EDS Device Server
User Guide

Part Number 900-433
Revision K March 2020
Intellectual Property

© 2020 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, XPort, MatchPort, and Evolution OS are registered trademark of Lantronix, Inc. in the United States and other countries. DeviceInstaller and is a trademark of Lantronix, Inc.

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

Windows and Internet Explorer are registered trademarks of the Microsoft Corporation. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. Chrome is a trademark of Google Inc. Safari is a registered trademark of Apple Inc. Opera is a registered trademark of Opera Software ASA Corporation Norway. 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 website at www.lantronix.com/support/warranty.

Contacts

Lantronix, Inc. Corporate Headquarters
7535 Irvine Center Drive
Suite 100
Irvine, CA 92618, USA
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: www.lantronix.com/support

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

Disclaimer

Note: This product has been designed to comply with the limits for a Class B digital device pursuant to Part 15 of FCC and EN55022:1998 Rules when properly enclosed and grounded. These limits are designed to provide reasonable protection against radio interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with this guide, may cause interference to radio communications. See the appendix, sCompliance (on page 145).

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.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Rev.</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2006</td>
<td>A</td>
<td>2006 A Initial Document</td>
</tr>
<tr>
<td>October 2006</td>
<td>B</td>
<td>EDS16PR and EDS32PR products added.</td>
</tr>
<tr>
<td>December 2006</td>
<td>C</td>
<td>Added German TUV certification.</td>
</tr>
<tr>
<td>January 2006</td>
<td>D</td>
<td>Added English TUV certification.</td>
</tr>
<tr>
<td>January 2007</td>
<td>E</td>
<td>EDS8PR product added.</td>
</tr>
<tr>
<td>November 2007</td>
<td>F</td>
<td>Added LPD, Terminal Host, RSS, and RT pages; updated XML and other pages.</td>
</tr>
<tr>
<td>November 2008</td>
<td>G</td>
<td>EDS8PS and EDS16PS products added.</td>
</tr>
<tr>
<td>May 2009</td>
<td>H</td>
<td>Updated for EDS8/16/32PR and EDS4100 v4.1.0.2.</td>
</tr>
<tr>
<td>April 2011</td>
<td>I</td>
<td>Updated for firmware version 5.2.0.0R24. Added support for Modbus protocol for EDS4100, configurable MTU, and additional VIP tunnel connect protocols; as well as improvements to SNMP, logging, and SSL.</td>
</tr>
<tr>
<td>July 2017</td>
<td>J</td>
<td>Updated for firmware version 5.4.0.1R1.</td>
</tr>
<tr>
<td>March 2020</td>
<td>K</td>
<td>Updated for firmware version 6.0.0.0R1. Updated with new default password, label, and security information.</td>
</tr>
</tbody>
</table>
Table of Contents

1: About This Guide 14
   Chapter and Appendix Summaries ................................................................. 14
   Additional Documentation .................................................................................. 15

2: Introduction 16
   EDS4100 Overview ............................................................................................ 17
   Key Features ...................................................................................................... 17
   EDS8PR, EDS16PR, and EDS32PR Overview ...................................................... 18
   Key Features ...................................................................................................... 19
   Applications ....................................................................................................... 19
   Protocol Support ................................................................................................. 19
   Evolution OS™ Application .............................................................................. 20
   Additional Features ............................................................................................ 20
      Modem Emulation .......................................................................................... 20
      Web-Based Configuration and Troubleshooting .............................................. 20
      Command-Line Interface (CLI) ...................................................................... 20
      SNMP Management ......................................................................................... 20
      XML-Based Architecture and Device Control ............................................... 20
      Really Simple Syndication (RSS) .................................................................. 21
      Enterprise-Grade Security ............................................................................. 21
      Terminal Server/Device Management ............................................................. 21
      Troubleshooting Capabilities ........................................................................ 22
   Configuration Methods ....................................................................................... 22
   Addresses and Port Numbers ............................................................................ 22
      Hardware Address ............................................................................................ 22
      IP Address ....................................................................................................... 23
      Port Numbers .................................................................................................. 23
      Product Information Label .............................................................................. 23

3: Installation of EDS4100 25
   Package Contents .............................................................................................. 25
   User-Supplied Items ........................................................................................... 25
   Identifying Hardware Components ..................................................................... 26
      Serial Ports ....................................................................................................... 27
      Ethernet Port ................................................................................................... 28
      Terminal Block Connector ............................................................................. 28
      LEDs ................................................................................................................ 28
      Reset Button .................................................................................................. 28
   Physically Installing the EDS4100 ................................................................. 29
   Finding a Suitable Location .............................................................................. 29
4: Installation of EDS8PR, EDS16PR and EDS32PR

- Package Contents
- User-Supplied Items
- Identifying Hardware Components
  - Serial Ports
  - Console Port
  - Ethernet Port
  - LEDs
  - Reset Button
- Installing the EDS8/16/32PR
  - Finding a Suitable Location
  - Connecting the EDS8/16/32PR

5: Using DeviceInstaller

- Installing DeviceInstaller
- Accessing the EDS Unit Using DeviceInstaller

6: Configuration Using Web Manager

- Accessing Web Manager
- Device Status Page
- Web Manager Page Components
- Navigating the Web Manager

7: Network Settings

- Network 1 (eth0) Interface Status
- Network 1 (eth0) Interface Configuration
- Network 1 Ethernet Link

8: Line and Tunnel Settings

- Line Settings
  - Line Statistics
  - Line Configuration
  - Line Command Mode
- Tunnel Settings
  - Tunnel – Statistics
  - Tunnel – Serial Settings
  - Tunnel – Packing Mode
  - Tunnel – Accept Mode
  - Tunnel – Connect Mode
- Connecting Multiple Hosts
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>9: Terminal and Host Settings</td>
<td>Terminal Settings</td>
</tr>
<tr>
<td></td>
<td>Terminal Network Configuration</td>
</tr>
<tr>
<td></td>
<td>Terminal Line Configuration</td>
</tr>
<tr>
<td></td>
<td>Host Configuration</td>
</tr>
<tr>
<td>10: Service Settings</td>
<td>DNS Settings</td>
</tr>
<tr>
<td></td>
<td>SNMP Settings</td>
</tr>
<tr>
<td></td>
<td>FTP Settings</td>
</tr>
<tr>
<td></td>
<td>TFTP Settings</td>
</tr>
<tr>
<td></td>
<td>Syslog Settings</td>
</tr>
<tr>
<td></td>
<td>HTTP Settings</td>
</tr>
<tr>
<td></td>
<td>HTTP Statistics</td>
</tr>
<tr>
<td></td>
<td>HTTP Configuration</td>
</tr>
<tr>
<td></td>
<td>HTTP Authentication</td>
</tr>
<tr>
<td></td>
<td>RSS Settings</td>
</tr>
<tr>
<td></td>
<td>LPD Settings</td>
</tr>
<tr>
<td></td>
<td>LPD Statistics</td>
</tr>
<tr>
<td></td>
<td>LPD Configuration</td>
</tr>
<tr>
<td></td>
<td>Print Test Page</td>
</tr>
<tr>
<td>11: Security Settings</td>
<td>SSH Settings</td>
</tr>
<tr>
<td></td>
<td>SSH Server Host Keys</td>
</tr>
<tr>
<td></td>
<td>SSH Server Authorized Users</td>
</tr>
<tr>
<td></td>
<td>SSH Client Known Hosts</td>
</tr>
<tr>
<td></td>
<td>SSH Client Users</td>
</tr>
<tr>
<td></td>
<td>SSL Settings</td>
</tr>
<tr>
<td></td>
<td>SSL Cipher Suites</td>
</tr>
<tr>
<td></td>
<td>SSL Certificates</td>
</tr>
<tr>
<td></td>
<td>SSL RSA</td>
</tr>
<tr>
<td></td>
<td>SSL Certificates and Private Keys</td>
</tr>
<tr>
<td></td>
<td>SSL Utilities</td>
</tr>
<tr>
<td></td>
<td>SSL Configuration</td>
</tr>
<tr>
<td>12: Modbus</td>
<td>Serial Transmission Mode</td>
</tr>
<tr>
<td></td>
<td>Modbus Statistics</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Short and Long Name Customization</td>
<td>140</td>
</tr>
<tr>
<td><strong>16: Updating Firmware</strong></td>
<td>141</td>
</tr>
<tr>
<td>Obtaining Firmware</td>
<td>141</td>
</tr>
<tr>
<td>Loading New Firmware</td>
<td>141</td>
</tr>
<tr>
<td><strong>Appendix A: Technical Support</strong></td>
<td>142</td>
</tr>
<tr>
<td><strong>Appendix B: Binary to Hexadecimal Conversions</strong></td>
<td>143</td>
</tr>
<tr>
<td>Converting Binary to Hexadecimal</td>
<td>143</td>
</tr>
<tr>
<td>Conversion Table</td>
<td>143</td>
</tr>
<tr>
<td>Scientific Calculator</td>
<td>144</td>
</tr>
<tr>
<td><strong>Appendix C: sCompliance</strong></td>
<td>145</td>
</tr>
<tr>
<td>RoHS, REACH and WEEE Compliance Statement</td>
<td>145</td>
</tr>
<tr>
<td>Lithium Battery Notice</td>
<td>146</td>
</tr>
<tr>
<td>Installationsanweisungen</td>
<td>146</td>
</tr>
<tr>
<td>Rackmontage</td>
<td>146</td>
</tr>
<tr>
<td>Energiezufuhr</td>
<td>146</td>
</tr>
<tr>
<td>Erdung</td>
<td>146</td>
</tr>
<tr>
<td>Installation Instructions</td>
<td>146</td>
</tr>
<tr>
<td>Rack Mounting</td>
<td>146</td>
</tr>
<tr>
<td>Input Supply</td>
<td>147</td>
</tr>
<tr>
<td>Grounding</td>
<td>147</td>
</tr>
<tr>
<td><strong>Appendix D: Lantronix Cables and Adapters</strong></td>
<td>148</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>149</td>
</tr>
</tbody>
</table>
List of Figures

Figure 2-1 EDS4100 4 Port Device Server _____________________________________________17
Figure 2-2 EDS8PR Device Server _____________________________________________________18
Figure 2-3 EDS16PR Device Server ____________________________________________________18
Figure 2-4 EDS32PR Device Server ____________________________________________________18
Figure 2-5 Sample Hardware Address ________________________________________________22
Figure 2-6 EDS4100 Product Label ___________________________________________________24
Figure 2-7 EDS8/16/32PR Product Label ______________________________________________24
Figure 2-8 EDS8/16PS Product Label ________________________________________________24
Figure 3-1 Front View of the EDS4100 _______________________________________________26
Figure 3-2 Back View of the EDS4100 ________________________________________________26
Figure 3-3 RS-232 Serial Port Pins (Serial Ports 1, 2, 3, 4) ___________________________________27
Figure 3-4 RS-422/RS-485 Serial Port Pins ___________________________________________27
Figure 3-5 Terminal Block Connector Pin Assignments ___________________________________28
Figure 3-7 Example of EDS4100 Connections __________________________________________30
Figure 4-1 Front View of the EDS16PR _______________________________________________32
Figure 4-2 Back View of the EDS16PR ________________________________________________32
Figure 4-3 RJ45 Serial Port _________________________________________________________33
Figure 4-5 Example of EDS16PR Connections __________________________________________35
Figure 6-1 Prompt for User Name and Password ________________________________________38
Figure 6-2 Web Manager Home Page ________________________________________________39
Figure 6-3 Components of the Web Manager Page ______________________________________40
Figure 7-1 Network 1 (eth0) Interface Status ___________________________________________43
Figure 7-2 Network 1 (eth0) Interface Configuration ____________________________________44
Figure 7-4 Network 1 Ethernet Link __________________________________________________46
Figure 8-1 Line 1 Statistics _________________________________________________________47
Figure 8-2 Line 1 Configuration _____________________________________________________48
Figure 8-4 Line 1 Command Mode ___________________________________________________50
Figure 8-6 Tunnel 1 Statistics (1 of 2) _______________________________________________53
Figure 8-7 Tunnel 1 Statistics (2 of 2) ________________________________________________54
Figure 8-8 Tunnel 1 Serial Settings ___________________________________________________55
Figure 8-10 Tunnel 1 Packing Mode (Mode = Disable) ___________________________________56
Figure 8-11 Tunnel 1 Packing Mode (Mode = Timeout) ___________________________________56
Figure 8-12 Tunnel 1 Packing Mode (Mode = Send Character) _____________________________57
Figure 8-14 Tunnel 1 Accept Mode ___________________________________________________59
Figure 8-16 Tunnel 1 - Connect Mode ________________________________________________62
List of Tables

Table 3-6 Back Panel LEDs ________________________28
Table 4-4 Back Panel LEDs ________________________34
Table 5-1 Device Details Summary __________________37
Table 6-4 Summary of Web Manager Pages __________41
Table 7-3 Network 1 (eth0) Interface Configuration __44
Table 7-5 Network 1 Ethernet Link _________________46
Table 8-3 Line Configuration ______________________49
Table 8-5 Line Command Mode _____________________50
Table 8-9 Tunnel - Serial Settings __________________55
Table 8-13 Tunnel Packing Mode ____________________57
Table 8-15 Tunnel Accept Mode _____________________59
Table 8-17 Tunnel Connect Mode ____________________62
Table 8-20 Tunnel Disconnect Mode _________________67
Table 8-21 Modem Emulation Commands and Descriptions ___67
Table 8-23 Tunnel Modem Emulation ________________69
Table 9-2 Terminal on Network Configuration ________71
Table 9-4 Terminal on Line 1 Configuration __________72
Table 9-6 Host Configuration ______________________73
Table 10-3 SNMP _________________________________76
Table 10-5 FTP Settings ___________________________77
Table 10-7 TFTP Server ___________________________77
Table 10-9 Syslog _________________________________79
Table 10-12 HTTP Configuration ____________________81
Table 10-14 HTTP Authentication ___________________83
Table 10-16 RSS __________________________________85
Table 10-19 LPD Configuration ______________________87
Table 11-2 SSH Server Host Keys Settings - Upload Keys Method _________________90
Table 11-3 SSH Server Host Keys Settings - Upload Keys Method _________________90
Table 11-4 SSH Server Host Keys Settings - Create New Keys Method ____________91
Table 11-6 SSH Server Authorized User Settings _______________________________92
Table 11-8 SSH Client Known Hosts __________________93
Table 11-10 SSH Client Users _______________________95
Table 11-11 Supported Cipher Suites __________________96
Table 11-13 SSL __________________________________100
Table 12-1 6 Byte Header of Modbus Application Protocol _________________________102
Table 12-2 Modbus Transmission Modes ................................................................. 102
Table 12-5 Modbus Configuration ........................................................................... 104
Table 13-3 Filesystem Browser .............................................................................. 107
Table 13-5 TCP Protocol Settings .......................................................................... 108
Table 13-7 IP Protocol Settings ............................................................................. 109
Table 13-9 ICMP Settings ...................................................................................... 110
Table 13-11 ARP Settings ...................................................................................... 111
Table 13-13 SMTP Settings ................................................................................... 112
Table 13-15 IP Address Filter Settings ................................................................. 113
Table 13-19 Requests for Comments (RFCs) ......................................................... 116
Table 13-22 Diagnostics: Ping ............................................................................. 118
Table 13-24 Diagnostics: Traceroute ................................................................. 118
Table 13-32 Clock Settings .................................................................................... 123
Table 13-34 Real Time Clock Settings ................................................................. 125
Table 13-36 System ......................................................................................... 126
Table 14-2 Email Configuration .......................................................................... 128
Table 14-5 CLI Configuration ............................................................................. 130
Table 14-7 XML Export Configuration .............................................................. 132
Table 14-9 XML Export Status .......................................................................... 134
Table 14-15 XML: Import Line(s) from Single Line Settings ................................ 139
1:  **About This Guide**

This user guide provides the information needed to configure, use, and update the Lantronix® EDS device server, which includes models: EDS8PR, EDS16PR, EDS32PR and EDS4100PR. It is intended for software developers and system integrators who are installing the EDS in their designs.

**Chapter and Appendix Summaries**

A summary of each chapter is provided below.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2: Introduction</td>
<td>Main features of the product and the protocols it supports. Includes technical specifications.</td>
</tr>
<tr>
<td>Chapter 3: Installation of EDS4100</td>
<td>Instructions for installing the EDS4100 device server.</td>
</tr>
<tr>
<td>Chapter 4: Installation of EDS8PR, EDS16PR, EDS32PR</td>
<td>Instructions for installing the EDS8PR, the EDS16PR, and the EDS32PR device/terminal server.</td>
</tr>
<tr>
<td>Chapter 5: Using DeviceInstaller</td>
<td>Instructions for viewing the current configuration using the Lantronix DeviceInstaller™ application.</td>
</tr>
<tr>
<td>Chapter 6: Configuration Using Web Manager</td>
<td>Instructions for accessing Web Manager and using it to configure settings for the device.</td>
</tr>
<tr>
<td>Chapter 7: Network Settings</td>
<td>Instructions for using the web interface to configure Ethernet settings.</td>
</tr>
<tr>
<td>Chapter 8: Line and Tunnel Settings</td>
<td>Instructions for using the web interface to configure line and tunnel settings.</td>
</tr>
<tr>
<td>Chapter 9: Terminal and Host Settings</td>
<td>Instructions for using the web interface to configure terminal and host settings.</td>
</tr>
<tr>
<td>Chapter 10: Service Settings</td>
<td>Instructions for using the web interface to configure settings for DNS, SNMP, FTP, and other services.</td>
</tr>
<tr>
<td>Chapter 11: Security Settings</td>
<td>Instructions for using the web interface to configure SSH and SSL security settings.</td>
</tr>
</tbody>
</table>
| Chapter 12: Modbus                           | Instructions for using the web interface to configure Modbus.  
  *Modbus is only available on the EDS4100 and is not supported on the EDS8PR, EDS16PR, EDS32PR, EDS8PS and EDS16PS.* |
| Chapter 13: Maintenance and Diagnostic Settings | Instructions for using the web interface to maintain the device, view statistics, files, and logs, and to diagnose problems.              |
| Chapter 14: Advanced Settings                | Instructions for using the web interface to configure email, CLI, and XML settings.                                                          |
| Chapter 15: Branding the EDS Unit            | Instructions for customizing the device.                                                                                                     |
| Chapter 16: Updating Firmware               | Instructions for obtaining the latest firmware and updating the device.                                                                       |
| Appendix B: Binary to Hexadecimal Conversions | Instructions for converting binary values to hexadecimals.                                                                                   |
| Appendix C: sCompliance                      | Lantronix compliance information.                                                                                                             |
### Additional Documentation

Visit the Lantronix web site at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation) for the latest documentation and the following additional documentation.

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EDS4100 Device Server Quick Start Guide</strong></td>
<td>Information about the EDS hardware installation and initial configuration of your EDS device.</td>
</tr>
<tr>
<td><strong>EDS4100 Device Server Command Reference</strong></td>
<td>Instructions for accessing Command Mode (the command line interface) using a Telnet connection or through the serial port. Detailed information about the commands. Also provides details for XML configuration and status.</td>
</tr>
<tr>
<td><strong>EDS8/16/32PR Device Server Quick Start Guide</strong></td>
<td>Information about the EDS hardware installation and initial configuration of your EDS device.</td>
</tr>
<tr>
<td><strong>EDS8/16/32PR Device Server Command Reference</strong></td>
<td>Instructions for accessing Command Mode (the command line interface) using a Telnet connection or through the serial port. Detailed information about the commands. Also provides details for XML configuration and status.</td>
</tr>
<tr>
<td><strong>DeviceInstaller Online Help</strong></td>
<td>Instructions for using the Lantronix Windows® based DeviceInstaller application to locate the device and to view its current settings.</td>
</tr>
<tr>
<td><strong>Com Port Redirector Quick Start and Online Help</strong></td>
<td>Instructions for using the Lantronix Windows based utility to create virtual com ports.</td>
</tr>
<tr>
<td><strong>Secure Com Port Redirector User Guide</strong></td>
<td>Instructions for using the Lantronix Windows based utility to create secure virtual com ports.</td>
</tr>
</tbody>
</table>
2: Introduction

This chapter introduces the Lantronix EDS family of device servers. It provides an overview of the product, lists the key features, and describes the applications for which they are suited.

The EDS is a unique, hybrid Ethernet terminal and multi-port device server product designed to remotely access and manage virtually all of your IT/networking equipment and servers. It is also designed to provide connectivity for edge devices such as medical equipment, kiosks, POS/retail terminals, security equipment, and more.

The EDS devices contain all the components necessary to deliver full network connectivity to virtually any kind of serial device. They boast a reliable TCP/IP protocol stack, a variety of remote management capabilities, and an innovative design based on the leading-edge Lantronix Evolution OS® software.

Delivering a data center-grade, programmable device computing and networking platform for integrating edge equipment into the enterprise network. Rack-mountable EDS models are available in 8, 16, and 32 port configurations. Desktop EDS models are available in 4, 8, and 16 port configurations.

This chapter contains the following sections:

◆ EDS4100 Overview
◆ EDS8PR, EDS16PR, and EDS32PR Overview
◆ Key Features
◆ Protocol Support
◆ Evolution OS™ Application
◆ Additional Features
◆ Configuration Methods
◆ Addresses and Port Numbers
◆ Product Information Label
EDS4100 Overview

The EDS4100 is a compact device server that allows you to network-enable asynchronous RS-232 and RS-422/485 serial devices. It can deliver fully transparent RS-232/422 point-to-point connections and RS-485 multi-drop connections without requiring modifications to existing software or hardware in your application.

- Ports 1 through 4 support RS-232 devices.
- Ports 1 and 3 also support RS-422/485.

Note: RS-485 circuits support 32 full-load devices or 128 quarter-load devices. Each RS-485 port, however, counts as one device, leaving up to 31 full-load or 127 quarter-load devices that can be connected to the RS-485 circuit.

The EDS4100 device server supports the Power-over-Ethernet (PoE) standard. With PoE, power is supplied to the EDS over the Ethernet cable, by either an Ethernet switch or a midspan device. Being able to draw power through the Ethernet cable eliminates power supply and cord clutter. It also allows the EDS to be located in areas where power is not typically available.

Key Features

The key features of the EDS4100 include:

- Dual-purpose Ethernet terminal server and device server design
- Four serial ports with hardware handshaking signals
- RS-232 and RS-422/485
- One RJ45 Ethernet port
- IEEE 802.3af standard for Power-over-Ethernet (PoE)
- 8 MB Flash memory
- 32 MB Random Access Memory (RAM)
- Lantronix Evolution OS software
- AES, SSH, or SSL secure data encryption
- Three configuration methods (Web, command line, and XML)
- Print server functionality (LPR/LPD)

See Chapter 3: Installation of EDS4100 for installation instructions.
EDS8PR, EDS16PR, and EDS32PR Overview

The EDS8PR (8 serial ports), EDS16PR (16 serial ports), and EDS32PR (32 serial ports) are compact easy-to-use, rack-mountable device servers that give you the ability to network-enable asynchronous RS-232 serial devices. They provide fully transparent RS-232 point-to-point connections without requiring modifications to existing software or hardware components in your application.

Figure 2-2  EDS8PR Device Server

Figure 2-3  EDS16PR Device Server

Figure 2-4  EDS32PR Device Server
Key Features

The key features of the EDS8PR, EDS16PR, and EDS32PR include:

- Dual-purpose Ethernet terminal server and device server design
- 8 (EDS8PR), 16 (EDS16PR) or 32 (EDS32PR) serial ports with hardware handshaking signals
- RS-232 support
- One RJ45 Ethernet port
- 8 MB Flash memory
- 32 MB Random Access Memory (RAM)
- Lantronix Evolution OS software
- A dedicated console port
- AES, SSH, or SSL secure data encryption
- Three configuration methods (Web, command line, and XML)
- Print server functionality (LPR/LPD)

Applications

EDS device server connects serial devices such as those listed below to Ethernet networks using the IP protocol family.

- ATM machines
- Data display devices
- Security alarms and access control devices
- Modems
- Time/attendance clocks and terminals
- Patient monitoring equipment
- Medical instrumentation
- Industrial Manufacturing/Automation systems
- Building Automation equipment
- Point of Sale Systems

Protocol Support

The EDS device server contains a full-featured TCP/IP stack. Supported protocols include:

- ARP, IP, UDP, TCP, ICMP, BOOTP, DHCP, AutoIP, Telnet, DNS, FTP, TFTP, HTTP/HTTPS, SSH, SSL/TLS, SNMP, SMTP, RSS, and Syslog for network communications and management.
- TCP, UDP, TCP/AES, UDP/AES, Telnet, SSH and SSL/TLS for tunneling to the serial port.
- TFTP, FTP, and HTTP for firmware upgrades and uploading files.
Evolution OS™ Application

The EDS device server incorporates the Lantronix Evolution operating system (OS). Key features of the Evolution OS include:

- Built-in Web server for configuration and troubleshooting from Web-based browsers
- CLI configurability
- SNMP management
- XML data transport and configurability
- Really Simple Syndication (RSS) information feeds
- Enterprise-grade security with SSL and SSH
- Comprehensive troubleshooting tools

Additional Features

Modem Emulation

In modem emulation mode, the EDS can replace dial-up modems. The unit accepts modem AT commands on the serial port, and then establishes a network connection to the end device, leveraging network connections and bandwidth to eliminate dedicated modems and phone lines.

Web-Based Configuration and Troubleshooting

Built upon Internet-based standards, the EDS enables you to configure, manage, and troubleshoot through a browser-based interface accessible anytime from anywhere. All configuration and troubleshooting options are launched from a web interface. You can access all functions via a Web browser, for remote access. As a result, you decrease downtime (using the troubleshooting tools) and implement configuration changes (using the configuration tools).

Command-Line Interface (CLI)

Making the edge-to-enterprise vision a reality, the EDS uses industry-standard tools for configuration, communication, and control. For example, the Evolution OS software uses a Command Line Interface (CLI) whose syntax is very similar to that used by data center equipment such as routers and hubs.

SNMP Management

The EDS supports full SNMP management, making it ideal for applications where device management and monitoring are critical. These features allow networks with SNMP capabilities to correctly diagnose and monitor EDS devices.

XML-Based Architecture and Device Control

XML is a fundamental building block for the future growth of M2M networks. The EDS supports XML-based configuration setup records that make device configuration transparent to users and administrators. The XML is easily editable with a standard text or XML editor.
Really Simple Syndication (RSS)

The EDS supports Really Simple Syndication (RSS) for streaming and managing on-line content. RSS feeds all the configuration changes that occur on the device. An RSS aggregator then reads (polls) the feed. More powerful than simple email alerts, RSS uses XML as an underlying Web page transport and adds intelligence to the networked device, while not taxing already overloaded email systems.

Enterprise-Grade Security

Evolution OS software provides the EDS the highest level of networking security possible. This ‘data center grade’ protection ensures that each device on the M2M network carries the same level of security as traditional IT networking equipment in the corporate data center.

With built-in SSH and SSL, secure communications can be established between the serial ports and the remote end device or application. By protecting the privacy of serial data transmitted across public networks, users can maintain their existing investment in serial technology, while taking advantage of the highest data-protection levels possible.

SSH and SSL are able to do the following:

- Verify the data received came from the proper source
- Validate that the data transferred from the source over the network has not changed when it arrives at its destination (shared secret and hashing)
- Encrypt data to protect it from prying eyes and nefarious individuals
- Provide the ability to run popular M2M protocols over a secure SSH or SSL connection

In addition to keeping data safe and accessible, the EDS has robust defenses to hostile Internet attacks such as denial of service (DoS), which can be used to take down the network. Moreover, the EDS cannot be used to bring down other devices on the network.

You can use the EDS with the Lantronix Secure Com Port Redirector (SCPR) to encrypt COM port-based communications between PCs and virtually any electronic device. SCPR is a Windows application that creates a secure communications path over a network between the computer and serial-based devices that are traditionally controlled via a COM port. With SCPR installed at each computer, computers that were formerly “hard-wired” by serial cabling for security purposes or to accommodate applications that only understood serial data can instead communicate over an Ethernet network or the Internet.

Terminal Server/Device Management

Remote offices can have routers, PBXs, servers and other networking equipment that require remote management from the corporate facility. The EDS easily attaches to the serial ports on a server, Private Branch Exchange (PBX), or other networking equipment to deliver central, remote monitoring and management capability.
Troubleshooting Capabilities
The EDS offers a comprehensive diagnostic toolset that lets you troubleshoot problems quickly and easily. Available from the Web Manager, CLI, and XML interfaces, the diagnostic tools let you:

- View critical hardware, memory, MIB-II, buffer pool, and IP socket information.
- Perform ping and traceroute operations.
- Conduct forward or backup DNS lookup operations.
- View all processes currently running on the EDS, including CPU utilization and total stack space available.

Configuration Methods
After installation, the EDS requires configuration. For the unit to operate correctly on a network, it must have a unique IP address on the network. There are four basic methods for logging into the EDS and assigning IP addresses and other configurable settings:

- **DeviceInstaller**: Configure the IP address and related settings and view current settings on the using a Graphical User Interface (GUI) on a PC attached to a network. See *Chapter 5: Using DeviceInstaller*.
- **Web Manager**: Through a web browser, configure the EDS settings using the Lantronix Web Manager. See *Chapter 6: Configuration Using Web Manager*.
- **Command Mode**: There are two methods for accessing Command Mode (CLI): making a Telnet connection or connecting a terminal (or a PC running a terminal emulation program) to the unit’s serial port. (See the appropriate *EDS Device Server Command Reference* for instructions and available commands. Lantronix documentation is available at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation).)
- **XML**: The EDS supports XML-based configuration and setup records that make device configuration transparent to users and administrators. XML is easily editable with a standard text or XML editor. (See the appropriate *EDS Device Server Command Reference* for instructions and available commands. Lantronix documentation is available at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation).)

Addresses and Port Numbers

Hardware Address
The hardware address is also referred to as the Ethernet address or MAC address. The first three bytes of the Ethernet address are fixed and read as either 00-20-4A or 08-04-13, identifying the unit as a Lantronix product. The fourth, fifth, and sixth bytes are unique numbers assigned to each unit.

![Figure 2-5 Sample Hardware Address](image_url)

<table>
<thead>
<tr>
<th>Ethernet Address</th>
<th>00-20-4A-14-01-18</th>
<th>or</th>
<th>00:20:4A:14:01:18</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>08-04-13-14-01-18</td>
<td>or</td>
<td>08:04:13:14:01:18</td>
</tr>
</tbody>
</table>
IP Address
Every device connected to an IP network must have a unique IP address. This address references the specific unit.

Port Numbers
Every TCP connection and every UDP datagram is defined by a destination and source IP address, and a destination and source port number. For example, a Telnet server commonly uses port number 23.

The following is a list of the default server port numbers running on the EDS device server.
- TCP Port 22: SSH Server (Command Mode configuration)
- TCP Port 23: Telnet Server (Command Mode configuration)
- TCP Port 80: HTTP (Web Manager configuration)
- TCP Port 443: HTTPS (Web Manager configuration)
- UDP Port 161: SNMP
- TCP Port 21: FTP
- UDP Port 69: TFTP
- UDP Port 514: Syslog
- TCP Port 515: LPD
- UDP Port 30718: LDP (Lantronix Discovery Protocol) port
- TCP/UDP Port 10001: Tunnel 1
- TCP/UDP Port 10002: Tunnel 2

Note: Multi-port products include one or more additional supported ports and tunnels with default sequential numbering. For instance: TCP/UDP Port 10002: Tunnel 2, TCP/UDP Port 10003: Tunnel 3, etc.

Product Information Label
The product information label on the unit contains the following information about the specific unit:
- Bar Code
- Revision
- Date of Manufacture
- Country of Manufacture
- Hardware Address (MAC address or serial number)
- Manufacturing Date Code
- Device ID
3: **Installation of EDS4100**

This chapter describes how to install the EDS4100 device server.

**Package Contents**

Your EDS4100 package includes the following items:

- One EDS4100 device server.
- One DB9F-to-DB9F null modem cable.
- A printed Quick Start Guide.

Your package may also include a power supply.

**User-Supplied Items**

To complete your EDS4100 installation, you need the following items:

- RS-232 and/or RS-422/485 serial devices that require network connectivity:
- A serial cable for each serial device. One end of the cable must have a female DB9 connector for the EDS4100 serial port.
- To connect an EDS4100 serial port to another DTE device, you will need a null modem cable, such as the one supplied in your EDS4100 package.
- To connect the EDS4100 serial port to a DCE device, you will need a straight-through (modem) cable.
- An available connection to your Ethernet network and an Ethernet cable.
- A working power outlet if the unit will be powered from an AC outlet.
Identifying Hardware Components

The following two figures show the front and back of the EDS4100.

**Figure 3-1 Front View of the EDS4100**

**Figure 3-2 Back View of the EDS4100**
Serial Ports

The front of the EDS4100 has four male DB9 serial ports. These ports allow you to connect up to four standard serial devices:

- All four serial ports support RS-232 devices. See Figure 3-3 for pin assignments.
- Serial ports 1 and 3 also support RS-422 and RS-485 serial devices. See Figure 3-4 for pin assignments.
- All four serial ports are configured as DTE.
- Ports 1 & 3 support up to 921600
- Ports 2 & 4 support up to 230400

**Figure 3-3  RS-232 Serial Port Pins (Serial Ports 1, 2, 3, 4)**

**Figure 3-4  RS-422/RS-485 Serial Port Pins**

*Note:* Multi-drop connections are supported in 2-wire mode only.
**Ethernet Port**

The back panel of the EDS4100 provides an RJ45 Ethernet port. This port can connect to an Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) network. The Speed LED on the back of the EDS4100 shows the connection of the attached Ethernet network. The EDS4100 can be configured to operate at a fixed Ethernet speed and duplex mode (half- or full-duplex) or otherwise (by default) auto-negotiate the connection to the Ethernet network.

**Terminal Block Connector**

The back of the EDS4100 has a socket for a terminal block screw connector (not included) for attaching to an appropriate power source, such as those used in automation and manufacturing industries. The terminal block connector supports a power range from 42 VDC to 56 VDC. It can be used with the EDS4100's barrel power connector and PoE capabilities as a redundant power source to the unit. Vendors who do supply this connector can be found by doing a web search for part 'Phoenix 1803581 MC 1,5/ 3-ST-3,81'.

![Figure 3-5 Terminal Block Connector Pin Assignments](image)

**LEDs**

Light-emitting diodes (LEDs) on the front and back panels show status information.

- **Back panel** - Each serial port has a Transmit and a Receive LED. The Ethernet connector has Speed and Activity LEDs. In addition, the back panel has a Power LED and a Status LED.
- **Front panel** - The front panel has a green Power LED.
- The table below describes the LEDs on the back of the EDS4100.

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit (green)</td>
<td>Blinking = EDS is transmitting data on the serial port.</td>
</tr>
<tr>
<td>Receive (yellow)</td>
<td>Blinking = EDS is receiving data on the serial port.</td>
</tr>
<tr>
<td>Power (green)</td>
<td>On = EDS receiving power.</td>
</tr>
<tr>
<td>Status (yellow)</td>
<td>Fast blink = initial startup (loading OS).</td>
</tr>
<tr>
<td>Speed (yellow)</td>
<td>On = EDS is connected to a 100 Mbps Fast Ethernet network.</td>
</tr>
<tr>
<td>Activity (green)</td>
<td>Blink = EDS sending data to or receiving data from the Ethernet network.</td>
</tr>
</tbody>
</table>

**Reset Button**

The reset button is on the back of the EDS4100, to the left of the power connector. Pressing this button reboots the EDS4100 and terminates all serial and Ethernet port data activity.
Physically Installing the EDS4100

Finding a Suitable Location

- Place the EDS4100 on a flat horizontal or vertical surface. The EDS4100 comes with mounting brackets installed for vertically mounting the unit, for example, on a wall.
- If using AC power, avoid outlets controlled by a wall switch.

Connecting the EDS4100

Observe the following guidelines when attaching serial devices:

- All four EDS4100 serial ports support RS-232 devices.
- Alternatively, ports 1 and 3 support RS-422/485 devices.
- To connect an EDS4100 serial port to another DTE device, use a null modem cable.
- To connect the EDS4100 serial port to a DCE device, use a straight-through (modem) cable.

Connect the EDS4100 to one or more serial devices.

1. Power off the serial devices.
2. Attach a serial cable between the EDS4100 and each serial device.
3. Connect an Ethernet cable between the EDS4100 Ethernet port and your Ethernet network.
4. Power-up the EDS4100. Use one or more of the following methods.
   
   These power-up methods can be used in combination to provide redundant backup power to the unit.
   - **PoE**: Power is supplied over the Ethernet cable by an Ethernet switch or a mid-span device.
   - **Barrel power connector**: The barrel power connector supports a power range of 9 to 30 VDC. Insert the round end of the supplied power cord into the barrel power connector on the back of the EDS4100. Plug the other end into an AC wall outlet.
   - **Terminal block connector**: The terminal block connector supports a power range of 42 VDC to 56 VDC. Attach the power source to the terminal block connector on the back of the EDS4100.
   
   As soon as you plug it in, the EDS4100 powers up automatically, the self-test begins, and the Evolution OS application starts.
5. Power up the serial devices.
Figure 3-7 Example of EDS4100 Connections

- Power
- Serial Devices
- 10/100 Base-T Ethernet
This chapter describes installing the EDS8PR, EDS16PR and EDS32PR device servers.

**Package Contents**

Your EDS package includes the following items:
- One EDS unit (EDS8PR, EDS16PR or EDS32PR).
- One RJ45-to-DB9F serial cable.
- A printed Quick Start guide.
- Your package may also include a power supply.

**User-Supplied Items**

To complete your EDS8/16/32PR installation, you need the following items:
- RS-232 serial devices that require network connectivity. Each EDS8/16/32PR serial port supports a directly connected RS-232 serial device.
- A serial cable for each serial device. All devices attached to the EDS device ports must support the RS-232C (EIA-232) standard. Category 5 cabling with RJ45 connections is used for the device port connections.

*Note:* To connect an EDS8/16/32PR serial port to a DTE device, you need a DTE cable, such as the one supplied in your EDS8/16/32PR package, or an RJ45 patch cable and DTE adapter. To connect the EDS8/16/32PR serial port to a DCE device, you need a DCE (modem) cable, or an RJ45 patch cable and DTE adapter.

For a list of the Lantronix cables and adapters you can use with the EDS8/16/32PR, see Appendix C: Lantronix Cables and Adapters.
- An available connection to your Ethernet network and an Ethernet cable.
- A working power outlet.
Identifying Hardware Components

The following two figures show the components on the front and back of the EDS16PR.

Figure 4-1  Front View of the EDS16PR

Figure 4-2  Back View of the EDS16PR

Serial Ports
All EDS serial ports are configured as DTE and support up to 230,400 baud.

- The EDS8PR has 8 serial ports.
- The EDS16PR has 16 serial ports.
- The EDS32PR has 32 serial ports.
Console Port
The front panel has an RJ45 Console port configured as DTE and supports up to 230,400 baud.

Figure 4-3  RJ45 Serial Port

Ethernet Port
The back panel has an RJ45 Ethernet port. This port can connect to an Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) network.

The Speed LED on the back panel shows the connection speed of the connected Ethernet network.

You can configure the EDS to operate at a fixed Ethernet speed and duplex mode (half- or full-duplex) or auto-negotiate the connection to the Ethernet network.

LEDs
Light-emitting diodes (LEDs) on the front and back panels show status information.

- **Front panel.** The front panel has a green Power LED.
- **Back panel.** Each serial port has a Transmit and a Receive LED. The Ethernet connector has Speed and Activity LEDs. There is also a Power LED and a Status LED.
The table below describes the LEDs on the back of the EDS.

### Table 4-4 Back Panel LEDs

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit (green)</td>
<td>Blinking = EDS is transmitting data on the serial port.</td>
</tr>
<tr>
<td>Receive (yellow)</td>
<td>Blinking = EDS is receiving data on the serial port.</td>
</tr>
<tr>
<td>Power (green)</td>
<td>On = EDS is receiving power.</td>
</tr>
</tbody>
</table>
| Status (yellow) | Fast blink = initial startup (loading OS).  
               | Slow blink (once per second) = operating system startup.  
               | On = unit has finished booting.                                            |
| Speed (yellow)  | On = EDS is connected to a 100 Mbps Fast Ethernet network.                  |
|               | Off = EDS is connected to a 10 Mbps Ethernet network.                       |
| Activity (green) | Blink = EDS is sending data to or receiving data from the Ethernet network. |

**Reset Button**

The reset button is on the back of the EDS to the left of the power connector.
Pressing this button for 2-to-3 seconds reboots the EDS8/16/32PR and terminates all data activity occurring on the serial and Ethernet ports.

**Installing the EDS8/16/32PR**

**Finding a Suitable Location**
You can install the EDS8/16/32PR either in an EIA-standard 19-inch rack (1U tall) or as a desktop unit. If using AC power, avoid outlets controlled by a wall switch.

**Connecting the EDS8/16/32PR**

1. Power off the serial devices that will be connected to the EDS8/16/32PR.
2. Attach a CAT 5 serial cable between the EDS8/16/32PR and your serial device. For a list of cables and adapters you can use with the EDS8/16/32PR, see Appendix C: Lantronix Cables and Adapters.
3. Connect an Ethernet cable between the EDS8/16/32PR Ethernet port and your Ethernet network.
4. Insert the power cord into the back of the EDS8/16/32PR. Plug the other end into an AC wall outlet. After power-up, the self-test begins.
5. Power up the serial devices.
Figure 4-5 Example of EDS16PR Connections

- 10/100 Base-T Ethernet
- Serial Device
- Power

4: Installation of EDS8PR, EDS16PR and EDS32PR
5: Using DeviceInstaller

This chapter covers the steps for locating a device and viewing its properties and details. The Lantronix DeviceInstaller application is a free utility program provided by Lantronix that discovers, configures, upgrades, and manages Lantronix device servers. It can be downloaded from the Lantronix website at www.lantronix.com/support/downloads.html. For instructions on using the DeviceInstaller application to configure the IP address, related settings or for more advanced features, see the DeviceInstaller Online Help.

Note: AutoIP generates a random IP address in the range of 169.254.0.1 to 169.254.255.254 if no BOOTP or DHCP server is found.

Installing DeviceInstaller

2. Run the executable to start the installation process.
3. Respond to the installation wizard prompts. (If prompted to select an installation type, select Typical.)

Accessing the EDS Unit Using DeviceInstaller

The device's factory default username is "admin" and factory default password is the last 8 characters of the Device ID (for devices manufactured after January 1, 2020) or "PASS" (for all older devices).

Note: Make note of the MAC address. It may be needed to perform various functions in the DeviceInstaller application.

1. Click Start > All Programs > Lantronix > DeviceInstaller 4.4 > DeviceInstaller.
   When DeviceInstaller starts, it will perform a network device search.
2. Click Search to perform additional searches, as desired.
3. Expand the EDS folder by clicking the + symbol next to the EDS folder icon. The list of available Lantronix EDS device types appear.
4. Click the desired EDS product type. A list of all URLs and IP addresses for online EDS devices will appear.
5. Select the EDS unit by clicking the EDS device URL or IP address to view its configuration.
6. On the right page, click the Device Info tab. The current EDS configuration appears. This is only a subset of the full configuration; the complete configuration may be accessed via Web Manager, CLI, or XML.

Note: The settings are Display Only in this table unless otherwise noted.
### Table 5-1 Device Details Summary

<table>
<thead>
<tr>
<th><strong>Current Settings</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name identifying the EDS device server.</td>
</tr>
<tr>
<td>DHCP Device Name</td>
<td>Shows the name associated with the current IP address, if the IP address was obtained dynamically.</td>
</tr>
<tr>
<td>Group</td>
<td>Configurable field. Enter a group to categorize the EDS device server. Double-click the field, type in the value, and press Enter to complete. This group name is local to this PC and is not visible on other PCs or laptops using the DeviceInstaller application.</td>
</tr>
<tr>
<td>Comments</td>
<td>Configurable field. Enter comments for the EDS device server. Double-click the field, type in the value, and press Enter to complete. This description or comment is local to this PC and is not visible on other PCs or laptops using DeviceInstaller.</td>
</tr>
<tr>
<td>Device Family</td>
<td>Shows the EDS device family type as “EDS”.</td>
</tr>
<tr>
<td>Short Name</td>
<td>Shows EDS4100 by default (for example).</td>
</tr>
<tr>
<td>Long Name</td>
<td>Shows “Lantronix EDS4100” by default (for example).</td>
</tr>
<tr>
<td>Type</td>
<td>Shows the specific device type, such as “EDS4100”.</td>
</tr>
<tr>
<td>ID</td>
<td>Shows the EDS ID embedded within the unit.</td>
</tr>
<tr>
<td>Hardware Address</td>
<td>Shows the EDS hardware (MAC) address.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Shows the firmware currently installed on the EDS.</td>
</tr>
<tr>
<td>Extended Firmware Version</td>
<td>Provides additional information on the firmware version.</td>
</tr>
<tr>
<td>Online Status</td>
<td>Shows the EDS status as Online, Offline, Unreachable (if the EDS is on a different subnet), or Busy (if the EDS is currently performing a task).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Shows the EDS device’s current IP address. To change the IP address, click the Assign IP button on the DeviceInstaller menu bar.</td>
</tr>
<tr>
<td>IP Address was Obtained</td>
<td>Displays Dynamically if the EDS automatically received an IP address (e.g., from DHCP). Displays Statically if the IP address was configured manually.</td>
</tr>
<tr>
<td></td>
<td>If the IP address was assigned dynamically, the following fields appear:</td>
</tr>
<tr>
<td></td>
<td>✦ Obtain via DHCP with value of True or False.</td>
</tr>
<tr>
<td></td>
<td>✦ Obtain via BOOTP with value of True or False.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Shows the subnet mask specifying the network segment on which the EDS resides.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Shows the IP address of the router of this network. There is no default.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Shows the types and URL of interfaces available.</td>
</tr>
<tr>
<td>Number of Serial Serial Ports</td>
<td>Shows the number of serial ports on this EDS unit.</td>
</tr>
<tr>
<td>Supports Configurable Pins</td>
<td>Shows False, indicating configurable pins are not available on the EDS unit.</td>
</tr>
<tr>
<td>Supports Email Triggers</td>
<td>Shows True, indicating email triggers are available on the EDS unit.</td>
</tr>
<tr>
<td>Telnet Supported</td>
<td>Indicates whether Telnet is enabled on this EDS unit. Shows True.</td>
</tr>
<tr>
<td>Telnet Port</td>
<td>Shows the EDS port for Telnet sessions.</td>
</tr>
<tr>
<td>Web Port</td>
<td>Shows the EDS port for Web Manager configuration.</td>
</tr>
<tr>
<td>Firmware Upgradable</td>
<td>Shows True, indicating the EDS firmware is upgradable as newer versions become available.</td>
</tr>
</tbody>
</table>
This chapter describes how to configure the EDS device server using Web Manager, the Lantronix browser-based configuration tool. The unit’s configuration is stored in nonvolatile memory and is retained without power. All changes take effect immediately, unless otherwise noted. It contains the following sections:

- Accessing Web Manager
- Web Manager Page Components
- Navigating the Web Manager
- Summary of Web Manager Pages

### Accessing Web Manager

**Note:** You can also access the Web Manager by selecting the Web Configuration tab on the DeviceInstaller window.

**To access Web Manager, perform the following steps:**

1. Open a standard web browser. Lantronix supports the latest version of Internet Explorer, Mozilla Suite, Mozilla Firefox, Safari, Chrome or Opera.

2. Enter the IP address of the EDS unit in the address bar. The IP address may have been assigned manually using the DeviceInstaller application (see Chapter 5: Using DeviceInstaller) or automatically by DHCP.

3. Enter your username and password. The factory default username is "admin" and factory default password is the last 8 characters of the Device ID (for devices manufactured after January 1, 2020) or "PASS" (for all older devices). The Device Status web page shown in Figure 6-2 displays configuration, network settings, line settings, tunneling settings, and product information.

**Note:** The Logout button is available on the upper right of any web page. Logging out of the web page would force re-authentication to take place the next time the web page is accessed.
Device Status Page
The Device Status page is the first page that appears after you log into Web Manager. It also appears when you click Status in the menu bar (Figure 6-2).

Figure 6-2  Web Manager Home Page
Web Manager Page Components

The layout of a typical Web Manager page is below.

The menu bar always appears at the left side of the page, regardless of the page shown. The menu bar lists the names of the pages available in the Web Manager. To bring up a page, click it in the menu bar.

The main area of the page has these additional sections:

- At the very top, many pages, such as the one in the example above, enable you to link to sub pages. On some pages, you must also select the item you are configuring, such as a line or a tunnel.
- In the middle of many pages, you can select or enter new configuration settings. Some pages show status or statistics in this area rather than allow you to enter settings.
- At the bottom of most pages, the current configuration is displayed. In some cases, you can reset or clear a setting.
- The information or help area shows information or instructions associated with the page.
- A Logout button is available at the upper right corner of every web page. In Chrome or Safari, it is necessary to close out of the browser to logout. If necessary, reopen the browser to log back in.
- The footer appears at the very bottom of the page. It contains copyright information and a link to the Lantronix home page.
Navigating the Web Manager

The Web Manager provides an intuitive point-and-click interface. A menu bar on the left side of each page provides links you can click to navigate from one page to another. Some pages are read-only, while others let you change configuration settings.

*Note:* There may be times when you must reboot the EDS for the new configuration settings to take effect. The chapters that follow indicate when a change requires a reboot.

<table>
<thead>
<tr>
<th>Web Manager Page</th>
<th>Description</th>
<th>See Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Shows product information and network, line, and tunneling settings.</td>
<td>39</td>
</tr>
<tr>
<td>CLI</td>
<td>Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.</td>
<td>129</td>
</tr>
<tr>
<td>Clock</td>
<td>Allows you to view and configure date and time for the device by either SNTP or manual settings. <em>Note:</em> This feature is available as Clock for EDS8/16/32 PR and RTC (see below) for EDS4100.</td>
<td>123</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Lets you perform various diagnostic procedures.</td>
<td>115</td>
</tr>
<tr>
<td>DNS</td>
<td>Shows the current configuration of the DNS subsystem and the DNS cache.</td>
<td>74</td>
</tr>
<tr>
<td>Email</td>
<td>Shows email statistics and lets you clear the email log, configure email settings, and send an email.</td>
<td>127</td>
</tr>
<tr>
<td>Filesystem</td>
<td>Shows file system statistics and lets you browse the file system to view a file, create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.</td>
<td>105</td>
</tr>
<tr>
<td>FTP</td>
<td>Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.</td>
<td>76</td>
</tr>
<tr>
<td>Host</td>
<td>Lets you view and change settings for a host on the network.</td>
<td>73</td>
</tr>
<tr>
<td>HTTP</td>
<td>Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.</td>
<td>79</td>
</tr>
<tr>
<td>IP Address Filter</td>
<td>Lets you specify all the IP addresses and subnets that are allowed to send data to this device.</td>
<td>113</td>
</tr>
<tr>
<td>Line</td>
<td>Shows statistics and lets you change the current configuration and Command mode settings of a serial line.</td>
<td>47</td>
</tr>
<tr>
<td>LPD</td>
<td>Shows LPD (Line Printer Daemon) Queue statistics and lets you configure the LPD and print a test page.</td>
<td>85</td>
</tr>
<tr>
<td>Modbus</td>
<td>Shows the current connection status of the Modbus servers listening on the TCP ports and lets you configure the Modbus settings for EDS4100.</td>
<td>102</td>
</tr>
<tr>
<td>Network</td>
<td>Shows status and lets you configure the network interface.</td>
<td>43</td>
</tr>
<tr>
<td>Protocol Stack</td>
<td>Lets you perform lower level network stack-specific activities.</td>
<td>108</td>
</tr>
<tr>
<td>Query Port</td>
<td>Lets you change configuration settings for the query port.</td>
<td>114</td>
</tr>
<tr>
<td>RSS</td>
<td>Lets you change current Really Simple Syndication (RSS) settings.</td>
<td>84</td>
</tr>
<tr>
<td>Web Manager Page (continued)</td>
<td>Description</td>
<td>See Page</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>RTC</td>
<td>Real Time Clock (RTC) allows you to view and configure date and time for the device by either SNTP or manual settings. <em>Note:</em> This feature is available as Clock for EDS8/16/32 PR (see above).</td>
<td>75</td>
</tr>
<tr>
<td>SNMP</td>
<td>Lets you change the current Simple Network Management Protocol (SNMP) configuration settings.</td>
<td>75</td>
</tr>
<tr>
<td>SSH</td>
<td>Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.</td>
<td>88</td>
</tr>
<tr>
<td>SSL</td>
<td>Lets you upload an existing certificate or create a new self-signed certificate.</td>
<td>96</td>
</tr>
<tr>
<td>Syslog</td>
<td>Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.</td>
<td>78</td>
</tr>
<tr>
<td>System</td>
<td>Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.</td>
<td>125</td>
</tr>
<tr>
<td>Terminal</td>
<td>Lets you change current settings for a terminal.</td>
<td>70</td>
</tr>
<tr>
<td>TFTP</td>
<td>Shows statistics and lets you change the current configuration for the Trivial File Transfer Protocol (TFTP) server.</td>
<td>77</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Lets you change the current configuration settings for a tunnel.</td>
<td>51</td>
</tr>
<tr>
<td>XML</td>
<td>Lets you export XML configuration and status records, and import XML configuration records.</td>
<td>131</td>
</tr>
</tbody>
</table>
7: Network Settings

This chapter describes how to access, view, and configure network settings from the Network web page. The Network web page contains sub-menus that enable you to view and configure the Ethernet network interface and link.

This chapter contains the following sections:

- Network 1 (eth0) Interface Status
- Network 1 (eth0) Interface Configuration
- Network 1 Ethernet Link

Network 1 (eth0) Interface Status

This page shows the status of the Ethernet network interface.

To view the network interface status:

1. Click Network on the menu then click Network 1 > Interface > Status at the top of the page. The Network 1 (eth0) Interface Status page appears.

![Figure 7-1 Network 1 (eth0) Interface Status](image)

### Network 1 (eth0) Interface Status

<table>
<thead>
<tr>
<th></th>
<th>Current</th>
<th>After Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTP Client</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>On [Renew]</td>
<td>On</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.19.100.199 (DHCP)</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td>Network Mask</td>
<td>255.255.0.0 (DHCP)</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>172.19.0.1 (DHCP)</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td>Hostname</td>
<td>&lt;None&gt;</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td>Domain</td>
<td>eng.lantronix.com (DHCP)</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td>DNS Suffix Search List</td>
<td>eng.lantronix.com, int.lantronix.com, lantronix.com</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td>DHCP Client ID</td>
<td>[0xd6, 0x01]</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>MTU</td>
<td>1500</td>
<td>&lt;DHCP&gt;</td>
</tr>
</tbody>
</table>
Network 1 (eth0) Interface Configuration

This page shows the configuration settings for the Ethernet connection and lets you change these settings.

To view and configure network interface settings:

1. Click Network on the menu bar and then Network 1 > Interface > Configuration at the top of the page. The Network 1 (eth0) Interface Configuration page appears.

![Figure 7-2 Network 1 (eth0) Interface Configuration](image)

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th><strong>Table 7-3 Network 1 (eth0) Interface Configuration</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network 1 Interface Configuration</strong></td>
</tr>
<tr>
<td><strong>BOOTP Client:</strong> On or Off. At boot up, the device will attempt to obtain an IP address from a BOOTP server.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td>✦ Overrides the configured IP address, network mask, gateway, hostname, and domain.</td>
</tr>
<tr>
<td>✦ When DHCP is On, the system automatically uses DHCP, regardless of whether BOOTP Client is On.</td>
</tr>
</tbody>
</table>
### Network 1 Interface Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP Client</strong></td>
<td>Select <strong>On</strong> or <strong>Off</strong>. At boot up, the device will attempt to lease an IP address from a DHCP server and maintain the lease at regular intervals.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Overrides BOOTP, the configured IP address, network mask, gateway, hostname, and domain.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Enter the device static IP address.</td>
</tr>
<tr>
<td></td>
<td>You may enter it alone, in CIDR format, or with an explicit mask.</td>
</tr>
<tr>
<td></td>
<td>The IP address consists of four octets separated by a period and is used if BOOTP and DHCP are both set to <strong>Off</strong>. Changing this value requires you to reboot the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When DHCP is enabled, the device tries to obtain an IP address from DHCP. If it cannot, the device uses an AutoIP address in the range of 169.254.xxx.xxx.</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>Enter the IP address of the router for this network. Or, clear the field (appears as <strong>&lt;None&gt;</strong>). This address is only used for static IP address configuration.</td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>Enter the device hostname. It must begin with a letter, continue with a sequence of letters, numbers, and/or hyphens, and end with a letter or number.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Enter the device domain name.</td>
</tr>
<tr>
<td><strong>DHCP Client ID</strong></td>
<td>Enter the ID if the DHCP server uses a DHCP ID. The DHCP server’s lease table shows IP addresses and MAC addresses for devices. The lease table shows the Client ID, in hexadecimal notation, instead of the device MAC address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> &quot;Binary&quot; entry mode allows a mixed mode of text and special characters in brackets. For example, &quot;abcd&lt;ctrl&gt;A&quot; would be entered &quot;abcd[0x01]&quot;.</td>
</tr>
<tr>
<td><strong>Primary DNS</strong></td>
<td>IP address of the primary name server. This entry is required if you choose to configure DNS (Domain Name Server) servers.</td>
</tr>
<tr>
<td><strong>Secondary DNS</strong></td>
<td>IP address of the secondary name server.</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>When DHCP is enabled, the MTU size is (usually) provided with the IP address. When not provided by the DHCP server, or using a static configuration, this value is used. The MTU size can be from 576 to 1500 bytes.</td>
</tr>
</tbody>
</table>

3. Click **Submit** to save changes. Some changes to the following settings require a reboot for the changes to take effect:
   - **BOOTP Client**
   - **DHCP Client**
   - **IP Address**
   - **DHCP Client ID**

**Note:** If DHCP or BOOTP fails, AutoIP intervenes and assigns an address. A new DHCP negotiation is attempted every 5 minutes to obtain a new IP address. When the DHCP is enabled, any configured static IP address is ignored.
Network 1 Ethernet Link

This page shows the current negotiated Ethernet settings and lets you change the speed and duplex settings.

To view and configure the Ethernet link:

1. Click Network on the menu bar and then click Network 1 > Link at the top of the page. The Network 1 (eth0) Ethernet Link page appears.

![Network 1 Ethernet Link](image)

The Status table shows the current negotiated settings. The Configuration table shows the current range of allowed settings.

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Table 7-5  Network 1 Ethernet Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network 1-Ethernet Link Settings</strong></td>
</tr>
<tr>
<td>Speed</td>
</tr>
<tr>
<td>Duplex</td>
</tr>
</tbody>
</table>

3. Click Submit. The changes take effect immediately.
8: Line and Tunnel Settings

This chapter describes how to view and configure lines and tunnels. It contains the following sections:

- Line Settings
- Tunnel Settings

Note: The number of lines and tunnels available for viewing and configuration differ between Lantronix products. For example, the XPort® Pro embedded networking module and the EDS1100 device server support only one line while other device networking products (such as the EDS2100, EDS4100, and MatchPort® b/g Pro embedded device servers, XPort® AR embedded networking module, EDS8/16PS and EDS8/16/32PR) provide additional lines and tunnels.

Line Settings

View statistics and configure serial interfaces by using the Line web page. Serial interfaces are referred to as lines in this user guide, and a different number of lines, from 1 to 32, may be available for selection depending on your product.

The following sub-menus may be used for a selected line number:

- Line Statistics—Displays statistics for the selected line number. For example, the bytes received and transmitted, breaks, flow control, parity errors, etc.
- Line Configuration—Enables the change of the name, interface, protocol, baud rates, and parity, etc.
- Line Command Mode—Enables the types of modes, wait time, serial strings, signon message, etc.

Note: The following sections describe the steps to view and configure specific line number settings. These instructions also apply to additional line instances of the device.

Line Statistics

This read-only web page shows the status and statistics for the serial line selected at the top of this page.

1. Select Line on the menu bar. The Line web page appears.
2. Select a line number at the top of the page.
4. Repeat above steps as desired, according to additional line(s) available on your product.

Note: The number of lines and tunnels available for viewing and configuration differ between Lantronix products. For example, the XPort® Pro embedded networking module and the EDS1100 device server support only one line while other device networking products (such as the EDS2100, EDS4100, and MatchPort® b/g Pro embedded device servers, XPort® AR embedded networking module, EDS8/16PS and EDS8/16/32PR) provide additional lines and tunnels.
Line Configuration

This page shows the configuration settings for the serial line selected at the top of the page and lets you change the settings for that serial line.

To configure a specific line:
1. Select Line on the menu bar, if you are not already in the Line web page.
2. Select a line number at the top of the page.
3. Select Configuration. The Configuration page for the selected line appears.

Figure 8-2 Line 1 Configuration
4. Enter or modify the following settings:

Table 8-3 Line Configuration

<table>
<thead>
<tr>
<th>Line - Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>If the Terminal Login Menu feature is being used, enter the name for the line. Leaving this field blank will disable this line from appearing in the Terminal Login Menu. The default Name is blank. See Terminal and Host Settings on page 70 for related configuration information.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface type from the drop-down menu. The default is RS232. <strong>Note:</strong> This option is only supported in XPort Pro, EDS4100, EDS1100 and EDS2100 device servers.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates whether the current line is enabled. To change the status, select Enabled or Disabled from the drop-down menu.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol from the drop-down menu. The default is Tunnel. <strong>Note:</strong> All protocols work in Connect and Accept Mode except the LPD or Tunnel protocol option which is supported only in Accept Mode.</td>
</tr>
<tr>
<td>Baud Rate</td>
<td>Select the baud rate from the drop-down menu. The default is 9600.</td>
</tr>
<tr>
<td>Parity</td>
<td>Select the parity from the drop-down menu. The default is None.</td>
</tr>
<tr>
<td>Data Bits</td>
<td>Select the number of data bits from the drop-down menu. The default is 8.</td>
</tr>
<tr>
<td>Stop Bits</td>
<td>Select the number of stop bits from the drop-down menu. The default is 1.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>Select the flow control from the drop-down menu. The default is None.</td>
</tr>
<tr>
<td>Xon Char</td>
<td>Specify the character to use to start the flow of data when Flow Control is set to Software. Prefix a decimal character with \ or a hexadecimal character with 0x, or provide a single printable character. The default Xon char is 0x11.</td>
</tr>
<tr>
<td>Xoff Char</td>
<td>Specify the character to use to stop the flow of data when Flow Control is set to Software. Prefix a decimal character with \ or a hexadecimal character with 0x, or provide a single printable character. The default Xoff char is 0x13.</td>
</tr>
<tr>
<td>Gap Timer</td>
<td>The driver forwards received serial bytes after the Gap Timer delay from the last character received. By default, the delay is four character periods at the current baud rate (minimum 1 ms).</td>
</tr>
<tr>
<td>Threshold</td>
<td>The driver will also forward received characters after Threshold bytes have been received.</td>
</tr>
</tbody>
</table>

5. Click Submit.

6. Repeat above steps as desired, according to additional line(s) available on your product.
Line Command Mode

Setting the Command Mode enables the CLI on the serial line.

To configure Command Mode on a specific line:

1. Select Line on the menu bar, if you are not already in the Line web page.
2. Select a line number at the top of the page.
3. Select Command Mode. The Command Mode page for the selected line appears.

4. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Table 8-5 Line Command Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Line – Command Mode</strong></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
</tr>
</tbody>
</table>
| Mode                        | Select the method of enabling Command Mode or choose to disable Command Mode.  
|                            | - **Always** = immediately enables Command Mode for the serial line.  
|                            | - **Use Serial String** = enables Command Mode when the serial string is read on the serial line during boot time.  
|                            | - **Disabled** = turns off Command Mode.  |
| Wait Time                   | Enter the wait time for the serial string during boot-up in milliseconds.  |
| Serial String               | Enter the serial string characters. Select a string type.  
|                            | - **Text** = string of bytes that must be read on the Serial Line during boot time to enable Command Mode. It may contain a time element in x milliseconds, in the format \{x\}, to specify a required delay.  
|                            | - **Binary** = string of characters representing byte values where each hexadecimal byte value starts with \0x and each decimal byte value starts with \.  |
| Echo Serial String          | Select **Yes** to enable echoing of the serial string at boot-up.  |
| Signon Message              |                                                        |
Click Submit.

6. Repeat above steps as desired, according to additional line(s) available on your product.

Tunnel Settings

Note: The number of lines and tunnels available for viewing and configuration differ between Lantronix products. For example, XPort Pro and EDS1100 device servers support only one line while other device networking products (such as EDS2100, EDS4100, XPort AR, EDS8/16PS and EDS8/16/32PR devices) provide additional lines and tunnels. The following sections describe the steps to view and configure specific tunnel settings. These instructions also apply to additional tunnel instances of the device.

Tunneling allows serial devices to communicate over a network, without “being aware” of the devices which establish the network connection between them. Tunneling parameters are configured using the Web Manager or Command Mode Tunnel Menu. See Configuration Using Web Manager (on page 38) or the appropriate EDS Device Server Command Reference for the full list of commands.

The EDS supports two tunneling connections simultaneously per serial port. One of these connections is Connect Mode; the other connection is Accept Mode. The connections on one serial port are separate from those on another serial port.

- **Connect Mode:** the EDS actively makes a connection. The receiving node on the network must listen for the Connect Mode’s connection. Connect Mode is disabled by default.
- **Accept Mode:** the EDS device listens for a connection. A node on the network initiates the connection. Accept Mode is enabled by default.
- **Disconnect Mode:** this mode defines how an open connection stops the forwarding of data. The specific parameters to stop the connection are configurable. Once the EDS Disconnect Mode observes the defined event occur, it will disconnect both Accept Mode and Connect Mode connections on that port.

When any character comes in through the serial port, it gets copied to both the Connect Mode connection and the Accept Mode connection (if both are active).

View statistics and configure a specific tunnel by using the Tunnel web page. When you select Tunnel from the Main Menu, tunnels available for your product will display. Select a specific tunnel to configure.
The following sub-menus listed may be used to configure a specific tunnel:

- **Tunnel – Statistics**
- **Tunnel – Serial Settings**
- **Tunnel – Packing Mode**
- **Tunnel – Accept Mode**
- **Tunnel – Connect Mode**
- **Tunnel – Disconnect Mode**
- **Tunnel – Modem Emulation**

The following sections describe the steps to view and configure specific tunnel number settings. These instructions also apply to additional tunnel menu options.

**Tunnel – Statistics**

The EDS logs statistics for tunneling. The **Dropped** statistic shows connections ended by the remote location. The **Disconnects** statistic shows connections ended by the EDS unit.

**To display statistics for a specific tunnel:**

1. Select **Tunnel** on the menu bar. The Tunnel web page appears.
2. Select a tunnel number at the top of the page.
3. Select **Statistics**. The Tunnel Statistics page for the specific tunnel appears.
   
   If a particular tunnel is connected, the following becomes available:
   
   - Identifying information about the tunnel connection (i.e., “Connect 1 Counters”)
   - Address of connection (i.e., “local:10001 -> 172.22.22.22.10001”)
   - **Kill Connection(s) link**: Click this link to terminate this active tunnel connection, as desired.
   - Octets forwarded from Serial
   - Octets forwarded from Network
   - Uptime
4. Repeat above steps as desired, according to additional tunnel(s) available on your product.

Figure 8-6 Tunnel 1 Statistics (1 of 2)

Additional information appears for each active tunnel connection including a link allowing you to terminate the connection.
Tunnel – Serial Settings

Serial line settings are configurable for the corresponding serial line of the specific tunnel. Configure the buffer size to change the maximum amount of data the serial port stores. For any active connection, the device sends the data in the buffer.

The modem control signal DTR on the selected line may be continuously asserted or asserted only while either an Accept Mode tunnel or a Connect Mode tunnel is connected.

To configure serial settings for a specific tunnel:
1. Select Tunnel on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select Serial Settings. The Serial Settings page for the specific tunnel appears.
4. View or modify the following settings:

**Table 8-9 Tunnel - Serial Settings**

<table>
<thead>
<tr>
<th>Tunnel - Serial Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Settings (display only)</td>
<td>Current serial settings for the line.</td>
</tr>
<tr>
<td>Protocol (display only)</td>
<td>The protocol being used on the line. In this case, Tunnel.</td>
</tr>
<tr>
<td>DTR</td>
<td>Select when to assert DTR.</td>
</tr>
<tr>
<td></td>
<td>Unasserted = never asserted</td>
</tr>
<tr>
<td></td>
<td>TruPort = asserted whenever either a connect or an accept mode tunnel connection is active with the Telnet Protocol RFC2217 saying that the remote DSR is asserted.</td>
</tr>
<tr>
<td></td>
<td>Asserted while connected = asserted whenever either a connect or an accept mode tunnel connection is active.</td>
</tr>
<tr>
<td></td>
<td>Continuously asserted = asserted regardless of the status of a tunnel connection.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

6. Repeat above steps as desired, according to additional tunnel(s) available on your product.

**Tunnel – Packing Mode**

Packing Mode takes data from the serial port, packs it together, and sends it over the network. Packing can be configured based on threshold (size in bytes, timeout (milliseconds), or a single character.

Size is set by modifying the threshold field. When the number of bytes reaches the threshold, a packet is sent immediately.

The timeout field is used to force a packet to be sent after a maximum time. The packet is sent even if the threshold value is not reached.

When Send Character is configured, a single printable character or control character read on the Serial Line forces the packet to be sent immediately. There is an optional trailing character parameter which can be specified. It can be a single printable character or a control character.
To configure the Packing Mode for a specific tunnel:

1. Select **Tunnel** on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select **Packing Mode**. The Packing Mode page for the specific tunnel appears.

Depending on the Mode selection, different configurable parameters for the specific tunnel number are presented to the user. The following figures show the display for each of the three packing modes.

**Figure 8-10 Tunnel 1 Packing Mode (Mode = Disable)**

![Image of Tunnel 1 Packing Mode (Mode = Disable)](image)

**Tunnel 1 - Packing Mode**

<table>
<thead>
<tr>
<th>Mode:</th>
<th>Disable</th>
<th>Timeout</th>
<th>Send Character</th>
</tr>
</thead>
</table>

**Figure 8-11 Tunnel 1 Packing Mode (Mode = Timeout)**

![Image of Tunnel 1 Packing Mode (Mode = Timeout)](image)

**Tunnel 1 - Packing Mode**

<table>
<thead>
<tr>
<th>Mode:</th>
<th>Disable</th>
<th>Timeout</th>
<th>Send Character</th>
</tr>
</thead>
</table>

**Threshold:** 512 bytes

**Timeout:** 1000 milliseconds
4. Enter or modify the following settings:

**Table 8-13 Tunnel Packing Mode**

<table>
<thead>
<tr>
<th>Tunnel - Packing Mode Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Select <strong>Disable</strong> to disable Packing Mode completely. Select <strong>Timeout</strong> to send data after the specified time has elapsed. Select <strong>Send Character</strong> to send the queued data when the send character is received.</td>
</tr>
<tr>
<td><strong>Threshold</strong> (Appears for both Timeout and Send Character Modes)</td>
<td>Send the queued data when the number of queued bytes reaches the threshold. When the buffer fills to this specified amount of data in bytes (and the timeout has not elapsed), the device packs the data and sends it out; applies only if the Packing Mode is not Disabled.</td>
</tr>
<tr>
<td><strong>Timeout</strong> (Appears for Timeout Mode)</td>
<td>Enter a time, in milliseconds, for the device to send the queued data after the first character was received. Specifies the time duration in milliseconds; applies only if the Packing Mode is Timeout.</td>
</tr>
<tr>
<td><strong>Send Character</strong> (Appears for Send Character Mode)</td>
<td>Enter the send character (single printable or control). Upon receiving this character, the device sends out the queued data. The data is packed until the specified send character is encountered. Similar to a start or stop character, the device packs the data until it sees the send character. The device then sends the packed data and the send character in the packet. Applies only if the Packing Mode is Send Character.</td>
</tr>
<tr>
<td><strong>Trailing Character</strong> (Appears for Send Character Mode)</td>
<td>Enter the trailing character (single printable or control). This character is sent immediately following the send character. This is an optional setting. If a trailing character is defined, this character is appended to data put on the network immediately following the send character.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

6. Repeat above steps as desired, according to additional tunnel(s) available on your product.
Tunnel – Accept Mode

Controls how a specific tunnel number behaves when a connection attempt originates from the network. In Accept Mode, the EDS waits for a connection from the network. The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. The default local port is 10001 for serial port 1 and increases sequentially for each additional serial port, if supported.

**Accept Mode supports the following protocols:**

- **SSH**
  The EDS device is the server in Accept Mode. When using this protocol, the SSH server host keys and at least one SSH authorized user must be configured.

- **SSL**

- **TCP**

- **TCP AES** encryption over TCP

- **Telnet**
  The EDS supports IAC codes. It drops the IAC codes when Telnetting and does not forward them to the serial port.

**Accept Mode has the following states:**

- **Disable**
  Never accepts a connection.

- **Always**
  Always listening for a connection.

- **Any Character**
  (If it receives any character from the serial port).

- **Start Character**
  (If it receives a specific ([configurable]) character from the serial port ([same start character as Connect Mode’s start character]).

- **Modem Control Asserted**
  (When the modem control pin is asserted on the serial line corresponding to the tunnel.)

- **Modem Emulation**

**To configure the Accept Mode of a specific tunnel:**

1. Select **Tunnel** on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select **Accept Mode**. The Accept Mode page for the specific tunnel appears.
4. Enter or modify the following settings:

**Table 8-15 Tunnel Accept Mode**

<table>
<thead>
<tr>
<th><strong>Tunnel - Accept Mode Settings</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>Select the method used to start a tunnel in Accept mode. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Disable</strong> = do not accept an incoming connection.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Always</strong> = accept an incoming connection (<em>default</em>)</td>
</tr>
<tr>
<td></td>
<td>- <strong>Any Character</strong> = start waiting for an incoming connection when any character is read on the serial line.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Start Character</strong> = start waiting for an incoming connection when the start character for the specific tunnel is read on the serial line.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Modem Control Asserted</strong> = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Modem Emulation</strong> = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.</td>
</tr>
<tr>
<td><strong>Local Port</strong></td>
<td>Enter the port number for use as the local port. The defaults are port 10001 for Tunnel 1. Additional tunnels, if supported, increase sequentially.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Select the protocol type for use with Accept Mode. The default protocol is TCP. If you select TCP AES you will need to configure the AES keys.</td>
</tr>
<tr>
<td><strong>TCP Keep Alive</strong></td>
<td>Enter the time, in seconds, the device waits during a silent connection before checking if the currently connected network device is still on the network. If the unit then gets no response after 8 attempts, it drops that connection.</td>
</tr>
<tr>
<td><strong>Flush Serial Data</strong></td>
<td>Select Enabled to flush the serial data buffer on a new connection.</td>
</tr>
</tbody>
</table>
5. Click Submit.

6. Repeat above steps as desired, according to additional tunnel(s) available on your product.

### Tunnel – Connect Mode

Connect Mode defines how the device makes an outgoing connection through a specific tunnel. When enabled, Connect Mode is always on and attempting a network connection if the connection mode condition warrants it. For Connect Mode to function, it must:

- Be enabled
- Have a remote host configured
- Have a remote port configured

Enter the remote host address as an IP address or DNS name. The EDS device will make a connection only if it can resolve the address. For DNS names, the EDS will re-evaluate the address after being established for 4 hours. If re-evaluation results in a different address, it will close the connection.

**Connect Mode supports the following protocols:**

- TCP
- AES encryption over TCP and UDP
  
  When setting AES encryption, both the encrypt key and the decrypt key must be specified. The encrypt key is used for data sent out. The decrypt key is used for receiving data. Both of the keys may be set to the same value.

- SSH
  
  To configure SSH, the SSH client username must be configured. In Connect Mode, the EDS unit is the SSH client. Ensure the EDS SSH client username is configured on the remote SSH server before using it with the EDS.

- SSL
8: Line and Tunnel Settings

- **UDP**
  Is only available in Connect Mode because it is a connectionless protocol. For Connect Mode using UDP, the EDS unit accepts packets from any device on the network. It will send packets to the last device that sent it packets.

- **Telnet**

  *Note:* The Local Port in Connect Mode is independent of the port configured in Accept Mode.

There are six different connect modes:

- **Disable**
  No connection is attempted.

- **Always**
  A connection is always attempted.

- **Any Character**
  A connection is attempted if it detects any character from the serial port.

- **Start Character**
  A connection is attempted if it detects a specific and configurable character from the serial port.

- **Modem Control Asserted**
  A connection is attempted when the modem control pin is asserted in the serial line.

  *Note:* Configure the Modem Control Asserted setting (for DSR or DTR) to start a Connect Mode connection when the signal is asserted. The unit will try to make a connection indefinitely. If the connection closes, it will not make another connection unless the signal is asserted again.

- **Modem Emulation**
  A connection is attempted by an ATD command.

*Note:* While in the “Any Character” or “Start Character” connection modes, the EDS waits and retries the connection if the connection cannot be made. Once it makes a connection and then disconnects, it will not reconnect until it sees another character or the start character again (depending on the configured setting).

To configure Connect Mode for a specific tunnel:

1. Select **Tunnel** on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select **Connect Mode**. The Connect Mode page for the specific tunnel appears.
4. Enter or modify the following settings:

**Table 8-17 Tunnel Connect Mode**

<table>
<thead>
<tr>
<th>Tunnel – Connect Mode Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Mode**                      | Select the method to be used to attempt a connection to a remote host or device. Choices are:  
  - **Disable** = an outgoing connection is never attempted.  
  - **Always** = a connection is attempted until one is made. If the connection gets disconnected, the EDS retries until it makes a connection. (default)  
  - **Any Character** = a connection is attempted when any character is read on the serial line.  
  - **Start Character** = a connection is attempted when the start character for the specific tunnel is read on the serial line.  
  - **Modem Control Asserted** = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made.  
  - **Modem Emulation** = a connection is attempted when triggered by modem emulation AT commands. |
| **Local Port**                | Enter the port for use as the local port. A random port is selected by default. Once you have configured a number, click the Random link in the Current Configuration to switch back to random. |
### Tunnel – Connect Mode Settings (continued)

<table>
<thead>
<tr>
<th>Host (Number)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Click &lt;None&gt;</strong> in the Host field to configure the Host parameters.</td>
<td></td>
</tr>
<tr>
<td><strong>Address</strong> = Enter the remote Host Address as an IP address or DNS name. It designates the address of the remote host to connect to. Displays configured IP address or DNS address.</td>
<td></td>
</tr>
<tr>
<td><strong>Port</strong> = Enter the port for use as the Host Port. It designates the port on the remote host to connect to. Displays configured Port.</td>
<td></td>
</tr>
<tr>
<td><strong>Protocol</strong> = Select the protocol type for use with Connect Mode. The default protocol is TCP. Additional fields may need to be completed depending on protocol chosen for the host:</td>
<td></td>
</tr>
<tr>
<td>➢ For <strong>SSH</strong>, also enter an <strong>SSH Username</strong>.</td>
<td></td>
</tr>
<tr>
<td>➢ For <strong>SSL</strong>, also select Enabled or Disabled for <strong>Validate Certificate</strong>.</td>
<td></td>
</tr>
<tr>
<td>➢ For <strong>SSL, TCP, TCP AES and Telnet</strong>, use the <strong>TCP Keep Alive</strong> field to adjust the value.</td>
<td></td>
</tr>
<tr>
<td>➢ For <strong>TCP AES</strong>, enter the <strong>AES Encrypt</strong> and <strong>AES Decrypt Keys</strong>. Both of keys may be set to the same value.</td>
<td></td>
</tr>
<tr>
<td>➢ For <strong>UDP</strong>, there are no additional fields to complete. In this mode, the device accepts packets from any device on the network and sends packets to the last device that sent it packets.</td>
<td></td>
</tr>
<tr>
<td>➢ For <strong>UDP AES</strong>, enter the <strong>AES Encrypt</strong> and <strong>AES Decrypt Keys</strong>.</td>
<td></td>
</tr>
<tr>
<td>➢ <strong>Validate Certificate</strong> = select to enable or disable the certificate. Enabling Validate Certificate requires the tunnel to verify the remote SSL server certificate when making a connection. Disabling causes the tunnel to skip verification of the remote SSL server certificate.</td>
<td></td>
</tr>
<tr>
<td>➢ <strong>SSH Username</strong> = Displays configured username, used only if SSH protocol is selected.</td>
<td></td>
</tr>
<tr>
<td>➢ <strong>TCP Keep Alive</strong> = Default is 45000 milliseconds. Enter zero to disable and blank the value to restore the default.</td>
<td></td>
</tr>
<tr>
<td>➢ <strong>AES Encrypt/Decrypt Key</strong> = Displays presence of key, used only if protocol with AES is selected.</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** If security is a concern, it is highly recommended that SSH be used. When using SSH, both the SSH Server Host Keys and SSH Server Authorized Users must be configured.

<table>
<thead>
<tr>
<th>Host Mode</th>
<th>Select the host mode if you have more than one host configured:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sequential</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Simultaneous</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** This field appears when multiple hosts are established. See Connecting Multiple Hosts on page 65 for more information.
5. Click **Submit**. The host is configured. A second host appears underneath the newly configured host.

6. Repeat these steps to configure additional hosts as necessary. EDS supports configuration of up to sixteen hosts.
Connecting Multiple Hosts

If more than one host is configured, a **Host Mode** option appears. Host Mode controls how multiple hosts will be accessed. For EDS, the Connect Mode supports up to sixteen Hosts. Hosts may be accessed sequentially or simultaneously:

- **Sequential** – Sequential host lists establish a prioritized list of tunnels. The host specified as Host 1 will be attempted first. If that fails, it will proceed to Host 2, 3, etc, in the order they are specified. When a connection drops, the cycle starts again with Host 1 and proceeds in order. Establishing the host order is accomplished with host list promotion (see **Host List Promotion on page 66**). Sequential is the default Host Mode.

- **Simultaneous** – A tunnel will connect to all hosts accepting a connection. Connections occur at the same time to all listed hosts. The device can support a maximum of 64 total aggregate connections.

![Figure 8-18 Host 1, Host 2, Host 3 Exchanged](image)
**Host List Promotion**

This feature allows Host IP promotion of individual hosts in the overall sequence.

To promote a specific Host:

1. Click the ![icon](image) in the desired Host field, for example Host 2 and Host 3.
2. The selected Host(s) exchanges its place with the Host above it.
3. Click Submit. The hosts change sequence.

**Tunnel – Disconnect Mode**

Relates to the disconnection of a specific tunnel. Disconnect Mode ends Accept Mode and Connect Mode connections. When disconnecting, the EDS unit shuts down the specific tunnel connection gracefully.

The following settings end a specific tunnel connection:

- The EDS receives the stop character.
- The timeout period has elapsed and no activity is going in or out of the EDS device. Both Accept Mode and Connect Mode must be idle for the time frame.
- The EDS unit observes the modem control inactive setting.

**Note:** To clear data out of the serial buffers upon a disconnect, enable “Flush Serial Data”.

To configure the Disconnect Mode for a specific tunnel:

1. Select Tunnel on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select Disconnect Mode. The specific tunnel Disconnect Mode page appears.

![Figure 8-19 Tunnel 1 Disconnect Mode](image)
4. Enter or modify the following settings:

**Table 8-20 Tunnel Disconnect Mode**

<table>
<thead>
<tr>
<th>Tunnel – Disconnect Mode Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Character</td>
<td>Enter the stop character in ASCII, hexadecimal, or decimal notation. Select &lt;None&gt; to disable.</td>
</tr>
<tr>
<td>Modem Control</td>
<td>Select <strong>Enabled</strong> to disconnect when the modem control pin is not asserted on the serial line.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Enter a time, in milliseconds, for the device to disconnect on a <strong>Timeout</strong>. The value 0 (zero) disables the idle timeout.</td>
</tr>
<tr>
<td>Flush Serial Data</td>
<td>Select <strong>Enabled</strong> to flush the serial data buffer on a disconnection.</td>
</tr>
</tbody>
</table>

5. Click Submit.

6. Repeat above steps as desired, according to additional tunnel(s) available on your product.

**Tunnel – Modem Emulation**

A tunnel in Connect Mode can be initiated using modem commands incoming from the Serial Line. This page enables you to configure the modem emulation settings when you select Modem Emulation as the Tunnel Connect Mode type. The Modem Emulation Command Mode supports the standard AT command set. For a list of available commands from the serial or Telnet login, enter AT?. Use ATDT, ATD, and ATDP to establish a connection. All of these commands behave like a modem. For commands that are valid but not applicable to the EDS, an “OK” message is sent (but the command is silently ignored).

The EDS unit attempts to make a Command Mode connection as per the IP/DNS/port numbers defined in Connect Mode. It is possible to override the remote address, as well as the remote port number.

The following table lists and describes the available commands.

**Table 8-21 Modem Emulation Commands and Descriptions**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+++</td>
<td>Switches to Command Mode if entered from serial port during connection.</td>
</tr>
<tr>
<td>AT?</td>
<td>Help.</td>
</tr>
<tr>
<td>ATDT&lt;Address Info&gt;</td>
<td>Establishes the TCP connection to socket (&lt;ipaddress&gt;:&lt;port&gt;).</td>
</tr>
<tr>
<td>ATDP&lt;Address Info&gt;</td>
<td>See ATDT.</td>
</tr>
<tr>
<td>ATD</td>
<td>Like ATDT. Dials default Connect Mode remote address and port.</td>
</tr>
<tr>
<td>ATD&lt;Address Info&gt;</td>
<td>Sets up a TCP connection. A value of 0 begins a command line interface session.</td>
</tr>
<tr>
<td>ATO</td>
<td>Switches to data mode if connection still exists. Vice versa to ‘+++’.</td>
</tr>
<tr>
<td>ATEn</td>
<td>Switches echo in Command Mode (off - 0, on - 1).</td>
</tr>
<tr>
<td>ATH</td>
<td>Disconnects the network session.</td>
</tr>
<tr>
<td>ATI</td>
<td>Shows modem information.</td>
</tr>
</tbody>
</table>
For commands that can take address information (ATD, ATDT, ATDP), the destination address can be specified by entering the IP Address, or entering the IP Address and port number. For example, `<ipaddress>:<port>`. The port number cannot be entered on its own.

For ATDT and ATDP commands less than 255 characters, the EDS replaces the last segment of the IP address with the configured Connect Mode remote station address. It is possible to use the last two segments also, if they are under 255 characters. For example, if the address is 100.255.15.5, entering `ATDT 16.6` results in 100.255.16.6.

When using ATDT and ATDP, enter 0.0.0.0 to switch to the Command Line Interface (CLI). Once the CLI is exited by using the CLI exit command, the EDS reverts to modem emulation mode. By default, the +++ characters are not passed through the connection. Turn on this capability using the modem echo pluses command.

### To configure modem emulation for a specific tunnel:

1. Select **Tunnel** on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select **Modem Emulation**. The Modem Emulation page for the specific tunnel appears.

#### Table 8-21 Modem Emulation Commands and Descriptions (continued)

<table>
<thead>
<tr>
<th>Command (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATQn</td>
<td>Quiet mode (0 - enable results code, 1 - disable results code.)</td>
</tr>
<tr>
<td>ATVn</td>
<td>Verbose mode (0 - numeric result codes, 1 - text result codes.)</td>
</tr>
<tr>
<td>ATXn</td>
<td>Command does nothing and returns OK status.</td>
</tr>
<tr>
<td>ATUn</td>
<td>Accept unknown commands. (n value of 0 = off, n value of 1 = on.)</td>
</tr>
<tr>
<td>AT&amp;V</td>
<td>Display current and saved settings.</td>
</tr>
<tr>
<td>AT&amp;F</td>
<td>Reset settings in NVR to factory defaults.</td>
</tr>
<tr>
<td>AT&amp;W</td>
<td>Save active settings to NVR.</td>
</tr>
<tr>
<td>ATZ</td>
<td>Restores the current state from the setup settings.</td>
</tr>
<tr>
<td>ATS0=n</td>
<td>Accept incoming connection.</td>
</tr>
<tr>
<td></td>
<td>♦ N value of 0—Disable</td>
</tr>
<tr>
<td></td>
<td>♦ N value of 1—Connect automatically</td>
</tr>
<tr>
<td></td>
<td>♦ N value of 2+—Connect with ATA command.</td>
</tr>
<tr>
<td>ATA</td>
<td>Answer incoming connection (if ATS0 is 2 or greater).</td>
</tr>
<tr>
<td>A/</td>
<td>Repeat last valid command.</td>
</tr>
</tbody>
</table>
4. Enter or modify the following settings:

![Figure 8-22 Tunnel 1 Modem Emulation](image)

**Table 8-23 Tunnel Modem Emulation**

<table>
<thead>
<tr>
<th>Tunnel-Modem Emulation Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo Pluses</td>
<td>Select <strong>Enabled</strong> to echo +++ when entering modem Command Mode.</td>
</tr>
<tr>
<td>Echo Commands</td>
<td>Select <strong>Enabled</strong> to echo the modem commands to the console.</td>
</tr>
<tr>
<td>Verbose Response</td>
<td>Select <strong>Enabled</strong> to send modem response codes out on the serial line.</td>
</tr>
<tr>
<td>Response Type</td>
<td>Select the type of response code: <strong>Text</strong> or <strong>Numeric</strong>.</td>
</tr>
</tbody>
</table>
| Error Unknown Commands          | Select whether an **ERROR** or **OK** response is sent in reply to unrecognized AT commands. Choices are:  
  - **Enabled** = **ERROR** is returned for unrecognized AT commands.  
  - **Disabled** = **OK** is returned for unrecognized AT commands. Default is **Disabled**. |
| Incoming Connection             | Select whether Incoming Connection requests will be **Disabled**, **Automatic** (accepted automatically), or **Manual** (accepted manually). Default is **Disabled**. |
| Connect String                  | Enter the connect string. This modem initialization string prepares the modem for communications. It is a customized string sent with the "CONNECT" modem response code. |
| Display Remote IP               | Selects whether the incoming RING sent on the Serial Line is followed by the IP address of the caller. Default is **Disabled**. |

5. Click **Submit**.

6. Repeat above steps as desired, according to additional tunnel(s) available on your product.
9: **Terminal and Host Settings**

This chapter describes how to view and configure the Terminal Login Connect Menu and associated Host configuration. It contains the following sections:

- **Terminal Settings**
- **Host Configuration**

The Terminal Login Connect Menu feature allows the EDS device server to present a menu of predefined connections when the device is accessed via telnet, ssh, or a serial port. From the menu, a user can choose one of the presented options and the device automatically makes the predefined connection.

The Terminal page controls whether a Telnet, SSH, or serial port connection presents the CLI or the Login Connect Menu. By default, the CLI is presented when the device is accessed. When configured to present the Login Connect Menu, the hosts configured via the Hosts page, and named serial lines are presented.

**Terminal Settings**

This page shows configuration settings for each terminal connection method. You can configure whether each serial line or the telnet/SSH server presents a CLI or a Login Connect menu when a connection is made.

**Terminal Network Configuration**

To configure menu features applicable to CLI access via the network:

1. Select **Terminal** on the menu bar, if you are not already in the Terminal web page.
2. Select **Network** at the top of the page. The Configuration submenu is automatically selected. The Terminal Configuration page appears for the network.

![Figure 9-1  Terminal on Network Configuration](image)

3. Enter or modify the following settings:
9: Terminal and Host Settings

### Table 9-2 Terminal on Network Configuration

<table>
<thead>
<tr>
<th>Terminal on Network Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Terminal Type                             | Enter text to describe the type of terminal. The text will be sent to a host via IAC.  
*Note: IAC means, “interpret as command.” It is a way to send commands over the network such as send break or start echoing.* |
| Login Connect Menu                        | Select the interface to display when the user logs in. Choices are:  
- **Enabled** = shows the Login Connect Menu.  
- **Disabled** = shows the CLI |
| Exit Connect Menu                         | Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are:  
- **Enabled** = a choice allows the user to exit to the CLI.  
- **Disabled** = there is no exit to the CLI. |
| Echo                                      | Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable Echo if your terminal echoes, in which case you will see double of each character typed. |

4. Click **Submit** to save changes.

**Terminal Line Configuration**

*To configure a specific line to support an attached terminal:*

1. Select Terminal on the menu bar. The Terminal web page appears.
2. Select the line number at the top of the page connected to the terminal you want to configure. The default is Line 1.

**Figure 9-3 Terminal on Line Configuration**

3. Enter or modify the following settings:
Table 9-4 Terminal on Line 1 Configuration

<table>
<thead>
<tr>
<th>Terminal on Line Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Terminal Type                          | Enter text to describe the type of terminal. The text will be sent to a host via IAC.  
   Note: IAC means, “interpret as command.” It is a way to send commands over the network such as send break or start echoing. |
| Login Connect Menu                     | Select the interface to display when the user logs in. Choices are:  
   ✶ Enabled = shows the Login Connect Menu.  
   ✶ Disabled = shows the CLI |
| Exit Connect Menu                      | Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are:  
   ✶ Enabled = a choice allows the user to exit to the CLI.  
   ✶ Disabled = there is no exit to the CLI. |
| Send Break                             | Enter the Send Break control character. If this specified character is received by the serial line, it will not be sent to the line; instead the line output will be forced inactive. Sample setting: <Control>Y. Blank the field to set to <None>. |
| Break Duration                         | Enter the time in milliseconds for how long the spacing condition will be placed on the line when a break is sent. |
| Echo                                   | Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable Echo if your terminal echoes, in which case you will see double of each character typed. |

4. Click Submit to save changes.

5. Repeat above steps as desired, according to the additional line(s) available on your product.
Host Configuration

This Host web page is where you may view and modify current settings for a selected remote host.

To configure a selected remote host:
1. Select Host on the menu bar. The Host web page appears.
2. Select a specific host number at the top of the page. The Host Configuration page for the selected host appears.

Note: Number of hosts available differ among Lantronix products. Hosts available for selection may appear listed on the screen (see Figure 9-5) or within a drop-down menu above the Configuration button.

3. Enter or modify the following settings:

Table 9-6 Host Configuration

<table>
<thead>
<tr>
<th>Host Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the host. This name appears on the Login Connect Menu. To leave a host out of the menu, leave this field blank.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol to use to connect to the host. Choices are: Telnet, SSH. Note: SSH keys must be loaded or created on the SSH page for the SSH protocol to work.</td>
</tr>
<tr>
<td>SSH Username</td>
<td>Enter a username to select a pre-configured Username/Password/Key (configured on the SSH: Client Users page), or leave it blank to be prompted for a username and password at connect time. Note: Appears if you selected SSH as the protocol.</td>
</tr>
<tr>
<td>Remote Address</td>
<td>Enter an IP address for the host to which the device will connect.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Enter the port on the host to which the device will connect.</td>
</tr>
</tbody>
</table>

4. Click Submit to save changes.
5. Repeat above steps as desired, according to additional host(s) available on your product.
10: Service Settings

This chapter describes the available services and how to configure each. It contains the following sections:

- DNS Settings
- SNMP Settings
- FTP Settings
- TFTP Settings
- Syslog Settings
- HTTP Settings
- RSS Settings
- LPD Settings

DNS Settings

The primary and secondary domain name system (DNS) addresses come from the active interface. The static addresses from the Network Interface Configuration page may be overridden by DHCP or BOOTP. The DNS web page enables you to view the status and cache.

When a DNS name is resolved using a forward lookup, the results are stored in the DNS cache temporarily. The EDS checks this cache when performing forward lookups. Each item in the cache eventually times out and is removed automatically after a certain period, or you can delete it manually.

To view the DNS status:

1. Select DNS on the menu bar. The DNS page appears.

![Figure 10-1  DNS Settings](image)
To find a DNS Name or IP Address:
1. Enter either a DNS name or an IP address in the field beside the **Lookup** button.
2. Click **Lookup**.
   - When a DNS name is resolved, the results appear in the DNS cache.
   - When an IP address is resolved, the results appear in a text below the Lookup field.

To clear cache entries:
1. Click **Remove All** to remove all listed cache entries.
2. Click **Delete** next to a specific cache entry to remove only that one.

**SNMP Settings**

Simple Network Management Protocol (SNMP) is a network management tool that monitors network devices for conditions that need attention. The SNMP service responds to SNMP requests and generates SNMP Traps.

This page is used to configure the SNMP agent.

**To configure SNMP:**
1. Select **SNMP** on the menu bar. The SNMP page opens and shows the current SNMP configuration.

**Figure 10-2 SNMP Configuration**

<table>
<thead>
<tr>
<th>SNMP</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State:</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Read Community:</strong></td>
<td>Configured</td>
</tr>
<tr>
<td><strong>Write Community:</strong></td>
<td>Configured</td>
</tr>
<tr>
<td><strong>System Contact:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>System Name:</strong></td>
<td>XP2000</td>
</tr>
<tr>
<td><strong>System Description:</strong></td>
<td>Lantronix XPort Pro V5.0.0R12 (0709287777DGFL)</td>
</tr>
<tr>
<td><strong>System Location:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Traps State:</strong></td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Traps Primary Destination:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Traps Secondary Destination:</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The system description string will reflect the specific Lantronix product.
2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>SNMP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select <strong>Enabled</strong> to enable SNMP.</td>
</tr>
<tr>
<td>Read Community</td>
<td>Enter the SNMP read-only community string.</td>
</tr>
<tr>
<td>Write Community</td>
<td>Enter the SNMP read/write community string.</td>
</tr>
<tr>
<td>System Contact</td>
<td>Enter the name of the system contact.</td>
</tr>
<tr>
<td>System Name</td>
<td>Enter the system name.</td>
</tr>
<tr>
<td>System Description</td>
<td>Enter the system description.</td>
</tr>
<tr>
<td>System Location</td>
<td>Enter the system location.</td>
</tr>
<tr>
<td><strong>Traps State</strong></td>
<td>Select <strong>Enabled</strong> to enable the transmission of SNMP Traps.</td>
</tr>
<tr>
<td><strong>Traps Primary Destination</strong></td>
<td>Enter the primary SNMP trap host.</td>
</tr>
<tr>
<td><strong>Traps Secondary Destination</strong></td>
<td>Enter the secondary SNMP trap host.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

**FTP Settings**

The FTP web page shows the current File Transfer Protocol (FTP) configuration and various statistics about the FTP server.

**To configure FTP:**

1. Select **FTP** on the menu bar. The FTP page opens to display the current configuration.

![Figure 10-4 FTP Configuration](image)

2. Enter or modify the following settings:
10: Service Settings

**Table 10-5  FTP Settings**

<table>
<thead>
<tr>
<th>FTP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select <strong>Enabled</strong> to enable the FTP server.</td>
</tr>
<tr>
<td>Admin Username</td>
<td>Enter the username to use when logging in via FTP.</td>
</tr>
<tr>
<td>Admin Password</td>
<td>Enter the password to use when logging in via FTP.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

**TFTP Settings**

In the TFTP web page, you can configure the server and view the statistics about the Trivial File Transfer Protocol (TFTP) server.

*To configure TFTP:*

1. Select **TFTP** on the menu bar. The TFTP page opens to display the current configuration.

**Figure 10-6  TFTP Configuration**

<table>
<thead>
<tr>
<th>TFTP Server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>State:</td>
<td><img src="on" alt="Enabled" />, <img src="off" alt="Disabled" /></td>
</tr>
<tr>
<td>Allow File Creation:</td>
<td><img src="on" alt="Enabled" />, <img src="off" alt="Disabled" /></td>
</tr>
<tr>
<td>Allow Firmware Update:</td>
<td><img src="on" alt="Enabled" />, <img src="off" alt="Disabled" /></td>
</tr>
<tr>
<td>Allow XCR Import:</td>
<td><img src="on" alt="Enabled" />, <img src="off" alt="Disabled" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status:</td>
<td>Running</td>
</tr>
<tr>
<td>Files Downloaded:</td>
<td><img src="off" alt=" " /></td>
</tr>
<tr>
<td>Files Uploaded:</td>
<td><img src="off" alt=" " /></td>
</tr>
<tr>
<td>File Not Found Errors:</td>
<td><img src="off" alt=" " /></td>
</tr>
<tr>
<td>File Read Errors:</td>
<td><img src="off" alt=" " /></td>
</tr>
<tr>
<td>File Write Errors:</td>
<td><img src="off" alt=" " /></td>
</tr>
<tr>
<td>Unknown Errors:</td>
<td><img src="off" alt=" " /></td>
</tr>
<tr>
<td>Last Client:</td>
<td>No device has connected</td>
</tr>
</tbody>
</table>

2. Enter or modify the following settings:

**Table 10-7  TFTP Server**

<table>
<thead>
<tr>
<th>TFTP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select <strong>Enabled</strong> to enable the TFTP server.</td>
</tr>
<tr>
<td>Allow File Creation</td>
<td>Select whether to allow the creation of new files stored on the TFTP server.</td>
</tr>
</tbody>
</table>
3. Click Submit.

Syslog Settings

The Syslog web page shows the current configuration and statistics of the system log. Here you may configure the syslog destination and the severity of the events to log.

To configure the Syslog:

Note: The syslog file is always saved to local storage, but it is not retained through reboots. Saving the syslog file to a server that supports remote logging services (see RFC 3164) allows the administrator to save the complete syslog history. The default port is 514.

1. Select Syslog on the menu bar. The Syslog page opens to display the current configuration.

![Figure 10-8 Syslog](image)

2. Enter or modify the following settings:
Table 10-9  Syslog

<table>
<thead>
<tr>
<th>Syslog Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select to enable or disable the syslog.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the IP address of the remote server to which system logs are sent for storage.</td>
</tr>
<tr>
<td>Local Port</td>
<td>Enter the number of the local port on the device from which system logs are sent.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Enter the number of the port on the remote server that supports logging services. The default is 514.</td>
</tr>
<tr>
<td>Severity Log Level</td>
<td>From the drop-down box, select the minimum level of system message the device should log. This setting applies to all syslog facilities. The drop-down list is in descending order of severity (e.g., Emergency is more severe than Alert.)</td>
</tr>
</tbody>
</table>

3. Click Submit.

HTTP Settings

Hypertext Transfer Protocol (HTTP) is the transport protocol for communicating hypertext documents on the Internet. HTTP defines how messages are formatted and transmitted. It also defines the actions web servers and browsers should take in response to different commands. HTTP Authentication enables the requirement of usernames and passwords for access to the EDS device.

This page has three links at the top for viewing statistics and for viewing and changing configuration and authentication settings.

- **HTTP Statistics**—Viewing statistics such as bytes received and transmitted, bad requests, authorizations required, etc.
- **HTTP Configuration**—Configuring and viewing the current configuration.
- **HTTP Authentication**—Configuring and viewing the authentication.

HTTP Statistics

*To view HTTP statistics:*

This page shows various statistics about the HTTP server.

1. Select HTTP on the menu bar and then Statistics at the top of the page. The HTTP Statistics page appears.
Figure 10-10  HTTP Statistics

<table>
<thead>
<tr>
<th>HTTP Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rx Bytes</strong></td>
<td>26295</td>
</tr>
<tr>
<td><strong>Tx Bytes</strong></td>
<td>190244</td>
</tr>
<tr>
<td><strong>200 - OK</strong></td>
<td>15</td>
</tr>
<tr>
<td><strong>301 - Moved Permanently</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>400 - Bad Request</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>401 - Authorization Required</strong></td>
<td>13</td>
</tr>
<tr>
<td><strong>404 - Not Found</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>408 - Request Timeout</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>413 - Request Too Large</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>500 - Internal Error</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>501 - Not Implemented</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Status Unknown</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Work Queue Full</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Socket Error</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Memory Error</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Logs:</strong></td>
<td>42 entries (6291 bytes) [View] [Clear]</td>
</tr>
</tbody>
</table>

**Note:** The HTTP log is a scrolling log, with the last Max Log Entries cached and viewable. You can change the maximum number of entries that can be viewed on the HTTP Configuration Page.
HTTP Configuration

On this page you may change HTTP configuration settings.

To configure HTTP:

1. Select HTTP on the menu bar and then Configuration at the top of the page. The HTTP Configuration page opens.

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>HTTP Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select <strong>Enabled</strong> to enable the HTTP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port for the HTTP server to use. The default is <strong>80</strong>.</td>
</tr>
<tr>
<td>Secure Port</td>
<td>Enter the port for the HTTPS server to use. The default is <strong>443</strong>. The HTTP server only listens on the HTTPS Port when an SSL certificate is configured.</td>
</tr>
</tbody>
</table>
### Secure Protocols
Select to enable or disable the following protocols:
- **TLS1.0** = Transport Layer Security version 1.0. TLS 1.0 is the successor of
  SSL3 as defined by the IETF.
- **TLS1.1** = Transport Layer Security version 1.1

The protocols are enabled by default.

*Note:* A server certificate and associated private key need to be installed in
the SSL configuration section to use HTTPS.

### Max Timeout
Enter the maximum time for the HTTP server to wait when receiving a
request. This prevents Denial-of-Service (DoS) attacks. The default is 10
seconds.

### Max Bytes
Enter the maximum number of bytes the HTTP server accepts when receiving
a request. The default is 40 KB (this prevents DoS attacks).

### Logging State
Select **Enabled** to enable HTTP server logging.

### Max Log Entries
Sets the maximum number of HTTP server log entries. Only the last Max Log
Entries are cached and viewable.

### Log Format
Set the log format string for the HTTP server. Follow these Log Format rules:
- **%a** - remote IP address (could be a proxy)
- **%b** - bytes sent excluding headers
- **%B** - bytes sent excluding headers (0 = '-')
- **%h** - remote host (same as '%a')
- **%(h)i** - header contents from request (h = header string)
- **%m** - request method
- **%p** - ephemeral local port value used for request
- **%q** - query string (prepend with '?' or empty '-')
- **%t** - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or
  '%(%T)t')
- **%u** - remote user (could be bogus for 401 status)
- **%U** - URL path info
- **%r** - first line of request (same as '%m %U%q <version>')
- **%s** - return status

### Authentication Timeout
The timeout period applies if the selected authentication type is either Digest
or SSL/Digest. After this period of inactivity, the client must authenticate
again.

3. Click **Submit**.

---

### HTTP Authentication
HTTP Authentication enables you to require usernames and passwords to access specific web pages or directories on the EDS built-in web server.

**To configure HTTP authentication settings:**

1. Select **HTTP** on the menu bar and then **Authentication** at the top of the page. The HTTP Authentication page opens.

   ![Figure 10-13 HTTP Authentication](image)

   **HTTP Authentication**
   
   **URI:**
   
   **Realm:**
   
   **AuthType:**
   
   **Username:**
   
   **Password:**
   
   **Submit**

   **Current Configuration**
   
   **URI:** /
   
   **Realm:** config
   
   **AuthType:** Digest
   
   **Users:** admin

2. Enter or modify the following settings:

   **Table 10-14 HTTP Authentication**

   **Note:** To properly view data entries in **RSS Settings** in certain web browsers, it may be necessary to first remove authentication from RSS. Enter the following under HTTP Authentication: URI: "rss", Realm: "rss", and AuthType: "None".

<table>
<thead>
<tr>
<th>HTTP Authentication Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URI</td>
<td>Enter the Uniform Resource Identifier (URI).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The URI must begin with '/' to refer to the filesystem.</td>
</tr>
<tr>
<td>Realm</td>
<td>Enter the domain, or realm, used for HTTP. Required with the URI field.</td>
</tr>
</tbody>
</table>
3. Click **Submit**.

4. To delete the URI and users, click **Delete** in the current configuration table.

   **Note:** The URI, realm, username, and password are user-specified, free-form fields. The URI must match the directory created on the EDS file system.

### RSS Settings

Really Simple Syndication (RSS) (sometimes referred to as Rich Site Summary) is a method of feeding online content to Web users. Instead of actively searching for EDS configuration changes, RSS feeds permit viewing only relevant and new information regarding changes made to the EDS device server via an RSS publisher. The RSS feeds may also be stored to the file system `cfg_log.txt` file.

To configure RSS settings:

1. Select **RSS** on the menu bar. The RSS page opens and shows the current RSS configuration.

   ![RSS Configuration](image)

   **RSS**

   **Configuration**
   - **RSS Feed:**
     - On
     - Off
   - **Persistent:**
     - On
     - Off
   - **Max Entries:** 100

   **Statistics**
   - **Data:** 0 entries (0 bytes)
   - [View] [Clear]
2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>RSS Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSS Feed</td>
<td>Select On to enable RSS feeds to an RSS publisher.</td>
</tr>
<tr>
<td>Persistent</td>
<td>Select On to enable the RSS feed to be written to a file (cfg_log.txt) and to be available across reboots.</td>
</tr>
<tr>
<td>Max Entries</td>
<td>Sets the maximum number of log entries. Only the last Max Entries are cached and viewable.</td>
</tr>
<tr>
<td>View</td>
<td>Click View to view current data entries. Note: It may be necessary to remove authentication from RSS access to view data entries on certain web browsers. Go to HTTP Authentication on page 82 for more information.</td>
</tr>
<tr>
<td>Clear</td>
<td>Click Clear to clear data entries.</td>
</tr>
</tbody>
</table>

3. Select Submit.

4. In the Current Status table, view and clear stored RSS Feed entries, as necessary.

**LPD Settings**

The EDS device acts as a print server if a printer gets connected to one of its serial ports. Selecting the Line Printer Daemon (LPD) link in the Main Menu displays the LPD web page. The LPD web page has three sub-menus for viewing print queue statistics, changing print queue configuration, and printing a test page. Because the LPD lines operate independently, you can specify different configuration settings for each.

**LPD Statistics**

This read-only page shows various statistics about the LPD server.

*To view LPD statistics for a specific LPD line:*

1. Select LPD on the menu bar. The LPD web page appears.
2. Select an LPD line at the top of the page.
4. Repeat above steps as desired, according to additional LPD(s) available on your product.

**LPD Configuration**

Here you can change LPD configuration settings.

*To configure LPD settings for a specific LPD line:*

1. Select LPD on the menu bar, if you are not already at the LPD web page.
2. Select a LPD line at the top of the page.
3. Select **Configuration**. The LPD Configuration for the selected LPD line appears.

4. Enter or modify the following settings:
Table 10-19  LPD Configuration

<table>
<thead>
<tr>
<th>LPD Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banner</td>
<td>Select Enabled to print the banner even if the print job does not specify to do so. Selected by default.</td>
</tr>
<tr>
<td>Binary</td>
<td>Select Enabled for the device to pass the entire file to the printer unchanged. Otherwise, the device passes only valid ASCII and valid control characters to the printer. Valid control characters include the tab, linefeed, formfeed, backspace, and newline characters. All others are stripped. Disabled by default.</td>
</tr>
<tr>
<td>Start of Job</td>
<td>Select Enabled to print a &quot;start of job&quot; string before sending the print data.</td>
</tr>
<tr>
<td>End of Job</td>
<td>Select Enabled to send an &quot;end of job&quot; string.</td>
</tr>
<tr>
<td>Formfeed</td>
<td>Select Enabled to force the printer to advance to the next page at the end of each print job.</td>
</tr>
<tr>
<td>Convert Newlines</td>
<td>Select Enabled to convert single newlines and carriage returns to DOS-style line endings.</td>
</tr>
<tr>
<td>SOJ String</td>
<td>If Start of Job (above) is enabled, enter the string to be sent to the printer at the beginning of a print job. The limit is 100 characters. Indicate whether the string is in text or binary format.</td>
</tr>
<tr>
<td>EOJ String</td>
<td>If End of Job (above) is enabled, enter the string to send at the end of a print job. The limit is 100 characters. Indicate whether the string is in text or binary format.</td>
</tr>
<tr>
<td>Queue Name</td>
<td>To change the name of the print queue, enter a new name. The name cannot have white space in it and is limited to 31 characters. The default is LPDQueueX (for line number X)</td>
</tr>
</tbody>
</table>

5. Click Submit.

6. Repeat above steps as desired, according to additional LPD lines available on your product.

Print Test Page
This selection can be chosen to print a test page.

To print a test page:
1. Select LPD on the menu bar, if you are not already at the LPD web page.
2. Select an LPD line at the top of the page.
4. Enter the numbers to print in the popup window.
5. Click OK.
11: Security Settings

The EDS unit supports Secure Shell (SSH) and Secure Sockets Layer (SSL). SSH is a network protocol for securely accessing a remote device. SSH provides a secure, encrypted communication channel between two hosts over a network. It provides authentication and message integrity services.

Secure Sockets Layer (SSL) is a protocol that manages data transmission security over the Internet. It uses digital certificates for authentication and cryptography against eavesdropping and tampering. It provides encryption and message integrity services. SSL is widely used for secure communication to a web server. SSL uses certificates and private keys.

Note: The EDS device server supports SSLv3 and its successors, TLS1.0 and TLS1.1. An incoming SSLv2 connection attempt is answered with an SSLv3 response. If the initiator also supports SSLv3, SSLv3 handles the rest of the connection.

This chapter contains the following sections:
- SSH Server Host Keys
- SSH Server Authorized Users
- SSH Client Known Hosts
- SSH Client Users
- SSL Cipher Suites
- SSL Certificates
- SSL RSA
- SSL Certificates and Private Keys
- SSL Utilities
- SSL Configuration

SSH Settings

SSH is a network protocol for securely accessing a remote device over an encrypted channel. This protocol manages the security of internet data transmission between two hosts over a network by providing encryption, authentication, and message integrity services.

Two instances require configuration: when the EDS unit is the SSH server and when it is an SSH client. The SSH server is used by the CLI (Command Mode) and for tunneling in Accept Mode. The SSH client is for tunneling in Connect Mode.

To configure the EDS device server as an SSH server, there are two requirements:
- Defined Host Keys: both private and public keys are required. These keys are used for the Diffie-Hellman key exchange (used for the underlying encryption protocol).
- Defined Users: these users are permitted to connect to the EDS SSH server.

This page has four links at the top for viewing and changing SSH server host keys, SSH server authorized keys, SSH client known hosts, and SSH client users.
SSH Server Host Keys

SSH Host Keys can be obtained in a few different ways:

- Uploading keys via PUTTY or other tools which generate RFC4716 format keys.
- Creating keys through the device.

The steps for creating or uploading keys is described below.

To upload SSH server host keys generated from PuTTY:

1. Create the keys with puttygen.exe. The keys are in PuTTY format.
2. Use puttygen.exe again to convert the private key to Open SSH format as follows:
   a. Import the private key using "Conversions…Import key."
   b. Create a new file using "Conversions…Export OpenSSH key."
3. Use ssh-keygen to convert the public key to OpenSSH format.
   `ssh-keygen -i -f putty_file > openssh_file`
4. Select SSH on the menu bar and SSH Server: Host Keys at the top of the page. The SSH Server Host Keys page appears.

5. Enter or modify the following settings in the part of the screen related to uploading keys:
To upload SSH server host RFC4716 format keys:
1. Use any program that can produce keys in the RFC4716 format.
2. Use ssh-keygen to convert the format to OpenSSH.
   
   ```bash
   ssh-keygen -i -f RFC4716_file > output_file
   ```
   
   **Note:** If the keys do not exist, follow directions under To create new SSH server host keys (on page 91).

3. Select SSH on the menu bar and SSH Server: Host Keys at the top of the page. The SSH Server Host Keys page appears.

4. Enter or modify the following settings in the part of the screen related to uploading keys:

<table>
<thead>
<tr>
<th>SSH Server: Host Keys Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private Key</strong></td>
<td>Enter the path and name of the existing private key you want to upload or use the Choose File button to select the key. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.</td>
</tr>
<tr>
<td><strong>Public Key</strong></td>
<td>Enter the path and name of the existing public key you want to upload or use the Choose File button to select the key.</td>
</tr>
</tbody>
</table>
| **Key Type**                             | Select a key type to use for the new key:  
   - **RSA** = use this key with the SSH1 and SSH2 protocols.  
   - **DSA** = use this key with the SSH2 protocol. |

5. Click Submit.

**Note:** SSH keys may be created on another computer and uploaded to the EDS device server. For example, use the following command using Open SSH to create a 1024-bit DSA key pair: `ssh-keygen -b 1024 -t dsa`
To create new SSH server host keys

Note: Generating new keys with large bit size results in longer key generation times.

1. Select SSH on the menu bar and SSH Server: Host Keys at the top of the page. The SSH Server Host Keys page appears.

2. Enter or modify the following settings in the part of the screen related to creating new keys:

<table>
<thead>
<tr>
<th>SSH Server: Host Keys Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Type</strong></td>
<td>Select a key type to use:</td>
</tr>
<tr>
<td></td>
<td>❖ <strong>RSA</strong> = use this key with SSH1 and SSH2 protocols.</td>
</tr>
<tr>
<td></td>
<td>❖ <strong>DSA</strong> = use this key with the SSH2 protocol.</td>
</tr>
<tr>
<td><strong>Note:</strong> RSA is more secure.</td>
<td></td>
</tr>
<tr>
<td><strong>Bit Size</strong></td>
<td>Select a bit length for the new key:</td>
</tr>
<tr>
<td></td>
<td>❖ 512</td>
</tr>
<tr>
<td></td>
<td>❖ 768</td>
</tr>
<tr>
<td></td>
<td>❖ 1024</td>
</tr>
<tr>
<td>Using a larger bit size takes more time to generate the key. Approximate times are:</td>
<td></td>
</tr>
<tr>
<td>❖ 10 seconds for a 512 bit RSA Key</td>
<td></td>
</tr>
<tr>
<td>❖ 15 seconds for a 768 bit RSA Key</td>
<td></td>
</tr>
<tr>
<td>❖ 1 minute for a 1024 bit RSA Key</td>
<td></td>
</tr>
<tr>
<td>❖ 30 seconds for a 512 bit DSA Key</td>
<td></td>
</tr>
<tr>
<td>❖ 1 minute for a 768 bit DSA Key</td>
<td></td>
</tr>
<tr>
<td>❖ 2 minutes for a 1024 bit DSA Key</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 1024 bits long. It can work with larger keys (up to 2048 bit) if they are imported or otherwise created.</td>
<td></td>
</tr>
</tbody>
</table>

3. Click Submit.

Note: SSH Keys from other programs may be converted to the required EDS format. Use Open SSH to perform the conversion.

SSH Server Authorized Users

On this page you can change SSH server settings for Authorized Users. SSH Server Authorized Users are accounts on the EDS device server that can be used to log into the EDS using SSH. For instance, these accounts can be used to SSH into the CLI or open an SSH connection to a device port. Every account must have a password.

The user's public keys are optional and only necessary if public key authentication is required. Using public key authentication allows a connection to be made without the password being asked.

Under Current Configuration, User has a Delete User link, and Public RSA Key and Public DSA Key have View Key and Delete Key links. If you click a Delete link, a message asks whether you are sure you want to delete this information. Click OK to proceed or Cancel to cancel the operation.
To configure the SSH server for authorized users:

1. Select SSH on the menu bar and then Server Authorized Users at the top of the page. The SSH Server: Authorized Users page appears.

![Figure 11-5  SSH Server: Authorized Users](image)

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>SSH Server: Authorized Users Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the name of the user authorized to access the SSH server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with the username.</td>
</tr>
<tr>
<td>Public RSA Key</td>
<td>Enter the path and name of the existing public RSA key you want to use with this user or use the Choose File button to select the key. If authentication is successful with the key, no password is required.</td>
</tr>
<tr>
<td>Public DSA Key</td>
<td>Enter the path and name of the existing public DSA key you want to use with this user or use the Choose File button to select the key. If authentication is successful with the key, no password is required.</td>
</tr>
</tbody>
</table>

3. Click Add/Edit.

Note: When uploading the security keys, ensure the keys are not compromised in transit.
SSH Client Known Hosts

On this page you can change SSH client settings for known hosts.

**Note:** You do not have to complete the fields on this page for communication to occur. However, completing them adds another layer of security that protects against Man-In-The-Middle (MITM) attacks.

**To configure the SSH client for known hosts:**

1. Select **SSH** on the menu bar and then **Client Known Hosts** at the top of the page. The SSH Client: Known Hosts page appears.

2. Enter or modify the following settings:

   **Table 11-8  SSH Client Known Hosts**

<table>
<thead>
<tr>
<th><strong>SSH Client: Known Hosts Settings</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>Enter the name or IP address of a known host. If you enter a server name, the name should match the name of the server used as the <strong>Remote Address</strong> in Connect mode tunneling.</td>
</tr>
<tr>
<td><strong>Public RSA Key</strong></td>
<td>Enter the path and name of the existing public RSA key you want to use with this known host or use the <strong>Choose File</strong> button to select the key.</td>
</tr>
<tr>
<td><strong>Public DSA Key</strong></td>
<td>Enter the path and name of the existing public DSA key you want to use with this known host or use the <strong>Choose File</strong> button to select the key.</td>
</tr>
</tbody>
</table>

   **Note:** These settings are not required for communication. They protect against Man-In-The-Middle (MITM) attacks.

3. Click **Submit**.
4. In the **Current Configuration** table, delete currently stored settings as necessary.
SSH Client Users

On this page you can change SSH client settings for users. To configure the EDS device server as an SSH client, an SSH client user must be both configured and also exist on the remote SSH server.

SSH client known users are used by all applications that play the role of an SSH client, specifically tunneling in Connect Mode. At the very least, a password or key pair must be configured for a user. The keys for public key authentication can be created elsewhere and uploaded to the device or automatically generated on the device. If uploading existing keys, be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

**Note:** If you are providing a key by uploading a file, make sure that the key is not password protected.

To configure the SSH client users:

1. Select **SSH** on the menu bar and then **SSH Client Users** at the top of the page. The SSH Client: Users page appears.

![SSH Client: Users](image)
2. Enter or modify the following settings:

### Table 11-10  SSH Client Users

<table>
<thead>
<tr>
<th>SSH Client: Users Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the name that the device uses to connect to a SSH server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with the username.</td>
</tr>
<tr>
<td>Remote Command</td>
<td>Enter the command that can be executed remotely. Default is <strong>shell</strong>, which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.</td>
</tr>
<tr>
<td>Private Key</td>
<td>Enter the name of the existing private key you want to use with this SSH client user. You can either enter the path and name of the key, or use the <strong>Browse</strong> button to select the key.</td>
</tr>
<tr>
<td>Public Key</td>
<td>Enter the path and name of the existing public key you want to use with this SSH client user or use the <strong>Browse</strong> button to select the key.</td>
</tr>
</tbody>
</table>

**Note:** If the user public key is known on the remote SSH server, the SSH server does not require a password. The Remote Command is provided to the SSH server upon connection. It specifies the application to execute upon connection. The default is a command shell.

**Note:** Configuring the SSH client’s known hosts is optional. It prevents Man-In-The-Middle (MITM) attacks.

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Select the key type to be used. Choices are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>use this key with the SSH1 and SSH2 protocols.</td>
</tr>
<tr>
<td>DSA</td>
<td>use this key with the SSH2 protocol.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create New Keys</th>
<th>Select the key type to be used for the new key. Choices are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the name of the user associated with the new key.</td>
</tr>
<tr>
<td>Key Type</td>
<td>Select the key type to be used for the new key. Choices are:</td>
</tr>
<tr>
<td>RSA</td>
<td>use this key with the SSH1 and SSH2 protocols.</td>
</tr>
<tr>
<td>DSA</td>
<td>use this key with the SSH2 protocol.</td>
</tr>
<tr>
<td>Bit Size</td>
<td>Select the bit length of the new key:</td>
</tr>
<tr>
<td>512</td>
<td>768</td>
</tr>
<tr>
<td>1024</td>
<td>Using a larger Bit Size takes more time to generate the key. Approximate times are:</td>
</tr>
<tr>
<td>10 seconds for a 512 bit RSA Key</td>
<td>15 seconds for a 768 bit RSA Key</td>
</tr>
<tr>
<td>1 minute for a 1024 bit RSA key</td>
<td>30 seconds for a 512 bit DSA key</td>
</tr>
<tr>
<td>1 minute for a 768 bit DSA key</td>
<td>2 minutes for a 1024 bit DSA key</td>
</tr>
</tbody>
</table>

**Note:** Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 1024 bits long. It can work with larger keys (up to 2048 bit) if they are imported or otherwise created.

3. Click **Submit**.

4. In the **Current Configuration** table, click **Delete User** to delete currently stored user settings as necessary.
SSL Settings

Secure Sockets Layer (SSL) is a protocol for managing the security of data transmission over the Internet. It provides encryption, authentication, and message integrity services. SSL is widely used for secure communication to a web server.

Certificate/Private key combinations can be obtained from an external Certificate Authority (CA) and downloaded into the unit. Self-signed certificates with associated private key can be generated by the device server itself.

For more information regarding Certificates and how to obtain them, see SSL Certificates and Private Keys (on page 97).

SSL uses digital certificates for authentication and cryptography against eavesdropping and tampering. Sometimes only the server is authenticated; sometimes both server and client are authenticated. The EDS device server can be server and/or client, depending on the application. Public key encryption systems exchange information and keys and set up the encrypted tunnel.

Efficient symmetric encryption methods encrypt the data going through the tunnel after it is established. Hashing provides tamper detection.

Applications that can make use of SSL are Tunneling, Secure Web Server, and WLAN interface. The EDS unit supports TLS1.0 and TLS1.1.

SSL Cipher Suites

The SSL standard defines only certain combinations of certificate type, key exchange method, symmetric encryption, and hash method. Such a combination is called a cipher suite. Supported cipher suites include the following:

Table 11-11 Supported Cipher Suites

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Key Exchange</th>
<th>Encryption</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>RSA</td>
<td>128 bits AES</td>
<td>SHA1</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA</td>
<td>Triple DES</td>
<td>SHA1</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA</td>
<td>128 bits RC4</td>
<td>MD5</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA</td>
<td>128 bits RC4</td>
<td>SHA1</td>
</tr>
<tr>
<td>RSA</td>
<td>1024 bits RSA</td>
<td>56 bits RC4</td>
<td>MD5</td>
</tr>
<tr>
<td>RSA</td>
<td>1024 bits RSA</td>
<td>56 bits RC4</td>
<td>SHA1</td>
</tr>
<tr>
<td>RSA</td>
<td>1024 bits RSA</td>
<td>40 bits RC4</td>
<td>MD5</td>
</tr>
</tbody>
</table>

Whichever side is acting as server decides which cipher suite to use for a connection. It is usually the strongest common denominator of the cipher suite lists supported by both sides.

Note: The SHA2 hash algorithm negotiates with the MD5 or SHA1 ciphers to establish a successful SSL connection.

SSL Certificates
The goal of a certificate is to authenticate its sender. It is analogous to a paper document that contains personal identification information and is signed by an authority, for example a notary or government agency.

The principles of Security Certificate require that in order to sign other certificates, the authority uses a private key. The published authority certificate contains the matching public key that allows another to verify the signature but not recreate it.

The authority’s certificate can be signed by itself, resulting in a self-signed or trusted-root certificate, or by another (higher) authority, resulting in an intermediate authority certificate. You can build up a chain of intermediate authority certificates, and the last certification will always be a trusted-root certificate.

An authority that signs other certificates is also called a Certificate Authority (CA). The last in line is then the root-CA. VeriSign is a famous example of such a root-CA. Its certificate is often built into web browsers to allow verifying the identity of website servers, which need to have certificates signed by VeriSign or another public CA. Since obtaining a certificate signed by a CA that is managed by another company can be expensive, it is possible to have your own CA. Tools exist to generate self-signed CA certificates or to sign other certificates.

A certificate request is a certificate that has not been signed and only contains the identifying information. Signing it makes it a certificate. A certificate is also used to sign any message transmitted to the peer to identify the originator and prevent tampering while transported.

**SSL RSA**

As mentioned above, the certificates contain a public key. Different key exchange methods require different public keys and thus different styles of certificate. The EDS device server supports key exchange methods that require a RSA-style certificate and key exchange methods that require a RSA-style certificate. If only one of these certificates is stored in the EDS unit, only those key exchange methods that can work with that style certificate are enabled. RSA is sufficient in most cases.

The creation of a self-signed SSL certificate supports MD5 hash algorithms with a 1024 bit key length. Uploading an SSL certificate will support MD5, SHA1 and SHA2 families (e.g., SHA256, SHA384, and SHA512 hash algorithms with key lengths of 1024 & 2048 bits).

**SSL Certificates and Private Keys**

You can obtain a certificate by completing a certificate request and sending it to a certificate authority that will create a certificate/key combo, usually for a fee, or you can generate your own. A few utilities exist to generate self-signed certificates or sign certificate requests. The EDS device server also has the ability to generate its own self-signed certificate/key combo.

You can use XML to export the certificate in PEM format, but you cannot export the key. Hence the internal certificate generator can only be used for certificates that are to identify that particular EDS unit.

Certificates and private keys can be stored in several file formats. Best known are PKCS12, DER and PEM. Certificate and key can be in the same file or in separate files. The key can be encrypted with a password or not. The EDS device server currently only accepts separate PEM files. The key needs to be unencrypted.
SSL Utilities
Several utilities exist to convert between the formats.

OpenSSL
Open source is a set of SSL related command line utilities. It can act as server or client. It can generate or sign certificate requests. It can convert all kinds of formats. Executables are available for Linux and Windows. To generate a self-signed RSA certificate/key combo use the following commands in the order shown:

```plaintext
openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout mp_key.pem -out mp_cert.pem
```

**Note:** Signing other certificate requests is also possible with OpenSSL. See [www.openssl.org](http://www.openssl.org) or [www.madboa.com/geek/openssl](http://www.madboa.com/geek/openssl) for more information.

Steel Belted RADIUS
Commercial RADIUS server by Juniper Networks that provides a GUI administration interface. It also provides a certificate request and self-signed certificate generator. The self-signed certificate has extension .sbrpvk and is in the PKCS12 format. OpenSSL can convert this into a PEM format certificate and key by using the following commands in the order shown:

```plaintext
openssl pkcs12 -in sbr_certkey.sbrpvk -nodes -out sbr_certkey.pem
```

The sbr_certkey.pem file contains both certificate and key. If loading the SBR certificate into EDS unit as an authority, you will need to edit it.

1. Open the file in any plain text editor.
2. Delete all info before the following: “----- BEGIN CERTIFICATE-----“
3. Delete all info after the following: “----- END CERTIFICATE-----“
4. Save as sbr_cert.pem. SBR accepts trusted-root certificates in the DER format.
5. Again, OpenSSL can convert any format into DER by using the following commands in the order shown:

```plaintext
openssl x509 -inform pem -in mp_cert.pem -outform der -out mp_cert.der
```

**Note:** With SBR, when the identity information includes special characters such as dashes and periods, SBR changes the format it uses to store these strings and becomes incompatible with the current EDS release. We will add support for this and other formats in future releases. Free RADIUS—Linux open-source RADIUS server. It is versatile, but complicated to configure.

Free RADIUS
Free RADIUS is a Linux open-source RADIUS server. It is versatile, but complicated to configure.
SSL Configuration

To configure SSL settings:

1. Select SSL from the main menu. The SSL page appears.

![SSL Configuration Page]

- **Upload Certificate**
  - New Certificate: Choose File, No file chosen
  - New Private Key: Choose File, No file chosen
  - Submit

- **Upload Authority Certificate**
  - Authority: Choose File, No file chosen
  - Submit

- **Create New Self-Signed Certificate**
  - Country (2 Letter Code):
  - State/Province:
  - Locality (City):
  - Organization:
  - Organization Unit:
  - Common Name:
  - Expires: 12/31/2020
  - Key length: 1024 bit
  - Type: RSA
  - Submit

- **Current SSL Certificates**
  - <None>

- **Current Certificate Authorities**
  - <None>
2. Enter or modify the following settings:

**Table 11-13 SSL**

<table>
<thead>
<tr>
<th>SSL Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Certificate</strong></td>
<td>This certificate identifies the device to peers. It is used for HTTPS and SSL Tunneling.</td>
</tr>
<tr>
<td></td>
<td>Enter the path and name of the certificate you want to upload, or use the Choose File button to select the certificate.</td>
</tr>
<tr>
<td></td>
<td>RSA certificates with 1024 or 2048 bit public keys are allowed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The format of the file must be PEM. The file must start with &quot;-----BEGIN CERTIFICATE-----&quot; and end with &quot;-----END CERTIFICATE-----&quot;. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.</td>
</tr>
<tr>
<td><strong>New Private Key</strong></td>
<td>Enter the path and name of the private key you want to upload, or use the Choose File button to select the private key. The key needs to belong to the certificate entered above.</td>
</tr>
<tr>
<td></td>
<td>The format of the file must be PEM. The file must start with &quot;-----BEGIN RSA PRIVATE KEY-----&quot; and end with &quot;-----END RSA PRIVATE KEY-----&quot;. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.</td>
</tr>
<tr>
<td><strong>Upload Authority Certificate</strong></td>
<td>One or more authority certificates are needed to verify a peer's identity. It is used for SSL Tunneling. These certificates do not require a private key.</td>
</tr>
<tr>
<td></td>
<td>Enter the path and name of the certificate you want to upload, or use the Choose File button to select the certificate.</td>
</tr>
<tr>
<td></td>
<td>RSA certificates with 1024 or 2048 bit public keys are allowed.</td>
</tr>
<tr>
<td></td>
<td>The format of the file must be PEM. The file must start with &quot;-----BEGIN CERTIFICATE-----&quot; and end with &quot;-----END CERTIFICATE-----&quot;. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.</td>
</tr>
<tr>
<td><strong>Create New Self-Signed Certificate</strong></td>
<td>Enter the 2-letter country code to be assigned to the new self-signed certificate.</td>
</tr>
<tr>
<td><strong>Country (2 Letter Code)</strong></td>
<td><strong>Examples</strong>: US for United States and CA for Canada</td>
</tr>
<tr>
<td><strong>State/Province</strong></td>
<td>Enter the state or province to be assigned to the new self-signed certificate.</td>
</tr>
<tr>
<td><strong>Locality (City)</strong></td>
<td>Enter the city or locality to be assigned to the new self-signed certificate.</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Enter the organization to be associated with the new self-signed certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: If your company is called Widgets, and you are setting up a web server for the Sales department, enter Widgets for the organization.</td>
</tr>
<tr>
<td><strong>Organization Unit</strong></td>
<td>Enter the organizational unit to be associated with the new self-signed certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong>: If your company is setting up a web server for the Sales department, enter Sales for your organizational unit.</td>
</tr>
</tbody>
</table>
3. Click **Submit**.
12: Modbus

Note: Modbus applies only to EDS4100, as this feature is not supported on EDS8/16/32PR and EDS8/16PS.

Modbus ASCII/RTU based serial slave devices can be connected via the Ethernet through an existing Modbus TCP/IP network. Any device having access to a given Modbus implementation will be able to perform full range of operations that the implementation supports. Modbus/TCP uses a reserved TCP port of 502 and includes a single byte function code (1=255) preceded by a 6 byte header:

<table>
<thead>
<tr>
<th>Transaction ID (2 bytes)</th>
<th>Identification of request/response transaction - copied by slave</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol ID (2 bytes)</td>
<td>0 - Modbus protocol</td>
</tr>
<tr>
<td>Length (2 bytes)</td>
<td>Number of following bytes includes the unit identifier</td>
</tr>
<tr>
<td>Address (1 byte)</td>
<td>Identification of remove slave</td>
</tr>
</tbody>
</table>

Table 12-1 6 Byte Header of Modbus Application Protocol

Serial Transmission Mode

Evolution OS® products can be set up to communicate on standard Modbus networks using either RTU or ASCII. Users select the desired mode and serial port communication parameters (baud rate, parity mode, etc) when in the line configuration options.

<table>
<thead>
<tr>
<th>RTU</th>
<th>ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address: 8 bits (0 to 247 decimal, 0 is used for broadcast)</td>
<td>Address: 2 CHARs</td>
</tr>
<tr>
<td>Function: 8 bits (1 to 255, 0 is not valid)</td>
<td>Function: 2 CHARs</td>
</tr>
<tr>
<td>Data: N X 8 bits (N=0 to 252 bytes)</td>
<td>Data: N CHARs (N=0 to 252 CHARs)</td>
</tr>
<tr>
<td>CRC Check: 16 bits</td>
<td>LRC Check: 2 CHARs</td>
</tr>
</tbody>
</table>

Table 12-2 Modbus Transmission Modes

The Modbus web pages allow you to check Modbus status and make configuration changes. This chapter contains the following sections:

- Modbus Statistics
- Modbus Configuration
Modbus Statistics

This read-only web page displays the current connection status of the Modbus servers listening on the TCP ports. When a connection is active, the remote client information is displayed as well as the number of PDUs that have been sent and received. Additionally, a Kill link will be present which can be used to kill the connection.

To view modbus statistics:

1. Click Modbus on the menu bar and click Statistics at the top of the page. The Modbus Statistics page appears.

![Figure 12-3 Modbus Statistics](image)

<table>
<thead>
<tr>
<th>TCP Server</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>State:</td>
<td>Up</td>
</tr>
<tr>
<td>Port:</td>
<td>502</td>
</tr>
<tr>
<td>Last Connection:</td>
<td>local 502 &lt; 172.19.205.10:3903</td>
</tr>
<tr>
<td>Uptime:</td>
<td>0 days 02:36:20</td>
</tr>
<tr>
<td>Total PDUs In:</td>
<td>0</td>
</tr>
<tr>
<td>Total PDUs Out:</td>
<td>0</td>
</tr>
<tr>
<td>Total Connections:</td>
<td>1</td>
</tr>
<tr>
<td>Current Connections:</td>
<td>[Kill]</td>
</tr>
<tr>
<td></td>
<td>local 502 &lt; 172.19.205.10:3903</td>
</tr>
<tr>
<td></td>
<td>Uptime: 0 days 02:36:48</td>
</tr>
<tr>
<td></td>
<td>PDUs In: 0</td>
</tr>
<tr>
<td></td>
<td>PDUs Out: 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional TCP Server</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>State:</td>
<td>Up</td>
</tr>
<tr>
<td>Port:</td>
<td>505</td>
</tr>
<tr>
<td>Last Connection:</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>Uptime:</td>
<td>0 days 02:35:53</td>
</tr>
<tr>
<td>Total PDUs In:</td>
<td>0</td>
</tr>
<tr>
<td>Total PDUs Out:</td>
<td>0</td>
</tr>
<tr>
<td>Total Connections:</td>
<td>0</td>
</tr>
<tr>
<td>Current Connections:</td>
<td>&lt;None&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Slave</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total PDUs In:</td>
<td>0</td>
</tr>
<tr>
<td>Total PDUs Out:</td>
<td>0</td>
</tr>
<tr>
<td>Exception Count:</td>
<td>0</td>
</tr>
</tbody>
</table>
Modbus Configuration

This web page shows the current negotiated Modbus settings and allows configuration changes.

To view and configure the Modbus Server:

1. Click Modbus on the menu bar and then click Configuration at the top of the page. The Modbus Configuration page appears.

![Modbus Configuration](image)

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Modbus Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Server State</td>
<td>If On, the Modbus server is active on TCP 502.</td>
</tr>
<tr>
<td>Additional TCP Server Port</td>
<td>If present, is used in addition to TCP port 502.</td>
</tr>
<tr>
<td>Response Timeout</td>
<td>The number of milliseconds to wait for a response on the serial side. The device returns exception code 11 to the network master controller if the slave serial device fails to reply within this time out.</td>
</tr>
<tr>
<td>RSS Trace Input</td>
<td>If On, each PDU received on the Modbus serial line creates a non-persistent descriptive item in the RSS feed.</td>
</tr>
</tbody>
</table>

3. Click Submit. The changes take effect immediately.

Note: The serial line protocol must also be configured for Modbus, in addition to configuring the Modbus server. See Chapter 8: Line and Tunnel Settings on page 47 for details.
13: **Maintenance and Diagnostic Settings**

This chapter describes maintenance and diagnostic methods and contains the following sections:

- Filesystem Settings
- Protocol Stack Settings
- IP Address Filter
- Query Port
- Diagnostics
- System Settings

**Filesystem Settings**

The EDS device server uses a flash filesystem to store files. Use the Filesystem option to view current file statistics or modify files. There are two subsections: Statistics and Browse.

The Statistics section of the Filesystem web page shows current statistics and usage information of the flash filesystem. In the Browser section of the Filesystem web page, you can create files and folders, upload files, copy and move files, and use TFTP.

**Filesystem Statistics**

This page shows various statistics and current usage information of the flash filesystem.

**To view filesystem statistics:**

1. Select **Filesystem** on the menu bar. The Filesystem page opens and shows the current filesystem statistics and usage.

**To compact or format the filesystem:**

1. Back up all files as necessary.
2. Select **Filesystem** on the menubar, if you are not already in the Filesystem page.
3. Click **Compact** in the Actions row.

**Note:** The compact should not be needed under normal circumstances as the system manages this automatically.

4. Back up all files before you perform the next (Format) step, because all user files get erased in that step.
5. Click **Format** in the Actions row. The configuration is retained and all files on the filesystem will be destroyed.
6. Click **OK** in the warning window which appears.

---

**Figure 13-1  Filesystem Statistics**

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Browse</th>
</tr>
</thead>
</table>

**Filesystem Statistics**

- **Filesystem Size:** 7.600000 Mbytes (7654320 bytes)
- **Available Space:** 7.474350 Mbytes (7837320 bytes) (99%)  
  **Clean Space:** 7.336333 Mbytes (7692972 bytes) (97%)
- **Dirty Space:** 140.956 kbytes (144348 bytes) (1%)
- **File & Dir Space Used:** 36.367 kbytes (37000 bytes) (0%)
- **Data Space Used:** 22.559 kbytes (23134 bytes)
- **Number of Files:** 0
- **Number of Dirs:** 0
- **Number of System Files:** 2
- **Opened Files:** 0
- **Locked Files:** 0
- **Opened for Sharing:** 0
- **Current Bank:** B
- **FW Sectors:** 02 - 07, 9 erase cycles
- **Bank A Sectors:** 06 - 07, 0 erase cycles
- **Bank B Sectors:** 06 - 12, 2 erase cycles
- **Busy:** No
- **Actions:** [Compact] [Format]
Filesystem Browser

*To browse the filesystem:*

1. Select **Filesystem** on the menu bar and then **Browse** at the top of the page. The Filesystem Browser page opens.

2. Select a filename to view the contents.

3. Click the **X** next to a filename to delete the file or directory. You can only delete a directory if it is empty.
4. Enter or modify the following settings:

**Note:** Changes apply to the current directory view. To make changes within other folders, select the folder or directory and then enter the parameters in the settings listed below.

### Table 13-3 Filesystem Browser

<table>
<thead>
<tr>
<th>Filesystem Browser Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create</strong></td>
<td></td>
</tr>
<tr>
<td>File</td>
<td>Enter the name of the file you want to create, and then click <strong>Create</strong>.</td>
</tr>
<tr>
<td>Directory</td>
<td>Enter the name of the directory you want to create, and then click <strong>Create</strong>.</td>
</tr>
<tr>
<td>Upload File</td>
<td>Enter the path and name of the file you want to upload by means of HTTP/HTTPS or use the <strong>Choose File</strong> button to select the file, and then click <strong>Upload</strong>.</td>
</tr>
<tr>
<td><strong>Copy File</strong></td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Enter the location where the file you want to copy resides.</td>
</tr>
<tr>
<td>Destination</td>
<td>Enter the location where you want the file copied. After you specify a source and destination, click <strong>Copy</strong> to copy the file.</td>
</tr>
<tr>
<td><strong>Move</strong></td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Enter the location where the file you want to move resides.</td>
</tr>
<tr>
<td>Destination</td>
<td>Enter the location where you want the file moved. After you specify a source and destination, click <strong>Move</strong> to move the file.</td>
</tr>
<tr>
<td><strong>TFTP</strong></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Select the action that is to be performed via TFTP:</td>
</tr>
<tr>
<td>Get</td>
<td>= a &quot;get&quot; command will be executed to store a file locally.</td>
</tr>
<tr>
<td>Put</td>
<td>= a &quot;put&quot; command will be executed to send a file to a remote location.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select a TFTP mode to use. Choices are:</td>
</tr>
<tr>
<td>ASCII</td>
<td></td>
</tr>
<tr>
<td>Binary</td>
<td></td>
</tr>
<tr>
<td>Local File</td>
<td>Enter the name of the local file on which the specified &quot;get&quot; or &quot;put&quot; action is to be performed.</td>
</tr>
<tr>
<td>Remote File</td>
<td>Enter the name of the file at the remote location that is to be stored locally (&quot;get&quot;) or externally (&quot;put&quot;).</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the IP address or name of the host involved in this operation.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the number of the port involved in TFTP operations on which the specified TFTP get or put command will be performed. Click <strong>Transfer</strong> to perform the TFTP transfer.</td>
</tr>
</tbody>
</table>
Protocol Stack Settings

In the Protocol Stack web page, you can configure TCP, IP, ICMP, SMTP and ARP.

TCP Settings

*To configure the TCP network protocol:*

1. Select **Protocol Stack** on the menu bar.
2. Select **TCP**.

3. Modify the following settings:

<table>
<thead>
<tr>
<th>Protocol Stack TCP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Send RSTs</strong></td>
<td>Click <strong>Enabled</strong> to send RSTs or <strong>Disabled</strong> to stop sending RSTs. TCP contains six control bits, with one or more defined in each packet. RST is one of the control bits. The RST bit is responsible for telling the receiving TCP stack to end a connection immediately. <strong>Note:</strong> Setting the RSTs may pose a security risk.</td>
</tr>
<tr>
<td><strong>Ack Limit</strong></td>
<td>Enter a number to limit how many packets get received before an ACK gets forced. If there is a large amount of data to acknowledge, an ACK gets forced. If the sender TCP implementation waits for an ACK before sending more data even though the window is open, setting the <strong>Ack Limit</strong> to 1 packet improves performance by forcing immediate acknowledgements.</td>
</tr>
<tr>
<td><strong>Send Data</strong></td>
<td>The <strong>Send Data</strong> selection governs when data may be sent into the network. The <strong>Standard</strong> implementation waits for an ACK before sending a packet less than the maximum length. Select <strong>Expedited</strong> to send data whenever the window allows it.</td>
</tr>
</tbody>
</table>
4. Click **Submit**.

**IP Settings**

*To configure the network protocol settings for IP:*

1. Select **Protocol Stack** on the menu bar.
2. Select **IP**.

3. Modify the following settings:

<table>
<thead>
<tr>
<th><strong>Table 13-7 IP Protocol Settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol Stack</strong></td>
</tr>
<tr>
<td><strong>TCP Settings</strong></td>
</tr>
<tr>
<td><strong>IP Settings</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Max Retrans</strong></td>
</tr>
<tr>
<td>Enter the maximum number of retransmissions of a packet that will be attempted before failing.</td>
</tr>
<tr>
<td><strong>Max Retrans Syn/Ack</strong></td>
</tr>
<tr>
<td>Enter the maximum number of retransmissions of a SYN that will be attempted before failing. It is lower than “Max Retrans” to thwart denial-of-service attacks.</td>
</tr>
<tr>
<td><strong>Max Timeout</strong></td>
</tr>
<tr>
<td>Enter the maximum time between retransmissions.</td>
</tr>
<tr>
<td><strong>Max Retrans</strong></td>
</tr>
<tr>
<td>Enter the maximum number of retransmissions of a packet that will be attempted before failing.</td>
</tr>
<tr>
<td><strong>Max Retrans Syn/Ack</strong></td>
</tr>
<tr>
<td>Enter the maximum number of retransmissions of a SYN that will be attempted before failing. It is lower than “Max Retrans” to thwart denial-of-service attacks.</td>
</tr>
<tr>
<td><strong>Max Timeout</strong></td>
</tr>
<tr>
<td>Enter the maximum time between retransmissions.</td>
</tr>
<tr>
<td><strong>Max Retrans</strong></td>
</tr>
<tr>
<td>Enter the maximum number of retransmissions of a packet that will be attempted before failing.</td>
</tr>
<tr>
<td><strong>Max Retrans Syn/Ack</strong></td>
</tr>
<tr>
<td>Enter the maximum number of retransmissions of a SYN that will be attempted before failing. It is lower than “Max Retrans” to thwart denial-of-service attacks.</td>
</tr>
<tr>
<td><strong>Max Timeout</strong></td>
</tr>
<tr>
<td>Enter the maximum time between retransmissions.</td>
</tr>
<tr>
<td><strong>Max Retrans</strong></td>
</tr>
<tr>
<td>Enter the maximum number of retransmissions of a packet that will be attempted before failing.</td>
</tr>
<tr>
<td><strong>Max Retrans Syn/Ack</strong></td>
</tr>
<tr>
<td>Enter the maximum number of retransmissions of a SYN that will be attempted before failing. It is lower than “Max Retrans” to thwart denial-of-service attacks.</td>
</tr>
<tr>
<td><strong>Max Timeout</strong></td>
</tr>
<tr>
<td>Enter the maximum time between retransmissions.</td>
</tr>
</tbody>
</table>

3. Modify the following settings:

<table>
<thead>
<tr>
<th><strong>Table 13-7 IP Protocol Settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol Stack</strong></td>
</tr>
<tr>
<td><strong>TCP Settings</strong></td>
</tr>
<tr>
<td><strong>IP Settings</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>IP Time to Live</strong></td>
</tr>
<tr>
<td>This value typically fills the Time To Live in the IP header. SNMP refers to this value as “ipDefaultTTL”. Enter the number of hops to be transmitted before the packet is discarded.</td>
</tr>
<tr>
<td><strong>Multicast Time to Live</strong></td>
</tr>
<tr>
<td>This value fills the Time To Live in any multicast IP header. Normally this value will be one so the packet will be blocked at the first router. It is the number of hops allowed before a Multicast packet is discarded. Enter the value to be greater than one to intentionally propagate multicast packets to additional routers.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
ICMP Settings

To configure the ICMP network protocol:

1. Select Protocol Stack on the menu bar.
2. Select ICMP.
3. Select the appropriate state.

Table 13-9 ICMP Settings

<table>
<thead>
<tr>
<th>Protocol Stack ICMP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The State selection is used to turn on/off processing of ICMP messages. This includes both incoming and outgoing messages. Choose Enabled or Disabled.</td>
</tr>
</tbody>
</table>

4. Click Submit.
ARP Settings

To configure the ARP network protocol:

1. Select Protocol Stack on the menu bar.
2. Select ARP.

3. Modify the following settings:

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Timeout</td>
<td>This is the maximum duration an address remains in the cache. Enter the time, in <strong>hours, minutes</strong> and <strong>seconds</strong>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address to add to the ARP cache.</td>
</tr>
</tbody>
</table>

Table 13-11 ARP Settings
13: Maintenance and Diagnostic Settings

Table 13-11 ARP Settings

<table>
<thead>
<tr>
<th>Protocol Stack ARP Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address to add to the ARP cache.</td>
</tr>
</tbody>
</table>

**Note:** Both the IP and MAC addresses are required for the ARP cache.

4. Click **Submit** for ARP or **Add** after supplying both address fields for ARP cache.

5. Remove entries from the ARP cache, as desired:
   - Click **Remove All** to remove all entries in the ARP cache.
   - OR
   - Click **Remove** beside a specific entry to remove it from the ARP cache.

SMTP Settings

SMTP is configuration for a basic SMTP proxy. An SMTP proxy in this sense is a simple forwarding agent.

**Note:** Lantronix does not support SMTP AUTH or any other authentication or encryption schemes for email. Please see Email Settings for additional information.

To configure the SMTP network protocol:

1. Select **Protocol Stack** on the menu bar.

2. Select **SMTP**.

3. Modify the following settings:

   **Table 13-13 SMTP Settings**

<table>
<thead>
<tr>
<th>Protocol Stack SMTP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay Address</td>
<td>Address of all outbound email messages through a mail server. Can contain either a hostname or an IP address.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Port utilized for the delivery of outbound email messages.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
IP Address Filter

The IP address filter specifies the hosts and subnets permitted to communicate with the EDS device server. When the filter list is empty, then all IP addresses are allowed.

**Note:** If using DHCP/BOOTP, ensure the DHCP/BOOTP server is in this list.

To configure the IP address filter:

1. Select **IP Address Filter** on the menu bar. The IP Address Filter page opens to display the current configuration.

![Figure 13-14  IP Address Filter Configuration](image)

**Note:** If you enter any filter, be careful to make sure that your network IP address is covered. Otherwise you will lose access to the EDS unit. You will have to then access the EDS device server from a different computer to reset the configuration.

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>IP Address Filter Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address to add to the IP filter table.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Enter the IP address' network mask in dotted notation.</td>
</tr>
</tbody>
</table>

3. Click **Add**.

**Note:** In the Current State table, click **Remove** to delete any existing settings, as necessary.
Query Port

The query port (0x77FE) is used for the automatic discovery of the device by the DeviceInstaller utility. Only 0x77FE discover messages from DeviceInstaller are supported. For more information on DeviceInstaller, see Using DeviceInstaller (on page 36).

To configure the query port server:

1. Select Query Port on the menu bar. The Query Port page opens to display the current configuration.

2. Select On to enable the query port server.

3. Click Submit.
Diagnostics

The EDS device server has several tools to perform diagnostics and view device statistics. These include information on:

- **Hardware**
- **MIB-II Statistics**
- **IP Sockets**
- **Ping**
- **Traceroute**
- **Log**
- **Memory**
- **Buffer Pools**
- **Processes**

**Hardware**

This read-only page shows the current device's hardware configuration.

**To display hardware diagnostics:**

1. Select **Diagnostics** on the menu bar. The Diagnostics: Hardware page opens and shows the current hardware configuration.

![Diagnostics: Hardware](image)
MIB-II Statistics

The MIB-II Network Statistics page shows the various SNMP-served Management Information Bases (MIBs) available on the EDS device server.

To view MIB-II statistics:

1. Select Diagnostics on the menu bar and then MIB-II at the top of the page menu. The MIB-II Network Statistics page opens.

2. Click any of the available links to open the corresponding table and statistics. For more information, refer to the table below:

<table>
<thead>
<tr>
<th>RFC 1213</th>
<th>Original MIB-II definitions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2011</td>
<td>Updated definitions for IP and ICMP.</td>
</tr>
<tr>
<td>RFC 2012</td>
<td>Updated definitions for TCP.</td>
</tr>
<tr>
<td>RFC 2013</td>
<td>Updated definitions for UDP.</td>
</tr>
<tr>
<td>RFC 2096</td>
<td>Definitions for IP forwarding.</td>
</tr>
</tbody>
</table>
13: Maintenance and Diagnostic Settings

IP Sockets

To display open IP sockets:

1. Select **Diagnostics** on the menu bar and then **IP Sockets** at the top of the page. The IP Sockets page opens and shows all of the open IP sockets on the device.

![Figure 13-20 IP Sockets](image)

### IP Sockets

<table>
<thead>
<tr>
<th>Protocol</th>
<th>RxQ</th>
<th>TxQ</th>
<th>LocalAddr:Port</th>
<th>RemoteAddr:Port</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.192:161</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.192:21</td>
<td>255.255.255.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.192:89</td>
<td>255.255.255.255</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.192:514</td>
<td>172.19.32.23:514</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.198:80</td>
<td>255.255.255.255</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.198:3076</td>
<td>172.19.220:32770</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.198:23</td>
<td>255.255.255.255</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.198:22</td>
<td>255.255.255.255</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>4</td>
<td>172.19.100.198:80</td>
<td>172.19.250:1844</td>
<td>ESTABLISHED</td>
</tr>
</tbody>
</table>

Ping

EDS device server uses 56 bytes of data in a ping packet. Ping size is not configurable.

To ping a remote device or computer:

1. Select **Diagnostics** on the menu bar and then **Ping** at the top of the page. The Diagnostics: Ping page opens.

![Figure 13-21 Diagnostics: Ping](image)

2. Enter or modify the following settings:
3. Click **Submit**. The results of the ping display in the page.

### Traceroute

Here you can trace a packet from the EDS unit to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes. If you visit a web site whose pages appear slowly, you can use traceroute to determine where the longest delays are occurring.

**To use Traceroute:**

1. Select **Diagnostics** on the menu bar and then **Traceroute** at the top of the page. The Diagnostics: Traceroute page opens.

2. Enter or modify the following setting:

   **Table 13-24 Diagnostics: Traceroute**

<table>
<thead>
<tr>
<th>Diagnostics: Traceroute Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the IP address or DNS hostname. This address is used to show the path between it and the device when issuing the traceroute command.</td>
</tr>
</tbody>
</table>

3. Click **Submit**. The results of the traceroute display in the page.
Log

Here you can enable a diagnostics log of configuration items:

To use diagnostics logging:

1. Select Diagnostics on the menu bar and then Log at the top of the page. The Diagnostics: Log page opens.

![Figure 13-25 Diagnostics: Log]

2. Select the Output type:
   - Disable (default)
   - Filesystem
   - Line <number>

![Figure 13-26 Diagnostics: Log (Filesystem)]
3. Enter the Max Length in kilobytes (if filesystem output type is selected).

4. Select the Severity Level (if a line or filesystem output type is selected):
   - Debug
   - Information
   - Notice
   - Warning
   - Error

**Memory**

This read-only web page shows the total memory and available memory (in bytes), along with the number of fragments, allocated blocks, and memory status.

*To display memory statistics:*

1. Select **Diagnostics** on the menu bar and then **Memory** at the top of the page. The Diagnostics: Memory page appears.
Buffer Pools
Several parts of the EDS system use private buffer pools to ensure deterministic memory management.

To display the buffer pools:
1. Select **Diagnostics** on the menu bar and then **Buffer Pools** at the top of the page. The Diagnostics: Buffer Pools page opens.

---

**Figure 13-29 Diagnostics: Buffer Pools**

<table>
<thead>
<tr>
<th>Hardware</th>
<th>MIB-II</th>
<th>IP Sockets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping</td>
<td>Traceroute</td>
<td>Log</td>
</tr>
<tr>
<td>Memory</td>
<td><strong>Buffer Pools</strong></td>
<td>Processes</td>
</tr>
</tbody>
</table>

### Diagnostics: Buffer pools

<table>
<thead>
<tr>
<th>Network Stack Buffer Pool</th>
<th>Total</th>
<th>Free</th>
<th>Used</th>
<th>MaxUsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Headers</td>
<td>512</td>
<td>510</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>Cluster Pool Size: 2048</td>
<td>255</td>
<td>254</td>
<td>2</td>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ethernet Driver Buffer Pool</th>
<th>Total</th>
<th>Free</th>
<th>Used</th>
<th>MaxUsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Headers</td>
<td>2048</td>
<td>1984</td>
<td>64</td>
<td>70</td>
</tr>
<tr>
<td>Cluster Pool Size: 2048</td>
<td>1024</td>
<td>960</td>
<td>64</td>
<td>69</td>
</tr>
</tbody>
</table>
13: Maintenance and Diagnostic Settings

Processes

The Processes web page shows all the processes currently running on the system. It shows the Process ID (PID), the percentage of total CPU cycles a process used within the last three seconds, the total stack space available, the maximum amount of stack space used by the process since it started, and the process name.

To display the processes running and their associated statistics:

1. Select **Diagnostics** on the menu bar and then **Processes** at the top of the page.

**Note:** The Adobe SVG plug-in is required to view the CPU Load Graph.
Clock

*Note:* Clock is available in EDS8/16/32PR device servers. RTC (Real Time Clock) is available in EDS4100 device servers.

The current date or time displayed on the EDS8/16/32PR unit can be viewed and modified through the Clock feature. The Clock settings page can be updated by one of two methods: manually entering the date and time or synchronizing with the SNTP.

**To configure Clock settings:**

1. Select Clock on the menu bar. The Clock page opens.

![Figure 13-31 Clock Page](image)

2. Modify the following settings to set change the current date and time:

<table>
<thead>
<tr>
<th>Table 13-32  Clock Settings</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Clock Page Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Method</strong></td>
<td>Select either Manual or SNTP method of setting the clock:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manual</strong>: allows you to manually select the year, month, day, hour, minute and second through drop-down fields.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SNTP</strong>: keeps time synchronized with the NTP Server.</td>
</tr>
<tr>
<td><strong>NTP Server</strong></td>
<td>Enter the NTP server’s IP address or hostname to set the NTP server.</td>
</tr>
<tr>
<td></td>
<td><em>Note: This option becomes available when the SNTP method is selected above.</em></td>
</tr>
</tbody>
</table>
3. Click **Submit**.

### Real Time Clock

*Note: RTC (Real Time Clock) is supported in EDS4100 device servers. Clock is supported in EDS8/16/32PR device servers.*

The current date or time displayed on the EDS8/16PS and EDS4100 device/terminal servers can be viewed and modified through the Real Time Clock feature. The EDS8/16/32PR unit utilizes the *Clock* feature described on page 123 to set date or time.

**To configure Real Time Clock settings:**

1. Select **0** on the menu bar. The Real Time Clock page opens.

<table>
<thead>
<tr>
<th>Clock Page Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
</table>
| Date                          | From the drop-down lists, select the **Year**, **Month**, and **Day** corresponding to the current date at the location of the EDS.  
  *Note: This option becomes available when the Manual method is selected above.* |
| Time (24 hour)                | From the drop-down list, select the **Hour**, **Min** (minutes), and **Sec** (seconds) corresponding to the current time at the location of the EDS.  
  *Note: This option becomes available when the Manual method is selected above.* |
| Time Zone                     | Select the time zone corresponding to the location of the EDS from the drop-down list. |
2. Modify the following settings to set the current date and time:

<table>
<thead>
<tr>
<th>Table 13-34 Real Time Clock Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Real Time Clock Page Settings</strong></td>
</tr>
<tr>
<td>Time Zone</td>
</tr>
<tr>
<td>Date</td>
</tr>
<tr>
<td>Time (24 hour)</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

**System Settings**

The EDS System web page allows for rebooting the device, restoring factory defaults, uploading new firmware, configuring the short and long name, and viewing the current system configuration.

*To configure system settings:*

1. Select **System** on the menu bar. The System page opens.

![Figure 13-35 System](image-url)
2. Configure the following settings:

### Table 13-36 System

<table>
<thead>
<tr>
<th>System Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot Device</td>
<td>Click Reboot to reboot the device. The system refreshes and redirects the browser to the device home page.</td>
</tr>
<tr>
<td>Restore Factory Defaults</td>
<td>Click Factory Defaults to restore the device to the original factory settings. All configurations will be lost. The device automatically reboots upon setting back to the defaults.</td>
</tr>
<tr>
<td>Upload New Firmware</td>
<td>Click Choose File to locate the firmware file location. Click Upload to install the firmware on the device. The device automatically reboots upon the installation of new firmware.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Close and reopen the web manager browser upon a firmware update.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a new Short Name and a Long Name (if necessary). The Short Name maximum is 32 characters. The Long Name maximum is 64 characters. Changes take place upon the next reboot.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Additional information about long and short name customization is available in Short and Long Name Customization on page 140 of Chapter 15: Branding the EDS Unit.</td>
</tr>
</tbody>
</table>

3. Click Submit.
14: **Advanced Settings**

This chapter describes the configuration of Email, CLI, and XML. It contains the following sections:

- **Email Settings**
- **Command Line Interface Settings**
- **XML Settings**

**Email Settings**

The EDS allows you to view and configure email alerts relating to the events occurring within the system. Please see *SMTP Settings on page 112* for additional information.

**Note:** The following section describes the steps to configure Email 1; these steps also apply to the other Email instances.

**Email Statistics**

This read-only page shows various statistics and current usage information about the email subsystem. When you transmit an email, the transmission to the SMTP server gets logged and displayed in the bottom portion of the page.

1. Select **Email** on the menu bar. The Email web page appears.
2. Select an email number at the top of the page.
3. Select **Statistics**. The Email Statistics page for the selected email appears.
4. Repeat above steps as desired, according to additional email(s) available.

![Figure 14-1 Email Statistics](image-url)
Email Configuration

The EDS device server allows you to view and configure email alerts relating to the events occurring within the system.

To configure email settings:
1. Select Email on the menu bar, if you are not already at the Email web page.
2. Select an email at the top of the page.
3. Select the Configuration submenu. The Email Configuration page opens to display the current email configuration.
4. Enter or modify the following settings:

![Email Configuration Interface]

Table 14-2  Email Configuration

<table>
<thead>
<tr>
<th>Email – Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td>Enter the email address to which the email alerts will be sent. Multiple addresses are separated by semicolon (;). Required field if an email is to be sent.</td>
</tr>
<tr>
<td>CC</td>
<td>Enter the email address to which the email alerts will be copied. Multiple addresses are separated by semicolon (;).</td>
</tr>
<tr>
<td>From</td>
<td>Enter the email address to list in the From field of the email alert. Required field if an email is to be sent.</td>
</tr>
<tr>
<td>Reply To</td>
<td>Enter the email address to list in the Reply-To field of the email alert.</td>
</tr>
<tr>
<td>Subject</td>
<td>Enter the subject for the email alert.</td>
</tr>
</tbody>
</table>
5. Click **Submit**.

To test your configuration:

a. Send an email immediately by clicking **Send Email** at the top of the page.

b. Refer back to the Statistics page for a log of the transaction.

6. Repeat above steps as desired, according to additional email(s) available.

### Command Line Interface Settings

The Command Line Interface (CLI) web page enables you to view statistics about the CLI servers listening on the Telnet and SSH ports and to configure CLI settings.

#### CLI Statistics

This read-only page shows the current connection status of the CLI servers listening on the Telnet and SSH ports. When a connection is active, the following display:

- Remote client information
- Number of bytes that have been sent and received
- A **Kill** link to terminate the connection

To view the CLI Statistics:

1. Select **CLI** on the menu bar. The Command Line Interface Statistics page appears.

<table>
<thead>
<tr>
<th>Description</th>
<th>Message File</th>
<th>Overriding Domain</th>
<th>Server Port</th>
<th>Local Port</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the path of the file to send with the email alert. This file appears within the message body of the email.</td>
<td>Enter the domain name to override the current domain name in EHLO (Extended Hello).</td>
<td>Enter the SMTP server port number. The default is port 25.</td>
<td>Enter the local port to use for email alerts. The default is a random port number.</td>
<td>Select the priority level for the email alert.</td>
<td></td>
</tr>
</tbody>
</table>
CLI Configuration
On this page you can change CLI settings.

To configure the CLI:
1. Select CLI on the menu and then Configuration at the top of the page. The Command Line Interface Configuration page appears.

![Figure 14-4 CLI Configuration](image)

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Command Line Interface Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Password</td>
<td>Enter the password for Telnet access.</td>
</tr>
<tr>
<td>Enable Level Password</td>
<td>Enter the password for access to the Command Mode Enable level. There is no password by default.</td>
</tr>
<tr>
<td>Quit Connect Line</td>
<td>Enter a string to terminate a connect line session and resume the CLI. Type <code>&lt;control&gt;</code> before any key the user must press when holding down the Ctrl key. An example of such a string is <code>&lt;control&gt;L</code>.</td>
</tr>
<tr>
<td>Inactivity Timeout</td>
<td>Set an Inactivity Timeout value so the CLI session will disconnect if no data is received after the designated time period. Default is 15 minutes. Enter a value of 0 to disable.</td>
</tr>
<tr>
<td>Login String State</td>
<td>Click to enable to disable Login String State. Enabling the login string state allows the display of the Login string. The login string cannot exceed 32 characters. By default Login String will be the device name.</td>
</tr>
</tbody>
</table>

Note: This configuration field appears when Login String State is enabled above. This Login String setting only applies to SSH or Telnet connections to the CLI. If the serial line is being used in Command Mode, for CLI access, then refer to the Line Command Mode section for those applicable settings.
XML Settings

An EDS device server allows for the configuration of devices by using XML configuration records (XCRs). You can export an existing configuration for use on other EDS devices or import a saved configuration file.

On the XML: Export Configuration web page, you can export the current system configuration in XML format. The generated XML file can be imported later to restore a configuration. It can also be modified and imported to update the configuration on this EDS unit or another. The XML data can be exported to the browser window or to a file on the file system.

By default, all groups are selected except those pertaining to the network configuration. This is so that if you later import the entire XML configuration, it will not break your network connectivity. You may select or clear the checkbox for any group.

In the XML: Import System Configuration Page you can import a system configuration from an XML file. The XML data can be imported from a file on the file system or uploaded using HTTP. The groups to import can be specified by toggling the respective group item or entering a filter string. When toggling a group item, all instances of that group will be imported. The filter string can be used to import specific instances of a group. The text format of this string is:

\(<g>:<i>;<g>:<i>;\ldots\)

For example, if you only wanted to import the line 1 setting from an XCR, use a filter string of line:1.

Each group name \(<g>\) is followed by a colon and the instance value \(<i>\). Each \(<g>:<i>\) value is separated with a semicolon. If a group has no instance, specify the group name \(<g>\) only.

**Note:** The number of lines available for importing and exporting differ between Lantronix products. The screenshots in this chapter represent one line, as available, for example, on an XPort Pro embedded networking module and EDS1100. However, other device networking products (such as EDS2100, EDS4100, XPort AR, MatchPort AR embedded networking modules, EDS8/16PS and EDS8/16/32PR) support additional lines.
**XML: Export Configuration**

On this web page you can export the current system configuration in XML format.

**To export the system configuration:**


2. Enter or modify the following settings:

**Note:** Number of lines and groups available for export configuration vary between Lantronix products.

---

![XML: Export Configuration](image)

*Figure 14-6 XML: Export Configuration*

---

**Table 14-7 XML Export Configuration**

<table>
<thead>
<tr>
<th>XML Export Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export to browser</td>
<td>Select this option to export the XCR data in the selected fields to a web browser.</td>
</tr>
<tr>
<td>Export to local file</td>
<td>Select this option to export the XCR data to a file on the device. If you select this option, enter a file name for the XML configuration record.</td>
</tr>
<tr>
<td>Export secrets</td>
<td>Only use this with extreme caution. If selected, secret password and key information will be exported. Use only with a secure link, and save only in secure locations. Check the Comments checkbox to include additional comment information.</td>
</tr>
</tbody>
</table>
3. Click Export. The groups display if exporting the data to the browser. If exporting the data to a local file, the file is stored on the file system.

   **Note:** Most browsers will interpret and display the XML data without the XML tags. To view the raw XML, choose the view file source feature of your browser.

### XML: Export Status

On this page you can export the current system status in XML format. The XML data can be exported to the browser page or to a file on the file system.

**To export the system status:**

1. Select XML on menu bar and then Export Status at the top of the page. The XML: Export Status page appears.

   The number of Lines to Export and the specific Groups to Export displayed on your screen may vary according to your particular product.

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th><strong>XML Export Configuration Settings (continued)</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lines to Export</td>
<td>Select the instances you want to export in the line, LPD, tunnel, and terminal groups. Click Clear All to clear all Lines to Export checkboxes. Click Select All to select all Lines to Export checkboxes.</td>
</tr>
<tr>
<td>Groups to Export</td>
<td>Check the configuration groups that are to be exported to the XML configuration record. Click Clear All to clear all Group checkboxes. Click Select All but Networking to select all the checkboxes available except for the networking-related group checkboxes.</td>
</tr>
</tbody>
</table>
Figure 14-8 XML Export Status

Note: Number of lines and groups available for export vary between Lantronix products.

Table 14-9 XML Export Status

<table>
<thead>
<tr>
<th>XML: Export System Status Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export to browser</td>
<td>Select this option to export the XML status record to a web browser.</td>
</tr>
<tr>
<td>Export to local file</td>
<td>Select this option to export the XML status record to a file on the device. If you select this option, enter a file name for the XML status record.</td>
</tr>
<tr>
<td>Lines to Export</td>
<td>Select the instances you want to export in the line, LPD, tunnel, and terminal groups. Click Clear All to clear all Lines to Export checkboxes. Click Select All to select all the Lines to Export checkboxes.</td>
</tr>
<tr>
<td>Groups to Export</td>
<td>Check the configuration groups that are to be exported into the XML status record. Click Clear All to clear all group checkboxes. Click Select All to select all group checkboxes.</td>
</tr>
</tbody>
</table>

3. Click Export. The groups display if exporting the data to the browser. If exporting the data to a local file system, the file is stored on the file system.

Note: Most browsers will interpret and display the XML data without the XML tags. To view the raw XML, choose the view file source feature of your browser.
XML: Import Configuration

Here you can import a system configuration from an XML file.

The XML data can be imported from a file on the file system or uploaded using HTTP. The groups
to import can be specified by toggling the respective group item or entering a filter string. When
toggling a group item, all instances of that group will be imported. The filter string can be used to
import specific instances of a group. The text format of this string is: `<g>;<i>;<g>;<i>;...`

Each group name `<g>` is followed by a colon and the instance value `<i>`. Each `<g>;<i>` value
is separated with a semicolon. If a group has no instance, specify the group name `<g>` only.

To import a system configuration:

1. Select XML on the menu bar and then Import Configuration at the top of the page. The XML:
   Import Configuration web page appears.

   ![Figure 14-10 XML: Import Configuration]

2. Click one of the following radio buttons:
   - Configuration from External file. See Import Configuration from External File on page 135.
   - Configuration from Filesystem. See Import Configuration from the Filesystem on
     page 136.
   - Line(s) from single line Settings on the Filesystem. See Import Line(s) from Single Line
     Settings on the Filesystem on page 138.

Import Configuration from External File

This selection shows a field for entering the path and file name of the entire external XCR file you
want to import. You can also browse to select the XCR file.

![Figure 14-11 XML: Import Configuration from External File]
**Import Configuration from the Filesystem**

This selection shows a page for entering the filesystem and your import requirements – groups, lines, and instances.

*Note:* Number of lines and groups available for import configuration vary between Lantronix products.

**Figure 14-12 XML: Import from Filesystem**
1. Enter or modify the following settings.

**Figure 14-13 XML: Import Configuration from Filesystem**

<table>
<thead>
<tr>
<th>Import Configuration from Filesystem Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filename</strong></td>
<td>Enter the name of the file on the device (local to its filesystem) that contains XCR data.</td>
</tr>
<tr>
<td><strong>Lines to Import</strong></td>
<td>Select the lines or network whose settings you want to import. Click the Select All link to select all the serial lines and the network lines. Click the Clear All link to clear all of the checkboxes. By default, all line instances are selected. Only the selected line instances will be imported in the line, LPD, tunnel, and terminal groups.</td>
</tr>
</tbody>
</table>
| **Whole Groups to Import**                    | Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group unless it is one of the Lines to Import.  
  **Note:** By default, all groups are checked except those pertaining to the network configuration; this is so that import will not break your network connectivity.  
  You may check or uncheck any group to include or omit that group from import. To import all of the groups, click the Select All but Networking link to import all groups. To clear all the checkboxes, click the Clear All link. |
| **Text List**                                 | Enter a string to import specific instances of a group. The textual format of this string is:  
  `<g>:<i>;<g>:<i>;...`  
  Each group name `<g>` is followed by a colon and the instance value `<i>` and each `<g>:<i>` value is separated by a semi-colon. If a group has no instance, then specify the group name `<g>` only. Use this option for groups other than those affected by Lines to Import. |

2. Click **Import**.
Import Line(s) from Single Line Settings on the Filesystem

This selection copies line settings from the single line instance in the input file to selected lines. The import file may only contain records from a single line instance; this is done by selecting a single Line to Export when exporting the file. The number of Lines to Import and the specific Whole Groups to Import displayed on your screen may vary according to your particular product.

To modify Single Line Settings on the Filesystem:

Figure 14-14 XML: Import Line(s) from Single Line Settings on the Filesystem
1. Enter or modify the following settings:

   Table 14-15  XML: Import Line(s) from Single Line Settings

<table>
<thead>
<tr>
<th>Import Line(s) Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Provide the name of the file on the device (local to its file system) that contains XCR data.</td>
</tr>
<tr>
<td>Lines to Import</td>
<td>Select the line(s) whose settings you want to import. Click the Select All link to select all the serial lines and the network lines. Click the Clear All link clear all of the checkboxes. By default, all serial line instances are selected.</td>
</tr>
<tr>
<td>Whole Groups to Import</td>
<td>Select the configuration groups to import from the XML configuration record. <strong>Note:</strong> By default, all groups are checked except those pertaining to the network configuration; this is so that import will not break your network connectivity. You may check or uncheck any group to include or omit that group from import. To import all of the groups, click the Select All but Networking link to import all groups. To clear all the checkboxes, click the Clear All link.</td>
</tr>
</tbody>
</table>

2. Click Import.
15: Branding the EDS Unit

This chapter describes how to brand your EDS device server by using Web Manager and Command Line Interface (CLI). It contains the following sections on customization:

- Web Manager Customization
- Short and Long Name Customization

Web Manager Customization

Customize the Web Manager's appearance by modifying index.html and style.css. The style (fonts, colors, and spacing) of the Web Manager is controlled with style.css and the text and graphics are controlled with index.html.

The Web Manager files are hidden and are incorporated directly into the firmware image but may be overridden by placing the appropriate file in the appropriate directory on the EDS device server file system.

Web Manager files can be retrieved and overridden with the following procedure:

1. FTP to the EDS device.
2. Make a directory (mkdir) and name it http/config
3. Change to the directory (cd) that you created in step 2. (http/config)
4. Get the file by using get <filename>
5. Modify the file as required or create a new one with the same name
6. Put the file by using put <filename>
7. Type quit. The overriding files appear in the file system’s http/config directory.
8. Restart any open browser to view the changes.
9. If you wish to go back to the default files in the firmware image, simply delete the overriding files from the file system.

Short and Long Name Customization

Short and long names may be customized in Web Manager according to the directions in System Settings. The names display in the CLI show command and in the System web page in the Current Configuration table. The short name is used for the show command. Both names display in the CLI Product Type field in the following example:

   (enable)# show

The long and short names appear in the Product Type field in the following format:

   Product Type: <long name> (<short name>)

For example:

   (enable)# show EDS
   Product Information:
   Product Type: Lantronix EDS (EDS)
16: Updating Firmware

Obtaining Firmware

Obtain up-to-date firmware and release notes for the unit from the Lantronix web site (http://www.lantronix.com/support/downloads) or by using anonymous FTP (ftp://ftp.lantronix.com/).

Loading New Firmware

Reload the firmware using the device web manager Filesystem page.

To upload new firmware:
1. Select System in the menu bar. The System page appears.

   ![System Page](image)

2. Click Choose File to browse to the firmware file.
3. Highlight the file and click Open.
4. Click Upload to install the firmware on the EDS device server. The device automatically reboots on the installation of new firmware.
5. Close and reopen the web manager Internet browser to view the device’s updated web pages.

Note: Alternatively, firmware may be updated by sending the file to the EDS device server over a FTP or TFTP connection.
Appendix A: Technical Support

Lantronix offers many resources to support our customers and products at http://www.lantronix.com/support. For instance, you can ask a question, find firmware downloads, access the FTP site and search through tutorials. At this site you can also find FAQs, bulletins, warranty information, extended support services and product documentation.

To contact technical support or sales, look up your local office at http://www.lantronix.com/about/contact.html. When you report a problem, please provide the following information:

- Your name, company name, address, and phone number
- Lantronix product and model number
- Lantronix MAC address or serial number
- Firmware version and current configuration
- Description of the problem
- Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem)
Appendix B: Binary to Hexadecimal Conversions

Many of the unit's configuration procedures require you to assemble a series of options (represented as bits) into a complete command (represented as a byte). The resulting binary value must be converted to a hexadecimal representation.

Use this chapter to learn to convert binary values to hexadecimals or to look up hexadecimal values in the tables of configuration options. The tables include:

- Command Mode (serial string sign-on message)
- AES Keys

Converting Binary to Hexadecimal

Conversion Table

Hexadecimal digits have values ranging from 0 to F, which are represented as 0-9, A (for 10), B (for 11), etc. To convert a binary value (for example, 0100 1100) to a hexadecimal representation, treat the upper and lower four bits separately to produce a two-digit hexadecimal number (in this case, 4C). Use the following table to convert values from binary to hexadecimal.

Table B-1  Binary to Hexadecimal Conversion Table

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Binary</th>
<th>Hex</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0001</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0010</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0011</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0100</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>0101</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>0110</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>0111</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>1000</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>1001</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>1010</td>
<td>A</td>
</tr>
<tr>
<td>11</td>
<td>1011</td>
<td>B</td>
</tr>
<tr>
<td>12</td>
<td>1100</td>
<td>C</td>
</tr>
<tr>
<td>13</td>
<td>1101</td>
<td>D</td>
</tr>
<tr>
<td>14</td>
<td>1110</td>
<td>E</td>
</tr>
<tr>
<td>15</td>
<td>1111</td>
<td>F</td>
</tr>
</tbody>
</table>
Scientific Calculator

Another simple way to convert binary to hexadecimal is to use a scientific calculator, such as the one available on the Windows operating systems. For example:

1. On the Windows Start menu, click Programs > Accessories > Calculator.
2. On the View menu, select Scientific. The scientific calculator appears.
3. Click Bin (Binary), and type the number you want to convert.
4. Click Hex. The hexadecimal value appears.
Appendix C: sCompliance

(According to ISO/IEC Guide 22 and EN 45014)

Manufacturer’s Name & Address:
Lantronix, Inc. 7535 Irvine Center Drive, Suite 100, Irvine, CA 92618 USA

Product Name Model: EDS4100 4 Port Device Server, EDS8PR 8 Port Device Server, EDS16PR 16 Port Device Server, and EDS32PR 32 Port Device Server.

Conform to the following standards or other normative documents:

Radiated and Conducted Emissions
Class B limits of EN55022: 1998

Direct & Indirect ESD
EN61000-4-2: 1995

RF Electromagnetic Field Immunity
EN61000-4-3: 1996

Electrical Fast Transient/Burst Immunity
EN61000-4-4: 1995

Surge Immunity
EN61000-4-5: 1995

RF Common Mode Conducted Susceptibility
EN61000-4-6: 1996

Power Frequency Magnetic Field Immunity
EN61000-4-8: 1993

Voltage Dips and Interrupts
EN61000-4-11: 1994

Manufacturer’s Contact
Lantronix, Inc.
7535 Irvine Center Drive
Suite 100
Irvine, CA 92618 USA
Tel: 949-453-3990
Fax: 949-453-3995

RoHS, REACH and WEEE Compliance Statement

Lithium Battery Notice

**ATTENTION:** DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER’S INSTRUCTIONS.

**ACHTUNG:** WIRD BEIM BATTERIEWECHSEL EINE FALSche BATTERIE EINGESETZT, BESTEHT EXPLOSIONSGEFAHR. SETZEN SIE Nur EINE BATTERIE DES GLEichen ODER EINES ENTSPRECHEndEN, VOM HERSTELLER EMPFOHLENEN TYPs EIN. ENTSORGEN SIE VERBRAUCHTE BATTERIEN GEMÄSS DEN ANWEISUNGEN DES HERSTELLERS.

Installationsanweisungen

**Rackmontage**

Bei Montage in ein geschlossenes Rack oder in ein Rack mit mehreren Einheiten ist unter Umständen eine weitere Prüfung erforderlich. Folgende Punkte sind zu berücksichtigen.

- Die Umgebungstemperatur innerhalb des Racks kann höher sein als die Raumtemperatur. Die Installation muss so durchgeführt werden, dass der für den sicheren Betrieb erforderliche Luftstrom nicht beeinträchtigt wird. In dieser Umgebung darf die maximale Temperatur von 50°C nicht überschritten werden. Dabei sind auch die maximalen Auslegungstemperaturen zu berücksichtigen.
- Die Installation ist so durchzuführen, dass auch bei ungleichmäßiger Lastverteilung die Stabilität gewährleistet bleibt.

**Energiezufuhr**

Anhand der Angaben auf dem jeweiligen Typenschild ist sicherzustellen, dass keine Überlastung an der Einspeisung erfolgt, die den Überstromschutz und die Versorgungsleitungen beeinträchtigt.

**Erdung**

Eine zuverlässige Schutzerdung dieser Ausrüstung muss gewährleistet sein. Dies gilt besonders bei Anschluss an Mehrfachsteckdosen.

Installation Instructions

**Rack Mounting**

If rack mounted units are installed in a closed or multi-unit rack assembly, they may require further evaluation by certification agencies. You must consider the following items:

- The ambient conditions within the rack may be greater than the room conditions. Installation should be so that the amount of air flow required for safe operation is not compromised. The maximum temperature for the equipment in this environment is 50°C. Consideration should be given to the maximum rated ambient conditions.
- Installation should be so that a hazardous stability condition is not achieved due to uneven loading.
**Input Supply**
Check nameplate ratings to assure there is no overloading of supply circuits that have an effect on over current protection and supply wiring.

**Grounding**
Reliable earthing of this equipment must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than direct connections to the branch circuit strips.
# Appendix D: Lantronix Cables and Adapters

Lantronix cables and adapters for use with the EDS devices are listed here according to part number and application.

<table>
<thead>
<tr>
<th>Lantronix P/N</th>
<th>Description</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>500-103</td>
<td>6’ RJ45-to DB9F</td>
<td>Included with EDS8/16/32PR for setup or device connectivity. Connects the RJ45 RS232 serial ports of EDS8/16/32PR to a DB9M DTE interface of a PC or serial device.</td>
</tr>
<tr>
<td>200.2062</td>
<td>Cable Ethernet CAT5; RJ45, 2 m (6.6 ft)</td>
<td>Connects the EDS8/16/32PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS8/16/32PR to another. Connects the EDS8/16/32PR serial RJ45 RS232 ports to a device using one of the adapters listed below.</td>
</tr>
<tr>
<td>200.2063</td>
<td>Cable Ethernet CAT5; RJ45, 5 m (16.4 ft)</td>
<td>Connects the EDS8/16/32PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS8/16/32PR to another. Connects the EDS8/16/32PR serial RJ45 RS232 ports to a device using one of the adapters listed below.</td>
</tr>
<tr>
<td>200.2064</td>
<td>Cable Ethernet CAT5; RJ45, 10 m (32.8 ft)</td>
<td>Connects the EDS8/16/32PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS8/16/32PR to another. Connects the EDS8/16/32PR serial RJ45 RS232 ports to a device using one of the adapters listed below.</td>
</tr>
<tr>
<td>200.2065</td>
<td>Cable Ethernet CAT5; RJ45, 15 m (49.2 ft)</td>
<td>Connects the EDS8/16/32PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS8/16/32PR to another. Connects the EDS8/16/32PR serial RJ45 RS232 ports to a device using one of the adapters listed below.</td>
</tr>
<tr>
<td>200.2066A</td>
<td>Adapter RJ45-to-DB25M</td>
<td>Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR RJ45 serial ports to the DB25F DTE interface of a serial device.</td>
</tr>
<tr>
<td>200.2067A</td>
<td>Adapter RJ45-to-DB25F</td>
<td>Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR RJ45 serial ports to the DB25M DTE interface of a serial device.</td>
</tr>
<tr>
<td>200.2069A</td>
<td>Adapter RJ45-to-DB9M</td>
<td>Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR RJ45 serial ports to the DB9F DTE interface of a serial device.</td>
</tr>
<tr>
<td>200.2070A</td>
<td>Adapter RJ45-to-DB9F</td>
<td>Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR to the DB9M DTE interface of a PC or serial device.</td>
</tr>
<tr>
<td>200.2073</td>
<td>Adapter RJ45-to-DB25M</td>
<td>Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR RJ45 serial ports to the DB25F DCE interface of a serial device.</td>
</tr>
<tr>
<td>200.2074</td>
<td>Adapter RJ45-to-DB25F</td>
<td>Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR RJ45 serial ports to the DB25M DCE interface of a serial device.</td>
</tr>
<tr>
<td>ADP010104-01</td>
<td>Adapter &quot;Rolled&quot; RJ45-to-RJ45</td>
<td>Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR to an RJ45 console port on products from Cisco and other manufacturers.</td>
</tr>
</tbody>
</table>
Index

A
Accept Mode 51
Accept Mode 58
Additional Documentation 15
Additional TCP Server Port 104
Address
  Ethernet 22
  Hardware 22, 23
  IP 23
  MAC 22, 23
Advanced Settings
  Email Configuration 128
  XML Configuration 131
Advanced Settings 127
AES 19
Allow Firmware Update 78
Allow TFTP File Creation 77
Allow XCR Import 78
Applications 19
ARP 19
ARP Settings 111, 112
ASCII 102
Auth Type 84
Authentication Type 84
Authority 100
AutoIP 19

B
Banner 87
Bar Code 23
Bin 144
Binary 87, 143
Binary to Hexadecimal Conversions 143
Block Network 60, 64
Block Serial 64
Block Serial Data 60
BOOTP 19, 44
Branding 140
  Web Manager Customization 140
Break Duration 72

C
CLI 20
CLI Configuration 130
CLI Statistics 129

Command Line Interface Settings 129
Command Mode 22
Command-Line Interface 20
Common Name 101
Compliance 145
Configuration Methods 22
Configuration Settings 74
Connect Mode 51
Connect Mode 60
Console Port 33
Convert Newlines 87
Count 118
Create New Keys 95
Create New Self-Signed Certificate 100

D
Date 124, 125
Default Gateway 45
Default Server Port Numbers 23
Device Control 20
Device Details 36
Device Details Summary 36
Device Management 21
Device Status 39
DeviceInstaller 36
DeviceInstaller 36
DHCP 19, 45
Diagnostic Toolset 22
Diagnostics 115
  Buffer Pools 121
  Hardware 115
  IP Sockets 117
  Memory 120
  MIB-II Statistics 116
  Ping 117
  Processes 122
Diagnostics Log 119
Disconnect Mode 51
Disconnect Mode 66
DNS 19, 45
DNS Settings 74

E
Echo 71, 72
Email on Connect 60, 64
Email on Disconnect 60, 64
Enable Level Password 130
Encryption 21
End of Job 87
Enterprise-Grade Security 21
EOJ String 87
Ethernet address 22
Ethernet Port 28, 33
Evolution OS 20
Exit Connect Menu 71, 72
Expires 101
Export Secrets 132
Export to Browser 132, 134
Export to Local File 132, 134

F
File System
   Browser 106
   Statistics 105
Filename 137, 139
Filesystem 41, 141
Firmware 141
Flush Serial Data 59, 64
Formfeed 87
FreeRADIUS 98
FTP 19, 141
FTP Configuration 76

G
Groups to Export 133, 134

H
Hardware Address 22, 23
Hardware Address 22
Hex 144
Hexadecimal 143
Host 63, 107, 118
Host Configuration 73
Host Configuration 73
Host IP Promotion 66
Hostname 45
HTTP 19
   Authentication 82
   Change Configuration 81
   Configuration 79
   Statistics 79

I
ICMP 19
ICMP Settings 110
Import Configuration from External File 135

Import Configuration from the Filesystem 136
Import Line(s) from Single Line Settings on the Filesystem 138
Inactivity Timeout 130
IP 19
   Address Filter 113
   Settings 109
ISO/IEC Guide 145

K
Key Length 101
Key Type 90, 95

L
Label 23
Lantronix Discovery Protocol 23
LEDs 28, 33
Line 1
   Configuration 48
   Statistics 47
Line Settings 47
Lines to Export 133, 134
Lines to Import 137, 139
Lithium Battery Notice 146
Loading New Firmware 141
Local Port 59, 62
Login Connect Menu 71, 72
Login Password 130
LPD
   Configuration Page 86, 87
   Settings 85
   LPD Statistics 85

M
MAC Address 22, 23
Maintenance and Diagnostics Settings
   Protocol Stack 108
Manufacturer’s Name & Address 145
Manufacturing Date Code 23
Max Entries 85
Modbus Configuration 104
Modbus Statistics 103
Modbus 102
Mode 62
Modem Emulation 20
Modem Emulation 67
MTU 45
Multiple Hosts 65
N
Name 126
Network 1 (eth0) Interface Configuration 44
Network 1 Ethernet Link 46
Network Settings
  Network 1 Interface Configuration 44
  Network 1 Interface Status 43
Network Settings 43
New Certificate 100
New Private Key 100

O
Obtaining Firmware 141
Organization Unit 100

P
Packing Mode 55
Password 60, 95
PBX 21
Persistent 85
Port 107
Port Numbers 22, 23
Ports
  Serial and Telnet 22
PPP Settings 75
Private Branch Exchange 21
Private Key 90, 95
Product Information Label 23
Product Name Model 145
Product Revision 23
Protocol 59, 73
Protocol Support 19
Public Key 90, 95

Q
Query Port 114
Queue Name 87
Quit Connect Line 130

R
Radiated and Conducted Emissions 145
Read Community 76
Really Simple Syndication 21
Reboot Device 126
Reconnect Timer 64
Remote Address 73
Remote Command 95
Remote Port 73
Reset Button 28, 34
Response Timeout 104
Restore Factory Defaults 126
RSS 19, 21
RSS Feed 85
RSS Settings 84
RSS Trace Input 104
RTC 124
RTU 102

S
Scientific 144
Scientific Calculator 144
SCPR 21
Secure Com Port Redirector 21
Secure Shell 88
Secure Sockets Layer 88, 96
Security
  Enterprise-Grade 21
  Settings 88
Security Settings 88
  SSL Certificates and Private Keys 97
  SSL Cipher Suites 96
  SSL Utilities 98
Send Break 72
Send Character 57
Serial Ports 27, 32
Serial Settings 54
Serial Transmission Mode 102
Services Settings 74
  LPD 85
Short and Long Name Customization 140
SMTP 19
SNMP 19
SNMP Configuration 75
SNMP Management 20
SOJ String 87
SSH 19, 88
  Client Known Hosts 93
  Server Authorized Users 91
  Server Host Keys 89
  Settings 88
SSH Client Known Hosts 93
SSH Client User Configuration 94
SSH Max Sessions 131
SSH Port 131
SSH Server Authorized Users 91
SSH Server Host Keys 89
SSH State 131
SSH Username 73
SSL 19, 88, 96
Settings 96
SSL Certificates 96
SSL Cipher Suites 96
SSL Configuration 99
SSL RSA or DSA 97
SSL Utilities 98
Start of Job 87
State 110
Steel Belted RADIUS 98
Syslog 19
Syslog Configuration 78
System Contact 76
System Description 76
System Location 76
System Name 76
System Settings 125

T
TCP 19
TCP Keep Alive 59
TCP Server State 104
TCP Settings 108
TCP/IP 102
Technical Support 142
Telnet 19
Telnet Max Sessions 131
Telnet Port 131
Telnet State 131
Terminal
Server 21
Settings 70
Terminal Block Connector 28
Terminal Type 71, 72
Text List 137
TFTP 19, 141
TFTP Configuration 77
Threshold 57
Time 124, 125
Time Zone 124, 125
Timeout 57, 118
TLS 19
Traceroute 118
Trailing Character 57
Traps Primary Destination 76
Traps Secondary Destination 76
Traps State 76
Troubleshooting 22
Troubleshooting Capabilities 22
Tunnel – Accept Mode 58
Tunnel – Connect Mode 60
Tunnel – Disconnect Mode 66
Tunnel – Packing Mode 55
Tunnel 1 – Statistics 52
Tunnel Settings
Connect Mode 60
Modem Emulation
Command Mode 67
Packing Mode 55
Tunnel Settings 51
Type 101

U
UDP 19
Uniform Resource Identifier 83
Updating Firmware 141
Upload Authority Certificate 100
Upload Certificate 100
Upload New Firmware 126
URI 83
Username 95

W
Web Manager
Device Status Web Page 39
Navigating 41
Page Components 40
Page Summary 41
Web Manager Customization 140
Web Manager 38
Web-Based Configuration 20
Whole Groups to Import 137, 139
WLAN
Settings
Network 1 Ethernet Link 46
Write Community 76

X
XML 22
Export Configuration 132
Export Status 133
Import System Configuration 135
XML-Based Architecture 20