to the same value, the precedence used to process the key sequences is:

- ◆ Escape Sequence
- ◆ Power Management Sequence
- ◆ View Port Log Sequence

It is also recommended that the key sequences not share a significant amount of overlap other than the first character. For example, if the View Port Log Sequence is set to **ABCD** and the Power Management Sequence is set to **ABCE**, the first three characters of both sequences are the same - this is not recommended.

When any portion of key sequences overlap, typing a complete escape sequence for one of the sequences will reset recognition of the other sequences back to the beginning of the key sequence. For example, with the default View Port Log sequence of **ESC-V** and the default Power Management sequence of **ESC-P**, if the user types "ESC-V" and views the port log and then returns to interacting with the device, they need to type "ESC-P" to view the Power Menu, and not just "P".

When detecting key sequences, after receiving the first character(s) of a sequence, the EMG will wait 3 or more seconds for the remaining characters, before timing out and sending all characters to the device. For example, if the Escape Sequence is **ABCD**, and the user types "AB", the EMG will wait at least 3 seconds for the next character ("C") before timing out and sending the "AB" characters to the device.

10: Remote Power Managers

The EMG supports managing remote power managers (RPMs) for devices from over 140 vendors. The RPM can be either a power distribution unit (PDU) or uninterruptible power source/supply (UPS), and can be managed via SNMP, serial port, network and USB connections. The RPMs web page displays a list of all currently managed RPMs with an overview of their current status, with options to control and view detailed status for each RPM, depending on its supported capabilities.

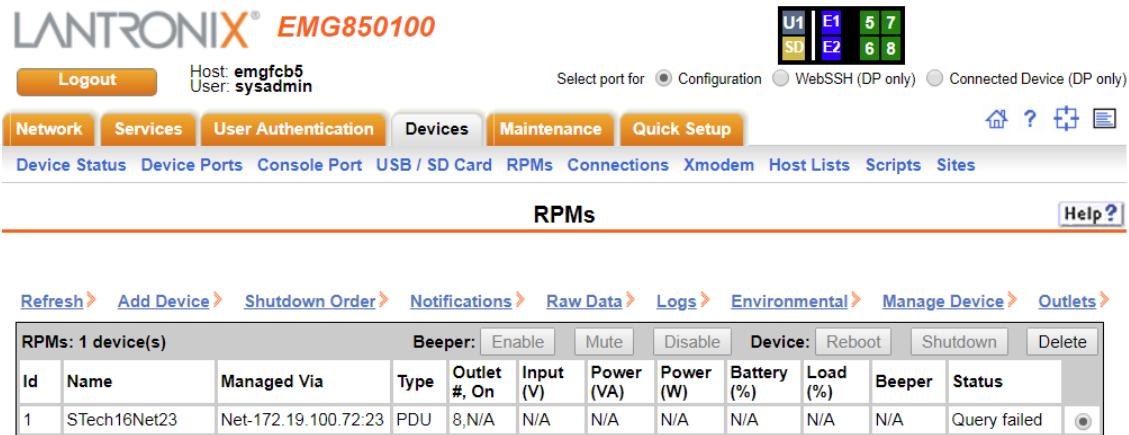
For notes on optimizing the management of specific devices, see [Optimizing and Troubleshooting RPM Behavior \(on page 204\)](#).

Devices - RPMs

To control or view status for an RPM:

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

Figure 10-1 Devices > RPMs



LANTRONIX® **EMG850100**

Logout Host: emgfb5 User: sysadmin Select port for Configuration WebSSH (DP only) Connected Device (DP only)

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

RPMs Help?

Refresh > Add Device > Shutdown Order > Notifications > Raw Data > Logs > Environmental > Manage Device > Outlets >

RPMs: 1 device(s)			RPMs													
			Beeper:		Mute		Disable		Device:		Reboot		Shutdown		Delete	
			Enable		Mute		Disable		Device:		Reboot		Shutdown		Delete	
Id Name Managed Via			Type	Outlet #, On	Input (V)	Power (VA)	Power (W)	Battery (%)	Load (%)	Beeper	Status					
1	STech16Net23	Net-172.19.100.72:23	PDU	8, N/A	N/A	N/A	N/A	N/A	N/A	N/A	Query failed					

2. In the RPMs table, select the RPM by clicking on the radio button in the far right column. The options that are available for that RPM will be displayed as active links above the RPMs table.
3. Select one of the following options:

Refresh	Refreshes the information in the RPMs table.
Add Device	Displays the Devices > RPMs - Add Device page to add a new managed PDU or UPS.
Shutdown Order	Displays the order in which all UPS devices are shutdown in the event that a UPS reaches a low battery state. See Figure 10-2 . For more information, see RPM Shutdown Procedure .

Notifications	Displays the notifications configured for each PDU and UPS. See Figure 10-3 .
Raw Data	Displays a window with all of the information returned by the driver when a query for status is requested. This option is available for all RPMs. See Figure 10-4 .
Logs	Displays a window with any logging information that has been accumulated for the selected RPM, if logging is enabled for the RPM. This option is available for all RPMs. See Figure 10-5 .
Environmental	Displays a window with any environmental (humidity and temperature) information that may be available for the selected RPM, if sensors are installed for the RPM. This option is available for all RPMs. See Figure 10-6 .
Managed Device	Displays the RPMs - Manage Device page, with the complete status and configuration for the selected RPM. This option is available for all RPMs.
Outlets	Displays the RPMs - Outlets page for RPMs that support individual outlet control and status.
Beeper: Enable, Mute, Disable	If the RPM has a beeper than can be controlled, these options allow the administrator to Enable , Mute , or Disable the beeper. If you try to use Mute to silence a beeper and the beeper continues to sound, the UPS most likely does not support mute, and the Disable option will be the only way to silence the beeper.
Reboot	Reboots the RPM immediately, which may interrupt the power provided by the RPM while it is rebooting. Some PDUs and UPSes have a default delay that they will wait before initiating a reboot; this setting may be visible in the raw data (see above) as "ups.delay.reboot".
Shutdown	Shuts down the RPM immediately, which will interrupt the power provided by the RPM. Some PDUs and UPSes have a default delay that they will wait before initiating a shutdown; this setting may be visible in the raw data (see above) as "ups.delay.shutdown".
Delete	Deletes the selected RPM, after a confirmation.

Figure 10-2 RPM Shutdown Order

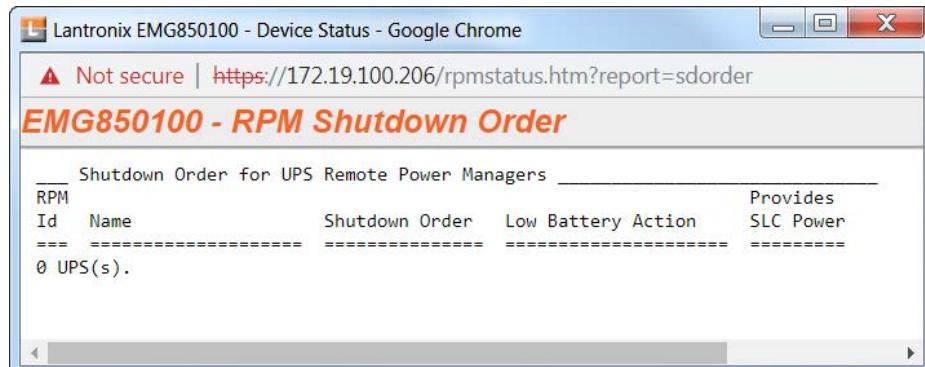
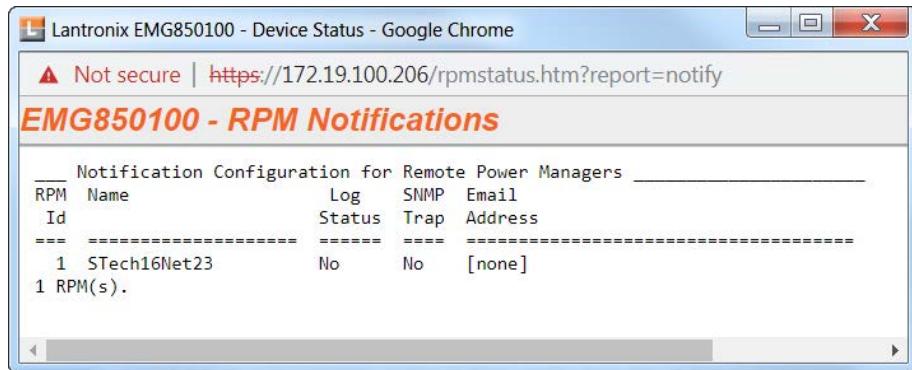


Figure 10-3 RPM Notifications

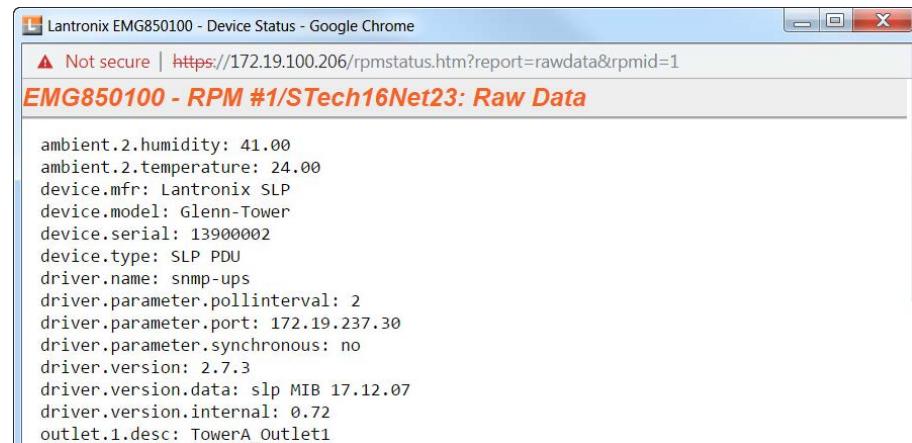


The screenshot shows a Google Chrome window with the title "Lantronix EMG850100 - Device Status - Google Chrome". The address bar displays a warning: "Not secure | https://172.19.100.206/rpmstatus.htm?report=notify". The main content area is titled "EMG850100 - RPM Notifications". It displays a table titled "Notification Configuration for Remote Power Managers" with the following data:

RPM Name	Log	SNMP	Email
Id	Status	Trap	Address
1 STech16Net23	No	No	[none]

Below the table, it says "1 RPM(s).".

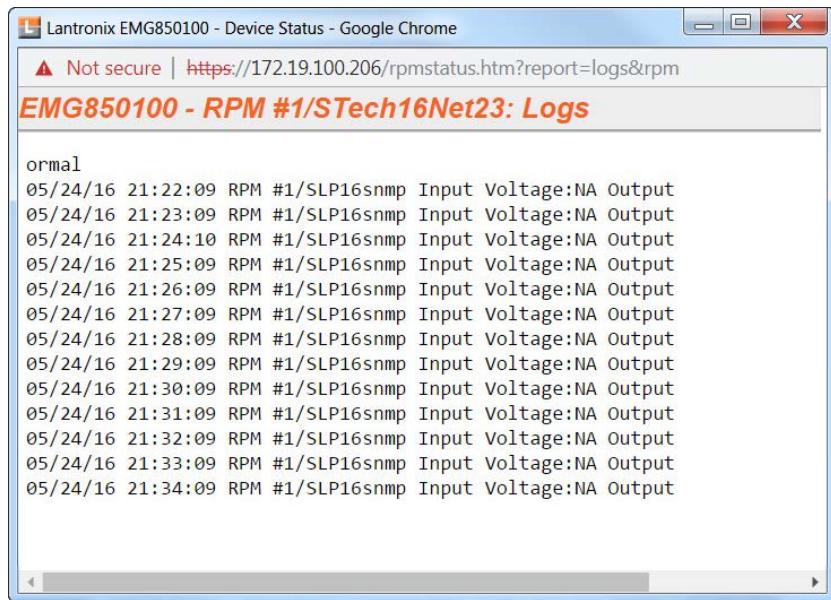
Figure 10-4 RPM Raw Data Log



The screenshot shows a Google Chrome window with the title "Lantronix EMG850100 - Device Status - Google Chrome". The address bar displays a warning: "Not secure | https://172.19.100.206/rpmstatus.htm?report=rawdata&rpmid=1". The main content area is titled "EMG850100 - RPM #1/STech16Net23: Raw Data". It displays a list of raw data parameters:

- ambient.2.humidity: 41.00
- ambient.2.temperature: 24.00
- device.mfr: Lantronix SLP
- device.model: Glenn-Tower
- device.serial: 13900002
- device.type: SLP PDU
- driver.name: snmp-ups
- driver.parameter.pollinterval: 2
- driver.parameter.port: 172.19.237.30
- driver.parameter.synchronous: no
- driver.version: 2.7.3
- driver.version.data: slp MIB 17.12.07
- driver.version.internal: 0.72
- outlet.1.desc: TowerA_Outlet1

Figure 10-5 RPM Logs

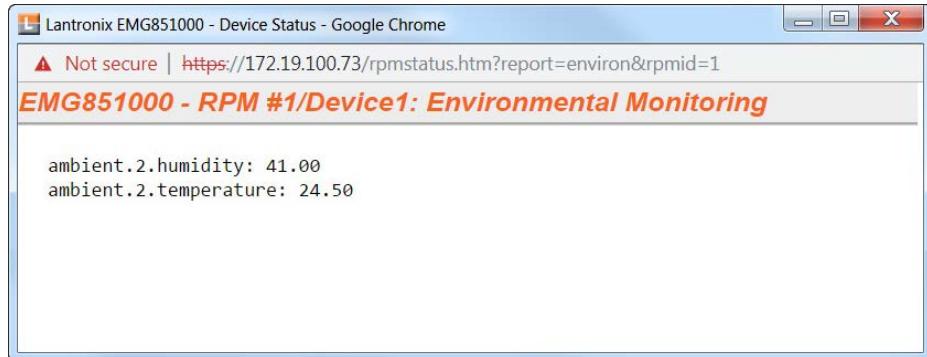


```

ormal
05/24/16 21:22:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:23:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:24:10 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:25:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:26:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:27:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:28:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:29:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:30:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:31:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:32:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:33:09 RPM #1/SLP16snmp Input Voltage:NA Output
05/24/16 21:34:09 RPM #1/SLP16snmp Input Voltage:NA Output

```

Figure 10-6 RPM Environmental Log



```

ambient.2.humidity: 41.00
ambient.2.temperature: 24.50

```

RPMs - Add Device

The **Add Device** page assists the administrator with adding a new managed RPM to the EMG configuration. With over 140 different vendors and nearly 1000 different models that are supported, the key to ensuring the EMG can properly manage a PDU or UPS is selecting the right model (with its associated driver) and any required driver options, especially for USB managed devices.

To add a new managed RPM :

1. Click the **Devices** tab and select the **RPMs** option. The RPMs page displays, as shown in [Figure 10-1](#).
2. On the [Devices > RPMs](#) page, click the **Add Device** link. [Figure 10-7](#) shows the RPMs - Add Device page.

Note: The [Devices > RPMs - Add Device](#) page with the same functionality can also be accessed through the [Device Ports > Settings \(1 of 2\)](#) page by selecting RPM in the Connected dropdown menu.

Figure 10-7 Devices > RPMs - Add Device

LANTRONIX® **EMG850100**

Logout Host: **emgfcb5** User: **sysadmin**

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

Devices **Maintenance** **Quick Setup**

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

RPMs - Add Device **Help?**

Vendor: **select one** (U) - USB, (S) - Serial, (N) - Network, (P) - SNMP

Model: **select one**

Managed via: USB Serial Network SNMP

USB Device: **select one**

Name:

of Outlets:

IP Address:

Port: Enter "0" for a front USB port.

Driver Opts:

Login:

Password:

Retype Password:

Log Status: No Yes, minutes:

Critical SNMP Traps:

Critical Emails:

Low Battery: Shutdown this UPS Shutdown all UPSes Allow battery failure Shutdown both EMG UPSes

Shutdown Order:

Provides EMG Power:

Apply

3. Enter the following:

Vendor	Select the correct vendor from the drop-down menu.
---------------	--

Model	Select the Model in the drop-down menu. The drop-down menu will be populated with models supported for the selected vendor. To the left of each model name is one or two letters in parentheses that indicate the type of control available for the selected model: P - SNMP, S - serial port, U - USB port, N - network. Some of the model names in the list may be truncated because the list of models is very long - in this case, hover over the model name and the complete model name(s) will be displayed.
Managed via	If there is more than one way to manage the selected model, select the appropriate management method.
USB Device	For USB controlled devices, if the RPM is connected to a USB port, the device should be displayed in the USB Device dropdown. Select the correct device. This will automatically fill in the Port with the correct port number and the Driver Opts with the USB vendor and product ID (see below).
Name	Specify the unique name of the RPM (up to 20 characters).
# of Outlets	Specify the number of outlets on the RPM (maximum of 120 outlets).
IP Address	For SNMP and Network (Telnet) managed RPMs, specify the IP address of the RPM.
Port	For network (Telnet) managed RPMs, this is assumed to be port 23 (if left blank), or it can be filled in with an alternate TCP port. For USB managed RPMs, this is the front USB port ("0") or the device port that the RPM is connected to on the EMG (this may be automatically filled in when the USB Device is selected). For serially controlled RPMs, this is the device port that the RPM is connected to on the EMG.
Driver Opts	For the driver associated with the RPM device, these are extra options which may be required to make the driver work. The most frequent use of the driver options is for USB devices (the vendor and product ID may be required so that the EMG can find the correct device on the USB bus), or in the event that the default driver options do not work with the RPM. The vendor and product ID may be automatically filled in if a USB Device is selected. There may also be other driver options that are filled in by the EMG from an internal table - these will be automatically set and can be viewed after the RPM has been added, and can always be overridden by driver options set by the user. For a complete list of RPM models, drivers and driver options, refer to the Network UPS Tools Hardware Compatibility List . The format of the driver options setting is one or more comma-separated parameters-value pairs, e.g. <parameter name>=<value>.
Login	For Network and serially managed RPMs, this is the administrator login.
Password/Retype Password	For Network and serially managed RPMs, this is the administrator password.
Read Community	For SNMP managed RPMs, this is the SNMP read (get) community.
Write Community/Retype Write Comm	For SNMP managed RPMs, this is the SNMP write (set) community.
Log Status	Indicates if the status of the RPM is periodically logged and the interval in minutes. Select Yes and enter a value between 1 and 60 minutes. The logs can be viewed by viewing the Devices > RPMs page and clicking on "Logs".
Critical SNMP Traps	If enabled, under critical conditions (UPS goes onto battery power, UPS battery is low, UPS forced shutdown in progress, UPS on line power, UPS battery needs to be replaced, RPM is unavailable, communications with RPM lost, communications with RPM established), a EMGEventRPMAction trap will be sent to the NMS configured in the SNMP settings. This requires that SNMP traps be enabled.

Critical Emails	If an email address is specified, under critical conditions (see Critical SNMP Traps above), an email notification will be sent to the email address. The Server and Sender configured in the SMTP settings will be used to send the email.
Low Battery	For UPS devices only. Indicates the behavior to take when the UPS reaches a low battery state. Options are to Shutdown this UPS - shutdown only the UPS that has reached a low battery state; Shutdown all UPSes - shutdown all UPSes managed by the EMG; Allow battery failure - allow the battery to completely fail, which may result in the unsafe shutdown of the devices it provides power to; Shutdown both EMG UPSes - shutdown both UPSes that provide power to the EMG, including the UPS with that has reached a low battery state (some EMGs have dual power supplies). For more information, see RPM Shutdown Procedure .
Shutdown Order	For UPS devices only. If any of the UPSes managed by the EMG reaches a low battery state AND is configured for Shutdown all UPSes for its Low Battery setting, this indicates the order in which this UPS will be shutdown. All UPSes with a shutdown order of "1" will be shutdown first, followed by all UPSes with a shutdown order of "2", etc. Shutdown orders are in the range of 1 to 49, with 50 being reserved for UPSes that provide power to the EMG - they will always be shutdown last (see Provides EMG Power below).
Provides EMG Power	For UPS devices only. Indicates if this UPS provides power to the EMG.

4. Click **Apply** to Save.

RPMs - Manage Device

The **Manage Device** page allows the administrator to modify the settings for a managed RPM.

To modify a managed RPM:

1. Click the **Devices** tab and select the **RPMs** option. [Figure 10-1 Devices > RPMs](#) shows the page which displays.
2. Select an RPM and click the **Manage Device** link. [Figure 10-8 RPMs - Manage Device](#) shows the page which displays.

Figure 10-8 RPMs - Manage Device

LANTRONIX® EMG850100

Logout Host: emgfcb5 User: sysadmin

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

Devices

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

RPMs - Manage Device [Help ?](#)

RPM Id: 1

Name: Managed via: **Network**

Status: IP Address: Port:

Vendor: **ServerTech** Driver Opts:

Model: **Sentry3, A1-8 (8 outlets)**

of Outlets: Login:

Outlets On: **N/A** Password:

F/W Version: **[none]** Retype Password:

Serial Num: **[none]** Log Status: No Yes, minutes:

MAC Address: **[none]** Critical SNMP Traps:

Apparent Power: **N/A** Critical Emails:

Nominal **N/A** Shutdown this UPS

Apparent Power: **N/A** Shutdown all UPSes

Real Power: **N/A** Allow battery failure

Nominal **N/A** Shutdown both EMG UPSes

Real Power: **N/A**

Shutdown Order:

Provides EMG Power:

[Outlets >](#)

3. Enter the following:

RPM Id (view only)	The unique number associated with the RPM.
Name	Specify the unique name of the RPM (up to 20 characters).
Status (view only)	The current status of the RPM. Any error status will be shown here.
Vendor (view only)	The manufacturer of the RPM.
Model (view only)	The model of the RPM. The model is read from the device, if it is provided; not all RPMs provide a model string. If the device normally provides the device model and becomes unreachable, or does not provide a model string, the Model is derived from the supported model list strings.
# of Outlets	Specify the number of outlets on the RPM (maximum of 120 outlets).
Outlets On (view only)	The number of outlets that are currently turned on, if this information is provided by the RPM.
F/W Version (view only)	The firmware version of the RPM, if this information is provided by the RPM.
Serial Num (view only)	The serial number of the RPM, if this information is provided by the RPM.
MAC Address (view only)	The MAC address of the RPM, if this information is provided by the RPM.

Current (view only)	The total current value for the RPM in Amperes, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own current value, both current values will be displayed, separated by a slash.
Input Voltage (view only)	The input voltage for the RPM in Volts, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own input voltage value, both voltage values will be displayed, separated by a slash.
Apparent Power (view only)	The apparent power value for the RPM in Volt-Amperes, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own apparent power value, both power values will be displayed, separated by a slash.
Nominal Apparent Power (view only)	The nominal apparent power value for the RPM in Volt-Amperes, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own nominal apparent power value, both power values will be displayed, separated by a slash.
Real Power (view only)	The real power value for the RPM in Watts, if this information is provided by the RPM. If the RPM consists of two separate towers or units, each with its own real power value, both power values will be displayed, separated by a slash.
Battery Charge (view only)	For UPS devices only. Displays the current charge level for the battery, as a percentage.
Battery Runtime (view only)	For UPS devices only. Displays the amount of time remaining in the UPS battery life.
Beeper Status (view only)	For UPS devices only. Displays the current state of the UPS beeper.
Managed via (view only)	Displays the method used to control the RPM device (SNMP, Network, Serial Port, USB port).
IP Address	For SNMP and Network (Telnet) managed RPMs, specify the IP address of the RPM.
Port	For network (Telnet) managed RPMs, this is assumed to be port 23 (if left blank), or it can be filled in with an alternate TCP port. For USB managed RPMs, this is one of the front USB ports ("0") or the device port that the RPM is connected to on the EMG. For serially controlled RPMs, this is the device port that the RPM is connect to on the EMG.
Driver Opts	For the driver associated with the RPM device, these are extra options which may be required to make the driver work. The most frequent use of the driver options is for USB devices (the vendor and product ID may be required so that the EMG can find the correct device on the USB bus), or in the event that the default driver options do not work with the RPM. There may also be other driver options that are filled in by the EMG from an internal table - these will be automatically set and can be viewed after the RPM has been added, and can always be overridden by driver options set by the user. For a complete list of RPM models, drivers and driver options, refer to Network UPS Tools Hardware Compatibility List . The format of the driver options setting is one or more comma-separated parameters-value pairs, e.g. "<parameter name>=<value>".
Login	For Network and serially managed RPMs, this is the administrator login.
Password/Retype Password	For Network and serially managed RPMs, this is the administrator password.
Read Community	For SNMP managed RPMs, this is the SNMP read (get) community.
Write Community/Retype Write Comm	For SNMP managed RPMs, this is the SNMP write (set) community.

Log Status	Indicates if the status of the RPM is periodically logged. Select Yes, minutes to log the status periodically and enter a value between 1 and 60 minutes. The logs can be viewed by viewing the RPMs web page and clicking on "Logs".
Critical SNMP Traps	If enabled, under critical conditions (UPS goes onto battery power, UPS battery is low, UPS forced shutdown in progress, UPS on line power, UPS battery needs to be replaced, RPM is unavailable, communications with RPM lost, communications with RPM established), a slcEventRPMAction trap will be sent to the NMS configured in SNMP settings. This requires that SNMP traps be enabled.
Critical Emails	If an email address is specified, under critical conditions (see Critical SNMP Traps above), an email notification will be sent to the email address. The Server and Sender configured in the SMTP settings will be used to send the email.
Low Battery	For UPS devices only. Indicates the behavior to take when the UPS reaches a low battery state. Options are to Shutdown this UPS - shutdown only the UPS that has reached a low battery state; Shutdown all UPSes - shutdown all UPSes managed by the EMG; Allow battery failure - allow the battery to completely fail, which may result in the unsafe shutdown of the devices it provides power to; Shutdown both EMG UPSes - shutdown both UPSes that provide power to the EMG, including the UPS with that has reached a low battery state (some EMGs have dual power supplies). For more information, see RPM Shutdown Procedure
Shutdown Order	For UPS devices only. If any of the UPSes managed by the EMG reaches a low battery state AND is configured for Shutdown all UPSes for its Low Battery setting, this indicates the order in which this UPS will be shutdown. All UPSes with a shutdown order of "1" will be shutdown first, followed by all UPSes with a shutdown order of "2", etc. Shutdown orders are in the range of 1 to 49, with 50 being reserved for UPSes that provide power to the EMG - they will always be shutdown last (see Provides EMG Power in the next field below).
Provides EMG Power	For UPS devices only. Indicates if this UPS provides power to the EMG.

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

RPMs - Outlets

The **Outlets** page allows the administrator to view the current status of each individual outlet on an RPM, and change the state of the outlets. Not all RPMS support individual outlet status and control.

To control and view status for RPM outlets:

1. Click the **Devices** tab and select the **RPMs** option. *Figure 10-1 Devices > RPMs* shows the page which displays.
2. Select an RPM and click the **Outlets** link. *Figure 10-9 RPMs - Outlets* shows the page which displays. This page will, at a minimum, list the outlet numbers and their state - **On** or **Off**. If the RPM provides additional information for the outlets, the custom name and the current reading in Amperes will also be displayed for each outlet.

Figure 10-9 RPMs - Outlets

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, it displays the host as 'emgfcf0' and the user as 'sysadmin'. The navigation bar includes links for Network, Services, User Authentication, Devices (which is selected), Maintenance, and Quick Setup. Below the navigation bar is a sub-navigation bar with links for Device Status, Device Ports, Console Port, USB / SD Card, RPMs (which is selected), Connections, Xmodem, Host Lists, Scripts, and Sites. The main content area is titled 'RPMs - Outlets' and contains a table with the following data:

RPM #3-STech16SNMP			Outlet:	Cycle Power	Turn On	Turn Off
Id	State	Description	Current (amps)			
1	on	Outlet1	0.00			<input type="checkbox"/>
2	on	TowerA_Outlet2	0.00			<input type="checkbox"/>
3	on	TowerA_Outlet3	0.00			<input type="checkbox"/>
4	on	TowerA_Outlet4	0.00			<input type="checkbox"/>
5	on	TowerA_Outlet5	0.00			<input type="checkbox"/>
6	on	TowerA_Outlet6	0.00			<input type="checkbox"/>

3. To change the state of one or more outlets, select the outlets, and click the **Cycle Power**, **Turn On** or **Turn Off** buttons. The command will be sent to the RPM and the page will refresh. It may take one or two minutes before the new outlet state(s) are reflected on the Outlets page.

RPM Shutdown Procedure

This section applies to UPS-type RPMS only, and does not apply to PDU-type RPMS. This section describes the shutdown process when a UPS managed by the EMG reaches a low battery state. When one UPS reaches a low battery state, the EMG can be configured to allow the UPS to

continue to run until its battery fails completely, to shutdown just the UPS with the low battery, or to shutdown one or more UPSes. UPS-type RPMs can report the following states:

- ◆ **OL** - On line power
- ◆ **OB** - On battery power
- ◆ **LB** - Low battery
- ◆ **HB** - High battery
- ◆ **RB** - The battery needs to be replaced
- ◆ **CHRG** - The battery is charging
- ◆ **DISCHRG** - The battery is discharging (inverter is providing load power)
- ◆ **BYPASS** - UPS bypass circuit is active - no battery protection available
- ◆ **CAL** - UPS is currently performing runtime calibration (on battery)
- ◆ **OFF** - UPS is offline and is not supplying power to the load
- ◆ **OVER** - UPS is overloaded
- ◆ **TRIM** - UPS is trimming incoming voltage
- ◆ **BOOST** - UPS is boosting incoming voltage
- ◆ **FSD** - UPS is in forced shutdown due to a critical condition

Once a UPS is on line power (status is **OL**) and goes off of line power and onto battery power (status is **OB**), it may reach a low battery state (status is **OB**, **LB** or **LB**). Switching from line power to battery power, and reaching a low battery state are critical states that can result in syslog, email and SNMP trap notifications. The exact point at which a UPS reaches a low battery state is device dependent and is related to the **battery.charge**, **battery.charge.low**, **battery.runtime** and **battery.runtime.low** settings which can be viewed in the "Raw Data" report.

Once a UPS reaches a low battery state, the **Shutdown Order**, **Low Battery Action** and **Provides EMG Power** settings determine which UPSes to shutdown, and in what order. The UPS with the low battery will be placed into **FSD** (Forced Shutdown) mode. The following actions will be performed based on the **Low Battery Action** setting for the UPS with the failed battery:

- ◆ **Allow Battery Failure** - The UPS battery will be allowed to run until it fails completely. If the UPS provides power to the EMG and the battery fails, the EMG will not be cleanly shutdown. In this scenario, the **Shutdown Order** setting will be ignored. The **Shutdown Order** setting may be used if another UPS reaches the low battery state (see **Shutdown all UPSes** below).
- ◆ **Shutdown This UPS** - If the UPS provides power to the EMG, the EMG will begin shutdown procedures, shutting down the UPS last. If the UPS does not provide power to the EMG, the UPS will be shutdown, but will continue to be monitored in case it comes back online.
- ◆ **Shutdown all UPSes** - The EMG will begin shutting down all UPSes with a non-zero **Shutdown Order**, shutting down UPSes with a shutdown order of "1" first, UPSes with a shutdown order of "2" second, etc. Any UPS which provides power to the EMG is always forced to have its **Shutdown Order** set to 50, which is the highest (and last) Shutdown Order. If the UPS with the failed battery provides power to the EMG (and thus has a Shutdown Order set to 50), the EMG will also begin shutdown procedures, shutting down the failed UPS last. If none of the UPSes provide power to the EMG, after they are all shutdown their drivers will remain running in case the UPS comes back online. In this case, any queries to an RPM while it is still offline may report "RPM driver data is stale". If the **Low Battery Action** for a UPS is set to **Allow Battery Failure**, but the UPS has a non-zero **Shutdown Order**, the UPS

will still be shutdown if another UPS reaches the low battery state and has its **Low Battery Action** set to **Shutdown all UPSes**.

- ◆ **Shutdown Both EMG UPSes** - This setting should only be used on dual-power EMG units which have each power supply connected to separate (different) UPS devices, and both UPS devices are being managed by the EMG. If a UPS is configured for **Shutdown Both EMG UPSes** but does not have **Provides EMG Power** enabled, this is an ambiguous configuration, and no shutdown action will occur.

For this configuration, when one of the UPSes providing power to the EMG reaches a low battery state, the event will be noted in the system log, and the EMG will continue to run with no further actions until the second UPS providing power to the EMG reaches a low battery state. At this point the EMG will begin shutdown procedures, shutting down both failed UPSes last.

Optimizing and Troubleshooting RPM Behavior

This section gives tips on how to optimize the management of specific PDUs and UPSes, and how to troubleshoot any problems with the EMG connecting to and managing an RPM.

- ◆ **Sentry3 - Network and Serially Managed PDUs** - Some Sentry3 PDUs have a CLI timeout, with a default setting of 5 minutes. This timeout may cause frequent query errors when requesting information from the Sentry3 PDU. It is recommended that the timeout be set as high as possible to reduce the frequency of the query errors.
- ◆ **Serially Managed RPMs with Administrator Logins** - Some serially managed devices will have an administrator login for the console port. It is recommended that any active sessions be logged out before adding the device as an RPM, otherwise the RPM may experience query errors.

If the EMG is unable to communicate with an RPM, or an RPM is displaying the error "driver is not running", the following steps can be used to troubleshoot the driver issues:

- ◆ **Correct Driver** - The CLI command `set rpm driver <RPM Id or Name> action show` can be used to display the current running driver for the RPM. Some serially and network managed RPMs do not have drivers; if this is the case for the RPM, the CLI command will indicate this. Otherwise it will display the driver that is running for the RPM, and it should match the driver listed for the device at [Network UPS Tools Hardware Compatibility List](#). If the wrong driver is shown, the RPM will need to be deleted and re-added, with the correct vendor and model selected. If no driver is shown, the driver may not be able to start for a variety of reasons; see remaining steps.
- ◆ **SNMP Settings** - For SNMP managed devices, verify the **IP Address**, **Read Community** and **Write Community** settings are correct.
- ◆ **Reverse Pinout Setting** - For serially managed devices, verify the **Reverse Pinout** setting (located in the [Device Ports - Settings](#) page) is set correctly.
- ◆ **VendorId and ProductId Driver Options** - For USB managed devices, verify the `vendorid` and `productid` shown in the RPM driver options are correct. These can be set automatically by the EMG from an internal table, set by the user by selecting a specific USB device when adding a USB-managed RPM, or changed by the user at any time. The CLI command `show usb devices` displays all connected USB devices with their port, Product ID and Vendor ID.
- ◆ **Extra Driver Options** - The driver documentation at [Network UPS Tools Hardware Compatibility List](#) may indicate that extra driver options are required for the RPM. Select the driver name link under the Driver column to see any special requirements for the UPS or PDU.

- ◆ **Driver Debug Mode** - The driver can be run in debug mode at the CLI and the output examined to determine why the driver is not starting or is unable to communicate with the RPM. The CLI command `set rpm driver <RPM Id or Name> action debug [level <1|2|3>]` will stop any currently running driver and restart the driver in debug mode with output sent to a local file. Running `set rpm driver <RPM Id or Name> action show` should show a driver running with one or more `-D` flags. The debug output can be examined or emailed with the `set rpm driver <RPM Id or Name> action viewoutput [email <Email Address>] [display <head|tail>] [numlines <Number or Lines>]` command. To return the driver to its normal non-debug state, run `set rpm driver <RPM Id or Name> action restart`. Note that drivers running in debug mode will generate copious output, and for disk space reasons should not be left running in debug mode for long periods of time (e.g. more than an hour).

RPM Commands

Go to [RPM Commands](#) to view CLI commands which correspond to the web page entries described above.

11: Scripts

This chapter describes how to use Scripts to automate tasks performed on the EMG CLI or on device ports. EMG supports the following types of scripts:

- ◆ **Interface Scripts** which use a subset of the Expect/Tcl scripting language to perform pattern detection and action generation on Device Port output.
- ◆ **Batch Scripts** which are a series of CLI commands.
- ◆ **Custom Scripts** are Expect, Tcl or Python scripts which use most of the Expect/Tcl/Python scripting language, can be run against the CLI or a Device Port, and can be [scheduled](#) to run at periodic intervals, with the results from each run saved to a file in a repository. Up to 10 Custom Scripts can be created. Each Custom Script run is an operation, and the [results](#) from each operation can be [viewed](#). Up to 50 script result files will be saved locally in the EMG storage. Once this maximum is reached and new result files are generated, the oldest result files will automatically be deleted to accommodate the new result files.

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

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

To add a script:

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

Figure 11-1 Devices > Scripts

The screenshot shows the EMG851000 web interface with the following details:

- Header:** LANTRONIX® EMG851000, Logout, Host: emgfcf0, User: sysadmin.
- Top Navigation:** Network, Services, User Authentication, **Devices** (selected), Maintenance, Quick Setup.
- Sub-Header:** Device Status, Device Ports, Console Port, USB / SD Card, RPMs, Connections, Xmodem, Host Lists, Scripts, Sites.
- Current Page:** Scripts.
- Script Table:** 1 Script(s) named "getdevicetemp".

Name	Type	Grp	State	Start Time	Freq (H)	Stop Time	Device	Status
getdevicetemp	Interface	Def	N/A	N/A	N/A	N/A	N/A	N/A
- Buttons:** Add Script, Rename Script, Refresh, Latest Script Results, Script Operations.

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

Figure 11-2 Adding or Editing New Scripts

LANTRONIX® EMG851000

Logout Host: emgfof0 User: sysadmin Select port for Configuration WebSSH (DP only) Connected Device (DP only)

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

Scripts Help?

Script Name:

Type: Interface Batch Custom

User Rights

Group: Default Users Power Users Administrators

Full Administrative: Local Users: Firmware & Configuration:
 Networking: Remote Authentication: Internal Modem:
 Services: SSH Keys: Device Port Operations:
 Secure Lantronix Network: User Menus: Device Port Configuration:
 Date/Time: Web Access: USB:
 Reboot & Shutdown: Diagnostics & Reports: SD Card:
 RPMs:

[Back to Scripts](#)

3. Enter the following script details:

Script Name	A unique identifier for the script.
Type	<ul style="list-style-type: none"> ◆ Select Interface for a script that utilizes Expect/Tcl to perform pattern detection and action generation on Device Port output. ◆ Select Batch for a script of CLI commands. ◆ Select Custom for an Expect, Tcl or Python script that can be run against a CLI session or a Device Port, either manually or scheduled to run at periodic intervals.

Script Text	In the free-form editing box, enter the contents of the script. Restrictions on the script format are described in Batch Script Syntax , Interface Script Syntax , and Custom Script Syntax .
Group	<p>Select the group to which the script will belong:</p> <ul style="list-style-type: none"> ◆ Default Users: This group has only the most basic rights. You can specify additional rights for the individual user. ◆ Power Users: This group has the same rights as Default Users plus Networking, Date/Time, Reboot & Shutdown, and Diagnostics & Reports. You can specify additional rights for the individual user. ◆ Administrators: This group has all possible rights. <p>For more information on how the group and rights are used with scripts, see To use a script at the CLI:</p>

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure Lantronix units (e.g., EMG or SLC devices) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the EMG unit.
RPMs	Right to view and enter Remote Power Manager (RPM) settings.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown.
Internal Modem	Right to configure internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port configurations.
USB	Right to enter modem settings for USB modems and to control USB storage devices.
SD Card	Right to view and enter settings for SD card.

5. To save, click the **Apply** button. If the type of script is **Interface** or **Custom**, the script will be validated before it is saved. Once the script is saved, the main [Devices > Scripts](#) page is displayed.

To view or update a script:

1. In the Scripts table, select the script and click the **Edit Script** button. The page for editing script attributes displays (see [Figure 11-2](#)).
2. Update the script attributes (see [To add a script](#) above).
3. To save, click the **Apply** button.

To rename a script:

1. In the Scripts table, select the script and enter a new script name in the **New Name** field.
2. Click the **Rename Script** button. The script will be renamed and the [Devices > Scripts](#) page redisplays.

To delete a script:

1. In the Scripts table, select the script to delete.
2. Click the **Delete Script** button. After a confirmation, the script will be deleted and the [Devices > Scripts](#) page redisplays.

To schedule a custom script:

1. In the Scripts table, select the script and click the **Schedule** button. The Custom Scripts - Schedule page displays.

Figure 11-3 Scripts > Custom Scripts - Scheduler

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, it displays 'LANTRONIX® EMG851000' and the host information 'Host: emgfcf0' and 'User: sysadmin'. A navigation bar includes 'Logout', 'Network', 'Services', 'User Authentication', 'Devices' (which is selected), 'Maintenance', 'Quick Setup', and icons for Home, Help, and Configuration. A port map shows four ports: U1, E1, 1, 3 (top row) and SD, E2, 2, 4 (bottom row). The main content area is titled 'Custom Scripts - Schedule'. It contains the following fields:

- Script Name:
- Device Type: CLI Device Port:
- State: Enable Disable Delete
- Command Line Arguments:
- Start Time: Now At Date/Time:
- Stop Time: Forever At Date/Time:
- Frequency: Hours Days

At the bottom are 'Back to Scripts' and 'Apply' buttons.

2. Enter the following (each Custom Script can be run against one device - CLI or Device Port -

with one schedule):

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

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

Notes on scheduling:

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

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

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

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

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

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

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

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

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

The results are displayed in a popup window.

To use a script at the CLI:

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

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

Script Commands

Go to [Script Commands](#) to view CLI commands which correspond to the web page entries described above.

Batch Script Syntax

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

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

```
sleep <value>
```

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

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

```

...
    CLI command n
}

```

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

Interface Script Syntax

This section describes the abbreviated scripting syntax for Interface Scripts. This limited syntax was created to prevent the creation of scripts containing potentially harmful commands. Script commands are divided into three groups: Primary, Secondary and Control Flow.

Primary commands provide the basic functionality of a script and are generally the first element on a line of a script, as in:

```
send_user "Password:"
```

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

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

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

Table 11-4 Interface Script Syntax Definitions

Term	Definition
Word	A contiguous group of characters delimited on either side by spaces. Not enclosed by double quotes.
Primary Command	One of the primary commands listed in this section.
Secondary Command	One of the secondary commands defined in this section.
Quoted String	A group of characters enclosed by double quote ("") characters. A quoted string may include any characters, including space characters. If a double quote character is to be included in a quoted string it must be preceded (escaped) by a backslash character ('\').
Variable Reference	A word (as defined above) preceded by a dollar sign character ('\$').
CLI Command	A quoted string containing a valid CLI show command.
Arithmetic Operator	A single character representing a simple arithmetic operation. The character may be one of the following: <ul style="list-style-type: none"> ◆ A plus sign (+) representing addition ◆ A minus sign (-) representing subtraction ◆ An asterisk sign (*) representing multiplication ◆ A forward slash (/) representing division ◆ A percent sign (%) representing a modulus

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

Primary Commands

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

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

Table 11-5 Primary Commands

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

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

Secondary Commands

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

Table 11-6 Secondary Commands

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

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

Control Flow Commands

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

Table 11-7 Control Flow Commands

Command	Description
while	The while command executes an associated block of commands as long as its Boolean expression evaluates to TRUE. After each iteration the Boolean expression is re-evaluated; when the Boolean expression evaluates to FALSE execution passes to the first command following the associated block. Each command within the block must be a Primary command. Syntax: while {<Boolean expression>} { command 1 command 2 ... command n }

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

Custom Script Syntax

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

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

Note:

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

◆ Expect script - CLI session

```
spawn clisession -U <username>
```

◆ Expect script - Device Port session

```
spawn portsession -p $devicePort
```

◆ Tcl script - CLI session

```
set io [open "| clisession -U <username>" r+]
```

◆ Tcl script - Device Port session

```
set io [open "| portsession -p $devicePort" r+]
```

◆ Python script - CLI session

```
subprocess.Popen(['clisession', '-U', '<username>'],
                stdin=subprocess.PIPE,
                stdout=subprocess.PIPE,
                stderr=subprocess.PIPE)
```

◆ Python script - Device Port session

```
subprocess.Popen(['portsession', '-p', devicePort],
                stdin=subprocess.PIPE,
                stdout=subprocess.PIPE,
                stderr=subprocess.PIPE)
```

5. It is recommended that scripts that spawn `clisession` only be used with the `set script runcli` command (and not the `connect script` command), and that scripts that spawn `portsession` only be used with the `connect script` command (and not the `set script runcli` command).
6. The script cannot contain commands which spawn or fork other commands, read or write files on the EMG filesystem, or interrogate the EMG filesystem. The list of commands that are not

allowed for Expect scripts includes "fork", "open", "exp_open", "exec", "system", "log_file", "pwd".

7. For scripts that return an exit code, the EMG will interpret an exit code of zero as a successful exit code, and any non-zero exit code as an error. Non-zero exit codes are displayed (at the CLI) or logged (for scripts that are run by the script scheduler).

Example Scripts

Interface Script—Monitor Port

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

```
set monPort 7
set monTime 5
set sleepTime 2
set prompt ">"
set login "sysadmin"
set pwd "PASS"
#Send CR to echo prompt
send "\r"
sleep $sleepTime
#Log in or check for Command Prompt
expect {
    #Did not capture "login" or Command Prompt
    timeout { send_user "Time out login.....\r\n"; return }
    #Got login prompt
    "login" {
        send_user "Logging in....\r\n"
        send "$login\r"
        expect {
            timeout { send_user "Time out waiting for pwd
                prompt.....\r\n"; return }
            #Got password prompt
            "password" {
                #Send Password
                send "$pwd\r"
                expect {
                    timeout { send_user "Time out waiting for prompt.....\r\n";
                        return }
                    $prompt {}
                }
            }
        }
    }
    #Already Logged in got Command Prompt
    $prompt {
        send_user "Already Logged....\r\n"
    }
}
```

```

        }
    }
#Get hostname info
send "show network port 1 host\r"
expect {
    timeout { send_user "Time out Getting Hostname 1\r\n"; return }
    "Domain" {
        #Get Hostname from EMG
        set hostname "[string range $expect_out(buffer) [string first
                      Hostname:
                      $expect_out(buffer)] [expr [string first Domain
                      $expect_out(buffer)]-2]]"
    }
}
send_user "\r\n\r\n\r\n\r\n\r\n"
send_user "Device [string toupper $hostname]\r\n"
send_user "_____\r\n"
send_user "Monitored Port: Port $monPort \r\n"
send_user "Monitor Interval Time: $monTime Seconds \r\n"
set loopCtr 0
set loopMax 2
while { $loopCtr < $loopMax } {
    #Get current time

```

The following is the screen output:

```

emg247]> conn script ex4 deviceport 7
login: Logging in.... sysadmin sysadmin
Password: PASS
Welcome to the Lantronix Edge Management Gateway
Model Number: EMG851101
For a list of commands, type 'help'.
[EMG251]> show network port 1
host show network port 1 host
    _____Current Hostname Settings_____
Hostname: EMG251
Domain: support.int.lantronix.com
[EMG251 Device HOSTNAME: EMG251

_____
Monitored Port: Port 7
Monitor Interval Time: 5 Seconds
[Current Time:21:16:43]
show portcounter deviceport 7
[EMG251]> show portcounter deviceport 7
Device Port: 7 Seconds since zeroed: 1453619
Bytes input: 0 Bytes output: 0
Framing errors: 0 Flow control errors: 0
Overrun errors: 0 Parity errors: 0
[EMG251]>
[Current Time:21:16:58]
show portcounter deviceport 7
show portcounter deviceport 7
Device Port: 7 Seconds since zeroed: 1453634

```

```
Bytes input: 0 Bytes output: 0
Framing errors: 0 Flow control errors: 0
Overrun errors: 0 Parity errors: 0 [
EMG251]>
Port Counter Monitor Script Ending.....
```

```
Login Out.....
logout
Returning to command line
[emg247]>
```

Batch Script—EMG CLI

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

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

The following is the screen output of the script:

```
[emg247]> se script runcli cli
[emg247]> show network port 1 host
____ Current Hostname Settings _____
Hostname: emg247
Domain: <none>
[emg247]>
[emg247]> show deviceport names
____ Current Device Port _____
Names _____
01 - SCS_ALIAS_Test 05 - Port-5
02 - Port-2 06 - Port-6
03 - Port-3 07 - EMG251
04 - Port-4 08 - Port-8
[emg247]>
[emg247]> show script
____ Interface Scripts _____ Group/Permissions _____
getSLC Adm/ad,nt,sv,dt,lu,ra,um,dp,pc,rs,fc,dr,sn,wb,sk,po,do
Test Adm/ad,nt,sv,dt,lu,ra,um,dp,pc,rs,fc,dr,sn,wb,sk,po,do
monport Adm/<none>
____ Batch Scripts _____ Group/Permissions _____
cli Adm/ad,nt,sv,dt,lu,ra,um,dp,pc,rs,fc,dr,sn,wb,sk,po,do,rp
[emg247]>
[emg247]> connect script monport deviceport 7
login: Logging in.....
sysadmin
sysadmin
Password: PASS
Welcome to the Lantronix Edge Management Gateway
Model Number: EMG851101
For a list of commands, type 'help'.
```

```
[EMG251]> show network port 1 host
show network port 1 host
  Current Hostname Settings
Hostname: EMG251
Domain: support.int.lantronix.com
Device HOSTNAME: EMG251
  Monitored Port: Port 7
  Monitor Interval Time: 5 Seconds
  [Current Time:21:25:04]
  show portcounter deviceport 7
[EMG251]> show portcounter deviceport 7
Device Port: 7 Seconds since zeroed: 1454120
  Bytes input: 0 Bytes output: 0
  Framing errors: 0 Flow control errors: 0
  Overrun errors: 0 Parity errors: 0
[EMG251]>
  [Current Time:21:25:20]
  show portcounter deviceport 7
  show portcounter deviceport 7
  Device Port: 7 Seconds since zeroed: 1454136
  Bytes input: 0 Bytes output: 0
  Framing errors: 0 Flow control errors: 0
  Overrun errors: 0 Parity errors: 0
[EMG251]>
  Port Counter Monitor Script Ending.....
```

```
Login Out.....
logout
Returning to command line
[emg247]>
```

Expect Custom Script - EMG CLI Session

An example of an Expect Custom Script that interacts with an EMG CLI session:

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

set emgPrompt ">"
set emgTemp    "unknown"
set location   ""

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

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

```

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

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

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

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

set timeout 10
log_user 0

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

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

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

```

```
set emgTemp $expect_out(1,string)
myprint "Temperature: $emgTemp"
```

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

This script can be run manually at the CLI:

```
[emga508] set script runcli cliExample parameters "East Data Center"
Internal temperature of the East Data Center SLC at 01/27/2019 02:07
Temperature: 48C (118F)
```

Expect Custom Script - EMG Device Port Session

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

```
#! expect
#
# Script to get the load of a ServerTech PDU outlet
#
set pduPrompt ">"
set pduLoad "unknown"

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

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

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

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

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

```

set timeout 10
log_user 0

#
# Login to the PDU
# The "Error:*" pattern matches all error messages output by portsession
#
send "\n"
expect {
    "Username:" { send "admnn\n" }
    "Error:*\r\n" { send_user $expect_out(0,string); abortSession 2 }
}
expect "Password:"
send "admnn\n"

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

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

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

expect $pduPrompt
exp_send "logout\n"

sleep .5
close
exit 0

```

Expect Custom Script - EMG Device Port Session

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

```
#! expect
#
# Save a copy of the running config of a Cisco server to a TFTP server
# The Cisco server is connected to an EMG device port
#
#proc myprint {str} {
#    send_user -- "$str\n"
#}
#
proc abortSession {err} {
    send_user "Error $err. Terminating session.\n"
    exit $err
}
#
if {$argc < 2} {
    myprint "Usage: script_md_cisco.exp <TFTP Server> <Backup File Name>"
    abortSession 1
}
#
set tftp [lindex $argv 0]
set configFile [lindex $argv 1]
set enablePassword "secret"
set timeout 10
#
set now [clock seconds]
set date [clock format $now -format {%D %R}]
myprint "Backing up Cisco Server to $tftp:$configFile at $date"
#
# spawn the port session on a device port
if {[catch {spawn -noecho portsession -p $devicePort} result]} {
    abortSession 2
}
set sessionId $spawn_id
#
# Handle eof
expect_after {
    -i $sessionId eof {
        myprint "Session unexpectedly terminated."
        abortSession 3
    }
}
#
log_user 0
#
# Send carriage return, see if we are connected
set loggedIn false
```

```

set execMode false
set passwordPrompt false
set cnt 1
while {! $loggedIn || ! $execMode} {
    if {$cnt == 5} {
        myprint "Timeout waiting for > or # prompt"
        abortSession 4
    }
    if {! $passwordPrompt} {
        send "\r"
    }
    expect {
        "*password: " { send "$enablePassword\r" }
        ">" { set loggedIn true; set passwordPrompt true; send "enable\r" }
        "#" { set loggedIn true; set execMode true }
        "Error:*\r\n" { send_user $expect_out(0,string); abortSession 5 }
        timeout {set cnt [expr {$cnt + 1}] }
    }
}
myprint "Logged in."

send "copy running-config tftp://$tftp/$configFile\r"
expect "$tftp"
send "\r"
expect "$configFile"
send "\r"
myprint "Backup initiated."
expect {
    "!!" { myprint "Successfully backed up." }
    timeout { myprint "Timeout waiting for backup to complete.";
    abortSession 6 }
}
send "exit\r"

sleep .5
close
exit 0

```

Python Custom Script - EMG CLI Session

An example of a Python Custom Script that interacts with a CLI session:

```

#! python
# Script to set the RADIUS authentication settings of the EMG
# Sets the first RADIUS server and secret, and enables RADIUS
# Note: passing secret as a command line parameter is a security
vulnerability
# Usage:
#   script_cli_radius.py <RADIUS server> <RADIUS secret>
#

```

```

import subprocess
import datetime
import sys

num_args = len(sys.argv) - 1
if num_args < 2:
    print("Usage: script_cli_radius.py <RADIUS server> <RADIUS secret>")
    sys.exit(1)

print("Settings RADIUS server on EMG at ", end="")
now = datetime.datetime.now()
print(now.strftime("%Y-%m-%d %H:%M"))

server = sys.argv[1]
secret = sys.argv[2]

proc = subprocess.Popen(['clisession', '-U', 'sysadmin'],
                      stdin=subprocess.PIPE,
                      stdout=subprocess.PIPE,
                      stderr=subprocess.PIPE)

# wait for prompt
while True:
    output_str = proc.stdout.readline()
    if b'list of commands' in output_str:
        proc.stdin.write(b'\n')
        proc.stdin.flush()
    if b']>' in output_str:
        break
    if b'Invalid local user' in output_str:
        print("Invalid local user passed to clisession.")
        proc.stdin.close()
        proc.terminate()
        proc.wait()
        sys.exit(1)

# Run the RADIUS command
s = "set radius server 1 host " + server + " secret " + secret + "\n"
b = bytearray(s.encode())
proc.stdin.write(b)
proc.stdin.flush()
while True:
    output_str = proc.stdout.readline()
    if b'RADIUS settings successfully updated' in output_str:
        break
    elif b'set radius' not in output_str:
        # RADIUS command returned an error
        s1 = str(output_str)
        s2 = s1.split("\r") [1]
        print("RADIUS command returned: " + s2.split("\n") [0])
    proc.stdin.close()
    proc.terminate()
    proc.wait()
    sys.exit(1)

```

```

proc.stdin.write(b'set radius state enable\n')
proc.stdin.flush()
while True:
    output_str = proc.stdout.readline()
    if b'RADIUS settings successfully updated' in output_str:
        break
    elif b'set radius' not in output_str:
        # RADIUS command returned an error
        s1 = str(output_str)
        s2 = s1.split("\r")[1]
        print("RADIUS command returned: " + s2.split("\n")[0])
        proc.stdin.close()
        proc.terminate()
        proc.wait()
        sys.exit(1)

print("RADIUS settings updated and enabled.")
proc.stdin.close()
proc.terminate()
proc.wait()
sys.exit(0)

```

Python Custom Script - EMG CLI Session

An example of a Python Custom Script that uses the `Pexpect` module to interact with the CLI session and the device ports to detect the prompt on any devices connected to the EMG, and set the device port name to be the same as the device prompt:

```

#! python
# Script to detect the prompt on a device connected to an EMG device
# port,
# and set the device port name to the prompt. Punctuation characters are
# removed and the device port number is appended to the name. Prompts
# ending
# in '>' are detected. For example, for a Cisco device attached to device
# port 3 and displays this prompt:
#   engcisco_cat3560>
# the name for device port 3 will be set to "engcisco_cat3560-3"

import pexpect
import datetime
import time
import sys
import re

now = datetime.datetime.now()
print("Detecting devices on EMG at ", end="")
print(now.strftime("%Y-%m-%d %H:%M"))

# start the CLI session to get number of device ports
p=pexpect.spawn('clisession -U sysadmin')

```

```

emgPrompt = ""
numPorts = 0
loggedIn = False

while not loggedIn:
    i = p.expect([pexpect.TIMEOUT, pexpect.EOF,
                  'Model Number: SLC80(\d*)\r\n', 'Model Number:
SLB882\r\n',
                  '(\[.*>)', timeout=10)
    if i == 0:  # Timeout
        print("Timeout waiting to login.")
        p.terminate(True)
        sys.exit(1)
    elif i == 1: # EOF
        print("Session unexpectedly terminated.")
        p.terminate(True)
        sys.exit(1)
    elif i == 2: # SLC8000 model number
        model = p.match.group(1)
        numPorts = int(model)
    elif i == 3: # SLB882 model number
        numPorts = 8
    elif i == 4: # prompt
        loggedIn = True
        slcPrompt = p.match.group(1).decode('utf-8')

if numPorts == 0:
    print("Cannot determine number of device ports.")
    p.terminate(True)
    sys.exit(1)

print("Number of device ports:", numPorts)

# Terminate the CLI session
p.sendline("logout")
time.sleep(.500)
p.wait()

skipPorts = False
devicePort = 1
pList = []

if numPorts == 24 or numPorts == 40:
    # Adjust port numbering for SLC8024 and SLC8040
    skipPorts = True
    numPorts = numPorts + 8

# Loop through device ports, connect and try to detect the prompt
while devicePort <= numPorts:
    if skipPorts and devicePort >= 9 and devicePort <= 16:
        devicePort = devicePort + 1
        pList.append('')
        continue

```

```

print("Scanning device port", devicePort, "...")
port = str(devicePort)
p=pexpect.spawn('portsession', ['-p', port])

# Login (if required), and wait for the first prompt
p.sendline("")
gotPrompt = False
emgDevice = False
cnt = 1
while not gotPrompt:
    i = p.expect([pexpect.TIMEOUT, pexpect.EOF,
                  'login:', 'Error: (.*)\r\n',
                  '>'], timeout=10)
    if i == 0:      # Timeout
        cnt = cnt + 1
        if cnt == 3:
            print("Timeout waiting to connect to DP", devicePort, ".")
            p.terminate(True)
            p.wait()
            break
        # may need to send a CR to get prompt
        p.send("\r")
    elif i == 1:    # EOF
        print("portsession on DP ", devicePort, "unexpectedly
terminated.")
        break
    elif i == 2:    # login prompt
        p.sendline("sysadmin")
        p.expect("Password:")
        p.sendline("PASS")
        emgDevice = True
        gotPrompt = True
    elif i == 3:    # error from portsession
        print(p.match.group(1).decode('utf-8'))
        p.terminate(True)
        p.wait()
        break
    elif i == 4:    # prompt
        gotPrompt = True
    # end if while not gotPrompt:

if not gotPrompt:
    devicePort = devicePort + 1
    pList.append('')
    continue

# Detect the prompt
devPrompt = ""
p.send("\n")
i = p.expect([pexpect.TIMEOUT, pexpect.EOF, '\r\n(.*)>'],
             timeout=10)
if i == 0 or i == 1:    # Timeout or EOF
    print("Timeout waiting for the prompt on DP", devicePort, ".")
    p.terminate(True)

```

```

        p.wait()
        devicePort = devicePort + 1
        pList.append('')
        continue
    if i == 2:                      # prompt
        devPrompt = p.match.group(1).decode('utf-8')

    if devPrompt == "":
        print("Timeout waiting for the prompt on DP", devicePort, ".")
        devicePort = devicePort + 1
        pList.append('')
        continue

    print("Detected prompt", devPrompt, ".")
    # Strip characters not allowed in DP names
    devPromptStrip = re.sub("[^0-9A-Za-z\._\-\-]", "", devPrompt)
    devPromptComplete = devPromptStrip + "-" + str(devicePort)
    pList.append(devPromptComplete)

    p.terminate(True)
    p.wait()
    devicePort = devicePort + 1
    # end of while devicePort <= numPorts:

# Connect to the EMG CLI and set the device port names
p=pexpect.spawn('clisession -U sysadmin')

loggedIn = False
while not loggedIn:
    i = p.expect([pexpect.TIMEOUT, pexpect.EOF,
                  'Model Number: SLC80(\d*)\r\n', 'Model Number:
SLB882\r\n',
                  '(\[.*\])'], timeout=10)
    if i == 0:    # Timeout
        print("Timeout waiting to login.")
        p.terminate(True)
        sys.exit(1)
    elif i == 1:  # EOF
        print("Session unexpectedly terminated.")
        p.terminate(True)
        sys.exit(1)
    elif i == 4:  # prompt
        loggedIn = True

devicePort = 1
while devicePort <= numPorts:
    if skipPorts and devicePort >= 9 and devicePort <= 16:
        devicePort = devicePort + 1
        continue
    if len(pList[devicePort - 1]) > 0:
        # Detected a prompt; set it
        print("Setting name on DP", devicePort, "to", pList[devicePort -
1], "...")
```

```

        s = "set deviceport port " + str(devicePort) + " name " +
pList[devicePort - 1]
        p.sendline(s)
        i = p.expect([pexpect.TIMEOUT,
                      'Device Port settings successfully updated.\r\n'],
                     timeout=10)
        if i == 0:    # Timeout
            print("Timeout waiting for response.")
        devicePort = devicePort + 1

# Terminate the CLI session
p.sendline("logout")
time.sleep(.500)
p.wait()
print("Script completed.")
sys.exit(0)

```

Tcl Custom Script - EMG CLI Session

An example of a Tcl Custom Script that interacts with a CLI session:

```

#! tcl
# Script to get the current internal temperature of the EMG
# Accepts one optional command line parameter for location

set emgTemp "unknown"
set location ""

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

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

set io [open "| clisession -U sysadmin" r+]

set loggedIn false
while {! $loggedIn} {
    set len [gets $io line]
    if {[string first "Invalid local user" $line] != -1} {
        puts "Invalid local user passed to clisession"
        break
    }
    if {[string first "For a list of commands" $line] != -1} {
        puts $io "\n"
        flush $io
    }
}

```

```
        }
        if {[string first ">" $line] != -1} {
            set loggedIn true
        }
    }

    if {! $loggedIn} {
        exit 1
    }

    puts $io "show temp"
    flush $io
    set gotTemp false
    while {! $gotTemp} {
        set len [gets $io line]
        if {[string first "Current Internal Temperature" $line] != -1} {
            set emgTemp [string range $line [expr {[string first ":" $line] +
1}]] end]
            set gotTemp true
        }
    }

    puts "Temperature: $emgTemp"

    puts $io "logout"
    flush $io
    exit 0
```

12: *Connections*

[Chapter 9: Device Ports](#) described how to configure and interact with an EMG port connected to an external device. This chapter describes how to use the [Devices > Connections](#) page to connect external devices and outbound network connections (such as Telnet or SSH) in various configurations.

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

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

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

- ◆ Immediately. These connections are always re-established after reboot.
- ◆ At a specified date and time. These connections connect after the date and time pass.
- ◆ After a specified amount of data or a specified sequence of data passes through the connection. Following reboot, the connection is not reestablished until the specified data passes through the connection.

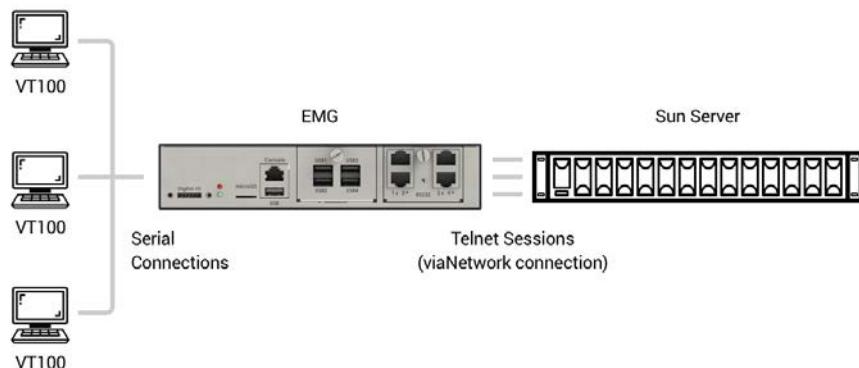
Typical Setup Scenarios for the EMG unit

Following are typical configurations in which EMG connections can be used, with references to settings on the [Devices > Connections](#) and [Device Ports > Settings \(1 of 2\)](#) web pages.

Terminal Server

In this setup, the EMG acts as a multiplexer of serial data to a single server computer. Terminal devices are connected to the serial ports of the EMG unit and configured as a Device Port to Telnet out type connection on the [Devices > Connections](#) page. The users of the terminals can access the server as if they were connected directly to it by local serial ports or a console.

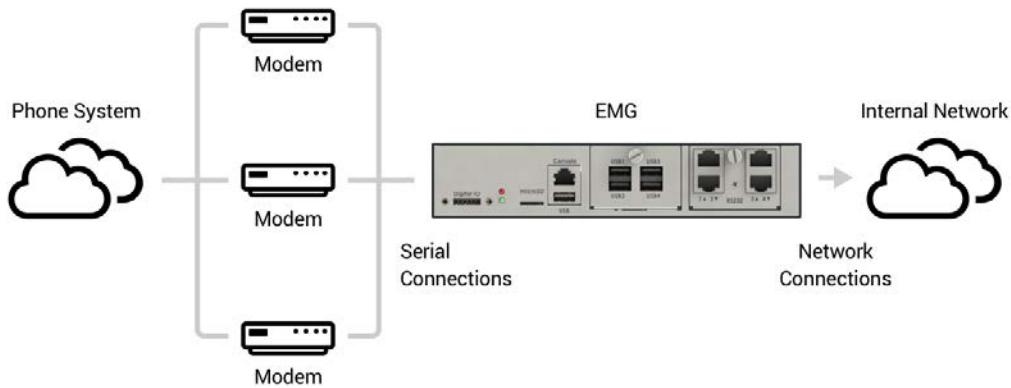
Figure 12-1 Terminal Server



Remote Access Server

In this setup, the EMG is connected to one or more modems by its device ports. Configure the device ports on the [Device Ports > Settings \(1 of 2\)](#) web page by selecting the Dial-in option in the Modem Settings section. Most customers use the modems in PPP mode to establish an IP connection to the EMG unit and either Telnet or SSH into the EMG. They could also select text mode where, using a terminal emulation program, a user could dial into the EMG unit and connect to the command line interface.

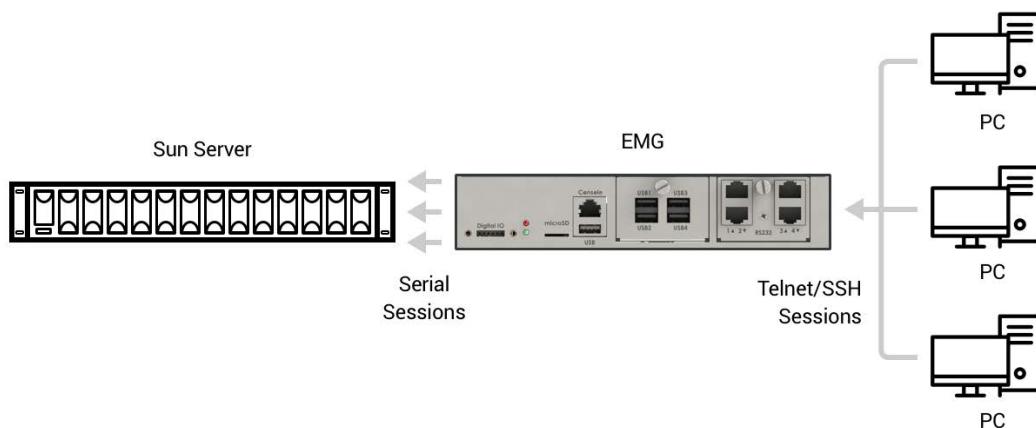
Figure 12-2 Remote Access Server



Reverse Terminal Server

In this scenario, the EMG has one or more device ports connected to one or more serial ports of a mainframe server. Users can access a terminal session by establishing a Telnet or SSH session to the EMG unit. To configure the EMG, select the **Enable Telnet In** or **Enable SSH In** option on the [Device Ports > Settings \(1 of 2\)](#) page.

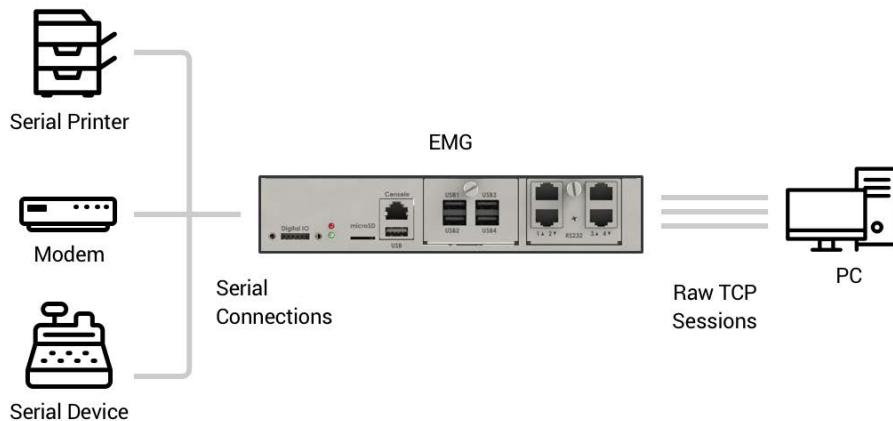
Figure 12-3 Reverse Terminal Server



Multipoint Device Server

A PC can use the device ports on the EMG unit as virtual serial ports, enabling the ports to act as if they are local ports to the PC. To use the EMG in this setup, the PC requires special software, for example, Com Port Redirector (available on www.lantronix.com) or similar software.

Figure 12-4 Multipoint Device Server

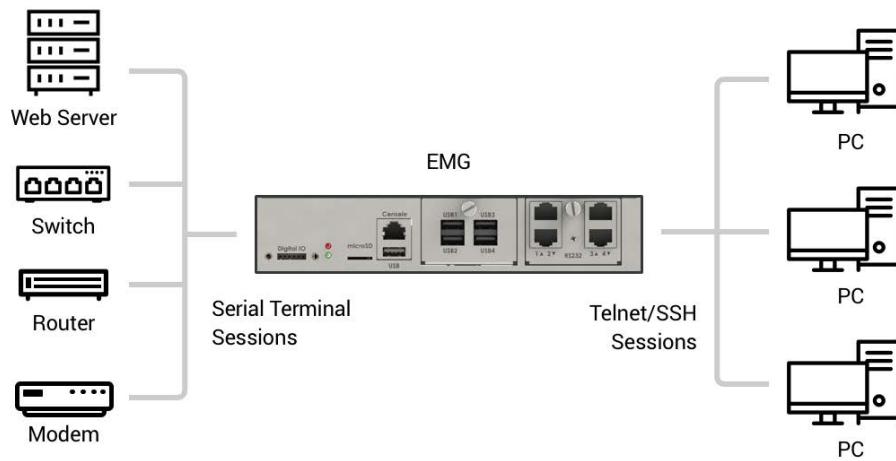


Console Server

The EMG unit is configured so that the user can manage a number of servers or pieces of network equipment using their console ports. The device ports on the EMG are connected to the console ports of the equipment. To manage a specific piece of equipment, the user can Telnet or SSH to a specific port or IP address on the EMG unit and be connected directly to the console port of the end server or device. To configure this setup, set the **Enable Telnet In** or **Enable SSH In** option on the [Device Ports > Settings \(1 of 2\)](#) page for the device port in question.

The user can implement an extra remote management capability by adding a modem to one of the device ports and setting the **Dial-in** option in the Modem Settings section of the [Device Ports > Settings \(1 of 2\)](#) page. A user could then dial into the EMG using another modem and terminal emulation program at a remote location.

Figure 12-5 Console Server



Connection Configuration

Note: These are advanced connection settings for specific applications. If the EMG is being used as a console or device server it is unlikely that you will need any of the Connection settings described below.

To create a connection:

1. Click the **Devices** tab and select **Connections**. The Connections page displays, as shown in [Figure 12-6](#).

Figure 12-6 Devices > Connections

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

Devices

U1 E1 1 3
SD E2 2 4

Network Services User Authentication Devices Maintenance Quick Setup

Device Status Device Ports Console Port USB / SD Card RPMs Connections Xmodem Host Lists Scripts Sites

Connections

Outgoing Connection Timeout: No Yes: 5 seconds

Connect: Device Port

Port: [Settings](#)

Data Flow:

to: Device Port

Hostname:

Port: [Settings](#)

SSH Out Options

User:

Version: None 1 2

Command:

Trigger: Connect now
 Connect at date/time: July 11 2019 04:47 pm
 Auto-connect on characters transferring:
 at least characters
 character sequence:

Apply

To view details for a connection, hold the mouse over the arrow icon in the Flow column.
If a connection can be modified, the fields above will be filled in; modify the connection and select 'Configure'.
To terminate a connection, select the radio button in the right column below and select 'Terminate'.
Web connections can be viewed [here](#).

Current Connections		Configure	Terminate	Keep Connection: <input type="checkbox"/>	Restart <input type="checkbox"/>
Port/Service	Flow	Port/Service	User	Time	
Device Port 2		Command Line	N/A	N/A	<input type="checkbox"/>

2. For a device port, enter the following:

Outgoing Connection Timeout	Select to turn on or turn off the connection timeout: <input checked="" type="radio"/> No for no timeout <input type="radio"/> Yes for a timeout. Specify the number of seconds in the seconds field.
Port	The number of the device port you are connecting. This device port must be connected to an external serial device and must not have command line interface logins enabled, be connected to a modem, or be running a loopback test. Note: To see the current settings for this device port, click the Settings link.
Data Flow	Select the arrow showing the direction (bidirectional or unidirectional) the data will flow in relationship to the device port you are connecting.
to	From the drop-down list, select a destination for the connection: a device port connected to a serial device, a device port connected to a modem, or an outbound network connection (Telnet out , SSH out , TCP Port , or UDP Port). Note: To see the current settings for a selected device port, click the Settings link.
Hostname	The host name or IP Address of the destination. This entry is required if the to field is set to Telnet out, SSH out, TCP port, or UDP port.

Port	If the to field is set to Device Port or Modem on Device Port , enter the number of the device port. For all other options, this is the TCP/UDP port number, which is optional for Telnet out and SSH out, but required for TCP Port and UDP Port. Note: If you select Device Port , it must not have command line interface logins enabled or be running a loopback test. To view the device port's settings, click the Settings link to the right of the port number.
SSH Out Options	Select one of the following optional flags to use for the SSH connection. ◆ User: Login ID to use for authenticating on the remote host. ◆ Version: Version of SSH. Select 1 or 2. ◆ Command: Enter a specific command on the remote host (for example, reboot).
Trigger	Select the condition that will trigger a connection. Options include: ◆ Connect now: Connects immediately, or if you reboot the EMG, immediately on reboot. ◆ Connect at date/time: Connects at a specified date and time. Use the drop-down lists to complete the date and time. Upon rebooting, the EMG unit reestablishes the connection if the date/time has passed. ◆ Auto-connect on characters transferring: Select the arrow indicating the direction of the data transfer and either the minimum number of characters or a specific character sequence that will trigger the connection. You can select the direction of the data transfer only if Data Flow is bidirectional. Upon rebooting, the EMG does not reestablish the connection until the specified data has passed through one of the endpoints of the connection.

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

To view, update, or disconnect a current connection:

The bottom of the [Devices > Connections](#) page displays current connections.

Figure 12-7 Current Connections

To view details for a connection, hold the mouse over the arrow icon in the Flow column. If a connection can be modified, the fields above will be filled in; modify the connection and select 'Configure'. To terminate a connection, select the radio button in the right column below and select 'Terminate'. Web connections can be viewed here .				

1. To view details about a connection, hold the mouse over the arrow in the **Flow** column.
2. To disconnect (delete) a connection, select the connection in the **Select** column and click the **Terminate** button.
3. To reestablish the connection, create the connection again in the top part of the page.
4. To view information about Web connections, click the [here](#) link in the text above the table. The [Maintenance > Firmware & Configurations](#) page displays.

Connection Commands

Go to [Connection Commands](#) to view CLI commands which correspond to the web page entries described above.

13: User Authentication

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

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

Note: *Regardless of whether local user authentication is enabled, the local user sysadmin account is always available for login. For security purposes, full administrative access to the EMG via the default sysadmin local user account can be limited to only the front console port of the EMG device. See [Limiting Sysadmin User Access on page 58](#).*

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

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

Example:

There is an LDAP user "joe" and an NIS user "joe" and the order of authentication methods is:

1. Local Users
2. LDAP
3. NIS

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

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

1. From the main menu, select **User Authentication**. The following page displays:

Figure 13-1 User Authentication > Auth Methods

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

Enabled methods
(in order of precedence):

- Local Users

Disabled methods:

- NIS
- LDAP
- RADIUS
- Kerberos
- TACACS+

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

Attempt next method on authentication rejection

Apply

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

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 identification and password. NIS uses the client/server model and the Remote Procedure Call (RPC) interface for communication between hosts. NIS consists of a server, a library of client programs, and some administrative tools. NIS is often used with the Network File System (NFS).
LDAP (Lightweight Directory Access Protocol)	A set of protocols for accessing information directories, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection-oriented transfer services.
RADIUS (Remote Authentication Dial-In User Service)	An authentication and accounting system used by many Internet Service Providers (ISPs). A client/server protocol, it enables remote access servers to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It increases security, allowing a company to set up a policy that can be applied at a single administered network point.
Kerberos	Kerberos is a network authentication protocol that enables two parties to exchange private information across an unprotected network. It works by assigning a unique electronic credential, called a ticket, to each user who logs on to the network. The ticket is embedded in messages to identify the sender.

TACACS+ (Terminal Access Controller Access Control System)	TACACS+ allows a remote access server to communicate with an authentication server to determine whether the user has access to the network. TACACS+ is a completely new protocol and is not compatible with TACACS or XTACACS. The EMG supports TACACS+ only.
Local Users	Local accounts on the EMG unit used to authenticate users who log in using SSH, Telnet, the web, or the console port.

3. To disable a method currently in the **Enabled methods** list, select the method and click the right  arrow between the lists.
4. To set the order in which the EMG unit will authenticate users, use the up  and down  arrows to the left of the **Enabled methods** list.
5. For **Attempt next method on authentication rejection**, you have the following options:
 - To enable the EMG to use all methods, in order of precedence, until it obtains a successful authentication, select the check box. This is the default.
 - To enable the EMG unit to use only the first authentication method that responds (in case a server is down or unavailable), clear the check box.

Note: When limiting accessibility of the sysadmin login to the physical EMG console manager device, make sure to uncheck **Attempt next method on authentication rejection**.
6. Click **Apply**.

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

Authentication Commands

Go to [Authentication Commands](#) to view CLI commands which correspond to the web page entries described above.

User Rights

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

- ◆ connect direct/listen
- ◆ set locallog/password/history/cli
- ◆ show datetime/deviceport/locallog/portstatus/portcounters/
- ◆ history/cli/user

The table below shows the mapping of groups and user rights.

Table 13-2 User Types and Rights

User Right	Administrator	Power Users	Default Users
Full Administrative Rights	X		
Networking	X	X	
Services	X		
Date/Time	X	X	
Local Users	X		
Remote Authentication	X		
SSH Keys	X		
User Menus	X		
Device Port Operations	X		
Device Port Configuration	X		
USB	X		
Reboot/Shutdown	X	X	
Firmware/Configuration	X		
Diagnostics and Reports	X	X	
Secure Lantronix Network	X		
Web Access	X	X	
Internal Modem	X		
RPMs	X		
SD Card	X		

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

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

Local and Remote User Settings

The system administrator can configure the EMG to use local accounts and remote accounts to authenticate users.

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

Figure 13-3 User Authentication > Local/Remote Users

The screenshot shows the LANTRONIX EMG851000 User Authentication > Local/Remote Users page. At the top, there are configuration buttons for port selection (U1, E1, 3, SD, E2, 2, 4) and user information (Host: emgfcf0, User: sysadmin). The navigation bar includes Network, Services, User Authentication (selected), Devices, Maintenance, Quick Setup, and links to Auth Methods, Local/Remote Users, NIS, LDAP, RADIUS, Kerberos, TACACS+, Groups, SSH Keys, and Custom Menus. The Local/Remote Users sub-page has a 'Help?' button. Configuration options include 'Enable Local Users' (checked), 'Multiple Sysadmin Web Logins' (unchecked), 'Sysadmin Access Limited to Console Port' (unchecked), 'Authenticate only remote users who are in the remote users list' (unchecked), and 'Deny access to remote users assigned to groups that do not map to EMG custom group' (unchecked). A note states: 'Local and remote accounts on the EMG are used to authenticate users who login to the EMG via SSH, Telnet, the Web or the Console Port.' A note also says: 'Note: remove Escape & Break Sequences for users making raw binary connections to Device Ports.' Below these are 'Local User Passwords' settings: 'Complex Passwords' (unchecked), 'Password Lifetime' (90 days), 'Allow Reuse' (checked), 'Warning Period' (7 days), 'Reuse History' (4), 'Max Login Attempts' (0), and 'Lockout Period' (0 minutes). Buttons for 'Add/Edit User' and 'Delete User' are present. A note at the bottom says: 'Select the radio button in the right column to edit or delete a user. Shaded users are locked (cannot login.).' A table at the bottom lists 'Local Users (1 users) & Remote Users (0 users)'. The table columns are Login, Auth, UID, Group, Permissions, Esc Seq, Brk Seq, Custom Menu, DB, Listen, Data, and Clear. The single user listed is sysadmin, with Local Auth, UID 0, Adm Group, and permissions fa,nt,sv,lu,ra,dt,sk,um,dp,do,ub,rs,fc,dr,sn,wb,sd,md,rp. The 'Permissions' column shows lx1bA and lx1bB. The 'DB' column shows N. The 'Listen' column shows 1-4,U1. The 'Data' column shows 1-4,U1. The 'Clear' column shows 1-4,U1. The 'Permissions' column for the user is shaded.

The top of the page has entry fields for enabling local and remote users and for setting password requirements. The bottom of the page displays a table listing and describing all local and remote users.

To enable local and/or remote users:

- 1) Enter the following:

Enable Local Users	Select to enable all local users except sysadmin. The sysadmin user is always available regardless of how you set the check box. Enabled by default.
Multiple Sysadmin Web Logins	Select to allow the sysadmin to have multiple simultaneous logins to the web interface. Disabled by default.
Sysadmin Access Limited to Console Port	Select to limit sysadmin logins to the physical EMG console port only. Disabled by default. Note: For security purposes, full administrative access to the EMG via the default sysadmin local user account can be limited to only the front console port of the EMG device. See Limiting Sysadmin User Access on page 58 .

Authenticate only remote users who are in the remote users list	Select the check box to authenticate users listed in the Remote Users list in the lower part of the page. Disabled by default.
Deny access to remote users assigned to groups that do not map to EMG custom group	Select the check box to authenticate remote users whose LDAP group or TACACS+ priv_lvl map to an EMG custom group, allow EMG access if matched. Disabled by default.

2) Continue to set **Local User Passwords**:

Complex Passwords	Select to enable the EMG unit to enforce rules concerning the password structure (e.g., alphanumeric requirements, number of characters, punctuation marks). Disabled by default. Complexity rules: Passwords must be at least eight characters long. They must contain one upper case letter (A-Z), one lower case letter (a-z), one digit (0-9), and one punctuation character ((`~!@#\$%^&*-+=\{}[];:"`<>.,?/_)).
Allow Reuse	Select to enable users to continue to reuse old passwords. If you disable the check box, they cannot use any of the Reuse History number of passwords. Enabled by default.
Reuse History	The number of passwords the user must use before reusing an old password. The default is 4 . For example, if you set reuse history to 4, the user may reuse an old password after using 4 other passwords.
Password Lifetime (days)	The number of days until the password expires. The default setting is 90 .
Warning Period (days)	The number of days ahead that the system warns that the user's password will expire. The default setting is 7 .
Max Login Attempts	The number of times (up to 8) the user can attempt to log in unsuccessfully before the system locks the user out. The default setting is 0 (disabled).
Lockout Period (minutes)	The number of minutes (up to 90) the locked-out user must wait before trying to log in to the web interface again. The default setting is 0 (disabled).

2. Click the **Apply** button.

Adding, Editing or Deleting a User

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

To add a user:

1. On the [User Authentication > Local/Remote Users](#), click the **Add/Edit User** button. The [User Authentication > Local/Remote User Settings](#) page displays.

Figure 13-4 User Authentication > Local/Remote User Settings

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin Select port for Configuration WebSSH (DP only) Connected Device (DP only)

Network Services User Authentication Devices Maintenance Quick Setup

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

Local/Remote User Settings

Login: Enable for Dial-back: Password:
 Authentication: Local Remote Dial-back Number: Retype Password:
 UID: Escape Sequence: Password Expires:
 Listen Ports: Break Sequence: Allow Password Change:
 Data Ports: Custom Menu: Change Password on Next Login:
 Clear Port Buffers: Display Menu at Login: Lock Account:
 Account Status: Active

Group: Default Users Power Users Administrators Custom Group: <none> Each user is a member of a group which has predefined user rights associated with it. User rights that are associated with a group cannot be modified for individual users.

Full Administrative: Local Users: Firmware & Configuration:
 Networking: Remote Authentication: Internal Modem:
 Services: SSH Keys: Device Port Operations:
 Secure Lantronix Network: User Menus: Device Port Configuration:
 Date/Time: Web Access: USB:
 Reboot & Shutdown: Diagnostics & Reports: SD Card:
 RPMs:

[Back to Local/Remote Users](#)

2. Enter the following information for the user:

Login	User ID of selected user.
Authentication	Select the type of authenticated user: <input checked="" type="radio"/> Local : User listed in the EMG database. <input type="radio"/> Remote : User not listed in the EMG database.
UID	A unique numeric identifier the system administrator assigns to each user. Valid UIDs are 101-4294967295. <i>Note: The UID must be unique. If it is not, EMG unit automatically increments it. Starting at 101, the EMG finds the next unused UID.</i>
Listen Ports	The device ports that the user may access to view data using the connect listen command. Enter the port numbers or the range of port numbers (for example, 1, 5, 8, 10-15). U1 denotes the USB port on the EMG unit.
Data Ports	The device ports with which the user may interact using the connect direct command. Enter the port numbers or the range of port numbers.
Clear Port Buffers	The device port buffers the users may clear using the set locallog clear command. Enter the port numbers or the range of port numbers.

Enable for Dial-back	Select to grant a local user dial-back access. Users with dial-back access can dial into the EMG unit and enter their login and password. Once the EMG authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number (specified on the Device Port - Settings page), or on a number that is associated with the user's login (specified here).
Escape Sequence	<p>A single character or a two-character sequence that causes the EMG unit to leave direct (interactive) mode. (To leave listen mode, press any key.)</p> <p>A suggested value is Esc+A (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as \x1bA, which is hexadecimal (\x) character 27 (1B) followed by an A.</p> <p>This setting allows the user to terminate the <code>connect direct</code> command on the command line interface when the endpoint of the command is <code>deviceport</code>, <code>tcp</code>, or <code>udp</code>.</p> <p>See Key Sequences on page 191 for notes on key sequence precedence and behavior.</p>
Break Sequence	<p>A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as \x1bB, which is hexadecimal (\x) character 27 (1B) followed by a B.</p> <p>See Key Sequences on page 191 for notes on key sequence precedence and behavior.</p>
Custom Menu	<p>If custom menus have been created, you can assign a default custom menu to the user. The custom menu will display at login.</p> <p>Note: In the Local Users table, if the menu assigned to a local user no longer exists, it is marked with an asterisk (*).</p>
Display Menu at Login	If custom menus have been created, select to enable the menu to display when the user logs into the CLI.
Password / Retype Password	When a user logs into the EMG, the EMG unit prompts for a password (up to 64 characters). The sysadmin establishes that password here.
Password Expires	If not selected, allows the user to keep a password indefinitely. If selected the user keeps the password for a set period. (See the section, Local and Remote User Settings (on page 245) for information on specifying the length of time before the password expires.)
Allow Password Change	Select to allow the user to change password.
Change Password on Next Login	Indicate whether the user must change the password at the next login.
Lock Account	Select to lock the account indefinitely.
Account Status	Displays the current account status: <ul style="list-style-type: none"> ◆ Active ◆ Locked ◆ Locked (invalid logins)

3. In the **User Rights** section, select the user group to which local/remote users will belong.

Group	Select the group to which the local or remote user will belong: <ul style="list-style-type: none"> ◆ Default Users: This group has only the most basic rights. You can specify additional rights for the individual user. ◆ Power Users: This group has the same rights as Default Users plus Web Access, Networking, Date/Time, Reboot & Shutdown, and Diagnostics & Reports. ◆ Administrators: This group has all possible rights. ◆ Custom Group: Select a custom group from the drop-down menu.
--------------	--

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage Secure Lantronix units (e.g., EMG, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the EMG unit.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown .
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
SD Card	Right to enter settings for SD card.
RPM	Right to manage and control remote power managers.

5. Click the **Apply** button.

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

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

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

Shortcut

To add a user based on an existing user:

1. Display the existing user on the [User Authentication > Local/Remote Users](#) page. The fields in the top part of the page display the current values for the user.
2. Change the Login to that of the new user. It is best to change the Password too.
3. Click the **Apply** button.

To edit a local user:

1. On the [User Authentication > Local/Remote Users](#) page, select the user and click the **Add/Edit User** button. The Local/Remote User Settings page displays.
2. Update values as desired.
3. Click the **Apply** button.

To delete a local user:

1. On the [User Authentication > Local/Remote Users](#) page, select the user and click the **Add/Edit User** button. The Local/Remote User Settings page displays.
2. Click the **Delete User** button.
3. Click the **Apply** button.

To change the sysadmin password:

1. On the [User Authentication > Local/Remote Users](#) page, select **sysadmin** and click the **Add/Edit User** button. The Local/Remote User Settings page displays.
2. Enter the new password in the Password and Retype Password fields.

Note: You can change Escape Sequence and Break Sequence, if desired. You cannot delete the UID or change the UID, port permissions, or custom menu.

3. Click the **Apply** button.

Local Users Commands

Go to [Local Users Commands](#) to view CLI commands which correspond to the web page entries described above.

Remote User Rights Commands

Go to [Remote User Commands](#) to view CLI commands which correspond to the web page entries described above.

NIS

The system administrator can configure the EMG to use NIS to authenticate users attempting to log in to the EMG unit through the Web, SSH, Telnet, or the console port. If NIS does not provide port permissions, you can use this page to grant device port access to users who are authenticated through NIS.

All NIS users are members of a group that has predefined user rights associated with it. You can assign additional user rights that are not defined by the group.

To configure the EMG unit to use NIS to authenticate users:

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

Figure 13-5 User Authentication > NIS

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, the title 'LANTRONIX® EMG851000' and the host 'emgfcc0' are displayed. The 'User Authentication' tab is selected, and the 'NIS' option is chosen. The main configuration area is titled 'NIS'.

Enable NIS: (checkbox is checked)

NIS Domain:

Note: The NIS Domain must match the NIS domain name on the NIS Server.

Broadcast for NIS Server:

NIS Master Server:

NIS Slave Server #1:

NIS Slave Server #2:

NIS Slave Server #3:

NIS Slave Server #4:

NIS Slave Server #5:

Custom Menu: <none> ▾

Escape Sequence: \x1bA

Break Sequence: \x1bB

Enable for Dial-back:

Data Ports: 1-4, U1

Listen Ports: 1-4, U1

Clear Port Buffers: 1-4, U1

Dial-back Number:

User Rights

Group: Default Users
 Power Users
 Administrators

Full Administrative:

Networking:

Services:

Secure Lantronix Network:

Date/Time:

Reboot & Shutdown:

RPMs:

Local Users:

Remote Authentication:

SSH Keys:

User Menus:

Web Access:

Diagnostics & Reports:

Firmware & Configuration:

Internal Modem:

Device Port Operations:

Device Port Configuration:

USB:

SD Card:

Apply

2. Enter the following:

Enable NIS	Displays selected if you enabled this method on the Authentication Methods page. If you want to set up this authentication method but not enable it immediately, clear the checkbox. Note: You can enable NIS here or on the first User Authentication page. If you enable NIS here, it automatically displays at the end of the order of precedence on the User Authentication page.
NIS Domain	The NIS domain of the EMG must be the same as the NIS domain of the NIS server.
Broadcast for NIS Server	If selected, the EMG unit sends a broadcast datagram to find the NIS Server on the local network.
NIS Master Server	The IP address or host name of the master server.
NIS Slave Servers #1 -5	The IP addresses or host names of up to five slave servers.
Custom Menu	If custom menus have been created you can assign a default custom menu to NIS users.
Escape Sequence	A single character or a two-character sequence that causes the EMG to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is Esc+A (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as \x1bA , which is hexadecimal (\x) character 27 (1B) followed by an A . This setting allows the user to terminate the connect direct command on the command line interface when the endpoint of the command is deviceport, tcp, or udp. See Key Sequences on page 191 for notes on key sequence precedence and behavior.
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as \x1bB , which is hexadecimal (\x) character 27 (1B) followed by a B .
Enable for Dial-back	Select to grant a user Dial-back (on page 187) . Users with dial-back access can dial into the EMG and enter their login and password. Once the EMG unit authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user's login (specified here).
Data Ports	The ports users are able to monitor and interact with using the connect direct command. Enter the port numbers or the range of port numbers (for example, 1, 5, 8, 10-15). U1 denotes the USB port on the front of the EMG unit.
Listen Ports	The ports users are able to monitor using the connect listen command.
Clear Port Buffers	The ports whose port buffer users may clear using the set locallog clear command.

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

Group	Select the group to which the NIS users will belong: <ul style="list-style-type: none"> ◆ Default Users: This group has only the most basic rights. You can specify additional rights for the individual user . ◆ Power Users: This group has the same rights as Default Users plus Web Access, Networking, Date/Time, Reboot & Shutdown, and Diagnostics & Reports. ◆ Administrators: This group has all possible rights.
--------------	--

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure Lantronix units (e.g., EMG, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the EMG unit.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown .
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
SD Card	Right to enter settings for SD card.
RPM	Right to manage and control remote power managers.

5. Click the **Apply** button.

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

NIS Commands

Go to [NIS Commands](#) to view CLI commands which correspond to the web page entries described above.

LDAP

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

LDAP allows EMG unit users to authenticate using a wide variety of LDAP servers, such as OpenLDAP and Microsoft Active Directory. The LDAP implementation supports LDAP servers that do not allow anonymous queries.

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

All LDAP users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

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

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

Figure 13-6 User Authentication > LDAP



Logout Host: emgfcf0 User: sysadmin

Network Services User Authentication Devices Maintenance Quick Setup

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

U1	E1	1	3
SD	E2	2	4

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

LDAP

Help?

Enable LDAP:

Server #1:

Server #2:

Port: 389

Base:
(example: dc=domain,dc=com)

Bind Name:

Bind Password:

Retype Password:

Bind with Login: '\$login' in the Bind Name will be substituted with the login

User Login Attribute:

Group Filter Objectclass:

Group Member Attribute:

Group Member Value: DN Name

Use LDAP Schema: for User Attributes and Permissions

Active Directory Support:

Encrypt Messages: Disabled Start TLS SSL

Certificate Authority: [Upload File](#)

Certificate File: [Upload File](#)

Key File: [Upload File](#)

The EMG can be configured to use LDAP to authenticate users who login to the EMG via SSH, Telnet, the Web or the Console Port. If port permissions are not provided via LDAP Schema, LDAP users are granted Device Port access through the port permissions below.

Custom Menu:

Escape Sequence:

Break Sequence:

Enable for Dial-back:

Data Ports:

Listen Ports:

Clear Port Buffers:

Dial-back Number:

User Rights

Group: Default Users Power Users Administrators

Full Administrative:

Networking:

Services:

Secure Lantronix Network:

Date/Time:

Reboot & Shutdown:

RPMs:

Local Users:

Remote Authentication:

SSH Keys:

User Menus:

Web Access:

Diagnostics & Reports:

Firmware & Configuration:

Internal Modem:

Device Port Operations:

Device Port Configuration:

USB:

SD Card:

2. Enter the following:

Enable LDAP	Displays selected if you enabled this method on the first User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox.
--------------------	---

Server #1 (or Server #2)	The IPv4 or IPv6 address or host name of the primary and secondary LDAP servers. The secondary LDAP server will be used for authentication in the event that the primary LDAP server cannot be reached.
Port	Number of the TCP port on the LDAP server to which the EMG talks. The default is 389 .
Base	The name of the LDAP search base (e.g., dc=company, dc=com). May have up to 80 characters.
Bind Name	The name for a non-anonymous bind to an LDAP server. This item has the same format as LDAP Base. One example is cn=administrator,cn=Users,dc=domain,dc=com
Bind Password / Retype Password	Password for a non-anonymous bind. This entry is optional. Acceptable characters are a-z, A-Z, and 0-9 . The maximum length is 127 characters.
Bind with Login	Select to bind with the login and password that a user is authenticating with. This requires that the Bind Name contain the \$login token, which will be replaced with the current login. For example, if the Bind Name is uid=\$login,ou=People,dc=lantronix,dc=com, and user roberts logs into the EMG, LDAP will bind with uid=roberts,ou=People,dc=lantronix,dc=com and the password entered by roberts.
User Login Attribute	The attribute used by the LDAP server for user logins. If nothing is specified for the user filter, the EMG unit will use "uid". For AD LDAP servers, the attribute for user logins is typically "sAMAccountName".
Group Filter Objectclass	The objectclass used by the LDAP server for groups. If nothing is specified for the group filter, the EMG will use "posixGroup". For AD LDAP servers, the objectclass for groups is typically "Group".
Group Member Attribute	The attribute used by the LDAP server for group membership. This attribute may be used to search for a name (ie, "msmith") or a Distinguished Name (ie, "uid=msmith,ou=People,dc=lantronix,dc=com"). Select either Name or DN as appropriate for the LDAP server. If nothing is specified for the group membership attribute, the EMG unit will use "memberUID" for name and "uniqueMember" for DN. For AD LDAP servers, the Group Membership Value is typically DN, with the Group Membership Attribute of "member".
Group Member Value	The attribute used by the LDAP server for group membership. This attribute may be used to search for a name (ie, "msmith") or a Distinguished Name (ie, "uid=msmith,ou=People,dc=lantronix,dc=com"). Select either Name or DN as appropriate for the LDAP server. If nothing is specified for the group membership attribute, the EMG will use "memberUID" for name and "uniqueMember" for DN. For AD LDAP servers, the Group Membership Value is typically DN, with the Group Membership Attribute of "member".
Use LDAP Schema	Select the check box to obtain remote user attributes (group/permissions and port access) from an Active Directory server's schema via the user attribute 'SecureLantronixPerms' (see details below). Disabled by default.
Active Directory Support	Select to enable. Active Directory is a directory service from Microsoft that is a part of Windows 2000 and later versions of Windows. It is LDAP- and Kerberos-compliant. Disabled by default.

Encrypt Messages	Select Start TLS or SSL to encrypt messages between the EMG unit and the LDAP server. If Start TLS is selected, the port will automatically be set to 389 and the StartTLS extension will be used to initiate a secure connection; if SSL is selected, the port will automatically be set to 636 and a SSL tunnel will be used for LDAP communication. The port number can be changed to a non-standard LDAP port; if the port number is set to anything other than 636, Start TLS will be used as the encryption method. Disabled by default.
Certificate Authority	A certificate can be uploaded to the EMG unit for peer authentication. In non-FIPS mode, the uploaded certificate may contain a Certificate Authority file, a Certificate file (with an optional Key file), or both. A Key file alone is not a valid certificate. The Certificate Authority and Certificate File are in PEM format, for instance:
Certificate File	
Key File	<pre>-----BEGIN CERTIFICATE----- (certificate in base64 encoding) -----END CERTIFICATE-----</pre> <p>The Key File is in PEM format, eg:</p> <pre>-----BEGIN RSA PRIVATE KEY----- (private key in base64 encoding) -----END RSA PRIVATE KEY-----</pre>
Custom Menu	If custom menus have been created, you can assign a default custom menu to LDAP users. (See "Custom Menus" on page 279 .)
Escape Sequence	<p>A single character or a two-character sequence that causes the EMG to leave direct (interactive) mode. (To leave listen mode, press any key.)</p> <p>A suggested value is Esc+A (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as \x1bA, which is hexadecimal (\x) character 27 (1B) followed by an A.</p> <p>This setting allows the user to terminate the <code>connect direct</code> command on the command line interface when the endpoint of the command is deviceport, tcp, or udp.</p> <p>See Key Sequences on page 191 for notes on key sequence precedence and behavior.</p>
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as \x1bB , which is hexadecimal (\x) character 27 (1B) followed by a B .
Enable for Dial-back	Select to grant a user dial-back access. Users with dial-back access can dial into the EMG unit and enter their login and password. Once the EMG authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user's login (specified here).
Data Ports	The ports users are able to monitor and interact with using the <code>connect direct</code> command. U1 denotes the USB port on the front of the EMG unit.
Listen Ports	The ports users are able to monitor using the <code>connect listen</code> command.
Clear Port Buffers	The ports whose port buffer users may clear using the <code>set locallog clear</code> command.

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

Group	Select the group to which the LDAP users will belong: <ul style="list-style-type: none"> ◆ Default Users: This group has only the most basic rights. You can specify additional rights for the individual user. ◆ Power Users: This group has the same rights as Default Users plus Web Access, Networking, Date/Time, Reboot & Shutdown, and Diagnostics & Reports. ◆ Administrators: This group has all possible rights.
--------------	---

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure Lantronix units (e.g., EMG, or SLC devices) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the EMG unit.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown .
Internal Modem	Right to configure internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port configurations.
USB	Right to enter modem settings for USB.
SD Card	Right to view and enter settings for SD card.
RPM	Right to manage and control remote power managers.

5. Click the **Apply** button.

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

LDAP Commands

Go to [LDAP Commands](#) to view CLI commands which correspond to the web page entries described above.

RADIUS

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

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

All RADIUS users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

To configure the EMG unit to use RADIUS to authenticate users:

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

Figure 13-7 User Authentication > RADIUS

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

Network Services User Authentication **Devices** Maintenance Quick Setup

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

RADIUS [Help?](#)

Enable RADIUS:

RADIUS Server #1:

Server #1 Port:

Server #1 Secret:

RADIUS Server #2:

Server #2 Port:

Server #2 Secret:

Timeout: seconds

Use VSA: for User Attributes and Permissions

The EMG can be configured to use RADIUS to authenticate users who login to the EMG via SSH, Telnet, the Web or the Console Port. RADIUS users are granted Device Port access through the port permissions below.

Custom Menu:

Data Ports:

Escape Sequence:

Listen Ports:

Break Sequence:

Clear Port Buffers:

Enable for Dial-back:

Dial-back Number:

User Rights

Group: Default Users Power Users Administrators

All RADIUS users are members of a group which has predefined user rights associated with it. Additional rights which are not defined by the group can be added.

Full Administrative: <input type="checkbox"/>	Local Users: <input type="checkbox"/>	Firmware & Configuration: <input type="checkbox"/>
Networking: <input type="checkbox"/>	Remote Authentication: <input type="checkbox"/>	Internal Modem: <input type="checkbox"/>
Services: <input type="checkbox"/>	SSH Keys: <input type="checkbox"/>	Device Port Operations: <input type="checkbox"/>
Secure Lantronix Network: <input type="checkbox"/>	User Menus: <input type="checkbox"/>	Device Port Configuration: <input type="checkbox"/>
Date/Time: <input type="checkbox"/>	Web Access: <input type="checkbox"/>	USB: <input type="checkbox"/>
Reboot & Shutdown: <input type="checkbox"/>	Diagnostics & Reports: <input type="checkbox"/>	SD Card: <input type="checkbox"/>
RPMs: <input type="checkbox"/>	Apply	

2. Enter the following:

Enable RADIUS	Displays selected if you enabled this method on the User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox. Note: You can enable RADIUS here or on the first User Authentication page. If you enable RADIUS here, it automatically displays at the end of the order of precedence on the User Authentication page.
RADIUS Server #1	IPv4 or IPv6 address or hostname of the primary RADIUS server. This RADIUS server may be a proxy for SecurID. SecurID is a two-factor authentication method based on the user's SecurID token and pin number. The SecurID token displays a string of digits called a token code that changes once a minute (some tokens are set to change codes every 30 seconds).
Server #1 Port	Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the EMG unit uses the default RADIUS port (1812).
Server #1 Secret	Text that serves as a shared secret between a RADIUS client and the server (EMG unit). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.
RADIUS Server #2	IPv4 or IPv6 address or host name of the secondary RADIUS server. This server can be used as a SecurID proxy.
Server #2 Port	Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the EMG uses the default RADIUS port (1812).
Server #2 Secret	Text that serves as a shared secret between a RADIUS client and the server (EMG unit). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.
Timeout	The number of seconds (1-30) after which the connection attempt times out. The default is 30 seconds.
Use VSA	Select the check box to obtain remote user attributes (group/permissions and port access) from the RADIUS server via the Vendor-Specific Attribute (VSA). For details on the format of the VSA, see User Attributes & Permissions from LDAP Schema or RADIUS VSA on page 262 .
Custom Menu	If custom menus have been created, you can assign a default custom menu to RADIUS users.
Escape Sequence	A single character or a two-character sequence that causes the EMG unit to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is Esc+A (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as \x1bA , which is hexadecimal (\x) character 27 (1B) followed by an A . This setting allows the user to terminate the connect direct command on the command line interface when the endpoint of the command is deviceport, tcp, or udp. See Key Sequences on page 191 for notes on key sequence precedence and behavior.
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as \x1bB , which is hexadecimal (\x) character 27 (1B) followed by a B .

Enable for Dial-back	Select to grant a user dial-back access. Users with dial-back access can dial into the EMG and enter their login and password. Once the EMG gateway authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user's login (specified here).
Data Ports	The ports users are able to monitor and interact with using the connect direct command. U1 denotes the USB port on the front of the EMG unit.
Listen Port	The ports users are able to monitor using the connect listen command.
Clear Port Buffers	The ports whose port buffer users may clear using the set locallog clear command.

Note: Older RADIUS servers may use **1645** as the default port. Check your RADIUS server configuration.

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

Group	Select the group to which the RADIUS users will belong: <ul style="list-style-type: none"> ◆ Default Users: This group has only the most basic rights. You can specify additional rights for the individual user. ◆ Power Users: This group has the same rights as Default Users plus Web Access, Networking, Date/Time, Reboot & Shutdown, and Diagnostics & Reports. ◆ Administrators: This group has all possible rights.
--------------	---

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage Secure Lantronix units (e.g., EMG, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the EMG unit.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown .
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.

Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
SD Card	Right to enter settings for SD card.
RPM	Right to manage and control remote power managers.

- Click the **Apply** button.

RADIUS Commands

Go to [RADIUS Commands](#) to view CLI commands which correspond to the web page entries described above.

User Attributes & Permissions from LDAP Schema or RADIUS VSA

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

- ◆ **rights** - User rights. The value string is a comma-separated list of two letter user permissions. Example: "nt,wb,ra".
- ◆ **data** - Data port access. The value string specifies the list of ports the user has 'direct' access to. Example: "2,4-18,U1".
- ◆ **listen** - Listen port access. The value string specifies the list of ports the user has 'listen' access to.
- ◆ **clear** - Clear port access. The value string specifies the list of port buffers the user has the right to clear.
- ◆ **group** - User group. Valid values for the value string are "default", "power", and "admin", and any EMG custom group name. If a custom group name is specified and it matches a current EMG custom group name, any rights attribute will be ignored, and the custom group's rights (permissions) will be used instead. A group name with spaces cannot be specified.
- ◆ **escseq** - Escape sequence. The value string specifies the user's escape sequence. Use "\x" to specify non-printable characters. For example, "\x1bA" specifies the sequence "ESC-A".
- ◆ **brkseq** - Break sequence. The value string specifies the user's break sequence.
- ◆ **menu** - Custom user menu. The value string specifies the user's custom user menu.
- ◆ **display** - Display custom user menu when a user logs into the CLI. Valid values for the value string are "yes" and "no".
- ◆ **dbnumber** - Dial-back number. The value string specifies the user's dial-back number for modem dial-back connections.
- ◆ **allowdb** - Allow a user to have dial-back access. Valid values for the value string are "yes" and "no".

RADIUS servers will need to be configured to support the Lantronix Vendor-Specific Attribute. For example, on a FreeRADIUS server, the dictionary will need to be updated with the Lantronix definition by including the contents below in a file named *dictionary.lantronix*, and including it in the RADIUS server dictionary definitions by adding the appropriate \$INCLUDE directive to the main dictionary file.

```
# dictionary.lantronix
#
# Lantronix Edge Management Gateway
# Provides EMG-specific user attributes
#
VENDOR Lantronix 244

BEGIN-VENDOR Lantronix

ATTRIBUTE Lantronix-User-Attributes 1 string

END-VENDOR Lantronix
```

Once this is complete, the users file can be updated to include the Lantronix VSA for any user:

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

Kerberos

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

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

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

All Kerberos users are members of a group that has predefined user rights associated with it. You can add additional user rights that are not defined by the group.

To configure the EMG to use Kerberos to authenticate users:

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

Figure 13-8 User Authentication > Kerberos

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, there is a navigation bar with tabs for Network, Services, User Authentication (which is selected), Devices, Maintenance, and Quick Setup. Below the navigation bar, there is a sub-navigation bar with tabs for Auth Methods, Local/Remote Users, NIS, LDAP, RADIUS, Kerberos, TACACS+, Groups, SSH Keys, and Custom Menus. The main content area is titled "Kerberos". It contains fields for "Enable Kerberos", "Realm", "KDC", "KDC IP Address", "KDC Port" (set to 88), "Use LDAP" (with a note about LDAP settings), "Custom Menu" (set to <none>), "Escape Sequence" (set to \x1bA), "Break Sequence" (set to \x1bB), "Data Ports" (set to 1-4,U1), "Listen Ports" (set to 1-4,U1), "Clear Port Buffers" (set to 1-4,U1), "Enable for Dial-back" (unchecked), and "Dial-back Number" (empty). To the right of these fields is a note: "The EMG can be configured to use Kerberos to authenticate users who login to the EMG via SSH, Telnet, the Web or the Console Port. Kerberos users are granted Device Port access through the port permissions below." Below this is a "User Rights" section with a "Group" dropdown set to "Default Users". It lists various permissions: Full Administrative, Networking, Services, Secure Lantronix Network, Date/Time, Reboot & Shutdown, Local Users, Remote Authentication, SSH Keys, User Menus, Web Access, Diagnostics & Reports, Firmware & Configuration, Internal Modem, Device Port Operations, Device Port Configuration, USB, and SD Card. Each permission has a corresponding checkbox. At the bottom of the "User Rights" section is an "Apply" button.

2. Enter the following:

Enable Kerberos	Check box displays as checked if this method is enabled on the User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox. Note: You can enable Kerberos here or on the first User Authentication page. If you enable Kerberos here, it automatically displays at the end of the order of precedence on the User Authentication page.
Realm	Enter the name of the logical network served by a single Kerberos database and a set of Key Distribution Centers. Usually, realm names are all uppercase letters to differentiate the realm from the Internet domain. Realm is similar in concept to an NT domain.
KDC	A key distribution center (KDC) is a server that issues Kerberos tickets. A ticket is a temporary set of electronic credentials that verify the identity of a client for a particular service. Enter the KDC in the fully qualified domain format (FQDN). An example is emg.local.
KDC IP Address	Enter the IPv4 or IPv6 address of the Key Distribution Center (KDC).

KDC Port	Port on the KDC listening for requests. Enter an integer with a maximum value of 65535. The default is 88 .
Use LDAP	Indicate whether Kerberos should rely on LDAP to look up user IDs and Group IDs. This setting is disabled by default. Note: Make sure to configure LDAP if you select this option.
Custom Menu	If custom menus have been created, you can assign a default custom menu to RADIUS users.
Escape Sequence	<p>A single character or a two-character sequence that causes the EMG to leave direct (interactive) mode. (To leave listen mode, press any key.)</p> <p>A suggested value is Esc+A (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as \x1bA, which is hexadecimal (\x) character 27 (1B) followed by an A.</p> <p>This setting allows the user to terminate the <code>connect direct</code> command on the command line interface when the endpoint of the command is <code>deviceport</code>, <code>tcp</code>, or <code>udp</code>.</p> <p>See Key Sequences on page 191 for notes on key sequence precedence and behavior.</p>
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as \x1bB , which is hexadecimal (\x) character 27 (1B) followed by a B .
Enable for Dial-back	Select to grant a user dial-back access. Users with dial-back access can dial into the EMG and enter their login and password. Once the EMG unit authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either dialed back on a fixed number, or on a number that is associated with the user's login (specified here).
Data Ports	The ports users are able to monitor and interact with using the <code>connect direct</code> command. U1 denotes the USB port on the front of the EMG unit.
Listen Port	The ports users are able to monitor using the <code>connect listen</code> command.
Clear Port Buffers	The ports whose port buffer users may clear using the <code>set locallog clear</code> command.

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

Group	Select the group to which the Kerberos users will belong: <ul style="list-style-type: none"> ◆ Default Users: This group has only the most basic rights. You can specify additional rights for the individual user. ◆ Power Users: This group has the same rights as Default Users plus Web Access, Networking, Date/Time, Reboot & Shutdown, and Diagnostics & Reports. ◆ Administrators: This group has all possible rights.
--------------	--

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure Lantronix units (e.g.,EMG, or SLC units) on the local subnet.

Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the EMG unit.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown .
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
SD Card	Right to enter settings for SD card.
RPM	Right to manage and control remote power managers.

- Click the **Apply** button.

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

Kerberos Commands

Go to [Kerberos Commands](#) to view CLI commands which correspond to the web page entries described above.

TACACS+

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

The system administrator can configure the EMG unit to use TACACS+ to authenticate users attempting to log in using the Web, Telnet, SSH, or the console port.

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

All TACACS+ users are members of a group with associated predefined user rights. You may add additional user rights that are not defined by the group.

TACACS+ Groups

This section describes how a `priv_lvl` assigned to a TACACS+ user can be mapped to a EMG custom [Groups](#), which will set the permissions and port rights for a TACACS+ user when they login to the EMG.

TACACS+ users are typically configured to have a privilege level 0-15, with each level representing a privilege level that is a superset of the next lower value. The privilege level can be assigned to individual users, or to groups that the user is a member of. When the EMG authenticates a TACACS+ user, it will first send an authentication request to the TACACS+ server, and wait for an authentication reply. If the user is successfully authenticated, the EMG will next send an authorization request to the TACACS+ server with the **Service** and optional **Protocol**. The EMG will wait for an authorization response that will indicate if the user was successfully authorized for the requested service and protocol, and also contains a set of attribute-value pairs which define the attributes associated with the TACACS+ user.

The **priv_lvl** or **priv-lvl** is the only attribute sent from the TACACS+ server that the EMG will recognize and utilize. The privilege level number will be used to map to a EMG custom user group by finding a group with a name that ends in the same number as the `priv_lvl`. For example, a EMG group called "admin15" will map to any TACACS+ users with `priv_lvl` equal to 15; a EMG group called "manager8" will map to any TACACS+ users with `priv_lvl` equal to 8, and a EMG group called "readonly0" will map to any TACACS+ users with `priv_lvl` equal to 0. If two EMG groups ending with the same number exist, the EMG will select the first matching group it finds while searching the group list; for consistency it is recommended that only one EMG group exist for each `priv_lvl`.

When a TACACS+ user authenticates to the EMG, the Authentication Log will record any `priv_lvl` attribute-value pair returned by the TACACS+ server:

```
Sep 21 15:44:38 2017 slc431d SLC-SLB/x15login[2839] :  
pam_sm_authenticate: server returned attribute `PRIV_LVL=14'
```

Any `priv_lvl` obtained for a TACACS+ user can also be viewed at the CLI with the `show user` command.

To configure the EMG unit to use TACACS+ to authenticate users:

1. Click the **TACACS+** tab and select **TACACS+**. The following page displays.

Figure 13-9 User Authentication > TACACS+

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, the title 'User Authentication > TACACS+' is displayed. The main configuration area for TACACS+ includes fields for 'TACACS+ Server #1', 'Secret', 'Retype Secret', 'Encrypt Messages' (checkbox), 'Authentication Service' (radio buttons for ASCII Login, PPP/PAP, PPP/CHAP), 'Service' (text input 'shell'), 'Protocol' (text input), and 'Timeout' (text input '5 seconds'). To the right, there is a note about using TACACS+ for authentication via SSH, Telnet, Web, or Console Port, mentioning Device Port access through port permissions. Below this are fields for 'Custom Menu', 'Escape Sequence', 'Break Sequence', 'Data Ports' (1-4, U1), 'Listen Ports' (1-4, U1), 'Clear Port Buffers' (1-4, U1), and 'Dial-back Number'. Under the 'User Rights' section, there are radio buttons for 'Default Users', 'Power Users', and 'Administrators', with a note that all TACACS+ users are members of a group with predefined rights. A list of rights includes: Full Administrative, Networking, Services, Secure Lantronix Network, Date/Time, Reboot & Shutdown, Local Users, Remote Authentication, SSH Keys, User Menus, Web Access, Diagnostics & Reports, Firmware & Configuration, Internal Modem, Device Port Operations, Device Port Configuration, USB, and SD Card. An 'Apply' button is located at the bottom of this section.

2. Enter the following:

Enable TACACS+	Displays selected if you enabled this method on the User Authentication page. If you want to set up this authentication method but not enable it immediately, clear the checkbox. You can enable TACACS+ here or on the first User Authentication page. If you enable TACACS+ here, it automatically displays at the end of the order of precedence on the User Authentication page.
TACACS+ Servers 1-3	IPv4 or IPv6 address or host name of up to three TACACS+ servers.
Secret/Retype Secret	Shared secret for message encryption between the EMG and the TACACS+ server. Enter an alphanumeric secret of up to 127 characters.
Encrypt Messages	Select the checkbox to encrypt messages between the EMG unit and the TACACS+ server. Selected by default.

Authentication Service	The type of service used to pass the authentication tokens (e.g., login and password) between the EMG and the TACACS+ server. Options are: ASCII , Login (login and password are transmitted in clear, unencrypted text), PPP/PAP (login and password are transmitted in clear, unencrypted text via a PAP protocol packet), and PPP/CHAP (the TACACS+ server sends a challenge that consists of a session ID and an arbitrary challenge string, and the user name and password are encrypted before they are sent back to the server). PPP/PAP is the default.
Service	The service to use when sending a TACACS+ authorization message to the server to obtain an authenticated user's <code>priv_lvl</code> . The <code>priv_lvl</code> is used to assign a EMG custom group to the authenticated user for permissions and port rights (see TACACS+ Groups). Suggested values are "slip", "ppp", "arap", "shell", "tty-daemon", "connection", "system" and "firewall". The default is "shell".
Protocol	The optional protocol associated with the Service, which is included in the TACACS+ authorization message sent to the server to obtain an authenticated user's <code>priv_lvl</code> . The <code>priv_lvl</code> is used to assign a EMG custom group to the authenticated user for permissions and port rights (see TACACS+ Groups). Suggested values are "lcp", "ip", "ipx", "atalk", "vines", "lat", "xremote", "tn3270", "telnet", "rlogin", "pad", "vpdn", "ftp", "http", "deccp", "osicp" and "unknown".
Timeout	The timeout in seconds when attempting to connect to a TACACS+ server. Timeout range is 1 to 10 seconds. 5 seconds is the default.
Custom Menu	If custom menus have been created (see Custom User Menu Commands), you can assign a default custom menu to TACACS+ users.
Escape Sequence	A single character or a two-character sequence that causes the EMG to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is Esc+A (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as \x1bA , which is hexadecimal (\x) character 27 (1B) followed by an A . This setting allows the user to terminate the <code>connect direct</code> command on the command line interface when the endpoint of the command is <code>deviceport</code> , <code>tcp</code> , or <code>udp</code> .
Break Sequence	A series of 1-10 characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as \x1bB , which is hexadecimal (\x) character 27 (1B) followed by a B . See Key Sequences for notes on key sequence precedence and behavior.
Enable for Dial-back	Select to grant a user Dial-back access. Users with dial-back access can dial into the EMG unit and enter their login and password. Once the EMG authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either Dial-back on a fixed number, or on a number that is associated with the user's login (specified here).
Data Ports	The ports users are able to monitor and interact with using the <code>connect direct</code> command. U1 denotes the USB port on the front of the EMG unit.
Listen Ports	The ports users are able to monitor using the <code>connect listen</code> command.
Clear Port Buffers	The ports whose port buffer users may clear using the <code>set locallog clear</code> command.

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

Group	Select the group to which the TACACS+ users will belong: <ul style="list-style-type: none"> ◆ Default Users: This group has only the most basic rights. You can specify additional rights for the individual user. ◆ Power Users: This group has the same rights as Default Users plus Web Access, Networking, Date/Time, Reboot & Shutdown, and Diagnostics & Reports. ◆ Administrators: This group has all possible rights.
--------------	--

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage secure Lantronix units (e.g., EMG, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the EMG unit.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown .
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
SD Card	Right to enter settings for SD card.
RPM	Right to manage and control remote power managers.

5. Click the **Apply** button.

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

TACACS+ Commands

Go to [TACACS+ Commands](#) to view CLI commands which correspond to the web page entries described above.

Groups

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

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

To configure Groups in the EMG unit:

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

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

Figure 13-10 User Authentication > Groups

Groups

Note: when deleting a group, all users in the group will either be deleted or changed to the default group.

View Group Delete Group

Groups									
Id	Name	Permissions	Esc Seq	Brk Seq	Custom Menu	DB	Listen	Data	Clear
3	auditor	do,dr	\x1bA	\x1bB		N	1-4,U1	1-4,U1	1-4,U1

Group Id: 0

Group Name:

Listen Ports: 1-4,U1

Enable for Dial-back:

Custom Menu: <none>

Data Ports: 1-4,U1

Dial-back Number:

Display Menu at Login:

Clear Port Buffers: 1-4,U1

Escape Sequence: \x1bA

Break Sequence: \x1bB

Full Administrative:

Local Users:

Firmware & Configuration:

Networking:

Remote Authentication:

Internal Modem:

Services:

SSH Keys:

Device Port Operations:

Secure Lantronix Network:

User Menus:

Device Port Configuration:

Date/Time:

Web Access:

USB:

Reboot & Shutdown:

Diagnostics & Reports:

SD Card:

RPMs:

2. Enter the following:

Group Name	Enter a name for the group.
Listen Ports	The ports users are able to monitor using the <code>connect listen</code> command.
Data Ports	The ports users are able to monitor and interact with using the <code>connect direct</code> command. U1 denotes the USB port on the front of the EMG unit.
Clear Port Buffers	The ports whose port buffer users may clear using the <code>set locallog clear</code> command.
Enable for Dial-back	Select to grant a user. Users with dial-back access can dial into the EMG unit and enter their login and password. Once the EMG authenticates them, the modem hangs up and dials them back. Disabled by default.
Dial-back Number	The phone number the modem dials back on depends on this setting for the device port. The user is either on a fixed number, or on a number that is associated with the user's login (specified here).

Escape Sequence	A single character or a two-character sequence that causes the EMG to leave direct (interactive) mode. (To leave listen mode, press any key.) A suggested value is Esc+A (escape key, then uppercase "A" performed quickly but not simultaneously). You would specify this value as \x1bA , which is hexadecimal (\x) character 27 (1B) followed by an A . This setting allows the user to terminate the <code>connect direct</code> command on the command line interface when the endpoint of the command is <code>deviceport</code> , <code>tcp</code> , or <code>udp</code> .
Break Sequence	A series of one to ten characters users can enter on the command line interface to send a break signal to the external device. A suggested value is Esc+B (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as \x1bB , which is hexadecimal (\x) character 27 (1B) followed by a B .
Custom Menu	If custom menus have been created you can assign a default custom menu to the group. See Custom Menus for more information.
Display Menu at Login	Check the checkbox to display the menu at login.

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

Full Administrative	Right to add, update, and delete all editable fields.
Networking	Right to enter Network settings.
Services	Right to enable and disable system logging, SSH and Telnet logins, SNMP, and SMTP.
Secure Lantronix Network	Right to view and manage Secure Lantronix units (e.g., EMG, or SLC units) on the local subnet.
Date/Time	Right to set the date and time.
Reboot & Shutdown	Right to shut down and reboot the EMG unit.
Local Users	Right to add or delete local users on the system.
Remote Authentication	Right to assign a remote user to a user group and assign a set of rights to the user.
SSH Keys	Right to set SSH keys for authenticating users.
User Menus	Right to create a custom user menu for the CLI.
Web Access	Right to access Web-Manager.
Diagnostics & Reports	Right to obtain diagnostic information and reports about the unit.
Firmware & Configuration	Right to upgrade the firmware on the unit and save or restore a configuration (all settings). Selecting this option automatically selects Reboot & Shutdown .
Internal Modem	Right to update internal modem settings.
Device Port Operations	Right to control device ports.
Device Port Configuration	Right to enter device port settings.
USB	Right to enter modem settings for USB devices and control USB storage devices.
SD Card	Right to enter settings for SD card.
RPM	Right to manage and control remote power managers.

4. Click the **Add Group** button.

To view or update a group:

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

To delete a group:

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

Group Commands

Go to [Groups Commands](#) to view CLI commands which correspond to the web page entries described above.

SSH Keys

The EMG can import and export SSH keys to facilitate shared key authentication for all incoming and outgoing SSH connections. By using a public/private key pair, a user can access multiple hosts with a single passphrase, or, if a passphrase is not used, a user can access multiple hosts without entering a password. In either case, the authentication is protected against security attacks because both the public key and the private key are required to authenticate. For both imported and exported SSH keys, the EMG unit supports both RSA and DSA keys, and can import and export keys in OpenSSH and SECSH formats. Imported and exported keys are saved with the EMG configuration, and the administrator has the option of retaining the SSH keys during a reset to factory defaults.

The EMG unit can also update the SSH RSA and DSA host keys that the SSH server uses with site-specific host keys or reset them to the default values.

Imported Keys

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

Exported Keys

The EMG can generate SSH keys for SSH connections out of the EMG for any EMG user. The EMG retains both the private and public key on the EMG unit, and makes the public key available for export via SCP, SFTP, FTP, or copy and paste. The name of the key is used to generate the name of the public key file that is exported (for example, <keyname>.pub), and the exported keys are organized by user and key name. Once a key is generated and exported, you can delete the key or view the public portion. Any SSH connection out of the EMG for the designated host/user combination uses the SSH key for authentication.

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

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

Figure 13-11 User Authentication > SSH Keys

LANTRONIX® EMG851000

Logout Host: emgfcf0 User: sysadmin

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

Network Services User Authentication Devices Maintenance Quick Setup

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

U1	E1	1	3
SD	E2	2	4

SSH Keys Help?

Imported Keys (SSH In)

Host & User Associated with Key
(not required if host and EMG Local User login are declared in imported key file; ignored if file contains multiple keys)

Host:
User:

Host & Login for Import

Import via:

Public Key:
Host:
Path:
Login:
Password:
Retype Password:

Exported Keys (SSH Out)

Export: New Key for User All Previously Created Keys
User:
Key Name:
Key Type: RSA DSA
Number of Bits:
Passphrase:
Retype Passphrase:
SECSH Format:
Public Key Filename:

Host & Login for Export

Export via:
Host:
Path:
Login:
Password:
Retype Password:

2. Enter the following:

Imported Keys (SSH In)

Host & User Associated with Key

These entries are required in the following cases:

- ◆ The imported key file does not contain the host that the user will be making an SSH connection from, or
- ◆ The EMG local user login for the connection is different from the user name the key was generated from or is not included in the imported key file, or
- ◆ The imported key file contains multiple keys; in this case, each key must include the user name and host at the end of the line in the standard <key> <user name>@<host> format.

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

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAEApUHCX9EWsHt+jmUGXa1YC3us
ABYxIXUhSU1N+NU9HNaUADUFD8LYz8/gUnUSH4Ksm8GRT7/8/Sn9jCVfGPh
UQ== asallaway@winserver
```

Host	The host name or IP address which will be associated with the SSH Key, typically the host that the key was generated on. Once imported, the key can be used to access the EMG from any host, not just the host associated with the key.
User	The User ID of the user being given secure access to the EMG unit.

Host & Login for Import

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

Exported Keys (SSH Out)

Export	Enables you to export created public keys. Select one of the following: <ul style="list-style-type: none"> ◆ New Key for User: Enables you to create a new key for a user and export the public key in a file. ◆ All Previously Created Keys: Does not create any keys, but exports all previously created public keys in one file.
User	User ID of the person given secure access to the remote server.

Key Name	Name of the key. This will generate the public key filename (e.g., <keyname>.pub).
Key Type	Select either the RSA or the DSA encryption standard. RSA is the default.
Number of Bits	Select the number of bits in the key (1024 , 2048 , 3072 , or 4096). The default is 2048 .
Passphrase / Retype Passphrase	Optionally, enter a passphrase associated with the key. The passphrase may have up to 50 characters. The passphrase is an optional password that can be associated with an SSH key. It is unique to each user and to each key. See Key Sequences for notes on key sequence precedence and behavior.
SECSH Format	Indicate whether the keys will be exported in SECSH format (by default the key is exported in OpenSSH format).
Public Key Filename	Filename of the public host key.

Host and Login for Export

Export via	Select the method (SCP , SFTP , FTP , HTTPS , or Copy/Paste) of exporting the key to the remote server. Copy/Paste , the default, requires no other parameters for export.
Host	IP address of the remote server to which the EMG will SCP, SFTP or FTP the public key file.
Path	Optional path of the file on the host to SCP, SFTP or FTP the public key too.
Login	User ID to use to SCP, SFTP or FTP the public key file.
Password / Retype Password	Password to use to SCP, SFTP or FTP the public key file.

To view or delete a key:

1. Select the key from the appropriate table. The **View** and **Delete** buttons become active.
2. To view the key, click the **View** button. A pop-up page displays the key.

Imported key for sysadmin@DaveSLM:
 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAxGxPGY9HsG9VqroDo98B89Cf
 haqB6jG//0tTMKkb3zrpPu0HHAXaiVXHAvv71Ate31VTpoXdLAXN0uCvuJLf
 aL/LvvGmoEWBuBSu5051QHfL70ijxZWOEV TJGFqUQTSq8Ls3/v31kUJEX51n
 2A1Qx0F40I5wNEC0+m3d5QE+FKc= sysadmin@DaveSLM

3. To delete the key, click the **Delete** button.

To view, reset, or import SSH RSA, And DSA host keys:

1. On the **User Authentication - SSH Keys** page, click the **SSH Server/Host Keys** link at the top right. The following page displays the current host keys. In the example below, the current keys are the defaults.

Figure 13-12 Current Host Keys

LANTRONIX® EMG851000

Logout Host: emgfccf0 User: sysadmin

Network Services User Authentication Devices Maintenance Quick Setup

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

SSH Server/Host Keys Help?

Current Host RSA Public Key (Default Key)

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDuDS4Rbaqh6oJgRdIWxDjfD1kUOUWoGdxZOAjYR2Z6
15igrvba181u7Vt3SvHTI34sjaNb4wDeXhWZHoefW35/9GyorzemqVHcfdfHz5CEGQ/4Rkz3UwV/2
cU2Gk1nTX7VnYdrXp95v8UZjAk568jWd04dJ1MVQpgKv+cLrh3ln1capmCCnFFE3R1iZcrX+/6i+su
mbp3gvYxufo9xFKgxhLcvaK6tup0j01IOkEp/7TJ+Uv6D8hiGTCmks0tgSjvpKEd8zCRQnIam98UMFT
aTW/u1g6/1LAoXeACC7ijo/71ZoaIzCfwnGe7I6/ehzVPB1rDNDZon2vJ0J root@(none)
```

Fingerprint:
2048 SHA256:SMYWJ5oseRRFgPR21SwveH+mtvIJX9QDa24kA4kBcug root@(none) (RSA)

Current Host DSA Public Key (Default Key)

```
ssh-dss AAAAB3NzaC1kc3MAAACBAK/gx4sNw/1g6nNi9T/mmcOyaYFFsFFVR1jmIVJ+T+mZwY+BQ53Z1
0frA45CeY8U062Kd70reIgXg32RmcwAUg7KdfyH0d8SV/0jIBLkZn+6Jty8ijm7vsvaHApRR6V8817
44jC5Bkmmh31pYY8xS6iDGk6bJFIFKPZUAuh4iVAAAAFQCj3P9ZGeaNU2oI2TuQ3LVPFt8cjhAAAIBU
T5TvoOSwjGu+9IWbQmkAANiWjibkp9PW+K3vrbuLiQ57mEdLL/tuI3sIYJR40BkTxeBzmmfRznpvs
2NLd1PCibcs1UBmgn4oLcB8N6EN+RMqe4b1QS5r0vZ8DVKeWbIN0c70/pTrv+76RMY6nT2FN6L9a8VGt
x1jb5L5ngAAAIBuIIIfWyiK3z4ARI/G9YWrNQs25gR+fsoc32PnUwtSYF5j52vJ65yqjyeXXCWNzMI11
LmU7A7a7Ju9DcOFA5KhkboiNJM2npHiQEIV+p1X+X57wRxtvvfIClkRNICxV21Qof84PeWphf1kbIj05
c+10hJpMH20N4hj22CozJXNs5w== root@(none)
```

Fingerprint:
1024 SHA256:k/j57+e/vTjwSDWtvL9K84t9hbZHhCwkbu+oo9dN4ps root@(none) (DSA)

Reset to Default Host Key: All Keys RSA DSA

Note: changing a host key requires a reboot for the update to take effect.

Import Host Key:
Type: RSA ▼
Import via: SFTP ▼
Public Key Filename: _____
Private Key Filename: _____

Host: _____
Path: _____
Login: _____
Password: _____
Retype Password: _____

◀ Back to SSH Keys

2. View or enter the following:

Reset to Default Host Key	Select the All Keys checkbox to reset all default key(s), or select one or more checkboxes to reset defaults for RSA , or DSA keys. All checkboxes are unselected by default.
Import Host Key	To import a site-specific host key, select the checkbox. Unselected by default.
Type	From the drop-down list, select the type of host key to import.
Import via	From the drop-down list, select the method of importing the host key (SCP or SFTP). The default is SFTP .
Public Key Filename	Filename of the public host key.
Private Key Filename	Filename of the private host key.
Host	Host name or IP address of the host from which to import the key.

Path	Path of the directory where the host key will be stored.
Login	User ID to use to SCP or SFTP the file.
Password / Retype Password	Password to use to SCP or SFTP the file.

3. Click the **Apply** button.
4. Repeat steps 2-3 for each key you want to import.
5. To return to the SSH Keys page, click the **Back to SSH Keys** link.

SSH Commands

Go to [SSH Key Commands](#) to view CLI commands that correspond to the web page entries described above.

Custom Menus

Users can have custom user menus as their command line interface, rather than the standard CLI command set. Each custom user menu can contain up to 50 commands ('logout' is always the last command). Instead of typing each command, the user enters the number associated with the command. Each command can also have a nickname associated with it, which can be displayed in the menu instead of the command. The commands `showmenu <Menu Name>` and `returnmenu` can be entered to display another menu from a menu, or to return to the prior menu. The command `returncli` can be used to break out of a menu and return to the regular CLI.

To add a custom menu:

1. Click the **User Authentication** tab and select the **Custom Menus** option. The Custom Menus page displays:

Figure 13-13 User Authentication > Custom Menus

The screenshot shows the 'Custom Menus' configuration page. At the top, there are tabs for Network, Services, User Authentication (selected), Devices, Maintenance, and Quick Setup. Below the tabs are sub-links for Auth Methods, Local/Remote Users, NIS, LDAP, RADIUS, Kerberos, TACACS+, Groups, SSH Keys, and Custom Menus. On the right, there is a port selection area with buttons for Configuration, WebSSH (DP only), and Connected Device (DP only), and a 4x4 grid of ports labeled U1, E1, 1, 3, SD, E2, 2, 4. The main area is titled 'Custom Menus' and contains a table with 'Name' columns for 'Menu1' and 'Menu2'. To the right of the table are buttons for 'View Custom Menu', 'Delete Custom Menu', and 'Copy Custom Menu'. A text input field 'New Menu Name:' is also present. Below this, there are fields for 'Menu Name:' and 'Title:', and checkboxes for 'Nicknames:' and 'Redisplay Menu:'. To the right are buttons for 'Clear Custom Menu', 'Add Custom Menu', and 'Edit Custom Menu'. On the left, there are fields for 'Command:' and 'Nickname:' with up and down arrow buttons. A 'QuickEdit Mode:' checkbox is checked. Below these are buttons for 'Delete Command & Nickname', 'Clear Command & Nickname', and 'Unselect Command & Nickname'. To the right is a scrollable list titled 'Commands/Nicknames List' containing 'logout(logout)' with up and down arrow buttons for reordering.

2. In the lower section of the page, enter the following:

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

Menu Name	Enter a name for the custom menu.
Title	Enter an optional title which will be displayed about the menu at the CLI.
Nicknames	Select to enable nicknames to be displayed in the menu instead of the commands. If the custom menu will have nicknames, this should also be selected prior to entering the commands in the web page, as this will facilitate entry of the nicknames.
Redisplay Menu	Select to redisplay the custom menu each time before the CLI prompt is displayed.

3. You have the following options:

- To save the custom menu without any more commands than the default **logout** command, click the **Add Custom Menu** button.
- To add menu commands, select the **QuickEdit Mode** box. This will move the cursor from

Command to Nickname and back to **Command** (if **Nicknames** is selected), or keep the cursor on **Command** (if **Nicknames** is not selected). Commands (and the optional nicknames) are added to the **Menu Commands/Nicknames** list when carriage return is entered at the **Command** field (if **Nicknames** is not selected) or the **Nickname** field (if **Nicknames** is selected). Most browsers have a "Select All" keystroke (such as Control-A) which allow you to select all of the text in a field; this can be used in conjunction with the Delete key to clear the contents of a field before entering a new command or nickname. The **Clear Command & Nickname** button can also be used to delete the contents of the **Command** and **Nickname** fields.

Commands can also be added to the list when **QuickEdit Mode** is not selected. Enter the command and the optional nickname and click the **right**  **arrow**. The command will be added before the logout command (if a command/nickname is not selected in the list) or will replace the currently selected command/nickname in the list. The **Unselect Command & Nickname** button can be used to unselect the currently selected command/nickname in the list.

4. To add more commands to the custom menu, repeat step 3.
5. You also have the following options:
 - To edit a command/nickname in the custom menu, select the command in the **Commands/Nicknames List** box and select the **left**  **arrow** button. Change the command and/or the nickname, and with the same command still selected in the list, select the **right**  **arrow** button.
 - To remove a command/nickname from the custom menu, select the command in the **Commands/Nicknames List** box and select the **Delete Command & Nickname** button.
 - To move a command higher up in the menu (the commands are shown in the order they will be presented in the custom menu, with command #1 listed first), select the command in the **Commands/Nicknames List** box and click the **up**  **arrow**.
 - To move a command further down in the menu, select the menu in the **Commands/Nicknames List** and click the **down**  **arrow**.
6. Click the **Add Custom Menu** button.

To view or update a custom menu:

1. In the **Custom Menus** table, select the custom menu and click the **View Custom Menu** button. The custom menu attributes appear in the lower part of the page.
2. Update the menu attributes following the instructions for adding a menu above.
3. Click the **Edit Custom Menu** button.

To delete a custom menu:

1. Select the custom menu in the **Custom Menus** table.
2. Click the **Delete Custom Menu** button.

To create a new custom menu from an existing custom menu:

1. Select the custom menu in the **Custom Menus** table.
2. Enter a name for the new menu in the **New Menu Name** field.
3. Click the **Copy Custom Menu** button.

Custom User Menu Commands

From the current menu, a user can display another menu, thus allowing menus to be nested. The special command `showmenu <Menu Name>` displays a specified menu. The special command `returnmenu` redisplays the parent menu if the current menu was displayed from a `showmenu` command.

The user with appropriate rights creates and manages custom user menus from the command line interface, but can assign a custom user menu to a user from either the command line or the web interface.

When creating a custom user menu, note the following limitations:

- ◆ Maximum of 20 custom user menus
- ◆ Maximum of 50 commands per custom user menu (`logout` is always the last command)
- ◆ Maximum of 15 characters for menu names
- ◆ Maximum of five nested menus can be called.
- ◆ No syntax checking (Enter each command correctly.)

Go to [Custom User Menu Commands](#) to view CLI commands which correspond to the web page entries described above.

14: Maintenance

The system administrator performs maintenance activities and operates the EMG using the options for the Maintenance tab and additional commands on the command line interface.

Firmware & Configurations

The Firmware & Configuration page allows the system administrator to:

- ◆ Configure the FTP, SFTP, or TFTP server that will be used to provide firmware updates and save/restore configurations. (TFTP is only used for firmware updates and configurations restored via DHCP/TFTP.)
- ◆ Set up the location or method that will be used to save or restore configurations (Local Disk, FTP, SFTP, NFS, CIFS, USB, HTTPS or SD card). Update the version of the firmware running on the EMG unit.
- ◆ Save a snapshot of all settings on the EMG device (save a configuration).
- ◆ Restore the configuration, either to a previously saved configuration, or to the factory defaults.
- ◆ Configurations can also be pushed to the EMG via the *HTTPS Push Configuration Restore* feature.

HTTPS Push Configuration Restore

The HTTPS Push Configuration feature allows a saved configuration to be pushed to a EMG via a command line tool such as "curl" that includes the configuration to upload:

```
% curl --insecure --request POST --form "file=@/home/users/admin/current-emgcfg.tgz" 'https://myemg.company.com/cfgupdate.htm?login=sysadmin&password=PASS&config=all&comment=FirmwareUpdate'
```

The arguments that are passed with the URL are:

- ◆ **login** - Login token to use for authentication. This must be a local user with firmware/config and reboot/shutdown rights.
- ◆ **password** - Clear text password for the login token.
- ◆ **config** - Indicates the portion of the configuration to restore, either all, or any combination of the following separated by commas: network, datetime, services, localusers, devports, usb, rpms, remoteauth, connections, events, ipfilter, groups, hostlist, nfscifs, maintenance, sites, scripts, slcnetwork, consoleport, menus, sshkeys, or sslcerts.
- ◆ **comment** - optional comment to include in the system log and audit log. If spaces are included in the comment they should be URL encoded as shown in this bash script:

```
#!/bin/bash

url="https://myemg.company.com/cfgupdate.htm?login=sysadmin&password=PASS&config=all&comment=Update
myemg.company.com with default configuration"
```

```
curl --insecure --request POST --form "file=@/home/users/admin/current-emgcfg.tgz" "$( echo $url | sed 's/ /%20/g' )"
```

If an HTTPS Push Config command is accepted and initiated by the EMG, the EMG will respond with "Configuration restore initiated; EMG will reboot.", the restore will be performed, a message will be logged to the audit log and the system log, and the EMG will reboot. Any errors in the process will result in an error message being displayed.

To configure settings:

1. Click the **Maintenance** tab. The following page displays.

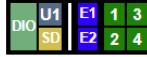
Figure 14-1 Maintenance > Firmware & Configurations



Logout Host: emgcfc0 User: sysadmin

Network Services User Authentication Devices **Maintenance** Quick Setup

Firmware/Config System Log Audit Log Email Log Diagnostics Status/Reports Events Banners



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

Firmware & Configurations

[Help?](#)

General

Reboot: Shutdown:

Internal Temperature

Current: 48 °C / 118 °F

Low: 0 °C / 32 °F

High: 65 °C / 149 °F

Calibrate Offset: 0 °C / 0 °F

Note: Temperatures can be entered in either Celsius or Fahrenheit; to indicate a temperature is Fahrenheit, append the degrees with an 'F', eg "75F".

Site Information

Data Center Rack Row:

Data Center Rack Cluster:

Data Center Rack:

Site Tag:

EMG Firmware

Current Version: 8.2.0.0R15

Clear FW Update Log: [Firmware Update Log](#)

Update Firmware:

Firmware Filename:

Key:

Load Firmware via:

Note: Firmware files stored on NFS, SD Card and USB can be managed by clicking the Manage link below.

Load Firmware Via Options

HTTPS: [Upload File](#)

NFS Mounted Dir:

USB Port: Port U1

FTP/SFTP/TFTP Server:

Path:

Login:

Password:

Retype Password:

Boot Banks and Bootloader Settings

Bank 1: 8.2.0.0R12

Bank 2: 8.2.0.0R15 (current)

Next Boot Bank: 2

Switch to Bank 1:

Watchdog Timer: seconds

Copy configuration from Bank 2 to Bank 1 during firmware update:

Boot Count:

Boot Limit:

Boot Delay: seconds

High Resolution Timers: Requires reboot to take effect.

Configuration Management

No Save/Restore

Save Configuration Tarball Format (HTTPS only)

Restore Factory Defaults

Restore Saved Configuration

Save with Config or Preserve with Restore:

SSH Keys SSL Certificate

Scripts

Preserve Configuration after Restore:

Networking Local Users

Date/Time Device Ports

Services USB

Remote Auth

Configuration Name to Save To or Restore From:

Location for Save, Restore or [Manage](#)

Local Disk Saved Configurations:

FTP Server Use: FTP SFTP

NFS Mounted Directory:

CIFS Share Saved Configurations:

USB Use: Port U1

Saved Configurations:

HTTPS [Upload File for Restore](#) File will be uploaded to Local Disk.

SD Card Saved Configurations:

Internal SD Card Saved Configurations:

2. Enter the following:

Reboot	Select this option to reboot the EMG immediately. The default is No .
Shutdown	Select this option to shut down the EMG unit. The default is No .

Internal Temperature

Current	Displays current temperature.
Low	Sets the acceptable minimum for the internal temperature of the EMG. If the temperature changes to be outside of this range, the EMG will issue an SNMP trap.
High	Sets the acceptable maximum for the internal temperature of the EMG unit. If the temperature changes to be outside of this range, the EMG unit will issue an SNMP trap.
Calibrate Offset	An offset for calibrating the internal temperature of the EMG unit. The offset will be applied one hour after setting the calibration value. Zeroing the offset will take effect immediately and will cancel any current and/or pending calibration.

Site Information

Data Center Rack Row	Set these fields to define the rack row the EMG unit is located within a large data center. The default for these fields is 1.
Data Center Rack Cluster	Set these fields to define the rack cluster the EMG is located within a large data center. The default for these fields is 1.
Data Center Rack	Set these fields to define the rack the EMG unit is located within a large data center. The default for these fields is 1.
Site Tag	Tag or description used to identify the location or some other attribute of the EMG.

EMG Firmware

Note: *The non-active boot bank is updated during the firmware update, without requiring a reboot. The configuration on the current boot bank may optionally be copied to the non-active boot bank during the firmware update.*

Current Version	Displays the current firmware version.
Clear FW Update Log (checkbox)	Clears the contents of the Firmware Update log file.
Firmware Update Log (link)	To view a log of all prior firmware updates, click the Firmware Update Log link.
Update Firmware	<ul style="list-style-type: none"> ◆ To update the EMG firmware, select the checkbox. If you select this option, the EMG unit reboots after you apply the update. The first time boot for each bank may take up to 5 minutes. Subsequent boot times will be approximately 2 minutes. ◆ To view a log of all prior firmware updates, click the Firmware Update Log link.
Firmware Filename	The name of the firmware update file downloaded from the Lantronix web site.
Key	A key for validating the firmware file. The key is provided with the firmware file (32 hex characters).

Load Firmware Via	From the drop-down list, select the method of loading the firmware. Options are FTP, TFTP, HTTPS, NFS, USB, and SD Card . FTP is the default. <ul style="list-style-type: none"> ◆ If you select HTTPS, the Upload File link becomes active. Select the link to open a popup window that allows you to browse to a firmware update file to upload. ◆ If you select NFS, the mount directory must be specified. ◆ The SD Card option must be selected if an SD card is to be used.
--------------------------	---

Boot Banks and Bootloader Settings

Bank 1	Displays the version of EMG firmware in bank 1. <p>Note: The word "current" displays next to the bank from which the EMG booted.</p>
Bank 2	Displays the version of EMG firmware in bank 2.
Next Boot Bank	Displays the current setting for bank to boot from at next reboot.
Switch to Bank 2	If desired, select the alternate bank to boot from at next reboot.
Copy configuration from Bank 1 to Bank 2 during firmware update	If checked, will copy the configuration from the current bank to the bank being updated. The two numbers are automatically generated so that the first number is the current bank.
Boot Count, Boot Delay, Boot Limit	Parameters that control how the EMG boots and when it switches to the alternate boot bank. <ul style="list-style-type: none"> ◆ Boot Delay - how many seconds the bootloader pauses before booting the EMG. Default is 3 seconds, range is 3 - 1800 seconds. ◆ Boot Limit - how many times the EMG will fail to boot before switching to the alternate boot bank. After the EMG fails to boot 2 times Boot limit (so it has attempted to boot Boot Limit times on each bank), the EMG will go into advanced recovery mode, which may require support from Technical Support to resolve so that the EMG can be booted again. Default is 3 boots, range is 3 - 20. ◆ Boot Count - how many times the EMG has failed to boot. If this value reaches Boot Limit, the EMG will switch to the alternate boot bank. The EMG will switch to the alternate boot bank only once. For example, if it fails to boot Boot Limit times on bank 1, it will automatically switch to bank 2; if it fails to boot Boot Limit times on bank 2, it will enter advanced recovery mode. If Boot Count has reached Boot Limit, setting this value to 0 will enable the EMG to boot again. Default is 0, range is 0 - 1.
High Resolution Timers	Enables or disables timers with a high degree of accuracy. High resolution timers are required for Performance Monitoring , but may affect EMG performance if they are enabled. Off by default. Changing this value requires a reboot for the change to take effect.
Watchdog Timer	Timer that will reboot the EMG if the boot fails to properly complete. If the timer expires without a successful boot of the EMG, the timer will automatically reboot the EMG. The default is 300 seconds. A value of zero will disable the watchdog timer.

Load Firmware Via Options

Note: Prior to firmware update, the current configuration is saved to the Local Disk location with the name "before_MMDDYY_HHMM".

HTTPS	Click Upload File to update the EMG firmware.
NFS Mounted Dir	Select the NFS mounted directory from the drop-down menu.
USB Port	Click to select USB port.
FTP/SFTP/TFTP Server	The IP address or host name of the server used for obtaining updates and saving or restoring configurations. May have up to 64 alphanumeric characters; may include hyphens and underscores.
Path	The default path on the server for obtaining firmware update files and getting and putting configuration save files.
Login	The userid for accessing the FTP server. May be blank.
Password / Retype Password	The FTP user password.

Configuration Management

Configuration Management	<p>From the option list, select one of the following:</p> <ul style="list-style-type: none"> ◆ No Save/Restore: Does not save or restore a configuration. ◆ Save Configuration: Saves all settings to file, which can be backed up to a location that is not on the EMG. If Tarball Format is checked, the configuration will be saved in the old (insecure) compressed tar file format, instead of the password protected zip file format. ◆ Restore Factory Defaults: Restores factory defaults. If you select this option, the EMG unit reboots after you apply the update. ◆ Restore Saved Configuration: Returns the EMG settings to a previously saved configuration. If you select this option, the EMG reboots after you apply the update.
Save with Config or Preserve with Restore	<ul style="list-style-type: none"> ◆ Select the SSH Keys checkbox to save any imported or exported SSH keys. ◆ Select the SSL Certificate checkbox to save an imported certificate. ◆ Select the Scripts checkbox to save any interface or batch scripts. Disabled by default.
Preserve Configuration after Restore	<p>Allows the user to keep a subset of the current configuration after restoring a configuration or resetting to factory defaults.</p> <p>Select the checkbox for each part of the current configuration you want to keep, for example, Networking, Services, or Device Ports.</p>
Configuration Name to Save to or Restore From	If you selected to save or restore a configuration, enter a name for the configuration file (up to 12 characters).

Location for Save, Restore, or Manage	<p>If you selected to save or restore a configuration, select one of the following options:</p> <ul style="list-style-type: none"> ◆ Manage: This link allows you to view and delete all configurations saved to the selected location. This feature is available for the Local Disk, NFS Mounts, CIFS Share, USB, and SD Card locations. See Manage Files on page 290. ◆ Local Disk – Saved Configurations: If restoring, select a saved configuration from the drop-down list. ◆ FTP Server: The FTP server specified in the FTP/SFTP/TFTP section. If you select this option, select FTP or SFTP to transfer the configuration file. ◆ NFS Mounted Directory: Local directory of the NFS server for mounting files. ◆ CIFS Share – Saved Configurations: If restoring, select a saved configuration from the drop-down list. ◆ USB: If a USB device is loaded into the USB port of the EMG and properly mounted, the configuration can be saved to or restored from this location. If you select this option, click a saved configuration from the drop-down list. ◆ HTTPS: For saving, the browser will prompt the user to save the configuration. For restoring, the configuration will be uploaded to the Local Disk location. ◆ SD Card: If an SD card is loaded into a card slot of the EMG and properly mounted, the configuration can be saved to or restored from this location. ◆ Internal SD Card: If installed, the internal SD card can be used for saving and restoring configurations. If restoring, select a saved configuration from the drop-down list.
--	---

3. To view a log of all prior firmware updates, click the **Firmware Update Log** (blue link near the center of the web page).
4. Click **Apply**.

Note: *If you selected an option that forces a reboot (restore configuration, update firmware, or reset factory defaults), the EMG unit automatically reboots at the end of the process.*

Figure 14-2 Network > Firmware/Config > Manage

Configurations - Local Disk				
Name	Date/Time Saved	SSH Keys	SSL Certificate	Scripts
before_070819_1044-slccfg.tgz	07/08/19 10:44:31	Y	Y	Y
before_070319_1414-slccfg.tgz	07/03/19 14:14:02	Y	Y	Y
before_070119_1600-slccfg.tgz	07/01/19 16:00:26	Y	Y	Y

New File Name:

Manage Files

The **Manage Files** web page allows you to view the firmware and configuration files saved to the selected location and rename, download or delete any of the files. This feature is available for the Local Disk, NFS Mounts, CIFS Share, USB, and SD card locations.

To manage files:

1. On the [Maintenance > Firmware & Configurations](#) page, click the **Manage** link. The [Network > Firmware/Config > Manage \(on page 290\)](#) page appears and displays the name and the time and date the file was saved.
2. To rename a file, select a file, enter the **New File Name**, and click the **Rename File** button.
3. To download a file, select a file and click the **Download File** button.
4. To delete files, select one, multiple files, or all files, and click the **Delete File** button. A verification message showing files deleted will appear. Click **Back to Manage Files** to return to the [Network > Firmware/Config > Manage](#) page.

Note: When deleting multiple files with a single command, the list of files that have been deleted will only be shown if 10 or fewer files are deleted.

Administrative Commands

Go to [Administrative Commands](#) to view CLI commands which correspond to the web page entries described above.

System Logs

The *Maintenance > System Logs* page allows you to view various system logs. (See [Chapter 7: Services](#) on page 114 for more information about system logs.) You can also clear logs on this page.

To view system logs:

1. Click the **Maintenance** tab and select the **System Logs** option. The following page displays:

Figure 14-3 Maintenance > System Logs

2. Enter the following to define the parameters of the log you would like to view:

Log	Select the type(s) of log you want to view: <ul style="list-style-type: none"> ◆ All ◆ Network ◆ Services ◆ Authentication ◆ Device Ports ◆ Diagnostics ◆ General ◆ Software
Level	Select the alert level you want to view for the selected log: <ul style="list-style-type: none"> ◆ Error ◆ Warning ◆ Info ◆ Debug
Starting at	Select the starting point of the range you want to view: <ul style="list-style-type: none"> ◆ Beginning of Log: to view the log from the earliest available beginning time and date. ◆ Date: to view the log starting from a specific starting date and time.

Ending at	Select the endpoint of the range you want to view: ◆ End of Log : to view the log from the latest available ending time and date. ◆ Date : to view the log up to the last available log ending date and time.
------------------	---

3. Click the **View Log** button. Your specified system log displays. For example, if you select the type **All** and the level **Error**, the EMG unit displays a log similar to this:

Figure 14-4 View System Logs

From a queried system log (e.g., [Figure 14-4](#)), you may email this information to a specific individual or to Lantronix Technical Support. See [Emailing Logs and Reports \(on page 300\)](#).

To clear system logs:

1. From the [Maintenance > System Logs](#) page, select **Maintenance - System Logs**.
2. Click the **Clear Log** button to clear all log information.

System Log Commands

Go to [System Log Commands](#) to view CLI commands which correspond to the web page entries described above.

Audit Log

The [Maintenance > Audit Log](#) page displays a log of all actions that have changed the configuration of the EMG. The audit log is disabled by default. Use the [Services > SSH/Telnet/Logging](#) page ([Chapter 7: Services](#)) to enable the audit log and to configure its maximum size.

Each entry in the log file contains a date/time stamp, user login, and the action performed by the user. The user may clear the log file and sort the log by date/time, user, and command. The audit log is saved through EMG reboots.

1. Click the **Maintenance** tab and select the **Audit Log** option. The following page displays:

Figure 14-5 Maintenance > Audit Log

Audit Log

Sorted by: **Date/Time** Sort by: **User** **Command**

Email Log Comment:
to:

Clear Log **Stop Refresh**

Date/Time	User	Action
Jul 12 14:06:56 2019	sysadmin	Web Authentication Success for user sysadmin
Jul 12 12:23:35 2019	sysadmin	Event Receive Trap deleted
Jul 12 12:23:10 2019	sysadmin	Event Receive Trap/Syslog added/updated
Jul 12 11:32:30 2019	sysadmin	Custom menu 'Menu2' created
Jul 12 11:31:48 2019	sysadmin	Custom menu 'Menu1' created
Jul 12 11:19:00 2019	sysadmin	Group settings updated
Jul 12 11:00:28 2019	sysadmin	Auth order: Local Users=1 NIS=0 LDAP=0 RADIUS=0 Kerberos=0 TACACS=0
Jul 12 10:58:37 2019	sysadmin	Web Authentication Success for user sysadmin
Jul 11 16:36:18 2019	sysadmin	Web Authentication Success for user sysadmin
Jul 11 13:17:21 2019	sysadmin	Web Authentication Success for user sysadmin
Jul 11 11:04:18 2019	sysadmin	Web Authentication Success for user sysadmin
Jul 10 17:11:36 2019	sysadmin	Web Authentication Success for user sysadmin
Jul 10 16:22:41 2019	sysadmin	Host List 'test' updated
Jul 10 16:20:30 2019	sysadmin	Host List 'test' updated
Jul 10 15:20:25 2019	sysadmin	Web Authentication Success for user sysadmin
Jul 10 13:12:29 2019	sysadmin	Web Authentication Success for user sysadmin
Jul 10 11:12:12 2019	sysadmin	Web Authentication Success for user sysadmin
Jul 10 11:01:57 2019	sysadmin	Device inserted at USB port U1
Jul 10 11:00:41 2019	sysadmin	Server settings updated

2. To select a sort option, click the appropriate button:
 - To sort by date and time, click the sort by **Date/Time** button (this is the default.)
 - To sort by user, click the sort by **User** button.
 - To sort by command/action, click the sort by **Command** button.
3. To email this log, follow the instructions in [Emailing Logs and Reports \(on page 300\)](#).
4. To clear the log, click the **Clear Log** button.
5. To freeze or stop automatic refreshing of the log, click the **Stop Refresh** button.

Audit Log Commands

Go to [Audit Log Commands](#) to view CLI commands which correspond to the web page entries described above.

Email Log

The [Maintenance > Email Log](#) page displays a log of all attempted emails. The log file can be cleared from here. The email log is saved through EMG reboots.

1. Click the **Maintenance** tab and select the Email Log option. The following page displays:

Figure 14-6 Maintenance > Email Log

The screenshot shows the LANTRONIX EMG851000 web interface. The top navigation bar includes 'Logout', 'Host: emgfcf0', 'User: sysadmin', and tabs for 'Network', 'Services', 'User Authentication', 'Devices', 'Maintenance' (which is selected), and 'Quick Setup'. Below the tabs are links for 'Firmware/Config', 'System Log', 'Audit Log', 'Email Log' (which is selected), 'Diagnostics', 'Status/Reports', 'Events', and 'Banners'. The main content area is titled 'Email Log'. It features a 'Clear Log' button, a 'Comment:' input field, and a 'to:' input field. Below these are two sections: 'Send Failures: 0', 'Emails Sent: 2', and 'Bytes Sent: 42822'; and a log table with two entries: '07/31/19 18:59 username@example.com' and '07/31/19 18:58 username@example.com'. To the right of the log table are two messages: 'Message Sent (EMG851000 Report (emgfcf0))' and 'Message Sent (EMG851000 Audit Log (emgfcf0))'. The top right of the interface includes a port selection area for 'U1', 'E1', '1 3', 'SD', 'E2', '2 4', and buttons for 'Configuration', 'WebSSH (DP only)', and 'Connected Device (DP only)'. The bottom right has a 'Help?' link.

2. To email this log, follow the instructions in [Emailing Logs and Reports \(on page 300\)](#).
3. To clear the log, click the **Clear Log** button.

Logging Commands

Go to [Logging Commands](#), [USB Device Commands](#), [USB Storage Commands](#), and [Internal Modem Commands](#) to view CLI commands which correspond to the web page entries described above.

Diagnostics

The **Maintenance > Diagnostics** page provides methods for diagnosing problems such as network connectivity and device port input/output problems. You can use equivalent commands on the command line interface.

1. Click the **Maintenance** tab and select the **Diagnostics** option. The following page displays:

Figure 14-7 Maintenance > Diagnostics

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, there is a port status indicator with ports U1, E1, 1, 2, 3, 4, and SD. Below the header, the navigation tabs are Network, Services, User Authentication, Devices, Maintenance (which is selected), and Quick Setup. The Maintenance tab has sub-options: Firmware/Config, System Log, Audit Log, Email Log, Diagnostics (which is selected), Status/Reports, Events, and Banners. The main content area is titled 'Diagnostics'. It contains a 'Select Diagnostics' section with checkboxes for All, IPv4 Arp Table, IPv6 Neighbor Table, Netstat, Host Lookup, Ping, Send Packet, Loopback, EMG Internals, USB Devices, and iPerf. Each diagnostic method has associated configuration fields like Protocol (TCP, UDP), Hostname, Port, String, Count, Device Port, Test (Internal, External), Tree Display, Map Device, iPerf Mode (Server, Client), iPerf Server, and iPerf Options. A 'Run Diagnostics' button is at the bottom.

2. Select **Diagnostics** from checklist (one or more diagnostic methods you want to run, or select **All** to run them all):

IPv4 ARP Table	The IPv4 Address Resolution Protocol (ARP) table used to view the IP address-to-hardware address mapping.
-----------------------	---

IPv6 Neighbor Table	The IPv6 Neighbor table is used to view a list of neighbor's IPv6 addresses on the same network, and their corresponding MAC addresses.
Netstat	Displays network connections. If you select the checkbox, select the TCP or UDP protocol, or select All for both protocols to control the output of the Netstat report.
Host Lookup	Select to verify that the EMG can resolve the host name into an IP address (if DNS is enabled). If selected, also enter a host name in the corresponding Hostname field,
Ping	Select to verify that the host is up and running. If selected, also do the following: <ul style="list-style-type: none"> ◆ Enter a host name in the corresponding Hostname field ◆ Specify Ethernet Port (Both, Eth1 or Eth2) ◆ Check if the IPv6 version of ping should be used.
Send Packet	This option sends an Ethernet packet out one of the Ethernet ports, mainly as a network connectivity test. For UDP, the number of times the string is sent is equal to the number of packets sent. For TCP, the number of times the string is sent may (or may not) be equal to the number of packets sent, because TCP controls how data is packetized and sent out. Enter the following: <ul style="list-style-type: none"> ◆ Protocol: Select the type of packet to send (TCP or UDP). ◆ Hostname: Specify a host name or IP address of the host to send the packet to. ◆ Port: Specify a TCP or UDP port number of the host to send the packet to. ◆ String: Enter a set of up to 64 characters. The string is encapsulated in the packet (so you could use a network sniffer to track the packet and, by looking at its contents, verify that it was sent). ◆ Count: The count is the number of times the string is sent.
Loopback	Specify loopback information: <ul style="list-style-type: none"> ◆ Device Port ◆ Select either an Internal or External test <p>Note: The External test is currently not supported for USB device ports</p>
EMG Internals	Select to display information on the internal memory, storage and processes of the EMG.
USB Devices	Select to display information about USB buses and the devices connected to them, including a mapping between a USB device and the EMG ports.

iPerf	<p>Select to start an iPerf3 server or client to measure network throughput. The server will run in “one-off” mode. This means that it will handle one client connection and then terminate. The server will wait indefinitely for the client to connect. The client will time out if a connection is not made to a server within 15 seconds. For more information, visit the iPerf website.</p> <ul style="list-style-type: none"> ◆ iPerf Mode: Select the mode (Server or Client). Two EMGs can be used to measure network throughput, one running in server mode and one running in client mode. ◆ iPerf Server: Specify the server name or IP address that the client connects to. ◆ iPerf Options: Enter options to configure the packets sent by the server or client. If no options are specified, the server or client will run with a default set of TCP packets. <ul style="list-style-type: none"> ➢ Set server port to listen on/connect to (default 5201): -p, --port n ➢ Format to report: -f, --format [kmgKMGtKMGT] ➢ Pause n seconds between reports: -i, --interval n ➢ Bind to a host, an interface or multicast address: -B, --bind ➢ More detailed output: -V, --verbose ➢ Output in JavaScript Object Notation (JSON) format: -J, --json <p>Note: The options below are supported on the client only:</p> <ul style="list-style-type: none"> ➢ Set length of buffer to n (default 8 KB): -l, --length n[KMG] ➢ Use UDP rather than TCP: -u, --udp ➢ TCP window size (socket buffer size): -w, --window n[KMG] ➢ Set TCP/SCTP maximum segment size (MTU): -M, --set-mss n ➢ Set TCP/SCTP no delay, disabling Nagle’s Algorithm: -N, --no-delay ➢ Set bandwidth to n bits/sec (default 1Mbit/sec, unlimited for TCP): -b, --bitrate n[KMG] ➢ Number of bytes to transmit (instead of -t): -n, --bytes n[KMG] ➢ Time in seconds to transmit for (default 10 secs): -t, --time n ➢ Set the IPv6 flow label: -L, --flowlabel n ➢ Omit the first n seconds: -O, --omit n ➢ Prefix every output line with this string: -T, --title str ➢ Number of blocks (packets) to transmit (instead of -t/-n): -k, --blockcount ➢ Set the IP type of service, 0-255. The usual prefixes for octal and hex can be used, i.e. 52, 064 and 0x34 all specify the same value: -S, --tos n ➢ Set the IP dscp value, either 0-63 or symbolic: --dscp n <p>Note: The EMG uses iPerf version 3.x, which is incompatible with older iPerf versions.</p>
--------------	---

3. Click the **Run Diagnostics** button. The *Diagnostics Output* page displays.

Figure 14-8 Diagnostics Output

4. To view a report, click the link for that report.

- To email this report, follow the instructions in [Emailing Logs and Reports \(on page 300\)](#).

Diagnostic Commands

Go to [Diagnostic Commands](#) to view CLI commands which correspond to the web page entries described above.

Status/Reports

On this page, you can view the status of the EMG ports and power supplies and generate a selection of reports.

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

- Click the **Maintenance** tab and select the **Status/Reports** option. The following page displays:

Figure 14-9 Maintenance > Status/Reports

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, there is a navigation bar with tabs: Network, Services, User Authentication, Devices, Maintenance (which is selected), and Quick Setup. Below the navigation bar, there is a sub-navigation bar with links: Firmware/Config, System Log, Audit Log, Email Log, Diagnostics, Status/Reports (which is selected), Events, and Banners. The main content area is titled "Status/Reports". It displays the following information:

- Device Ports:**
 - Eth1: Up (green)
 - Eth2: Down (red)
 - Console Port: Not Connected (red)
 - Internal Temperature: 49 °C (120 °F) (green)
- Power Supplies:**

U1	E1	1	3
SD	E2	2	4
- View Report:** A list of report types with checkboxes:
 - All
 - Port Status
 - Port Counters
 - IP Routes
 - Connections
 - System Configuration - Complete
 - System Configuration - Basic
 - System Configuration - Authentication
 - System Configuration - Devices
- Generate Report** button.

The top half of the page displays the status of each port, power supply, and the internal modem:

- Green** indicates that the port connection or power supply is active and functioning correctly.
- Red** indicates an error or failure or that the device is off.

- Select the desired reports to view under **View Report**:

View Report

All	Displays all reports.
-----	-----------------------

Port Status	Displays the status of each device port: mode, user, any related connections, and serial port settings.
Port Counters	Displays statistics related to the flow of data through each device port.
IP Routes	Displays the routing table.
Connections	Displays all active connections for the EMG unit: Telnet, SSH, TCP, UDP, device port, and modem.
System Configuration – Complete	Displays a complete snapshot of the EMG settings.
System Configuration – Basic	Displays a snapshot of the EMG unit's basic settings (for example, network, date/time, routing, services, console port).
System Configuration – Authentication	Displays a snapshot of authentication settings only (including a list of all localusers).
System Configuration - Devices	Displays a snapshot of settings for each device port, USB Port, Modem, and Host Lists.

3. Click the **Generate Report** button. In the upper left of the *Generated Status/Reports* page displays a list of reports generated.

Figure 14-10 Generated Status/Reports

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, it displays the host as `emgfcf0` and the user as `sysadmin`. A navigation bar includes links for Network, Services, User Authentication, Devices, Maintenance (which is selected), and Quick Setup. Below the navigation bar, a sub-menu bar offers options like Firmware/Config, System Log, Audit Log, Email Log, Diagnostics, Status/Reports (selected), Events, and Banners. A port status indicator shows ports U1, E1, 1, 2, 3, and 4. The main content area is titled "Status/Reports". It includes fields for "Report(s)" (with "Email Output" selected), "Comment", and "to". Below these fields are links for Port Status, Port Counters, and IP Routes. The "Port Status" section lists four ports (1, 2, 3, 4) with their respective DSR/CD, DTR, CTS, and RTS settings. The "Port Counters" section lists various counters for each port, such as bytes input, framing errors, overrun errors, and parity errors. The "IP Routes" section is currently empty.

4. To email these report(s), follow the instructions in [Emailing Logs and Reports \(on page 300\)](#).

Status Commands

Go to [Status Commands](#) to view CLI commands which correspond to the web page entries described above.

Emailing Logs and Reports

The following logs and reports can be directly emailed to a specific individual or to Lantronix Technical Support directly from the log page:

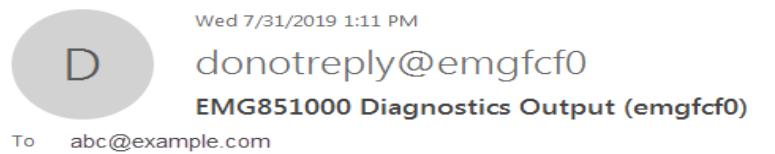
- ◆ System Log ([Figure 14-4](#))
- ◆ Audit Log ([Figure 14-5](#))
- ◆ Email Log ([Figure 14-6](#))

- ◆ Diagnostic Reports ([Figure 14-8](#))
- ◆ Status/Reports ([Figure 14-10](#))

To email a log to an individual:

1. In the **Comment** field of a particular log or report page, enter a comment (if desired).
2. Select the **to** field beside the empty field where you then enter the person's email address.
3. Press the **Email Output** button. An email is immediately sent and a confirmation appears on the screen.

Figure 14-11 Emailed Log or Report



EMG851000 Diagnostics Output (emgfcf0)
Comment: EMG diagnostics ping
Generated 07/31/2019 20:11:15 GMT

Diagnostics Output: Ping (172.19.216.2)

```
PING 172.19.216.2 (172.19.216.2): 56 data bytes
64 bytes from 172.19.216.2: seq=0 ttl=64 time=0.607 ms
64 bytes from 172.19.216.2: seq=1 ttl=64 time=0.308 ms
64 bytes from 172.19.216.2: seq=2 ttl=64 time=0.366 ms
```

```
--- 172.19.216.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.308/0.427/0.607 ms
```

To view information about the EMG unit and contact information for Lantronix:

1. Click the  button on the upper right portion of any web page to access the **About EMG** page (see [Figure 14-12](#)).

Figure 14-12 About EMG

LANTRONIX® EMG851000

Logout Host: **emgfcf0**
User: **sysadmin**

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

Network Services User Authentication Devices Maintenance Quick Setup

About EMG851000

Model: **EMG851000**
Number of USB Ports: **1**
Cellular Modem: **Not Installed**
Wifi: **Not Installed**
Power Supply: **external DC**
S/N: **0080A38BFCF0**

Memory: **1024 MB**
Flash Size: **1024 MB**
Eth1 HW Address: **00:80:a3:8b:fc:f0**
Eth2 HW Address: **00:80:a3:8b:fc:f1**

Uptime: **0 days, 1 hour, 17 minutes**

Firmware Version: **8.2.0.0R4**
OS Version:
Bootloader Version: **2.0.0.0R10**
Main Board Revision: **unknown**
I/O Module Type(s): **RJ45-04**,
I/O Module Revision(s): **04SPB**,
Connectivity Module Type(s): ,
Connectivity Module Revision(s): ,

Software Revisions:
Kernel: **3.6.5**
SSH/SSL: **OpenSSH_7.8p1, OpenSSL 1.0.2r 26 Feb 2019**
Telnet: **netkit-telnet-0.17**
NTP: **ntpd 4.2.6p5**
SMB/CIFS: **Version 3.6.14**
RIP: **zebra version 1.2.4**
Web Server: **mini_httpd/1.24**
PAM/NIS: **1.3.1**
LDAP: **153**
RADIUS: **1.4.0**
Kerberos: **2.4.8**
TACACS+: **1.4.1**
ShellInABox: **2.19**
VPN: **Linux strongSwan U5.6.3/K3.6.5**
Expect: **5.45.4**
Tcl: **8.6**
Python: **3.6.7**

Bootloader Configuration:
Number of Ports: **4**
Model Number: **116**
Product Name: **EMG**
Options: **00000000000000000000000000000000ffff02**

Events

On this *Maintenance > Events* page, you can define what action you want to take for events that may occur in the EMG unit.

1. Click the **Maintenance** tab and select the **Events** option. The following page displays:

Figure 14-13 Maintenance > Events

The screenshot shows the LANTRONIX EMG85110 web interface. The top navigation bar includes 'Logout', 'Host: emgfce', 'User: sysadmin', and tabs for Network, Services, User Authentication, Devices, Maintenance (selected), Quick Setup, Firmware/Config, System Log, Audit Log, Email Log, Diagnostics, Status/Reports, Events (selected), and Banners. The main content area is titled 'Events' and contains configuration fields for a trigger (Receive Trap) and an action (Syslog). It also includes options for Host to Ping, RPM, Outlet, Threshold, DIO Port, Ethernet Port (Eth1 selected), Modem Connection (USB Port U1 selected), NMS/Host to forward trap to, SNMP Community, SNMP Trap OID, and Email Address. Below these fields are buttons for 'Add Event', 'Edit Event', and 'Delete Event'. A note says 'To edit or delete an event, select the radio button in the right column below.' At the bottom is a table with columns 'Id', 'Trigger', 'Options', 'Action', and 'Options', and an 'Apply' button.

2. Enter the following:

Event Trigger	From the drop-down list, select the type of incident that triggers an event. Currently, the options are: <ul style="list-style-type: none"> ◆ Receive Trap ◆ Temperature Over/Under Limit (for Sensorsoft devices) ◆ Humidity Over/Under Limit (for Sensorsoft devices) ◆ Device Port Data Drop ◆ No Internal Modem Dial Tone ◆ Ping Host Fails ◆ RPM Load Over Threshold ◆ DIO Port State Change ◆ DIO Port State Abnormal
Host to Ping	When the trigger is set to Ping Host Fails , enter the hostname, IPv4 address or IPv6 address of the host to ping. The host will be pinged every 2 minutes.
RPM	When the trigger is set to RPM Load over Threshold , select the RPM that will be monitored for a current that exceeds a defined threshold. The RPM needs to support providing a current level as part of its status information. The RPM current will be checked every 2 minutes.

Outlet	When the trigger is set to RPM Load over Threshold , select the outlet that will be monitored for a current that exceeds a defined threshold. The RPM needs to support providing a current level for the selected outlet as part of its status information. If an outlet is not specified, the current level for the entire device will be monitored. The RPM current will be checked every 2 minutes.
Threshold	When the trigger is set to RPM Load over Threshold , specify the maximum allowable threshold for the current; any current readings over this threshold will trigger the selected action. The threshold can be specified in Amps (e.g. 8.5) or as a percentage (e.g. 90%).
DIO Port	When the trigger is set to DIO Port State Change or DIO Port State Abnormal , select the DIO port to monitor. For state change, the selected action will be triggered if the state changes from On to Off or from Off to On. For state abnormal, the selected action will be triggered if the state changes from the Normal state to the opposite state (see DIO Port on page 175 for more information).
Action	From the drop-down list, select the action taken because of the trigger. For example, the action can be writing an entry into the syslog with details of the event or sending the trap(s) to the Ethernet or modem connection. <ul style="list-style-type: none"> ◆ Syslog ◆ Forward All Traps to Ethernet ◆ Forward Selected Trap to Ethernet ◆ Forward all Traps to a Modem Connection ◆ Forward Selected Trap to a Modem Connection ◆ Email Alert ◆ SNMP Trap ◆ Turn DIO Relay On
Ethernet	For actions that require an Ethernet connection (for example, Forward All Traps to Ethernet), select the Ethernet port to use.
Modem Connection on	For actions that require a modem connection (for example, Forward All Traps to a Modem Connection), select which modem connection to use (Device Port , USB Port U1 , or the Internal Modem).
NMS/Host to forward trap to	For actions that forward a trap, enter the IP address of the computer to forward the trap to. The computer does not have to be an SNMP NMS; it just has to be capable of receiving SNMP traps.
SNMP Community	Forwarded traps are sent with this SNMP community value There is no default.
SNMP Trap OID	Enter a unique identifier for an SNMP object. (An SNMP object is anything that can hold a value and can be read using an SNMP "get" action.) The OID consists of a string of numbers separated by periods (for example, 1.1.3.2.1). Each number is part of a group represented by the number on its left.
Email Addresses	Enter an email address to receive email alerts.

3. You have the following options:

- To add the defined event, click the **Add Event** button. The event displays in the Events table at the bottom of the page.
- To edit an event, select the event from the Events table and click the **Edit Event** button. The [Maintenance > Events](#) page displays the event.
- To delete an event, select the event from the Events table and click the **Delete Event** button. A message asks for confirmation. Click **OK**.

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

Events Commands

Go to [Events Commands](#) to view CLI commands which correspond to the web page entries described above.

Banners

The [Maintenance > Banners](#) page allows the system administrator to customize text messages that display to users.

To configure banner settings:

1. Click the Maintenance tab and select Banners option.

Figure 14-14 Maintenance > Banners

The screenshot shows the LANTRONIX EMG851000 web interface. At the top, it displays 'LANTRONIX® EMG851000' and the host and user information: Host: emgfcf0, User: sysadmin. Below this is a navigation bar with tabs: Network, Services, User Authentication, Devices, Maintenance (which is selected), and Quick Setup. Under the Maintenance tab, there are sub-links: Firmware/Config, System Log, Audit Log, Email Log, Diagnostics, Status/Reports, Events, and Banners. The main content area is titled 'Banners'. It contains four input fields for 'Welcome Banner', 'Login Banner', 'Logout Banner', and 'SSH Banner', each with a placeholder text. Below these fields is a note: 'Note: Line feeds can be included in the banners with the '\n' character sequence. The web banner can be configured [here](#).' At the bottom right of the form is an 'Apply' button.

2. Enter the following fields.

Welcome Banner	The text to display on the command line interface before the user logs in. May contain up to 1024 characters. Single quote and double quote characters are not supported. Welcome to the EMG is the default. Note: To create more lines use the <code>\n</code> character sequence.
Login Banner	The text to display on the command line interface after the user logs in. May contain up to 1024 characters. Single quote and double quote characters are not supported. Default is blank. Note: To create more lines, use the <code>\n</code> character sequence.
Logout Banner	The text to display on the command line interface after the user logs out. May contain up to 1024 characters. Single quote and double quote characters are not supported. Default is blank. Note: To create more lines use, the <code>\n</code> character sequence.

SSH Banner	The text to display when a user logs into the EMG via SSH, prior to authentication. May contain up to 1024 characters. Single quote and double quote characters are not supported. Blank by default. Note: To create more lines use the <code>\n</code> character sequence.
-------------------	---

3. Click **Apply** to save.

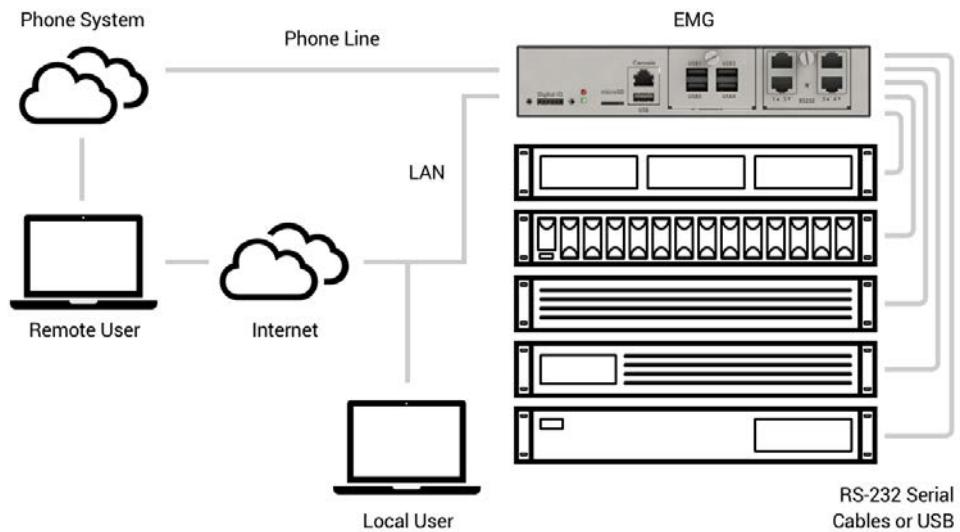
Administrative Banner Commands

Go to [Administrative Commands](#) to view CLI commands which correspond to the web page entries described above.

15: Application Examples

Each EMG has multiple serial ports and two network ports. Each serial port can be connected to the console port of an IT device. Using a network port (in-band) or a modem (out-of-band) for dial-up connection, an administrator can remotely access any of the connected IT devices using Telnet or SSH.

Figure 15-1 EMG - Configuration

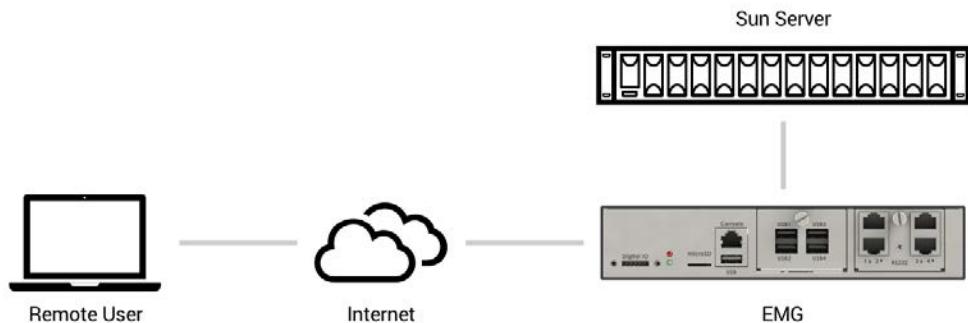


This chapter includes three typical scenarios for using the EMG unit. The scenarios assume that the EMG is connected to the network and has already been assigned an IP address. In the examples, we use the command line interface. You can do the same things using the web page interface except for directly interacting with the EMG unit (direct command).

Telnet/SSH to a Remote Device

The following figure shows a Sun server connected to port 2 of the EMG.

Figure 15-2 Remote User Connected to a SUN Server via the Console Manager



In this example, the sysadmin would:

1. Display the current settings for device port 2:

```
[EMG]> show deviceport port 2
  Current Device Port
Settings
Number: 2  Name: Port-2

Modem Settings-----Data Settings-----IP Settings-----
Modem State: disabled      Baud Rate: 9600      Telnet: disabled
Modem Mode: text           Data Bits: 8        Telnet Port: 2002
Timeout Logins: disabled   Stop Bits: 1        SSH: disabled
Local IP: negotiate        Parity: none       SSH Port: 3002
Remote IP: negotiate       Flow Control: xon/xoff IP: <none>
Authentication: PAP        Logins: disabled
CHAP Host: <none>          Break Sequence: \x1bbB
CHAP Secret: <none>        Check DSR: disabled
NAT: disabled              Close DSR: disabled
Dial-out Login: <none>
Dial-out Password: <none>
Dial-out Number: <none>
Dial-back Number: usernumber
Initialization Script: <none>

Logging Settings-----
Local Logging: disabled    USB Logging: disabled
Email Logging: disabled    Log to: upper slot
Byte Threshold: 100        Max number of files: 10
Email Delay: 60  seconds  Max size of files: 2048
Restart Delay: 60  seconds
Email To: <none>
Email Subject: Port %d Logging
Email String: <none>
```

```
NFS File Logging: disabled
Directory to log to: <none>
Max number of files: 10
Max size of files: 2048
```

2. Change the baud to 57600 and disable flow control:

```
[EMG]> set deviceport port 2 baud 57600 flowcontrol none
Device Port settings successfully updated.
```

3. Connect to the device port:

```
[EMG]> connect direct deviceport 2
```

4. View messages from the SUN server console:

```
Mar 15 09:09:44 tssf280r sendmail[292]: [ID 702911 mail.info] starting
daemon (8.12.2+Sun): SMTP+queueing@00:15:00
Mar 15 09:09:44 tssf280r sendmail[293]: [ID 702911 mail.info] starting
daemon (8.12.2+Sun): queueing@00:15:00
Mar 15 14:44:40 tssf280r sendmail[275]: [ID 702911 mail.info] starting
daemon (8.12.2+Sun): SMTP+queueing@00:15:00
Mar 15 14:44:40 tssf280r sendmail[276]: [ID 702911 mail.info] starting
daemon (8.12.2+Sun): queueing@00:15:00
```

5. Reboot the SUN server:

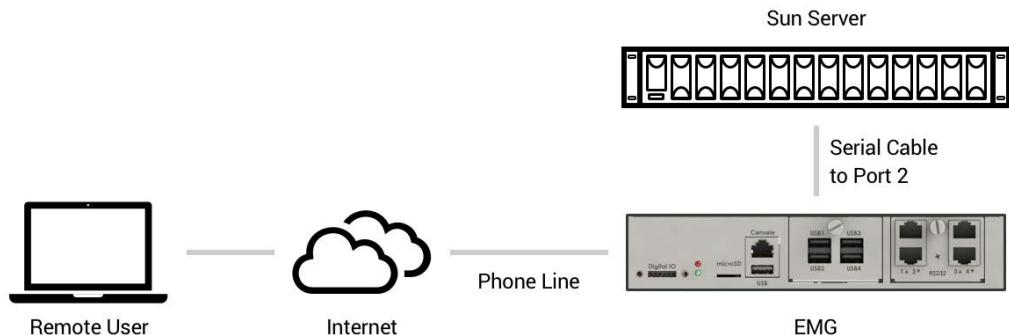
```
Reboot
<shutdown messages from SUN>
```

6. Use the escape sequence to escape from direct mode back to the command line interface.

Dial-in (Text Mode) to a Remote Device

This example shows a phone line connection to the internal modem of the EMG, and a Sun server connected to a device port. You can configure the modem for text mode dial-in, so a remote user can dial into the modem using a terminal emulation program and access the Sun server.

Figure 15-3 Dial-in (Text Mode) to a Remote Device



In this example, the sysadmin would:

1. Configure the device port that the modem is connected to for dial-in:

```
[EMG]> set deviceport port 1 modemmode text
Device Port settings successfully updated.
[EMG]> set deviceport port 1 initscript "AT&F&K3&C1&D2%C0A"
Device Port settings successfully updated.
[EMG]> set deviceport port 1 auth pap
Device Port settings successfully updated.
[EMG]> set deviceport port 1 localsecret "password"
Device Port settings successfully updated.
[EMG]> set deviceport port 1 modemstate dialin
Device Port settings successfully updated.
[EMG]>
```

2. Configure the device port that is connected to the console port of the Sun UNIX server:

```
[EMG]> set deviceport port 2 baud 57600 flowcontrol none
Device Port settings successfully updated.
```

3. Dial into the EMG via the modem using a terminal emulation program on a remote PC. A command line prompt displays.

4. Log into the EMG unit.

```
CONNECT 57600
Welcome to the EMG
login: sysadmin
Password:
Welcome to the EMG Console Manager
Model Number: EMG851000
For a list of commands, type 'help'.
[EMG]>
```

5. Connect to the SUN Unix server using the direct command.

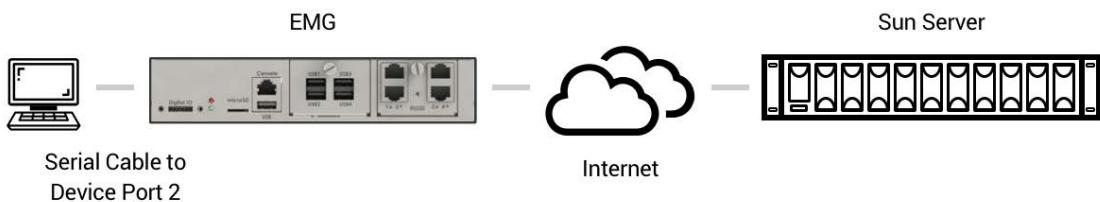
```
[EMG]> connect direct deviceport 2
SunOS 5.7
login: frank
Password:
Last login: Wed Jul 14 16:07:49 from computer
Sun Microsystems Inc. SunOS 5.7 Generic October 1998
SunOS computer 5.7 Generic_123485-05 sun4m sparc SUNW, SPARCstation-20
$
```

6. Use the escape sequence to escape from direct mode back to the command line interface.

Local Serial Connection to Network Device via Telnet

This example shows a terminal device connected to an EMG device port, and a Sun server connected over the network to the EMG device. When a connection is established between the device port and an outbound Telnet session, users can access the Sun server as though they were directly connected to it. (See [Chapter 12: Connections on page 235](#)).

Figure 15-4 Local Serial Connection to Network Device via Telnet



In this example, the sysadmin would:

1. Display the current settings for device port 2:

```
[EMG]> show deviceport port 2
____ Current Device Port
Settings_____
Number: 2 Name: Port-2
Modem Settings-----Data Settings-----IP Settings-----
Modem State: disabled Baud Rate: 9600 Telnet: disabled
Modem Mode: text Data Bits: 8 Telnet Port: 2002
Timeout Logins: disabled Stop Bits: 1 SSH: disabled
Local IP: negotiate Parity: none SSH Port: 3002
Remote IP: negotiate Flow Control: xon/xoff IP: <none>
Authentication: PAP Logins: disabled
CHAP Host: <none> Break Sequence: \x1bb
CHAP Secret: <none> Check DSR: disabled
NAT: disabled Close DSR: disabled
Dial-out Login: <none>
Dial-out Password: <none>
Dial-out Number: <none>
Dial-back Number: usernumber
Initialization Script: <none>

Logging Settings-----
Local Logging: disabled USB Logging: disabled
Email Logging: disabled Log to: upper slot
Byte Threshold: 100 Max number of files: 10
Email Delay: 60 seconds Max size of files: 2048
Restart Delay: 60 seconds
Email To: <none>
Email Subject: Port %d Logging
Email String: <none>
NFS File Logging: disabled
Directory to log to: <none>
```

Max number of files: 10
Max size of files: 2048

2. Change the serial settings to match the serial settings for the vt100 terminal - changes baud to 57600 and disables flow control:

```
[EMG]> set deviceport port 2 baud 57600 flowcontrol none  
Device Port settings successfully updated.
```

3. Create a connection between the vt100 terminal connected to device port 2 and an outbound telnet session to the server. (The IP address of the server is 192.168.1.1):

```
[EMG]> connect bidirection 2 telnet 192.168.1.1  
Connection settings successfully updated.
```

4. At the VT100 terminal, hit <return> a couple of times. The Telnet prompt from the server displays:

```
Trying 192.168.1.1...  
Connected to 192.168.1.1.  
Escape character is '^]'.
```

```
Sun OS 8.0  
login:
```

At this point, a user can log in and interact with the Sun server at the VT100 terminal as if directly connected to the server.

16: Command Reference

After an introduction to using commands, this chapter lists and describes all of the commands available on the EMG command line interface accessed through Telnet, SSH, or a serial connection. The commands are in alphabetical order by category.

Introduction to Commands

Following is some information about command syntax, command line help, and tips for using commands.

Command

Syntax

Commands have the following format:

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

where

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

<category> is a group of related parameters whose settings you want to configure or view. Examples are ntp, deviceport, and network.

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

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

Table 16-1 Actions and Category Options

Action	Category
set	auth cellular cflow cifs cli command consoleport datetime deviceport dio groups history hostlist ipfilter kerberos ldap localusers log menu network nfs nis ntp password perfmon radius remoteusers routing rpm script sdcard security services site slcnetwork sshkey tacacs+ temperature usb vpn xmodem
show	auth auditlog cellular cflow cifs cli connections consoleport datetime deviceport dio emaillog groups history hostlist ipfilter kerberos ldap localusers log menu network nfs nis ntp perfmon portcounters portstatus radius remoteusers routing rpm script sdcard security services site slcnetwork sshkey sysconfig syslog sysstatus tacacs+ temperature usb user vpn xmodem

Action	Category
connect	bidirection direct global listen restart script terminate unidirection
diag	arp arp6 internals iperf lookup loopback netstat nettrace perfstat ping ping6 sendpacket top traceroute usb
admin	banner chip clear config events feature firmware ftp memory quicksetup reboot shutdown site version web
logout	Terminates CLI session.

Command Line Help

For general Help and to display the commands to which you have rights, type:

```
help
```

For general command line Help, type:

```
help command line
```

For release notes for the current firmware release, type:

```
help release
```

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

```
help set network or help admin firmware
```

Tips

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


```
set network port 1 state static ipaddr 122.3.10.1 mask 255.255.0.0
to
se net po 1 st static ip 122.3.10.1 ma 255.255.0.0
```
- ◆ Use the Tab key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** either to complete the name if only one is possible, or to display the possible names if more than one is possible. Following a space after the preceding name, Tab displays all possible names.
- ◆ Should you make a mistake while typing, backspace by pressing the Backspace key and/or the Delete key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the left  and right  arrow keys to move within a command.
- ◆ Use the up  and down  arrows to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.
- ◆ To clear an IP address, type 0.0.0.0, or to clear a non-IP address value, type CLEAR.

- ◆ When the number of lines displayed by a command exceeds the size of the window (the default is 25), the command output is halted until the user is ready to continue. To display the next line, press **Enter**, and to display the page, press the space bar. You can override the number of lines (or disable the feature altogether) with the `set cli` command.
- ◆ Keyboard Shortcuts:
 - Control-a**: move to the start of the line
 - Control-e**: move to the end of the line
 - Control-b**: move back to the start of the current word
 - Control-f**: move forward to the end of the next word
 - Control-u**: erase from cursor to the beginning of the line
 - Control-k**: erase from cursor to end of the line

Administrative Commands

admin banner login

Syntax

```
admin banner login <Banner Text>
```

Description

Configures the banner displayed after the user logs in.

Note: To go to the next line, type `\n` and press **Enter**.

admin banner logout

Syntax

```
admin banner logout <Banner Text>
```

Description

Configures the banner displayed after the user logs out.

Note: To go to the next line, type `\n` and press **Enter**.

admin banner show

Syntax

```
admin banner show
```

Description

Displays the welcome, SSH, login, and logout banners.

admin banner ssh**Syntax**

```
admin banner ssh <Banner Text>
```

Description

Configures the banner that displays prior to SSH authorization.

admin banner welcome**Syntax**

```
admin banner welcome <Banner Text>
```

Description

Configures the banner displayed before the user logs in.

Note: To go to the next line, type **\n** and press **Enter**.

admin config checksum**Syntax**

```
admin config checksum
```

Description

Displays a checksum for the current configuration. Can be used to determine if the configuration has changed.

admin config copy**Syntax**

```
admin config copy <current|Config Name>
    [location <local|nfs|cifs|usb|sdcard>
     [nfsdir <NFS Mounted Directory>] [usbport <U1>] ]
```

Description

Copies the current configuration (or optionally, a configuration from another location) to the other bank (for dual-boot EMGs).

admin config rename|delete**Syntax**

```
admin config delete <Config Name> location <local|nfs|cifs|usb|sdcard>
    [usbport <U1>] [nfsdir <NFS Mounted Directory>]
```

```
admin config rename <Config Name> location <local|nfs|cifs|usb|sdcard>
[usbport <U1>] [nfsdir <NFS Mounted Directory>]
```

Description

Deletes or renames a configuration.

admin config factorydefaults

Syntax

```
admin config factorydefaults [savesshkeys <enable|disable>] [savesslcert
<enable|disable>] [preserveconfig <Config Params to Preserve>]
[savescripts <enable|disable>]
```

<Config Params to Preserve> is a comma-separated list of current configuration parameters to retain after the config restore or config factorydefaults:

nt	Networking
sv	Services
dt	Date/Time
lu	Local Users
dp	Device Ports
ra	Remote Authentication
ub	USB Port/SD Card

Description

Restores the EMG unit to factory default settings.

admin config restore

Syntax

```
admin config restore <Config Name>
location <local|ftp|sftp|nfs|cifs|usb|sdcard|intsd>
[nfsdir <NFS Mounted Directory>] [usbport <U1>]
[savesshkeys <enable|disable>][savesslcert <enable|disable>]
```

<Config Params to Preserve> is a comma-separated list of current configuration parameters to retain after the config restore or factorydefaults:

nt	Networking
sv	Services
dt	Date/Time
lu	Local Users
ra	Remote Authentication
dp	Device Ports
ub	USB Port/SD Card

Description

Restores a saved configuration to the EMG.

admin config save**Syntax**

```
admin config save <Config Name>
location <local|ftp|sftp|nfs|cifs|usb|sdcard|intsd>
[nfsdir <NFS Mounted Dir>] [usbport <U1>]
[savesshkeys <enable|disable>]
[savesslcert <enable|disable>]
```

Description

Saves the current EMG configuration to a selected location.

admin config show**Syntax**

```
admin config show <local|ftp|sftp|nfs|cifs|usb|sdcard> [nfsdir <NFS
Mounted Dir>] [usbport <U1>]
```

Description

Lists the configurations saved to a location.

admin firmware bootbank**Syntax**

```
admin firmware bootbank <1|2>
```

Description

Sets the boot bank to be used at the next EMG reboot.

admin firmware bootcount**Syntax**

```
admin firmware bootcount <0|1>
```

Description

Configures bootcount parameter that control how many times the EMG has failed to boot. If this value reaches Boot Limit, the EMG will switch to the alternate boot bank. The EMG will switch to the alternate boot bank only once. For example, if it fails to boot Boot Limit times on bank 1, it will automatically switch to bank 2; if it fails to boot Boot Limit times on bank 2, it will enter advanced recovery mode. If Boot Count has reached Boot Limit, setting this value to 0 will enable the EMG to boot again. Default is 0, range is 0 - 1.

admin firmware bootlimit**Syntax**

```
admin firmware bootlimit <3-20>
```

Description

Configures bootlimit parameters that control how many times the EMG will fail to boot before switching to the alternate boot bank. After the EMG fails to boot 2 times Boot limit (so it has attempted to boot Boot Limit times on each bank), the EMG will go into advanced recovery mode, which may require support from Technical Support to resolve so that the EMG can be booted again. Default is 3 boots, range is 3 - 20.

admin firmware bootdelay**Syntax**

```
admin firmware bootdelay <3-1800>
```

Description

Configures bootcount parameters that control how seconds the bootloader pauses before booting the EMG. The default is 3 seconds and the range is between 3 and 1800 seconds.

admin firmware highrestimers**Syntax**

```
admin firmware highrestimers <enable|disable>
```

Description

Enables high resolution timers required for Performance Monitoring or disables high resolution timers (the default). Changing this setting requires a reboot in order for the change to take effect.

admin firmware watchdog**Syntax**

```
admin firmware watchdog <disable|180-1800 seconds>
```

Description

Configures how long the EMG waits for boot completion before forcing a reboot.

admin firmware show**Syntax**

```
admin firmware show [viewlog <enable|disable>]
```

Description

Lists the current firmware revision, the boot bank status, and optionally displays the log containing details about firmware updates.

admin firmware update**Syntax**

```
admin firmware update <ftp|tftp|sftp|nfs|usb|sdcard> file <Firmware File> key <Checksum Key> [nfsdir <NFS Mounted Dir>] [usbport <U1>]
```

Description

Updates EMG firmware to a new revision.

You should be able to access the firmware file using the settings `admin ftp show` displays if FTP, TFTP or SFTP are used to load the firmware file. The EMG automatically reboots after successful update.

admin firmware clearlog**Syntax**

```
admin firmware clearlog
```

Description

Clears the firmware update log.

admin ftp password**Syntax**

```
admin ftp password
```

Description

Sets the FTP server password and prevent it from being echoed.

admin ftp server**Syntax**

```
admin ftp server <IP Address or Hostname> [login <User Login>] [path <Directory>]
```

Description

Sets the FTP/TFTP/SFTP server used for firmware updates and configuration save/restore.

admin ftp show**Syntax**

```
admin ftp show
```

Description

Displays FTP settings.

admin memory show**Syntax**

```
admin memory show
```

Description

Displays information about EMG memory usage.

admin memory swap add**Syntax**

```
admin memory swap add <Size of Swap in MB> usbport <U1>
```

Description

Creates a swap space from an external storage device.

admin memory swap delete**Syntax**

```
admin memory swap delete
```

Description

Deletes the swap space from an external storage device.

admin quicksetup**Syntax**

```
admin quicksetup
```

Description

Runs the quick setup script.

admin reboot**Syntax**

```
admin reboot
```

Description

Immediately terminates all connections and reboots the EMG.

admin shutdown**Syntax**

```
admin shutdown
```

Description

Prepares the EMG to be powered off.

admin site**Syntax**

```
admin site row <Data Center Rack Row Number>
admin site cluster <Data Center Rack Group Number>
admin site rack <Data Center Rack Number>
admin site tag <Site Description>
admin site show
```

Description

Configures information about the site where the EMG is located.

admin version**Syntax**

```
admin version
```

Description

Displays current hardware and firmware information.

admin web certificate import**Syntax**

```
admin web certificate import via <sftp|scp> [rootfile
    <Cert Authority File>]
    certfile <Certificate File> privfile <Private Key File>
    host <IP Address or Name> login <User Login> [path <Path to Files>]
```

Description

Imports an SSL certificate.

admin web certificate reset

Syntax

```
admin web certificate reset
```

Description

Resets the web server to the default SSL certificate.

admin web certificate custom

Syntax

```
admin web certificate custom
```

Description

Generates a custom self-signed SSL certificate. The SHA256 hashing algorithm will be used to generate the certificate.

admin web certificate show

Syntax

```
admin web certificate show
```

Description

Displays the web server SSL certificate.

admin web group

Syntax

```
admin web group <Local or Remote Group Name>
```

Description

Configures the group that can access the web.

admin web server

Syntax

```
admin web server <enable|disable>
```

Description

Enables or disables running the web server (TCP ports 80 and 443).

admin web sha2***Syntax***

```
admin web sha2 <enable|disable>
```

Description

Enables using only SHA2 and higher ciphers.

admin web timeout***Syntax***

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

Description

Configures the timeout for web sessions.

admin web terminate***Syntax***

```
admin web terminate <Session ID>
```

Description

Terminates a web session.

admin web show***Syntax***

```
admin web show [viewcipherlist <enable|disable>]
```

Description

Displays the current sessions, with optional extra sessions or current ciphers.

admin web banner***Syntax***

```
admin web banner
```

Description

Configures the banner displayed on the web home page.

admin web iface**Syntax**

```
admin web iface <none,eth1,eth2,ppp>
```

Description

Defines a list of network interfaces the web is available on.

admin web cipher**Syntax**

```
admin web cipher <high|himed|fips>
```

Description

Note: FIPS functionality is not available in the current release.

Configures the strength of the cipher used by the web server (high is 256, 168 and some 128 bit, medium is 128 bit).

admin web sha2**Syntax**

```
admin web sha2 <enable|disable>
```

Description

Enable using only SHA2 and higher ciphers.

admin web tlsv10**Syntax**

```
admin web tlsv10 <enable|disable>
```

Description

Enables or disables TLS v1.0.

admin web tlsv11**Syntax**

```
admin web tlsv11 <enable|disable>
```

Description

Enables or disables TLS v1.1.

admin web restart**Syntax**

```
admin web restart
```

Description

Restarts the web server.

Warning: *The following admin chip commands should only be used under the direction of Lantronix Technical Support.*

admin chip resetmodem**Description**

Resets the internal modem chip in key system chips.

Syntax

```
admin chip resetmodem
admin chip reseti2cmux
```

Description

Resets the I2C Mux chip in key system chips.

Syntax

```
admin chip reseti2cmux
admin chip resetsfp ethport <1|2>
```

Description

Resets the SFP chip in key system chips.

Syntax

```
admin chip resetsfp ethport <1|2>
```

Audit Log Commands

show auditlog**Syntax**

```
show auditlog [command|user|clear]
```

Description

Displays audit log. By default, shows the audit log sorted by date/time. You can sort it by user or command, or clear the audit log.

Authentication Commands

set auth**Syntax**

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

Parameters

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

Description

Sets ordering of authentication methods.

Local Users authentication is always the first method used. Any methods omitted from the command are disabled.

show auth**Syntax**

```
show auth
```

Description

Displays authentication methods and their order of precedence.

show user**Syntax**

```
show user
```

Description

Displays attributes of the currently logged in user.

Kerberos Commands

set kerberos

Syntax

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

Parameters

```
allowdialback <enable|disable>
clearports <Port List>
custommenu <Menu Name>
dataports <Port List>
dialbacknumber <Phone Number>
breakseq <1-10 Chars>
escapeseq <1-10 Chars>
group <default|power|admin>
ipaddr <Key Distribution Center IP Address>
kdc <Key Distribution Center>
listenports <Port List>
permissions <Permission List>
```

Note: See [User Permissions Commands \(on page 338\)](#) for information on groups and user rights.

```
port <Key Distribution Center TCP Port>
realm <Kerberos Realm>
state <enable|disable>
useldapforlookup <enable|disable>
```

Description

Configures the EMG to use Kerberos to authenticate users who log in via the Web, SSH, Telnet, or the console port.

show kerberos

Syntax

```
show kerberos
```

Description

Displays Kerberos settings.

LDAP Commands

set ldap

Syntax

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

Parameters

```
state <enable|disable>
server1 <IP Address or Name>
server2 <IP Address or Name>
port <TCP Port>
base <LDAP Base>
bindname <Bind Name>
bindwithlogin <enable|disable>
useldapschema <enable|disable>
adsupport <enable|disable>
filteruser <User Login Attribute>
filtergroup <Group Objectclass>
grmemberattr <Group Membership Attribute>
grmembervalue <dn|name>
encrypt <starttls|ssl|disable>
dataports <Port List>
listenports <Port List>
clearports <Port List>
escapeseq <1-10 Chars>
breakseq <1-10 Chars>
custommenu <Menu Name>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
group <default|power|admin>
permissions <Permission List>
```

Note: See [User Permissions Commands \(on page 338\)](#) for information on groups and user rights.

Description

Configures the EMG to use LDAP to authenticate users who log in via the Web, SSH, Telnet, or the console port.

set ldap bindpassword

Description

Set the LDAP bind password.

Syntax

```
set ldap bindpassword
```

set ldap certificate import**Description**

To upload X.509/PEM certificate for Start TLS encrypted connections:

Syntax

```
set ldap certificate import via <sftp|scp> rootfile <Cert Auth File>
    certfile <Certificate File> keyfile <Key File>
    host <IP Address or Name> login <User Login> [path <Path to Files>]
```

set ldap certificate delete**Description**

To delete an LDAP certificate.

Syntax

```
set ldap certificate delete
```

show ldap**Syntax**

```
show ldap
```

Description

Displays LDAP settings.

Local Users Commands

set localusers add|edit**Syntax**

```
set localusers add|edit <User Login> <one or more parameters>
```

Parameters

```
allowdialback <enable|disable>
breakseq <1-10 Chars>
changenextlogin <enable|disable>
changepassword <enable|disable>
clearports <Port List>
dataports <Port List>
dialbacknumber <Phone Number>
displaymenu <enable|disable>
escapeseq <1-10 Chars>
```

```
listenports <Port List>
custommenu <Menu Name>
uid <User Identifier>
group <default|power|admin|Custom Group Name>
passwordexpires <enable|disable>
permissions <Permission List>
```

Note: See [User Permissions Commands \(on page 338\)](#) for information on groups and user rights. Remove Escape & Break Sequences for users making raw binary connections to Device Ports.

Description

Configures local accounts (including sysadmin) who log in to the EMG by means of the Web, SSH, Telnet, or the console port.

set localusers allowreuse

Syntax

```
set localusers allowreuse <enable|disable>
```

Description

Sets whether a login password can be reused.

set local users complexpasswords

Syntax

```
set localusers complexpasswords <enable|disable>
```

Description

Sets whether a complex login password is required. Complex passwords require at least one uppercase character, one lowercase character, one digit, and one non-alphanumeric character.

set localusers state

Syntax

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

Description

Enables or disables authentication of local users.

set localusers delete

Syntax

```
set localusers delete <User Login>
```

Description

Deletes a local user.

set localusers lifetime**Syntax**

```
set localusers lifetime <Number of Days>
```

Description

Sets the number of days the login password may be used. The default is 90 days.

set localusers maxloginattempts**Syntax**

```
set localusers maxloginattempts <Number of Logins>
```

Description

Sets the maximum number of login attempts before the account is locked. Disabled by default.

set localusers password**Syntax**

```
set localusers password <User Login>
```

Description

Sets a login password for the local user.

set localusers periodlockout**Syntax**

```
set localusers periodlockout <Number of Minutes>
```

Description

Sets the number of minutes after a lockout before the user can try to log in again. Disabled by default.

set localusers periodwarning**Syntax**

```
set localusers periodwarning <Number of Days>
```

Description

Sets the number of days the system warns the user that the password will be expiring. The default is 7 days.

set localusers reusehistory**Syntax**

```
set localusers reusehistory <Number of Passwords>
```

Description

Sets the number of passwords the user must use before reusing an old password. The default is 4.

set localusers multipleadminlogins**Syntax**

```
set localusers multipleadminlogins <enable|disable>
```

Description

Allows multiple admin logins among local users to the web server.

set localusers consoleonlyadmin**Syntax**

```
set localusers consoleonlyadmin <enable|disable>
```

Description

Sets local users. to console only admin setting. If enabled, the admin user can only log into the EMG via the console, and will be prevented from logging in via the web, SSH or Telnet.

show localusers**Syntax**

```
show localusers [display <brief|extended>] [user <User Login>]
```

Description

Displays local users.

set localusers lock**Syntax**

```
set localusers lock <User Login>
```

Description

Blocks (locks) a user's ability to login.

set localusers unlock**Syntax**

```
set localusers unlock <User Login>
```

Description

Allows (unlocks) a user's ability to login.

set localusers permissions**Syntax**

```
set localusers add|edit <user> permissions <Permission List>
```

where

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

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

Description

Sets a local user's permissions (not defined by the user group).

NIS Commands

set nis**Syntax**

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

Parameters

```
allowdialback <enable|disable>
broadcast <enable|disable>
clearports <Port List>
custommenu <Menu Name>
dialbacknumber <Phone Number>
dataports <Port List>
domain <NIS Domain Name>
breakseq <1-10 Chars>
escapeseq <1-10 Chars>
group <default|power|admin>
listenports <Port List>
```

```
master <IP Address or Hostname>
permissions <Permission List>
```

Note: See *User Permissions Commands* on page 338 for information on groups and user rights.

```
slave1 <IP Address or Hostname>
slave2 <IP Address or Hostname>
slave3 <IP Address or Hostname>
slave4 <IP Address or Hostname>
slave5 <IP Address or Hostname>
state <enable|disable>
```

Description

Configures the EMG to use NIS to authenticate users who log in via the Web, SSH, Telnet, or the console port.

show nis

Syntax

```
show nis
```

Description

Displays NIS settings.

RADIUS Commands

set radius

Syntax

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

Parameters

```
state <enable|disable>
allowdialback <enable|disable>
clearports <Port List>
custommenu <Menu Name>
dataports <Port List>
dialbacknumber <Phone Number>
breakseq <1-10 Chars>
escapeseq <1-10 Chars>
group <default|power|admin>
listenports <Port List>
permissions <Permission List>
```

Note: See *User Permissions Commands* on page 338 for information on groups and user rights.

```
timeout <enable|1-30>
```

Note: Sets the number of seconds after which the connection attempt times out. It may be 1-30 seconds.

Description

Configures the EMG to use RADIUS to authenticate users who log in via the Web, SSH, Telnet, or the console port.

```
set radius server
```

Syntax

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

Description

Identifies the RADIUS server(s), the text secret, and the number of the TCP port on the RADIUS server.

Note: The default port is 1812.

```
show radius
```

Syntax

```
show radius
```

Description

Displays RADIUS settings.

TACACS+ Commands

```
set tacacs+
```

Syntax

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

Parameters

```
state <enable|disable>
server1 <IP Address or Name>
server2 <IP Address or Name>
server3 <IP Address or Name>
```

```
encrypt <enable|disable>
authservice <login|pap|chap>
service <Service to Authorize>
protocol <Protocol for Service>
timeout <1-10 seconds>
dataports <Port List>
listenports <Port List>
clearports <Port List>
escapeseq <1-10 Chars>
breakseq <1-10 Chars>
custommenu <Menu Name>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
group <default|power|admin>
permissions <Permission List>
```

Note: See [User Permissions Commands \(on page 338\)](#) for information on groups and user rights.

Set the TACACS+ secret (any extra parameters will be ignored):

```
set tacacs+ secret
```

Description

Configures the EMG to use TACACS+ to authenticate users who log in via the Web, SSH, Telnet, or the console port.

```
show tacacs+
```

Syntax

```
show tacacs+
```

Description

Displays TACACS+ settings.

User Permissions Commands

```
set localusers group
```

Syntax

```
set localusers add|edit <user> group <default|power|admin|custom group name>
```

Description

Adds a local user to a user group or changes the group the user belongs to.

set localusers lock**Syntax**

```
set localusers lock <User Login>
```

Description

Blocks (locks) a user's ability to login.

set localusers unlock**Syntax**

```
set local users unlock <User Login>
```

Description

Allows (unlocks) a user's ability to login.

set localusers permissions**Syntax**

```
set localusers add|edit <user> permissions <Permission List>
```

where

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

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

Description

Sets a local user's permissions (not defined by the user group).

set <nis|ldap|radius|kerberos|tacacs+> permissions**Syntax**

```
set <nis|ldap|radius|kerberos|tacacs> permissions <Permission List>
```

where

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

Description

Sets permissions not already defined by the assigned permissions group.

show user**Syntax**

```
show user
```

Description

Displays the rights of the currently logged-in user.

Remote User Commands

set remoteusers add|edit**Syntax**

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

Parameters

```
dataports <Port List>
breakseq <1-10 Chars>
escapeseq <1-10 Chars>
listenports <Port List>
clearports <Port List>
custommenu <Menu Name>
displaymenu <enable|disable>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
group <default|power|admin|Custom Group Name>
permissions <Permissions List>
```

where

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

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

Note: See 'help user permissions' for information on groups and user rights.

Description

Sets attributes for users who log in by a remote authentication method. Access to authenticated remote users whose LDAP group or TACACS+ priv_lvl map to a EMG custom group.

set remoteusers listonlyauth**Syntax**

```
set remoteusers listonlyauth <enable|disable>
```

Description

Configure whether remote users who are not part of the remote user list will be authenticated.

set remoteusers denyaccessnocustomgroup

Syntax

```
set remoteusers denyaccessnocustomgroup <enable|disable>
```

Description

Access to authenticated remote users whose LDAP group or TACACS+ priv_lvl map to a EMG custom group:.

set remoteusers lock|unlock

Syntax

```
set remoteusers lock|unlock <User Login>
```

Description

Allow (unlock) or block (lock) a user's ability to login.

set remoteusers delete

Syntax

```
set remoteusers delete <User Login>
```

Description

Removes a remote user.

show remoteusers

Syntax

```
show remoteusers [display <brief|extended>] [user <User Login>]
```

Description

Displays settings for all remote users.

set <nis|ldap|radius|kerberos|tacacs+> group

Syntax

```
set <nis|ldap|radius|kerberos|tacacs> group <default|power|admin>
```

Description

Sets a permission group for remotely authorized users.

Cellular Modem Commands

set cellular**Syntax**

```
set cellular <parameters>
```

Parameters

```
state <dhcp|disable>
apn <APN of Mobile Carrier>
roam <enable|disable>
cellauth <none|pap|chap>
celluser <username>
simlock <enable|disable>
```

Transfer files to initiate a firmware update on the cellular modem:

```
set cellular update <ftp|sftp|scp|usb|sdcard>
    fwfile <Firmware File> prifile <carrier PRI File>
    [host <IP Address or Name>] [login <User Login>] [path <File Path>]
```

```
set cellular simpin
set cellular reboot
set cellular cellpass
show cellular [config|status]
```

Description

Configure cellular modem settings.

ConsoleFlow Commands

set cflow client**Syntax**

```
set cflow client <enable|disable>
```

Description

Configure interaction with ConsoleFlow management server. The communication with the server is enabled by default, and can be disabled.

set cflow statusinterval**Syntax**

```
set cflow statusinterval <1-60 minutes> fwconfiginterval <1-72 hours>
```

Description

Set interval between status updates, and firmware and configuration checks.

set cflow fwupdate**Syntax**

```
set cflow fwupdate <enable|disable> configupdate <enable|disable>
```

Description

Enable or disable firmware and configuration updates via ConsoleFlow.

set cflow rebootafterupdate**Syntax**

```
set cflow rebootafterupdate <enable|disable>
```

Description

Enable or disable reboots after firmware or configuration updates.

set cflow connection**Syntax**

```
set cflow connection <cloud|onpremise> <one or more parameters>
```

Parameters

```
host <IP Address or Name>
port <TCP Port>
secureport <enable|disable>
validatecerts <enable|disable>
mqttstate <enable|disable>
mqtthost <IP Address or Name>
mqttport <TCP Port>
mqttsecurity <enable|disable>
projecttag <Project Tag>
```

Description

Configure ConsoleFlow Cloud or On-Premise settings.

set cflow devicename**Syntax**

```
set cflow devicename <Device Name> description <Device Description>
```

Description

Configure the device name and description used for registration.

set cflow timeoutcli**Syntax**

```
set cflow timeoutcli <1-1800 seconds>
set cflow timeoutdp <1-1800 seconds>
```

Description

Configure the timeout for the ConsoleFlow Web Terminal sessions.

set cflow digitalprobe**Syntax**

```
set cflow digitalprobe <Device Port # or List or Name>
    frequency <disable|15-3600 seconds>
```

Description

Configures the device port digital probe for determining managed device connection status.

set cflow id**Syntax**

```
set cflow id
```

Description

Set the device ID.

set cflow key**Syntax**

```
set cflow key
```

Description

Set the ConsoleFlow key

show cflow**Syntax**

```
show cflow
show cflow status
show cflow perfmon
show cflow scripts
show cflow probes
```

Description

Show ConsoleFlow settings

CLI Commands

set cli**Syntax**

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

Parameters

```
set cli scscommands <enable|disable>
set cli terminallines <disable|Number of Lines>
set cli menu <start|Menu Name>
show cli
```

Description

Allows you to use SCS-compatible commands as shortcuts for executing commands. It is disabled by default.

Note: *Settings are retained between CLI sessions for local users and users listed in the remote users list.*

set cli menu**Description**

If a menu is associated with the current user and the menu was not displayed at login, 'start' will run the menu. Users with full administrative or menu user rights can also specify the name of any menu to run.

Syntax

```
set cli menu <start|Menu Name>
set cli terminallines
set cli terminallines <disable|Number of lines>
```

Description

Sets the number of lines in the terminal emulation (screen) for paging through text one screenful at a time, if the EMG cannot detect the size of the terminal automatically.

Note: *Settings are retained between CLI sessions for local users and users listed in the remote users list.*

show cli**Syntax**

```
show cli
```

Description

Displays current CLI settings.

show user**Syntax**

```
show user
```

Description

Displays attributes of the currently logged in user.

set history**Syntax**

```
set history clear
```

Description

Clears the commands that have been entered during the command line interface session.

show history**Syntax**

```
show history
```

Description

Displays the last 100 commands entered during the session.

Connection Commands

connect bidirection

Syntax

```
connect bidirection <Port # or Name> <endpoint> <one or more Parameters>
```

Parameters

Endpoint is one of:

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

where <SSH flags> is one or more of:

```
user <Login Name>
version <1|2>
command <Command to Execute>
```

```
tcp <IP Address> [port <TCP Port>]
telnet <IP Address or Name> [port <TCP Port>]
trigger <now|datetime|chars>
```

If the trigger is **datetime** (establish connection at a specified date/time), enter the **date** parameter. If the trigger is **chars** (establish connection on receipt of a specified number or characters or a character sequence), enter the **charxfer** parameter and either the **charcount** or the **charseq** parameter.

```
udp <IP Address> [port <UDP Port>]
```

Description

Connects a device port to another device port or an outbound network connection (data flows in both directions).

connect direct

Syntax

```
connect direct <endpoint>
```

Parameters

Endpoint is one of:

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

where <SSH flags> is one or more of:

```
user <Login Name>
version <1|2>
command <Command to Execute>
```

```
tcp <IP Address> [port <TCP Port>]
telnet <IP Address or Name> [port <TCP Port>]
udp <IP Address> [port <UDP Port>]
hostlist <Host List>
```

Description

Connects to a device port to monitor and/or interact with it, or establishes an outbound network connection.

connect global outgoingtimeout

Syntax

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

Description

Sets the amount of time the EMG will wait for a response (sign of life) from an SSH/Telnet server that it is trying to connect to.

Note: *This is not a TCP timeout.*

connect listen deviceport

Syntax

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

Description

Monitors a device port.

connect terminate

Syntax

```
connect terminate <Connection ID>
```

Description

Terminates a connection.

connect unidirection

Syntax

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

Parameters

Endpoint is one of:

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

  where <SSH flags> is one or more of:
    user <Login Name>
    version <1|2>
    command <Command to Execute>

tcp <IP Address> [port <TCP Port>]
telnet <IP Address or Name> [port <TCP Port>]
trigger <now|datetime|chars>

If the trigger is datetime (establish connection at a specified date/time), enter the date
parameter. If the trigger is chars (establish connection on receipt of a specified number or
characters or a character sequence), enter either the charcount or the charseq parameter.

udp <IP Address> [port <UDP Port>]
```

Description

Connects a device port to another device port or an outbound network connection (data flows in one direction).

show connections

Syntax

```
show connections [email <Email Address>]
```

Description

Displays connections and their IDs. You can optionally email the displayed information.

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

show connections connid

Syntax

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

Description

Displays details for a single connection. You can optionally email the displayed information.

Console Port Commands

set consoleport

Syntax

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

Parameters

```
baud <300-921600>
databits <7|8>
flowcontrol <none|xon/xoff|rts/cts>
group <Local or Remote Group Name>
parity <none|odd|even>
showlines <disable|1-50 lines>
stopbits <1|2>
timeout <disable|1-30>
```

Description

Configures console port settings.

show consoleport

Syntax

```
show consoleport
```

Description

Displays console port settings.

Custom User Menu Commands

When creating a custom user menu, note the following limitations:

- ◆ Maximum of 20 custom user menus.
- ◆ Maximum of 50 commands per custom user menu (`logout` is always the last command).
- ◆ Maximum of 15 characters for menu names.
- ◆ Maximum of five nested menus can be called.
- ◆ No syntax checking. (Enter each command correctly.)

set localusers

Syntax

```
set localusers add|edit <User Login> custom menu <Menu Name>
```

Description

Assigns a custom user menu to a local user.

set menu add**Syntax**

```
set menu add <Menu Name> [command <Command Number>]
```

Description

Creates a new custom user menu or adds a command to an existing custom user menu.

```
set menu edit
```

Syntax

```
set menu edit <Menu Name> <parameter>
```

Parameters

```
command <Command Number>
nickname <Command Number>
redisplaymenu <enable|disable>
shownicknames <enable|disable>
title <Menu Title>
```

Description

Changes a command within an existing custom user menu. Changes a nickname within an existing custom user menu. Enables or disables the redisplay of the menu before each prompt. Enables or disables the display of command nicknames instead of commands. Sets the optional title for a menu.

set menu delete**Syntax**

```
set menu delete <Menu Name> [command <Command Number>]
```

Description

Deletes a custom user menu or one command within a custom user menu.

set <nis|ldap|radius|kerberos|tacacs+> custommenu**Syntax**

```
set <nis|ldap|radius|kerberos|tacacs> custommenu <Menu Name>
```

Description

Assigns a custom menu to users who authenticate via NIS, LDAP, Radius, Kerberos, or TACACS+.

set remoteusers add|edit

Syntax

```
set remoteusers add|edit <User Login> custommenu <Menu Name>
```

Description

Sets a default custom menu for remotely authorized users.

show menu

Syntax

```
show menu <all|Menu Name>
```

Description

Displays a list of all menu names or all commands for a specific menu.

Date and Time Commands

set datetime

Syntax

```
set datetime <one parameter>
```

Parameters

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

Note: If you do not know a valid <Time Zone>, enter 'timezone <invalid time zone>' and you will be guided through selecting one from the available time zones.

Description

Sets the local date, time, and local time zone (one parameter at a time).

show datetime

Syntax

```
show datetime
```

Description

Displays the local date, time, and time zone.

set ntp**Syntax**

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

Parameters

```
localserver1 <IP Address or Hostname>
localserver2 <IP Address or Hostname>
localserver3 <IP Address or Hostname>
poll <local|public>
publicserver <IP Address or Hostname>
state <enable|disable>
sync <broadcast|poll>
```

Description

Synchronizes the EMG with a remote time server using NTP.

show ntp**Syntax**

```
show ntp
```

Description

Displays NTP settings.

Device Commands

set command**Syntax**

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

Parameters

```
sensorsoft lowtemp <Low Temperature>
```

Sets the lowest temperature permitted for the port.

```
sensorsoft hightemp <High Temperature>
```

Sets the highest temperature permitted for the port.

```
sensorsoft lowhumidity <Low Humidity %>
```

Sets the lowest humidity permitted for the port.

```
sensorsoft highhumidity <High Humidity %>
```

Sets the lowest humidity permitted for the port.

```
sensorsoft degrees <celsius|fahrenheit>
```

Enables or disables temperature settings as celcius or fahrenheit.

```
sensorsoft traps <enable|disable>
```

Enables or disables traps when specified conditions are met.

```
sensorsoft status
```

Displays the status of the port.

```
sensorsoft showall
```

Displays the status for all connected Sensorsoft devices and ignores the device port\list.

Note: The Sensorsoft lowtemp and hightemp settings are given in the scale specified by the degrees setting.

Description

Sends commands to (or control) a device connected to an EMG device port over the serial port.

Note: Currently the only devices supported for this type of interaction are Sensorsoft devices.

Device Port Commands

set deviceport port

Description

Sets the dialout password.

Syntax

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

Example: set deviceport port 2-5,6,12,15-16 baud 2400

Parameters

```
actiondelay <Action Delay>  
actionrestart <Restart Delay>  
assertdtr <enable|disable>  
auth <pap|chap>  
banner <Banner Text>  
baud <300-921600>  
breakseq <1-10 Chars>  
bytethreshold <# of Characters>
```

```

calleridcmd <Modem Command String>
calleridlogging <enable| disable>
cbcptype <admin|user>
cbcpnocallback <enable|disable>
chapauth <chaphost|localusers>
chaphost <CHAP Host or User Name>
checkdsr <enable|disable>
closedsr <enable|disable>
connectedmsg <enable|disable>
databits <7|8>
device <none|sensorsoft|rpm>
detectname <enable|disable>
detecttokens <Name Detection Tokens>
dialbackdelay <PPP Dial-back Delay>
dialbacknumber <usernumber|Phone Number>
dialbackretries <1-10>
dialinlist <Host List for Dial-in>
dialoutlogin <Remote User Login>
dialoutnumber <Phone Number>
dodauth <pap|chap>
dodchaphost <CHAP Host or User Name>
dtrcontrol <none|toggledtr|autodtr>
emailsubj <Email Subject>
mailto <Email Address>
flowcontrol <none|xon/xoff|rts/cts>
group <Local or Remote Group Name>
idletimeoutmsg <enable|disable>
initscript <Modem Initialization Script>
ipaddr <IP Address[/Mask Bits]>
locallogging <enable|disable>
maxdirect <1-15>

```

Note: We recommend preceding the *initscript* with **AT** and include **E1 V1 x4 Q0** so that the EMG may properly control the modem.

```

localipaddr <negotiate|IP Address>
logins <enable|disable>
minimizelatency <enable|disable>
modemmode <text|ppp>
modemstate <disable|dialin|dialout|dialback|dialinhostlist|dialondemand|
            dialin+ondemand|dialback+ondemand|cbcpcclient|cbcpcserver>
modemtimeout <disable|1-9999 seconds>
name <Device Port Name>
nat <enable|disable>
newusermsg <enable|disable>
nfsdir <Logging Directory>
nfslogging <enable|disable>
nfsmaxfiles <Max # of Files>
nfsmaxsize <Size in Bytes>
numsessionsmsg <enable|disable>
parity <none|odd|even>
portlogseq <1-10 Chars>
poweraction <on|off|cycle>
powermgmtseq <1-10 Chars>

```

```
powersupply <Managed Power Supply Name>
remoteipaddr <negotiate|IP Address>
restartdelay <PPP Restart Delay>
reversepinout<enable|disable>
sendstring <String to Send|QUOTEDSTRING>
sendtermstr <enable|disable>
showlines <disable|1-50 lines>
slmlogging <enable|disable>
slmnms <NMS IP Address>
slmthreshold <Threshold>
slmtime <Time Frame>
sshauth <enable|disable>
sshdatadir <netin|netout|both>
sshin <enable|disable>
sshport <TCP Port>
sshtimeout <disable|1-3600 seconds>
stopbits <1|2>
sysloglogging <enable|disable>
tcpauth <enable|disable>
tcpdatadir <netin|netout|both>
tcpin <enable|disable>
tcpport <TCP Port>
tcptimeout <disable|1-3600 seconds>
telnetauth <enable|disable>
telnetdatadir <netin|netout|both>
telnetin <enable|disable>
telnetport <TCP Port>
telnetsoftiac <enable|disable>
telnettimeout <disable|1-3600 sec>
termstr <Termination String>
timeoutlogins <disable or 1-30 minutes>
tokenaction <List of none,log,trap,email,string,power>
tokendatadetect <enable|disable>
tokenstring <Regex String>
tokentrigger <bytecnt|charstr>
usbchannel <1-2>
usblogging <enable|disable>
usbmaxfiles <Max # of Files>
usbmaxsize <Size in Bytes>
usbport <U1|SD|INTSD>
usbvbus <enable|disable>
usesites <enable|disable>
viewportlog <enable|disable>
```

Description

Configures a single port or a group of ports.

Set the modem password and CHAP secrets (any extra parameters will be ignored):

```
set deviceport port <Device Port # or List or Name> dialoutpassword
set deviceport port <Device Port # or List or Name> chapsecret
set deviceport port <Device Port # or List or Name> dodchapsecret
```

Reset a device port, terminating and restarting all relevant connections:

```
set deviceport port <Device Port # or List or Name> reset
```

Configure up to 4 managed power supplies for device connected to a device port:

```
set deviceport port <Device Port # or Name> managepower
```

Reset a device port, terminating and restarting all relevant connections:

```
set deviceport port <Device Port # or List or Name> reset
```

Note: A group of device ports can be configured by specifying a comma-separated list of ports (i.e., '1-4,8,10-12') or 'ALL'. Remove breakseq for Device Ports connected to raw binary connections. The logging level for the Device Ports log must be set to 'Info' to view Syslog entries for Device Port logging. It is recommended that the 'initscript' be prepended with 'AT' and include 'E1 V1 x4 Q0' so that the EMG may properly control the modem.

set deviceport global

Syntax

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

Parameters

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

Description

Configures settings for all or a group of device ports.

show deviceport global

Syntax

```
show deviceport global
```

Description

Displays global settings for device ports.

show deviceport names

Syntax

```
show deviceport names
```

Description

Displays a list of all device port names.

show deviceport port**Syntax**

```
show deviceport port <Device Port List or Name>
    [display <ip|data|modem|logging|device>]
```

Description

Displays the settings for one or more device ports.

show deviceport types**Syntax**

```
show deviceport types
```

Description

Displays the list of port types (RJ45 or USB) for all device ports.

show portcounters**Syntax**

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

Description

Displays device port statistics and errors for one or more ports. You can optionally email the displayed information.

show portcounters zerocounters**Syntax**

```
show portcounters zerocounters <Device Port List or Name>
```

Description

Zeros the port counters for one or more device ports.

show portstatus**Syntax**

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

Description

Displays the modes and states of one or more device port(s). You can optionally email the displayed information.

DIO Commands

Digital Input/Output Port Command Synopsis

set dio port**Syntax**

```
set dio port <inf1|inf2> <parameters>
```

Parameters

```
name <DIO Port Name>
normalstate <on|off>
```

Description

Configure the DIO input ports #1 or #2 on the front of the EMG:

set dio port relayf**Syntax**

```
set dio port relayf <parameters>
```

Parameters

```
name <DIO Port Name>
wakeup <on|off>
state <on|off>
normalstate <on|off>
latch <enable|disable>
```

Description

Configure the DIO relay/output port on the front of the EMG:

```
show dio
```

Diagnostic Commands

diag arp

Syntax

```
diag arp|arp6 [email <Email Address>]
```

Description

Displays the Address Resolution Protocol table (for IPv4) or the Neighbor table (for IPv6) for mapping IP Addresses to hardware addresses.

diag internals

Syntax

```
diag internals [email <Email Address>]
```

Enable debug printing on the next EMG reboot:

```
diag internals [printapplication <enable|disable>
                printconnection <enable|disable>
                printmanagement <enable|disable>]
```

Description

Displays information on the internal memory, storage and processes of the EMG. You can optionally email the displayed information.

diag iperf

Syntax

```
diag iperf mode <server|client> [host <iPerf Server IP Address or Name>]
                                    [options <iPerf options>] [email <Email Address>]
```

Options

iPerf Options (enclose all options in quotes):

Set server port to listen on/connect to (default 5201):	-p, --port n
Format to report:	-f, --format [kmgtKMG]
Pause n seconds between reports:	-i, --interval n
Bind to a host, an interface or multicast address	-B, --bind <host>
More detailed output:	-V, --verbose
Output in JSON format:	-J, --json
Options below are supported on client only:	
Set length of buffer to n (default 8 KB):	-l, --length n[KMG]
Use UDP rather than TCP:	-u, --udp
TCP window size (socket buffer size):	-w, --window n[KMG]
Set TCP/SCTP maximum segment size (MTU):	-M, --set-mss n
Set TCP/SCTP no delay, disabling Nagle's Algorithm:	-N, --no-delay

```
Set bandwidth to n bits/sec (default 1Mbit/sec, unlimited for TCP);          -b, --bitrate n[KMG]
Number of bytes to transmit (instead of -t):                                -n, --bytes n[KMG]
Time in seconds to transmit for (default 10 secs):                           -t, --time n
Set the IPv6 flow label:                                                       -L, --flowlabel n
Use a 'zero copy' method of sending data:                                     -Z, --zerocopy
Omit the first n seconds:                                                    -O, --omit n
Prefix every output line with this string:                                    -T, --title str
# of blocks (packets) to transmit (instead of -t/-n):                      -k, --blockcount
Set the IP type of service, 0-255.                                            -S, --tos n
The usual prefixes for octal and hex can be used, i.e. 52, 064 and 0x34 all specify the same value: --dscp n
Set the IP dscp value, either 0-63 or symbolic:                                --dscp n
```

Description

Runs an iPerf server or client to measure network throughput. You can optionally email the output. The EMG uses iPerf version 3.X, which is incompatible with older versions (2.x).

diag lookup

Syntax

```
diag lookup <Name> [email <Email Address>]
```

Description

Resolves a host name into an IP address. You can optionally email the displayed information.

diag loopback

Syntax

```
diag loopback <Device Port Number or Name> [<parameters>]
```

Parameters

```
test <internal|external>
xferdatasize <Size In Kbytes to Transfer>
Defaults: test=external, xferdatasize=1K
```

Description

Tests a device port by transmitting data out the port and verifying that it is received correctly.

A special loopback cable comes with the EMG. To test a device port, plug the cable into the device port and run this command. The command sends the specified Kbytes to the device port and reports success or failure. The test is performed at 9600 baud. Only an external test requires a loopback cable. The External test is currently not supported for USB device ports.

diag netstat**Syntax**

```
diag netstat [protocol <all|tcp|udp>] [email <Email Address>]  
Defaults: protocol=all
```

Description

To display a report of network connections. You can optionally email the displayed information.

diag nettrace**Syntax**

```
diag nettrace <one or more parameters>
```

Parameters

```
ethport <1|2>  
protocol <tcp|udp|icmp|esp>  
host <IP Address or Name>  
numpackets <Number of Packets>  
verbose <low|medium|high|disable>  
pcapfile <File Name> location <usb:sdcard> [usbport <U1>]
```

Description

Displays all network traffic, applying optional filters (the output can be saved to a Wireshark pcap file on external storage). This command is available in the CLI but not the web.

diag perfstat**Description**

Display performance statistics for an Ethernet Port or Device Port, averaged over the last 5 seconds. Must specify an Ethernet Port or Device Port.

Syntax

```
diag perfstat [ethport <1|2>] [deviceport <Device Port # or Name>]
```

diag ping|ping6**Description**

Verifies if the EMG can reach a host over the network.

```
diag ping|ping6 <IP Address or Name> [<parameters>]
```

Parameters

```
count <Number Of Times To Ping>  
packetsize <Size In Bytes>
```

```
ethport <1|2>
Defaults: count=5, packetsize=64
```

diag sendpacket host

Description

Generate and send Ethernet packets.

Syntax

```
diag sendpacket host <IP Address or Name> port <TCP or UDP Port Number>
[string <Packet String>] [protocol <tcp|udp>]
[count <Number of Packets>]
```

diag top

Syntax

```
diag top [parameters]
```

Description

Displays CPU usage, memory usage and tasks.

Parameters

```
continuous <enable|disable>
count <Number of Iterations to Display>
delay <Delay in Seconds>
numlines <Number of Lines to Display>
```

Defaults:

count=1, delay = 5 seconds

diag traceroute

Syntax

```
diag traceroute <IP Address or Hostname>
```

Description

Displays the route that packets take to get to a network host.

diag usb

Syntax

```
diag usb [<parameters>]
```

Description

To display information about USB buses and the devices connected to them, including the mapping between a USB device and the EMG port. For "mapdevice enable", the port numbers will be displayed at the end of the line in square brackets.

Parameters

```
treedisplay <enable|disable>
mapdevice <enable|disable>
email <Email Address>
Defaults: treedisplay=enable
```

Events Commands

admin events add

Syntax

```
admin events add <trigger> <response>
```

<trigger> is one of:

dpdatadrop, humidlimit, pingfails, receivetrap, dioportchange,
dioportabnormal, rpmload, or templimit.

<response> is one of:

```
action syslog
action emailalert emailaddress <destination email address>
action snmptrap nms <SNMP NMS> community <SNMP Community>
action diorelayon
action <fdalltrapseth|fdseltrapseth> ethport <1|2|cell> nms <SNMP
NMS>
community <SNMP Community> [oid <SNMP OID>]
action <fdalltrapsmodem|fdseltrapmodem> deviceport <Device Port #
or Name> nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap
OID>]
action <fdalltrapsmodem|fdseltrapmodem> usbport <U1>
nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap OID>]
action <fdalltrapsmodem|fdseltrapmodem> internal modem
nms <SNMP NMS> community <SNMP Community> [oid <SNMP Trap OID>]
```

Description

Defines events.

admin events delete**Syntax**

```
admin events delete <Event ID>
```

Description

Deletes an event definition.

admin events edit**Syntax**

```
admin events edit <Event ID> <parameters>
```

Parameters

```
community <SNMP Community>
deviceport <Device Port # or Name>
ethport <1|2>
host <IP Address or Name>
internal modem
nms <SNMP NMS>
oid <SNMP Trap OID>
outlet <Outlet #>
rpm <RPM Id or Name>
threshold <Load Percentage|Current in Amps>
dioport <inf1|inf2|relayf>
usbport <U1>
```

Description

Edits event definitions.

admin events show**Syntax**

```
admin events show
```

Description

Displays event definitions.

Groups Commands

```
set groups add|edit <Group Name> [<parameters>]
```

Syntax

```
set groups add|edit <Group Name> [<parameters>]
```

Parameters

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

Note: See 'help user permissions' for information on user rights.

Rename a group:

```
set groups rename <Group Name> newname <New Group Name>
```

Delete a group:

```
set groups delete <Group Name>
```

Show one or more groups:

```
show groups [name <Group Name>] members <enable|disable>
```

Description

Configure custom group attributes.

Host List Commands

```
set hostlist add|edit <Host List Name>
```

Syntax

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

Parameters

```
name <Host List Name> (edit only)
```

```
retrycount <1-10>
```

Default: retrycount=3, auth=enable.

```
auth <enable|disable>
```

Description

Configures a prioritized list of hosts to be used for modem dial-in connections.

```
set hostlist add|edit <Host List Name> entry
```

Syntax

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

Parameters

```
host <IP Address or Name>  
protocol <ssh|telnet|tcp>  
port <TCP Port>  
escapeseq <1-10 Chars>
```

Description

Adds a new host entry to a list or edit an existing entry.

```
set hostlist edit <Host List Name> move
```

Syntax

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

Description

Moves a host entry to a new position in the host list.

```
set hostlist delete
```

Syntax

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

Description

Deletes a host list, or a single host entry from a host list.

```
show hostlist
```

Syntax

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

Description

Displays the members of a host list.

Internal Modem Commands

Configure the internal modem:

```
set intmodem <parameters>
```

Parameters

```
modemstate <disable|dialin|dialout|dialback> usesites <enable|disable>
modemmode <text|ppp> group <Local or Remote Group Name>
timeoutlogins <disable|1-30 minutes> modemtimeout <disable|1-9999 sec>
localipaddr <negotiate|IP Address> restartdelay <PPP Restart Delay>
remoteipaddr <negotiate|IP Address> calleridlogging <enable|disable>
auth <pap|chap> calleridcmd <Modem Command String>
chaphost <CHAP Host or User Name> initscript <Modem Init Script>
chapauth <chaphost|localusers> nat <enable|disable>
dialbacknumber <usernumber|Phone Number> checkdialtone <disable|5-600 min>
dialbackdelay <PPP Dialback Delay> dialoutnumber <Phone Number>
dialbackretries <1-10> dialoutlogin <Remote User Login>
```

Set the modem password and CHAP secret (any extra parameters will be ignored):

```
set intmodem dialoutpassword
set intmodem chapsecret
```

Note: It is recommended that the initscript be prepended with 'AT' and include 'E1 V1 x4 Q0' so that the EMG may properly control the modem.

Display settings for the internal modem:

```
show intmodem
```

IP Filter Commands

set ipfilter state

Syntax

```
set ipfilter state <enable|disable> [testtimer <disable|1-120 minutes>]
```

Description

Enables or disables IP filtering for incoming network traffic.

set ipfilter mapping**Syntax**

```
set ipfilter mapping <parameters>
```

Parameters

```
ethernet <1|2|bond0> state <disable>
ethernet <1|2|bond0> state <enable> ruleset <Ruleset Name>
deviceport <1..48> state <disable>
deviceport <1..48> state <enable> ruleset <Ruleset Name>
usbport <U1> state <disable>
usbport <U1> state <enable> ruleset <Ruleset Name>
internal modem state <disable>
internal modem state <enable> ruleset <Ruleset Name>
```

Description

Maps an IP filter to an interface.

set ip filter rules**Syntax**

```
set ipfilter rules <parameters>
```

Parameters

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

Edit Parameters

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

Description

Sets IP filter rules.

Logging Commands

set deviceport port**Syntax**

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

Parameters

```
actiondelay <Action Delay>
actionrestart <Restart Delay>
bytethreshold <# of Characters>
emailsubj <Email Subject>
emailto <Email Address>
locallogging <enable|disable>
nfsdir <Logging Directory>
nfslogging <enable|disable>
nfsmaxfiles <Max # of Files>
nfsmaxsize <Size in Bytes>
poweraction <on|off|cycle>
powersupply <Managed Power Supply Name>
sendstring <String to Send|QUOTEDSTRING>
tokenaction <List of none,log,trap,email,string,power>
tokendatadetect <enable|disable>
tokenstring <Regex String>
tokentrigger <bytecnt|charstr>
usblogging <enable|disable>
usbmaxfiles <Max # of Files>
usbmaxsize <Size in Bytes>
usbport <U1|SD|INTSD>
sysloglogging <enable|disable>
```

Description

Configures logging settings for one or more device ports.

Local logging must be enabled for a device port for the `locallog` commands to be executed. To use the `set locallog clear` command, the user must have permission to clear port buffers (see [Chapter 13: User Authentication](#).)

Example

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

show locallog
```

Syntax

```
show locallog <Device Port # or Name> [<parameters>]
Parameters:      [bytes <Bytes To Display>]
                  [startbyte <Byte Index>]
Defaults:      bytes=1000, startbyte=1
```

Description

Displays a specific number of bytes of data for a device port. **1K** is the default.

set locallog clear**Syntax**

```
set locallog clear <Device Port # or Name>
```

Description

Clears the local log for a device port.

The locallog commands can only be executed for a device port if local logging is enabled for the port. The set locallog clear command can only be executed if the user has permission to clear port buffers (see [Chapter 13: User Authentication](#)).

set log clear modem**Syntax**

```
set log clear modem
```

Description

Clear the modem log (the modem log is automatically pruned when it reaches 50K):

set log modem ppplog**Syntax**

```
set log modem ppplog <enable|disable>
```

Description

Enables PPP activity messages in the modem log.

set log modem ppplog <enable|disable>**Syntax**

```
set log modem pppdebug
```

Description

Enables PPP debugging messages in the modem log:

set log modem pppdebug <enable|disable>**Syntax**

```
show log modem
```

Description

View the modem activity log for external modems and USB modems:

```
show log modem [display <head|tail>] [numlines <Number of Lines>]
```

show log local

Syntax

```
show log local
```

Description

View the log for local, NFS, or USB logging (NFS and USB use the current logging settings for the Device Port). Default is to show the log tail:

```
show log local|nfs|usb|sdcard|intsd <Device Port # or Name>  
[<parameters>]
```

Parameters

```
display <head|tail>  
numlines <Number of Lines>  
bytes <Bytes to Display>  
startbyte <Byte Index>  
logfile <NFS, USB or SD card Log File>  
Defaults: bytes=1000, startbyte=1, numlines=40
```

Lists the NFS, USB, or SD card log files, either for a specific device port, or all log files in a USB, NFS, or SD card location:

```
show log files nfs|usb|sdcard|intsd [localdir <NFS Mount Local  
Directory>]  
[usbport <U1>]  
[deviceport <Device Port # or name>]
```

Network Commands

set network

Syntax

```
set network <parameters>
```

Parameters

```
startprobes <1-99999 Seconds>  
probes <Number of Probes>  
interval <1-99999 Seconds>  
ipforwarding <enable|disable>  
ip6forwarding <enable|disable>
```

Description

Sets TCP Keepalive and IP Forwarding network parameters.

set network bonding**Syntax**

```
set network bonding <disabled|active-backup|802.3ad|load-balancing>
```

Description

Configure Ethernet Bonding.

set network dns**Syntax**

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

Description

Configures up to three DNS servers.

set network dnsipv4prec**Syntax**

```
set network dnsipv4prec <enable|disable>
```

Description

Configures IPv4/IPv6 lookup precedence.

set network gateway**Syntax**

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

Parameters

```
default <IP Address>
ipv6default <IPv6 Address>
precedence <dhcp|default>
failover <IP Address>
pingip <IP Address>
ethport <1|2>
failoverport <2|cell>
pingdelay <1-250 seconds>
failedpings <1-250>
faildevice <none|hspa|sierra>
faildevapn <Fail-over Device: APN of Mobile Carrier>
faildevlockpin <enable|disable>
faildevlogin <Fail-over Device: Admin Login>
faildevcelluser <Fail-over Device: SIM Login>
faildevcellpwd <Fail-over Device: SIM Password>
```

```
faildevcelldialstr <Fail-over Device: Dialup Str>
faildevcellroam <enable|disable>
```

Transfer firmware update files to the EMG to initiate a firmware update on the fail-over device:

```
set network gateway faildevupdate <ftp|sftp|scp|usb|sdcard>
    gwfile <Firmware File> radiofile <Radio File> [usbport <U1>]
    [host <IP Address or Name>] [login <User Login>] [path <File
Path>]
```

Reboot the fail-over device, or set the fail-over device SIM Card PIN #, SIM Personal Unblocking Key or Admin Password (any extra parameters will be ignored):

```
set network gateway reboot
set network gateway faildevpin
set network gateway faildevpuk
set network gateway faildevpassword
```

Description

Set default & fail-over gateways (the fail-over gateway is used if an IP address usually accessible through the default gateway fails to return 1 or more pings), and configure settings for supported fail-over devices.

set network host

Syntax

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

Description

Sets the EMG host name and domain name.

set network fqdnlist

Syntax

```
set network fqdnlist <1-15> ipaddr <IP Address> fqdn <hostname>
```

Description

Updates the local hosts table for DNS lookup of FQDNs.

set network port

Syntax

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

Parameters

```
state <dhcp|bootp|static|disable> [ipaddr <IP Address> mask <Mask>]
ipv6addr <IPv6 Address/Prefix>
mode <auto|10mbit-half|100mbit-half|10mbit-full|100mbit-full|
      1000mbit-full>
mtu <Maximum Transmission Unit>
activeport <rj45|sfp>

set network ipv6 <enable|disable>
```

Description

Displays DNS settings.

show network dns**Syntax**

```
show network dns
```

Description

Displays DNS settings.

show network gateway**Syntax**

```
show network gateway
```

Description

Displays gateway settings.

show network host**Syntax**

```
show network host
```

Description

Displays the network host name of the EMG.

show network port**Syntax**

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

Description

Displays Ethernet port settings and counters.

show network ipv6**Syntax**

```
show network ipv6
```

Description

Displays all ipv6 settings.

```
show network sfp
```

Syntax

```
show network sfp
```

Description

Displays network port 1 and port 2 SFP diagnostics.

show network all**Syntax**

```
show network all
```

Description

Displays all network settings.

NFS and SMB/CIFS Commands

set nfs mount**Syntax**

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

Parameters

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

Enables or disables read/write access to remote directory.

Description

Mounts a remote NFS share.

The `remdir` and `loaddir` parameters are required, but if they have been specified previously, you do not need to provide them again.

set nfs unmount**Syntax**

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

Description

Unmounts a remote NFS share.

set cifs**Syntax**

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

Parameters

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

Description

Configures the SMB/CIFS share, which contains the system and device port logs.

The `admin config` command saves EMG configurations on the SMB/CIFS share.

set cifs password**Syntax**

```
set cifs password
```

Description

Changes the password for the SMB/CIFS share login (default is `cifsuser`).

show cifs**Syntax**

```
show cifs
```

Description

Displays SMB/CIFS settings.

`show nfs`***Syntax***

```
show nfs
```

Description

Displays NFS share settings.

Performance Monitoring Commands

`show perfmon`***Syntax***

```
show perfmon
```

Parameters

```
show perfmon [probe <all|Probe Id or Name>]
```

Description

Display global settings and all probes, or a selected probe.

`show perfmon status`***Syntax***

```
show perfmon status
```

Parameters

```
show perfmon status [probe <Probe Id or Name>]
```

Description

Display the running status of all probes or a selected probe.

`show perfmon operations`***Syntax***

```
show perfmon operations
```

Parameters

```
show perfmon operations <Probe Id or Name>
```

Description

Display list of completed operation sets for a probe.

set perfmon results**Syntax**

```
set perfmon results
```

Parameters

```
show perfmon results <Probe Id or Name> [set <Operation Set Number>]  
[display <head|tail>] [numlines <Number of Lines>]  
[email <Email Address>]
```

Description

Display round trip times (RTT) for last completed operation set or selected set, and optionally email the complete results.

show perfmon accumulated**Syntax**

```
show perfmon accumulated
```

Parameters

```
show perfmon accumulated <Probe Id or Name> [set <Operation Set Number>]  
[email <Email Address>]
```

Description

Display accumulated statistics for last completed operation set or selected set, and optionally email the statistics.

set perfmon repo**Syntax**

```
set perfmon repo <local|usb|sdcard> [usbport <U1>]
```

Description

Set repository where probe operations are stored.

set perfmon keep**Syntax**

```
set perfmon keep <Number of Operations to Keep>
```

Description

Set number of operations stored for each probe.

set perfmon udpjitterresp**Syntax**

```
set perfmon udpjitterresp <enable|disable>
```

Description

Enable responders for UDP jitter.

set perfmon udpechoresp**Syntax**

```
set perfmon udpechoresp <UDP Port Number|disable>
```

Description

Enable responders for UDP echo.

set perfmon tcpconnectresp**Syntax**

```
set perfmon tcpconnectresp <TCP Port Number|disable>
```

Description

Enable responders for TCP connect.

set perfmon add**Syntax**

```
set perfmon add <Probe Name>
type <dns|http|icmp|tcpconnect|udpecho|udpjitter|udpjittervoip>
```

Parameters

```
name <Probe Name>
starttime <now|HH:MM[:SS] [MMDD] | afterHH:MM:SS>
operations <Number of Operations to Perform>
frequency <Seconds between Operations>
```

```
packets <Number of Packets to Send>
interval <Milliseconds between Packets>
timeout <Milliseconds to Wait for Response>
host <Destination IP Address or Name>
port <Destination Port>
precision <milli|micro>
datasize <Payload Data Size in Bytes>
verifydata <enable|disable>
codec <g729a|g711alaw|g711mulaw>
tos <none|Type of Service>
interface <none|eth1|eth2>
nameserver <IPv4 Address>
```

Description

Add a new probe.

set perfmon edit

Syntax

```
set perfmon edit <Probe Id or Name> [<parameters>]
```

Parameters

```
name <Probe Name>
      starttime <now|HH:MM[:SS] [MMDD]|afterHH:MM:SS>
      operations <Number of Operations to Perform>
      frequency <Seconds between Operations>
      packets <Number of Packets to Send>
      interval <Milliseconds between Packets>
      timeout <Milliseconds to Wait for Response>
      host <Destination IP Address or Name>
      port <Destination Port>
      precision <milli|micro>
      datasize <Payload Data Size in Bytes>
      verifydata <enable|disable>
      codec <g729a|g711alaw|g711mulaw>
      tos <none|Type of Service>
      interface <none|eth1|eth2>
      nameserver <IPv4 Address>
```

Description

Edit an existing probe.

set perfmon delete

Syntax

```
set perfmon delete <Probe Id or Name> [data <all|# of Sets to Keep>]
```

Description

Delete a probe, or delete all operation data for a probe, or delete all but the most recent operation sets for a probe.

set perfmon state**Syntax**

```
set perfmon state <all|Probe Id or Name> action <restart>
```

Description

Set the running state of all probes or a single a probe.

Routing Commands

set routing**Syntax**

```
set routing [parameters]
```

Parameters

```
rip <enable|disable>
route <1-64> ipaddr <IP Address> mask <Netmask> gateway <IP Address>
static <enable|disable>
version <1|2|both>
```

Description

Configures static or dynamic routing.

To delete a static route, set the IP address, mask, and gateway parameters to **0.0.0.0**.

show routing**Syntax**

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

Description

Sets the routing table to display IP addresses (disable) or the corresponding host names (enable). You can optionally email the displayed information.

RPM Commands

set rpm add

Syntax

```
set rpm add <RPM Name>
```

Description

Adds an RPM to be managed (prompts will guide selection of RPM vendor and model).

set RPM command

Syntax

```
set rpm command <RPM Id or Name>
    outlet <all|Outlet # or List> state <on|off|cyclepower>
```

Description

Sends a command to control one or more outlets on an RPM.

Syntax

```
set rpm command <RPM Id or Name> device <reboot|shutdown>
```

Description

Sends a command to control an RPM device.

Syntax

```
set rpm command <RPM Id or Name> beeper <mute|enable|disable>
```

Description

Sends a command to control an RPM beeper.

set rpm delete

Syntax

```
set rpm delete <RPM Id or Name>
```

Description

Deletes an RPM.

set rpm driver**Syntax**

```
set rpm driver <RPM Id or Name> action restart
set rpm driver <RPM Id or Name> action debug [level <1|2|3>]
set rpm driver <RPM Id or Name> action show
set rpm driver <RPM Id or Name> action viewoutput [email <Email Address>]
    [display <head|tail>] [numlines <Number of Lines>]
```

Description

Control and debug the RPM driver if the driver is not properly communicating with the PDU or UPS: restart the driver; restart the driver with debug output to a file; show the running driver; view and email the driver debug output.

Note: Drivers running in debug mode will generate copious output and for disk space reasons should not be left running in debug mode for long periods of time.

set rpm edit**Syntax**

```
set rpm edit <RPM Id or Name> <one or more parameters>
```

Parameters

```
name <New RPM Name>
outlets <# of Outlets>
ipaddr <IP Address>
port <TCP or Device Port>
login <RPM Admin Login>
rocommunity <SNMP Read-Only Community>
rwcommunity <SNMP Read-Write Community>
logstatus <disable|1-60 minutes>
snmptraps <enable|disable>
emailaddress <Email Address>
upsbattery <shutdown|shutdownall|shutdownboth|allowfailure>
sdorder <disable|1-49>
powertoslc <enable|disable>
driveropts <Driver Options Override>
```

Description

Configure and control Remote Power Managers (RPMs), including PDUs and UPSes.

set rpm password**Syntax**

```
set rpm password <RPM Id or Name>
```

Description

Set RPM administrative password.

show RPM**Syntax**

```
show rpm [type <ups|pdu>]
           [config <sdorder|notify>]
           [device <RPM Name or Id> [data <raw|logs|envmon>]]
```

Note: The *show rpm envmon* command for RPM-configured ServerTech Serial/Network Mode is not supported by NUT/Powerman.

Description

Display a list of all RPMs, RPMs of a specific type, UPS shutdown and notification configuration, or details and outlets for a single RPM device.

Script Commands

set script import**Syntax**

```
set script import <interface|batch|custom> via <ftp|scp|copypaste>
           [file <Script File>] [name <Script Name>] [host <IP Address
           or Name>]
           [login <User Login>] [path <Path to Script File>]
           [filetype <expect|tcl|python>]
```

Note: Interface scripts will be given default/do user rights; Batch and Custom scripts will be given admin/ad user rights. The name of the script will be the same as the file name (if it is a valid script name), otherwise a script name must be specified for import.

Description

Import a script.

set script update**Syntax**

```
set script update <interface|batch|custom> name <Script Name>
           [group <default|power|admin>] [permissions <Permission List>]
```

Note: See 'help user permissions' for information on groups and user rights.

Description

Update a script.

set script rename**Syntax**

```
set script rename <interface|batch|custom> name <Script Name>
    newname <New Script Name>
```

Description

Rename a script.

set script delete**Syntax**

```
set script delete <interface|batch|custom> name <Script Name>
```

Description

Delete a script.

set script runcli**Syntax**

```
set script runcli <Script Name> [parameters <Command Line Parameters>]
    [debug <enable|disable>]
```

Description

Run a CLI batch or custom script one time (script output will be displayed in the current terminal; custom script output will be saved in the repository).

connect script**Syntax**

```
connect script <Script Name> deviceport <Device Port # or Name>
    [parameters <Command Line Parameters>] debug
        <enable|disable>]
```

Description

Connect an interface or custom script to a Device Port and run it one time (script output will be displayed in the current terminal; custom script output will be saved in the repository).

set script schedule**Syntax**

```
set script schedule <Script Name> [device <cli|Device Port # or Name>]
    [state <enable|disable|delete>] [parameters
        <Cmd Line Parameters>]
    [starttime <now|HH:MM[MMDD]|afterHH:MM>]
    [frequency <Hours/Days between each operation>]
    [stoptime <forever|HH:MM[MMDD]|afterHH:MM>]
```

Description

Schedule a custom script to be run at a certain time, either once or recurring; frequency is specified as hours (4H for 4 hours) or days (2D for 2 days).

show script**Syntax**

```
show script [type <interface|batch|custom> [name <Script Name>]]
```

Description

Display list of scripts, or view the details and contents of a script.

show script status**Syntax**

```
show script status [script <Script Name>]
```

Description

Display the running status of all custom scripts or a single custom script.

show script operations**Syntax**

```
show script operations <Script Name>
```

Description

Display list of completed results for a custom script.

show script results

```
show script results <Script Name> [set <all|Operation Set Number>]
    [display <head|tail>] [numlines <Number of Lines>]
    [email <Email Address>]
```

Description

Display the results for the last completed custom script operation or a selected operation, and optionally email the results.

SD Card Commands

Enables or disables access to SD Card devices:

```
set sdcard access <enable|disable>
```

Mounts a SD Card for use as a storage device. The SD Card can be used for saving configurations, firmware updates and device logging.

```
set sdcard mount
```

Unmounts a SD Card:

```
set sdcard unmount
```

Formats a SD Card:

```
set sdcard format [filesystem <ext2|fat16|fat32|ntfs>]
```

Defaults: filesystem=ext2

Runs a filesystem check on a SD Card (recommended if it does not mount):

```
set sdcard fsck
```

Displays a directory listing of an internal or external SD Card:

```
set sdcard|intsd dir [subdir <Directory Path>]
```

Renames a file on a SD Card:

```
set sdcard rename <Filename> newfile <New Filename>
```

Copies a file on a SD Card:

```
set sdcard copy <Filename> newfile <New Filename>
```

Removes a file on a SD Card:

```
set sdcard delete <Current Filename>
```

Displays information about the SD Card device:

```
show sdcard
```

Security Commands

set security

Description

Configures EMG security and FIPS settings.

Note: FIPS functionality is not available in the current release.

Parameters

```
set security <parameters>
```

fipsmode**Parameters**

```
fipsmode <enable|disable>
```

show security**Description**

Displays security settings and current status.

Parameters

```
show security
```

Services Commands

set services**Syntax**

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

Parameters

netlog <off error warning info debug>	auditlog <enable disable>
authlog <off error warning info debug>	auditsize <1-500 Kbytes>
diaglog <off error warning info debug>	clicommands <enable disable>
servlog <off error warning info debug>	includesyslog <enable disable>
devlog <off error warning info debug>	snmp <enable disable>
genlog <off error warning info debug>	v1 <enable disable>
syslogserver1 <IP Address or Name>	v2c <enable disable>
syslogserver2 <IP Address or Name>	traps <enable disable>
rpmlogsize <5-40 Kbytes>	trapversion <1 2 3>
otherlogsize <5-400 Kbytes>	nms1 <IP Address or Name>
telnet <enable disable>	nms2 <IP Address or Name>;
timeouttelnet <disable 1-30 minutes>	alarmdelay <1-6000 Seconds>
telnetdatadir <netin netout both>	location <Physical Location>
webtelnet <enable disable>	contact <Admin Contact Info>
escapeseqtelnet <1-10 Chars>	rocommunity <Read-Only Community>
outgoingtelnet <enable disable>	rwcommunity <Read-Write Community>
ssh <enable disable>	trapcommunity <Trap Community>
portssh <TCP Port>	v3user <v3 RO User>
timeoutssh <disable 1-30 minutes>	v3rwuser <v3 RW User>
sshdatadir <netin netout both>	v3trapuser <v3 Trap User>
dsakeys <enable disable>	v3security <noauth auth authencrypt>

```
sha2 <enable|disable>
webssh <enable|disable>
smtpserver <IP Address or Name>
smtpsender <Email Address>
termbufsize <Number of Lines>
v3auth <md5|sha|sha2_224|sha2_256|
sha2_384|sha2_512>
v3encrypt <des|aes>
phonehome <enable|disable>
phoneip <IP Address>
```

Description

Configures services (system logging, SSH and Telnet access, SSH and Telnet timeout, SNMP agent, email [SMTP] server, and audit log.)

set services v3password

Syntax

```
set services v3password|v3phrase|v3rwpASSWORD|v3rwphrase|v3trappASSWORD
|v3trapphrase
```

Description

Set SNMP v3 read-only, read-write and trap password/passphrase.

show services

Syntax

```
show services
```

Description

Displays current service settings.

Site Commands

Configure a set of site-oriented modem parameters that can be activated by various modem-related events (authentication, outbound network traffic for DOD connections, etc.). The site parameters will override any parameters configured for the modem. To use sites with a modem, enable 'usesites'. Sites can be used with the following modem states: dialin, dialback, cbcpsERVER, dialondemand, dialin+ondemand, and dialback+ondemand.

set site add|edit

Syntax

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

Parameters

```
name <Site Name> (edit only)
deviceport <Device Port # or Name or none> dialoutnumber <Phone Number>
usbport <U1> dialoutlogin <User Login>
```

```
internal modem
auth <pap|chap>
loginhost <User Login/CHAP Host>
localipaddr <negotiate|IP Address>
remoteipaddr <negotiate|IP Address>
routeipaddr <IP Address>
routemask <Mask>
routegateway <Gateway>
nat <enable|disable>
allowdialback <enable|disable>
dialbacknumber <Phone Number>
dialbackdelay <Dial-back Delay>
dialbackretries <1-10>
timeoutlogins <disable|1-30 minutes>
modemtimeout <disable|1-9999 secs>
restartdelay <PPP Restart Delay>
cbc nocallback <enable|disable>
```

Set the site password and CHAP secret (any extra parameters will be ignored):

```
set site dialoutpassword <Site Name>
set site chapsecret <Site Name>
```

Deletes a site:

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

SLC Network Commands

Displays all SLC, SLB, EMG, and Spider units on the local network.

set slcnetwork

Syntax

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

Parameters

```
add <IP Address>
delete <IP Address>
search <localsubnet|ipaddrlist|both>
```

Description

Detects and displays all EMG or user-defined IP addresses on the local network.

show slcnetwork

Syntax

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

Description

Detects and displays all SLC, SLB, and EMG on the local network.

Without the `ipaddrlist` parameter, the command searches the local network. With the `ipaddrlist` parameter, the command displays a sorted list of all IP addresses or displays the IP addresses that match the mask (for example, 172.19.255.255 would display all IP addresses that start with 172.19).

SSH Key Commands

set sshkey all export

Syntax

```
set sshkey allexport <ftp|sftp|scp|copypaste> [pubfile <Public Key  
File>] [host <IP Address or Name>] [login <User Login>] [path <Path to Copy  
Keys>]
```

Description

Exports the public keys all of the previously created SSH keys.

set sshkey delete

Syntax

```
set sshkey delete <one or more parameters>
```

Parameters

```
keyhost <SSH Key Host>  
keyname <SSH Key Name>  
keyuser <SSH Key User>
```

Description

Deletes an ssh key.

Specify the `keyuser` and `keyhost` to delete an imported key; specify the `keyuser` and `keyname` to delete exported key.

set sshkey export

Syntax

```
set sshkey export <ftp|sftp|scp|copypaste> <one or more parameters>
```

Parameters

```
[format <openssh|secsh>]  
[host <IP Address or Name>]  
[login <User Login>]  
[path <Path to Copy Key>]  
[bits <1024|2048|3072|4096>]  
keyname <SSH Key Name>  
keyuser <SSH Key User>  
type <rsa|dsa>
```

Description

Exports an sshkey.

set sshkey import**Syntax**

```
set sshkey import
```

Description

```
set sshkey import <ftp|sftp|scp|copypaste> <one or more parameters>
```

Parameters

```
[keyhost <SSH Key IP Address or Name>]  
[keyuser <SSH Key User>]  
[path <Path to Public Key File>]  
file <Public Key File>  
host <IP Address or Name>  
login <User Login>
```

Description

Imports an SSH key.

set sshkey server import type**Syntax**

```
set sshkey server import type <rsa|dsa> via <sftp|scp>  
pubfile <Public Key File> privfile <Private Key File>  
host <IP Address or Name> login <User Login> [path <Path to Key File>]
```

Description

Imports an EMG host key.

set sshkey server reset**Syntax**

```
set sshkey server reset [type <all|rsa|dsa>]
```

Description

Resets defaults for all or selected host keys.

show sshkey export**Syntax**

```
show sshkey export <one or more parameters>
```

Parameters

```
[keyhost <SSH Key IP Address or Name>]  
[keyname <SSH Key Name>]  
[keyuser <SSH Key User>]  
[viewkey <enable|disable>]
```

Description

Displays all exported keys or keys for a specific user, IP address, or name.

show sshkey import**Syntax**

```
show sshkey import <one or more parameters>]
```

Parameters

```
[keyhost <SSH Key IP Address or Name>]  
[keyuser <SSH Key User>]  
[viewkey <enable|disable>]
```

Description

Displays all keys that have been imported or keys for a specific user, IP address, or name.

show sshkey server**Syntax**

```
show sshkey server [type <all|rsa|dsa>]
```

Description

Displays host keys (public key only).

Status Commands

show connections**Syntax**

```
show connections [email <Email Address>]
```

Description

Displays a list of current connections. Optionally emails the displayed information. The connection IDs are in the left column of the resulting table. The connection ID associated with a particular connection may change if the connection times out and is restarted.

show connections connid**Syntax**

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

Description

Provides details, for example, endpoint parameters and trigger, for a specific connection. Optionally emails the displayed information.

Note: Use the basic *show connections* command to obtain the Connection ID.

show portcounters**Syntax**

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

Description

Generates a device port statistics report for one or more ports. Optionally emails the displayed information.

show portstatus**Syntax**

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

Description

Displays device port modes and states for one or more ports. Optionally emails the displayed information.

show sysconfig**Syntax**

```
show sysconfig [display <basic|auth|devices>] [email <Email Address>]
```

Description

Displays a snapshot of all configurable parameters. Optionally emails the displayed information.

show sysstatus**Syntax**

```
show sysstatus [email <Email Address>]
```

Description

To display the overall status of all EMG units. Optionally emails the displayed information.

System Log Commands

show syslog**Syntax**

```
show syslog [<parameters>]
```

Parameters

```
[email <Email Address>]  
level <error|warning|info|debug>  
log <all|netlog|servlog|authlog|devlog|diaglog|genlog>  
display <head|tail> [numlines <Number of Lines>]  
starttime <MMDDYYhhmm[ss]>  
endtime <MMDDYYhhmm[ss]>
```

Description

Displays the system logs containing information and error messages.

Note: The level, display, and time parameters cannot be used simultaneously.

show syslog clear**Syntax**

```
show syslog clear <all|netlog|servlog|authlog|devlog|diaglog|genlog>
```

Description

Clears one or all of the system logs.

USB Access Commands

set usb access**Syntax**

```
set usb access <enable|disable>
```

Description

Enables or disables access to USB devices.

USB Device Commands

show usb devices

Syntax

```
show usb devices
```

Description

Displays all USB devices with the port each device is connected to.

diag usb

Syntax

```
diag usb [<parameters>]
```

Parameters

```
treedisplay <enable|disable>  
mapdevice <enable|disable>  
email <Email Address>
```

Defaults: treedisplay=enable

Description

Displays information about USB buses and the devices connected to them, including the mapping between a USB device and the EMG port.

Note: For "mapdevice enable", the port names will be displayed at the end of the line in square brackets. To see a list of USB devices with vendor id and product id, use 'treedisplay disable'.

USB Storage Commands

set usb storage dir

Syntax

```
set usb storage dir <U1> [subdir <Directory Path>]
```

Description

Views a directory listing of a USB flash drive.

set usb storage fsck**Syntax**

```
set usb storage fsck <U1>
```

Description

Runs a file system check on a thumb drive (recommended if it does not mount).

set usb storage format**Syntax**

```
set usb storage format <U1> [filesystem <ext2|fat16|fat32>]
```

Description

Formats a USB flash drive.

set usb storage mount**Syntax**

```
set usb storage mount <U1>
```

Description

Mounts a USB flash drive in the EMG for use as a storage device.

The USB flash drive must be formatted with an ext2 or FAT file system before you mount it.

set usb storage unmount**Syntax**

```
set usb storage unmount <U1>
```

Description

Unmounts a USB flash drive. Enter this command before removing the USB device.

set usb storage rename**Description**

Renames a file on a thumb drive.

Syntax

```
set usb storage rename <U1> file <Filename> newfile <New Filename>
```

set usb storage copy**Description**

Copies a file on a thumb drive.

Syntax

```
set usb storage copy <U1> file <Filename> newfile <New Filename>
```

set usb storage delete**Description**

Removes a file on a thumb drive.

Syntax

```
set usb storage delete <U1> file <Current Filename>
```

show usb storage**Description**

Display product information and settings for any USB thumb drive.

Syntax

```
show usb storage
```

show usb**Description**

Display currently attached USB devices with product information and settings.

Syntax

```
show usb
show usb modem
```

Description

Display product information and settings for any USB modem:

Syntax

```
show usb modem
```

USB Modem Commands

set usb modem

Syntax

```
set usb modem <ul> <parameters>
```

Parameters

auth <pap|chap>
baud <300-115200>

9600 is the default.

```
calleridcmd <Modem Command String>
calleridlogging <enable|disable>
cbc nocallback <enable|disable>
cbc type <admin|user>
chap auth <chap host|local users>
chap host <CHAP Host or User Name>
check dial tone <disable|5-600 minutes>
data bits <7|8>
dial back delay <PPP Dialback Delay>
dial back number <user number|Phone Number>
dial back retries <1-10>
dial in list <Host List for Dial-in>
dial out login <Remote User Login>
dial out number <Phone Number>
do auth <pap|chap>
do chap host <CHAP Host or User Name>
flow control <none|xon/xoff|rts/cts>
group <Local or Remote Group Name>
init script <Modem Init Script>
local ip addr <negotiate|IP Address>
modem mode <text|ppp>
modem state
<disable|dial in|dial out|dial back|cbc server|cbc client|dial on demand|
  dial in+ondemand|dial back+ondemand|dial in host list>
modem timeout <disable|1-9999 sec>
nat <enable|disable>
parity <none|odd|even>
remote ip addr <negotiate|IP Address>
restart delay <PPP Restart Delay>
service <none|telnet|ssh|tcp>
ssh auth <enable|disable>
ssh port <TCP Port>
stop bits <1|2>
tcp auth <enable|disable>
tcp port <TCP Port>
telnet auth <enable|disable>
telnet port <TCP Port>
timeout logins <disable|1-30 minutes>
use sites <enable|disable>
```

Description

Configures a currently loaded USB Modem.

Note: *It is recommended that the initscript be prepended with 'AT' and include 'E1 V1 x4 Q0' so that the EMG may properly control the modem.*

Set the dialout password and CHAP secrets:

```
set usb modem <U1> dialoutpassword
set usb modem <U1> chapsecret
set usb modem <U1> dodchapsecret
```

show usb modem

Description

Display product information and settings for any USB modem:

Syntax

```
show usb modem
```

VPN Commands

set vpn

Syntax

```
set vpn <parameters>
```

Description

Configures setting for an IPsec VPN tunnel.

Parameters

Parameters:

```
tunnel <enable|disable>
name <VPN Tunnel Name>
auth <rsa|psk|x509>
remotehost <Remote Host IP Address or Name>
remoteid <Authentication Name>
remotehop <IP Address>
remotesubnet <one or more subnets in CIDR notation>
remotessourceip <config|CIDR|IP Address Range|poolname>
localip <IP Address>
localid <Authentication name>
localhop <IP Address>
localsubnet <one or more subnets in CIDR notation>
localsourceip <config4|config6|IP Address>
ikenegotiation <main|aggressive>
```

```

ikeenc <any|3des|aes|aes192|aes256>
ikeauth <any|sha1|md5|sha2_256|sha2_384|sha2_512>
ikedhgroup <any|dh2|dh5|dh14|dh15|dh16|dh17|dh18|dh19>
ikever <any|ikev1|ikev2>
espenc <any|3des|aes|aes192|aes256>
espauth <any|sha1|md5|sha2_256|sha2_512|sha2_256_96>
espdhgroup <any|dh2|dh5|dh14|dh15|dh16|dh17|dh18|dh19>
lifetime <SA Lifetime in Seconds (3600) or Bytes with 'b' suffix (3600b)>
xauthclient <enable|disable>
xauthlogin <User Login>
ciscounity <enable|disable>
modeconfig <push|pull>
forceencaps <enable|disable>
deadpeerdelay <disable|1-300 seconds>
deadpeertimeout <5-1200 seconds>
deadpeeraction <restart|hold|clear>
tunnelrestart <enable|disable>
email <Email Address>

```

Enter Pre-Shared Key of remote host:

```
set vpn key
```

Enter XAUTH password (any extra parameters will be ignored):

```
set vpn xauthpassword
```

Configure X.509 certificate for remote peer or local peer.

```

set vpn certificate local via <sftp|scp> rootfile <Cert Authority File>
    certfile <Certificate File> keyfile <Private Key File>
    host <IP Address or Name> login <User Login> [path <Path to Files>
set vpn certificate remote via <sftp|scp> [rootfile
    <Cert Authority File>
    certfile <Certificate File> host <IP Address or Name>
    login <User Login> [path <Path to Files>]

```

Delete X.509 certificate for local and/or remote peer.

```
set vpn certificate delete
```

Generate RSA Key for the EMG (any extra parameters will be ignored):

```

set vpn genrsakey
set vpn peerrsaaction upload via <sftp|scp> host <IP address or Name>
    login <User Login> rsafile <rsa key file>
    [path <Path to key file>]
set vpn peerrsaaction delete

```

Display all VPN settings and current status:

```
show vpn [email <Email Address>]
```

Display detailed VPN status:

```
show vpn status [email <Email Address>]
```

Display VPN logs:

```
show vpn viewlog [numlines <Number of Lines>] [email <Email Address>]
```

Display RSA public key of the EMG:

```
show vpn rsakey
```

Display X.509 certificate for local peer (EMG) and remote peer:

```
show vpn certificate
```

Download IPSec conf file (VPN tunnel must be enabled to generate ipsec.conf for download; can be customized and uploaded to access more strongSwan options):

```
set vpn confaction download via <sftp|scp> host <IP address or Name>
    login <User Login> [path <Directory for download>]
```

Upload IPSec conf file to the EMG:

```
set vpn confaction upload via <sftp|scp> host <IP address or Name>
    login <User Login> conffile <Conf File> [path <Path to conf file>]
```

Delete the uploaded conf file:

```
set vpn confaction delete
```

Display all VPN settings and current status:

```
show vpn [email <Email Address>]
```

Display detailed VPN status:

```
show vpn status [email <Email Address>]
```

Display VPN logs:

```
show vpn viewlog [numlines <Number of Lines>] [email <Email Address>]
```

Display X.509 certificate for local peer (EMG) and remote peer:

```
show vpn certificate
```

Display RSA public key of the local peer (EMG) and remote peer:

```
show vpn rsakey
```

Display the uploaded or auto-generated IPSec conf file:

```
show vpn vpnconf
```

Temperature Commands

set temperature

Syntax

```
set temperature
```

Description

Sets the acceptable range for the internal temperature sensor (an SNMP trap is sent if the temperature is outside of this range). Temperatures can be entered in either Celsius or Fahrenheit; to indicate a temperature is Fahrenheit, append the degrees with an 'F', i.e., "75F".

Parameter

```
set temperature <one or more parameters>
Parameters: low <Low Temperature in C. or F.>
high <High Temperature in C. or F.>
calibrate <Temperature Calibration in C. or F.|cancel>
```

Note: The calibration offset will be applied one hour after setting the value.

Description

Displays the acceptable range and the current reading from the internal temperature sensor.

show temperature**Syntax**

```
show temperature
```

Description

Shows the temperature.

Xmodem Commands

set xmodem repo**Syntax**

```
set xmodem repo import <Xmodem File> via <ftp|sftp|scp>
host <IP Address or Name> login <User Login>
[path <Path to Xmodem File>]
set xmodem repo rename <Xmodem File> newfile <New Filename>
set xmodem repo delete <Xmodem File>
```

Description

Manages a repository of files that can be sent to or received from a device port with Xmodem, Ymodem, or Zmodem. The maximum file size is 20 MB, and the maximum total repository size is 25 MB.

set xmodem send/receive**Syntax**

```
set xmodem send <Device Port # or Name> file <Xmodem File>
protocol <xmodem|ymodem|zmodem> xfer <binary|ascii>
set xmodem receive <Device Port # or Name> [file <Xmodem File>]
protocol <xmodem|ymodem|zmodem> xfer <binary|ascii>
[overwrite <enable|disable>]
```

Description

Send or receive files with Xmodem, Ymodem or Zmodem (by default receive will not overwrite a file in the repository with the same name).

show xmodem

Syntax

show xmodem

Description

Shows the Xmodem repository files.

Appendix A: Security Considerations

The EMG provides data path security by means of SSH or Web/SSL. Even with the use of SSH/SSL, however, do not assume you have complete security. Securing the data path is only one measure needed to ensure security. This appendix briefly discusses some important security considerations.

Security Practice

Develop and document a Security Practice. The Security Practice should state:

- ◆ The dos and don'ts of maintaining security. For example, the power of SSH and SSL is compromised if users leave sessions open or advertise their password.
- ◆ The assumptions that users can make about the facility and network infrastructure, for example, how vulnerable the CAT 5 wiring is to tapping.

Factors Affecting Security

External factors affect the security provided by the EMG unit, for example:

- ◆ Telnet sends the login exchange as clear text across Ethernet. A person snooping on a subnet may read your password.
- ◆ A terminal to the EMG may be secure, but the path from the EMG to the end device may not be secure.
- ◆ With the right tools, a person with physical access to open the EMG unit may be able to read the encryption keys.
- ◆ There is no true test for a denial-of-service attack. There is always a legitimate scenario for a request storm. A denial-of-service filter locks out some high-performance automated/scripted requests. The EMG will attempt to service all requests and will not filter out potential denial-of-service attacks.

Appendix B: Safety Information

Note: This section will be replaced when certifications are complete

Safety Precautions

Please follow the safety precautions described below when installing and operating the EMG.

Caution: **EQUIPMENT IS FOR INDOOR USE ONLY!**

Fuse Caution Statement

For protection against fire, replace the power-input-module fuse with the same type and rating.

Pour préserver la protection contre l'incendie, remplacez toujours le fusible du module d'alimentation électrique par un modèle du même type et de la même capacité.

Ersetzen Sie die Netzzeilsicherung nur durch eine Sicherung desselben Typs und derselben Nennstromstärke um die Gefahr eines Brandes zu vermeiden.

Para proteger la unidad contra el fuego, sustituya el fusible del módulo de entrada de alimentación por otro del mismo tipo y capacidad.

Предупреждение : Для защиты от пожара заменяйте предохранитель блока питания на предохранитель такого же типа и с такой же характеристикой.

Cover

- ◆ Do not remove the cover of the chassis. There are no user-serviceable parts inside. Opening or removing the cover may expose you to dangerous voltage that could cause fire or electric shock.
- ◆ Refer all servicing to Lantronix.

Power Plug

- ◆ Connect the power plug in the following order: 1) Connect the DC plug to the EMG first. 2) Connect the AC cable to the external power supply. 3) Connect the AC cable to the power source. When removing power, the AC cable to the power source should be unplugged first.
- ◆ Always connect the power cord to a properly wired and grounded power source. Do not use adapter plugs or remove the grounding prong from the cord.
- ◆ When disconnecting the power cable from the socket, pull on the plug, not the cord.
- ◆ Only use a power cord with a voltage and current rating greater than the voltage and current rating marked on the EMG unit.
- ◆ The EMG unit must be connected to a branch circuit provided with 15A or 20A, single pole circuit breaker.
- ◆ Install the EMG near an AC outlet that is easily accessible.
- ◆ Always connect any equipment used with the product to properly wired and grounded power sources.

- ◆ To help protect the product from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- ◆ Do not connect or disconnect this product during an electrical storm.

Input Supply

Caution: *Disconnect all power supply sources before servicing to avoid electric shock.*

- ◆ Check nameplate ratings to assure there is no overloading of supply circuits that could affect over current protection and supply wiring.

Grounding

1. Maintain reliable grounding of this product.
2. Pay particular attention to supply connections when connecting to power strips, rather than directly to the branch circuit.

Rack Mounting

If rack mounted EMGs are installed in a closed or multi-unit rack assembly, they may require further evaluation by Certification Agencies. The following items must be considered:

- ◆ Do not install the EMG unit in a rack in such a way that a hazardous stability condition results because of uneven loading. A drop or fall could cause injury.
- ◆ The ambient temperature (Tma) inside the rack may be greater than the room ambient temperature. Make sure to install the EMG in an environment with an ambient temperature less than the maximum operating temperature of the EMG unit. See *Hardware Specifications (on page 37)*.
- ◆ Install the equipment in a rack in such a way that the amount of airflow required for safe operation of the equipment is not compromised.
- ◆ Mount the equipment in the rack so that a hazardous condition is not achieved due to uneven mechanical loading.
- ◆ Maintain reliable earthing of rack-mounted equipment. Give particular attention to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- ◆ Before operating the EMG, make sure the EMG unit is secured to the rack.

Wall Mounting

If wall-mounted units are installed, the following items must be considered:

- ◆ Do not install the unit in such a way that a hazardous stability condition results because of uneven loading. A drop or fall could cause injury.
- ◆ Make sure to install the EMG unit in an environment with an ambient temperature less than the maximum operating temperature of the EMG unit. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- ◆ Maintain reliable earthing of wall-mounted equipment. Give particular attention to supply connections other than direct connections to the branch circuit (e.g. use of power strips) because of the effect that overloading of the circuits might have on overcurrent protection and

supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

- ◆ Before operating the EMG, make sure the device mounting is secured.

Port Connections

- ◆ Only connect the network port to an Ethernet network that supports 10/100/1000 Base-T.
- ◆ Only connect device ports to equipment with serial ports that support EIA-232 (formerly RS-232C).
- ◆ Only connect the console port to equipment with serial ports that support EIA-232 (formerly RS-232C).
- ◆ Only connect a telephone line to the MODEM port.

Caution: *To reduce the risk of fire, use only number 26 AWG or larger (e.g., 24 AWG) UL-listed or CSA-certified telecommunication line cord.*

Appendix C: Adapters and Pinouts

The serial device ports of the EMG products match the RJ45 pinouts of the console ports of many popular devices found in a network environment. The EMG uses conventional straight-through Category 5 fully pinned network cables for all connections when used with Lantronix adapters. The cables are available in various lengths.

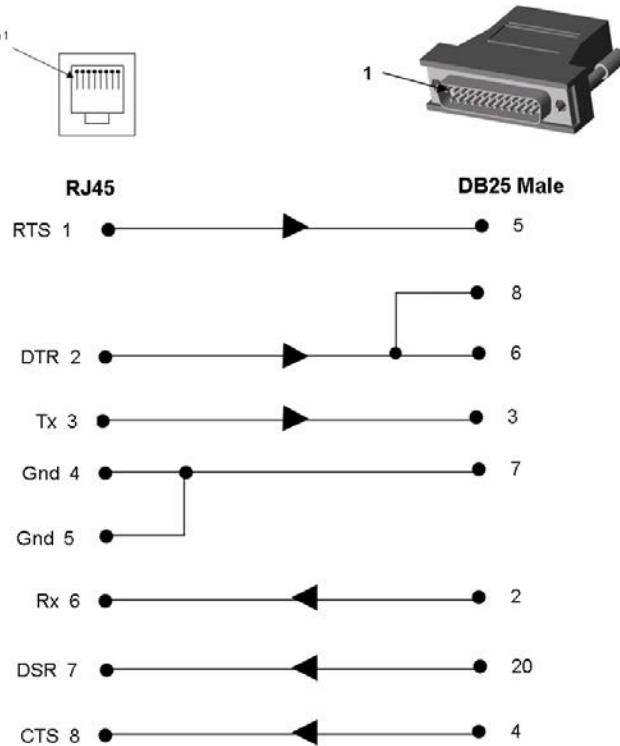
In most cases, you will need an adapter for your serial devices. Lantronix offers a variety of RJ45-to-serial connector adapters for many devices. These adapters convert the RJ45 connection on the EMG unit to a 9-pin or 25-pin serial connector found on other manufacturers' serial devices or re-route the serial signals for connections to other devices that use RJ45 serial connectors.

The console port is wired the same way as the device ports and has the same signal options.

Note: You can view or change the console port settings using the [Device Ports](#) page or the command line interface `show console port` and set `consoleport commands`.

The adapters illustrated below are compatible with the Lantronix EMG models.

Figure C-1 RJ45 Receptacle to DB25M DCE Adapter for the EMG Unit (PN 200.2066A)



Use PN 200.2066A adapter with a dumb terminal or with many SUN applications.

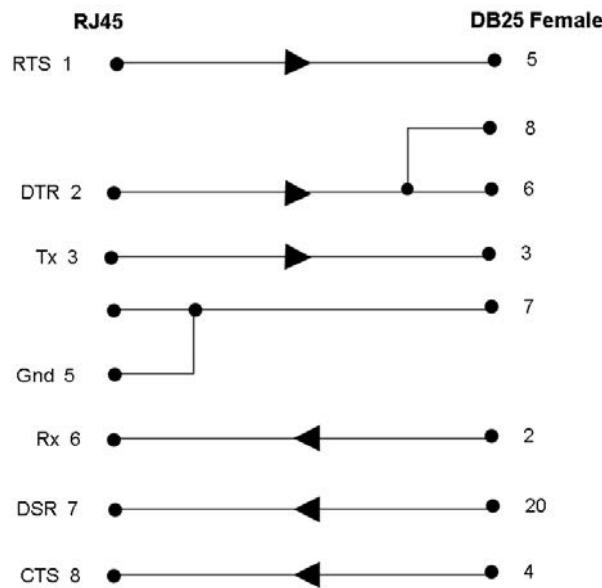
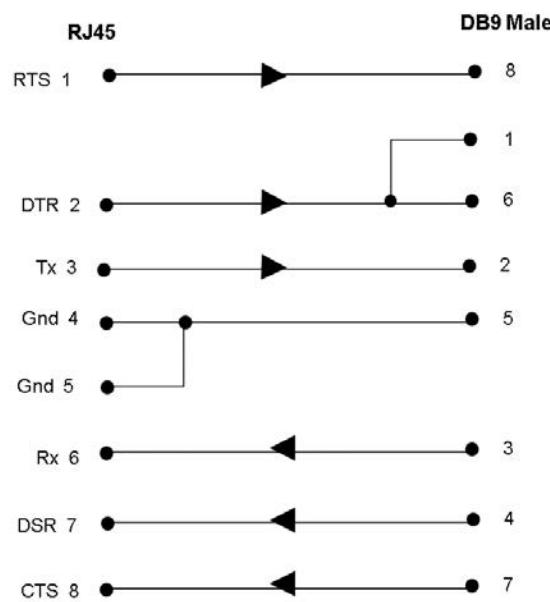
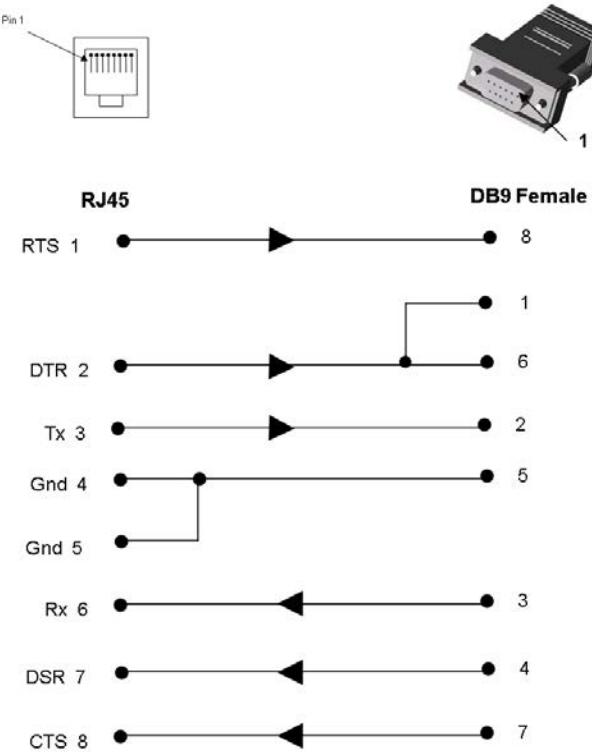
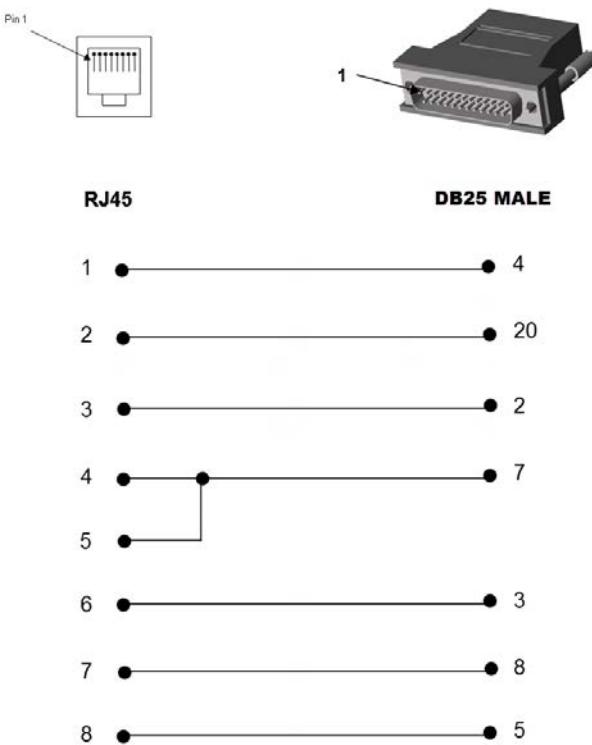
Figure C-2 RJ45 Receptacle to DB25F DCE Adapter for the EMG Unit (PN 200.2067A)**Figure C-3 RJ45 Receptacle to DB9M DCE Adapter for the EMG Unit (PN 200.2069A)**

Figure C-4 RJ45 Receptacle to DB9F DCE Adapter for the EMG Unit (PN 200.2070A)



Use PN 200.2070A adapter with a PC's serial port.

Figure C-5 RJ45 Receptacle to DB25M DTE Adapter (PN 200.2073)



Appendix D: Protocol Glossary

BOOTP (Bootstrap Protocol)

Similar to DHCP, but for smaller networks. Automatically assigns the IP address for a specific duration of time.

CHAP (Challenge Handshake Authentication Protocol)

A secure protocol for connecting to a system; it is more secure than the PAP.

DHCP (Dynamic Host Configuration Protocol)

Internet protocol for automating the configuration of computers that use TCP/IP.

DNS (Domain Name Servers)

A system that allows a network nameserver to translate text host names into numeric IP addresses.

FTP (File Transfer Protocol)

A protocol for transferring files between computers on a network that is insecure by design and susceptible to interception. See also SCP, SFTP, and TFTP.

IKEv1 and IKEv2 (Internet Key Exchange)

A protocol used to set up a security association in the IPsec protocol suite that allows two parties to send data securely.

IPsec

A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

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.

MIB (Management Information Base)

MIB is part of the Simple Network Management Protocol (SNMP) and describes the set of manageable objects within a network device.

NAT (Network Address Translation)

An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This enables a company to shield internal addresses from the public Internet.

NFS (Network File System)

A protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer. You can use NFS to mount all or a portion of a file system. Users can access the portion mounted with the same privileges as the user's access to each file.

NIS (Network Information System)

System developed by Sun Microsystems for distributing system data such as user and host names among computers on a network.

NMS (Network Management System)

NMS acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP.

NTP (Network Time Protocol)

A protocol used to synchronize time on networked computers and equipment.

PAP (Password Authentication Protocol)

A method of user authentication in which the username and password are transmitted over a network and compared to a table of name-password pairs.

PPP (Point-to-Point Protocol)

A protocol for creating and running IP and other network protocols over a serial link.

RADIUS (Remote Authentication Dial-In User Service)

An authentication and accounting protocol. Enables remote access servers to communicate with a central server to authenticate dial-in users and their access permissions. A company stores user profiles in a central database that all remote servers can share.

SCP (Secure Copy Protocol)

A file transfer protocol that is similar to SFTP in that it uses SSH encryption and authentication, but is slightly faster.

SFTP (SSH File Transfer Protocol)

Secure file transfer protocol over SSH Commands and data in transit are encrypted.

SMB/CIFS (Server Message Block/Common Internet File System)

: Microsoft's protocol for allowing all applications as well as Web browsers to share files across the Internet. CIFS runs on TCP/IP and uses the SMB protocol in Microsoft Windows for accessing files. With CIFS, users with different platforms and computers can share files without having to install new software.

SNMP (Simple Network Management Protocol)

A protocol that system administrators use to monitor networks and connected devices and to respond to queries from other network hosts.

SMTP (Simple Mail Transfer Protocol)

TCP/IP protocol for sending email between servers.

SSL (Secure Sockets Layer)

A protocol that provides authentication and encryption services between a web server and a web browser.

SSH (Secure Shell)

A secure transport protocol based on public-key cryptography.

TACACS+ (Terminal Access Controller Access Control System)

A method of authentication used in UNIX networks. It allows a remote access server to communicate with an authentication server to determine whether the user has access to the network.

Telnet

A terminal protocol that provides an easy-to-use method of creating terminal connections to a network host.

TFTP (Trivial File Transfer Protocol)

Simpler version of FTP that doesn't require any type of authentication.

Xmodem

A file transfer protocol that allows file transfer between two computers across the serial port. Subsequent modified versions of the protocol are called Ymodem and Zmodem.

Appendix E: Compliance Information

Note: This is the Planned Compliance - It will be replaced when certification is complete.

Manufacturer's Name & Address

Lantronix Inc., 7535 Irvine Center Drive, Suite 100, Irvine, CA 92618 USA

Declares that the following product:

Product Name(s): EMG™ Edge Management Gateway

Conforms to the following standards or other normative documents:

Safety

- ◆ IEC 60950
- ◆ EN 60950
- ◆ UL 60950

Electromagnetic Emissions

- ◆ FCC Part 15, Subpart B, Class A EN 55022: 2011 (IEC/CISPR 22: 2009), class A
- ◆ EN 55032: 2012 + AC: 2013 (IEC/CISPR 32: 2015), class A

Electromagnetic Immunity

- ◆ EN 55024: 2010 Information Technology Equipment-Immunity Characteristics
- ◆ EN 61000-4-2: 2008 Electro-Static Discharge Test
- ◆ EN 61000-4-3: 2010 Radiated Immunity Field Test
- ◆ EN 61000-4-4: 2012 Electrical Fast Transient Test
- ◆ EN 61000-4-5: 2014 Power Supply Surge Test
- ◆ EN 61000-4-6: 2013 Conducted Immunity Test
- ◆ EN 61000-4-8: 2009 Magnetic Field Test
- ◆ EN 61000-4-11: 2004 Voltage Dips & Interrupts

Supplementary Information

This Class A digital apparatus complies with Canadian ICES-003 (CSA) and has been verified as being compliant within the Class A limits of the FCC Radio Frequency Device Rules (FCC Title 47, Part 15, Subpart B CLASS A), measured to CISPR 22: 2008 limits and methods of measurement of Radio Disturbance Characteristics of Information Technology Equipment. The product complies with the requirements of the Low Voltage Directive 72/23/EEC and the EMC Directive 89/336/EEC.

Additional Agency Approvals and Certifications

This product carries the CE mark since it has been tested and found compliant with the following standards:

- ◆ Safety: EN 60950-1

- ◆ Emissions: EN 55022, EN 55032 Class A
- ◆ Immunity: EN 55024

RoHS, REACH and WEEE Compliance Statement

Please visit <http://www.lantronix.com/legal/rohs/> for Lantronix's statement about RoHS, REACH and WEEE compliance.