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 A digital device pursuant to Part 15 of FCC Subpart B and EN55024:1998 +A2:2003 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, Compliance (on page 143).

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>September 2009</td>
<td>A</td>
<td>Initial document.</td>
</tr>
<tr>
<td>December 2010</td>
<td>B</td>
<td>Updated for firmware version 5.2.0.0R20. Added support for Modbus protocol, configurable MTU, and additional VIP tunnel connect protocols; as well as improvements to SNMP, logging, and SSL.</td>
</tr>
<tr>
<td>April 2016</td>
<td>C</td>
<td>Updated for firmware version 5.4.0.0. New features include CLI login string, send break, break duration settings, support for SHA2 SSL certificate, and key size changes in SSL. VIP content and host mode configuration options removed.</td>
</tr>
<tr>
<td>March 2020</td>
<td>D</td>
<td>Updated for firmware version 6.0.0.0. Updated with new default password, label, and security settings.</td>
</tr>
</tbody>
</table>
# Table of Contents

Intellectual Property ................................................................. 2
Warranty .................................................................................. 2
Contacts ................................................................................. 2
Disclaimer ................................................................................. 2
Revision History ......................................................................... 3
List of Figures ........................................................................... 9
List of Tables ............................................................................ 12

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

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

3: Installation of EDS1100 ....................................................... 22
   Package Contents ................................................................... 22
   User-Supplied Items ............................................................. 22
   Hardware Components .......................................................... 23
       Back Panel ..................................................................... 24
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Transmission Mode</td>
<td>100</td>
</tr>
<tr>
<td>Modbus Statistics</td>
<td>101</td>
</tr>
<tr>
<td>Modbus Configuration</td>
<td>102</td>
</tr>
<tr>
<td><strong>13: Maintenance and Diagnostics Settings</strong></td>
<td>103</td>
</tr>
<tr>
<td>Filesystem Settings</td>
<td>103</td>
</tr>
<tr>
<td>Filesystem Statistics</td>
<td>103</td>
</tr>
<tr>
<td>Filesystem Browser</td>
<td>104</td>
</tr>
<tr>
<td>Protocol Stack Settings</td>
<td>106</td>
</tr>
<tr>
<td>TCP Settings</td>
<td>106</td>
</tr>
<tr>
<td>IP Settings</td>
<td>107</td>
</tr>
<tr>
<td>ICMP Settings</td>
<td>108</td>
</tr>
<tr>
<td>ARP Settings</td>
<td>109</td>
</tr>
<tr>
<td>SMTP Settings</td>
<td>110</td>
</tr>
<tr>
<td>IP Address Filter</td>
<td>111</td>
</tr>
<tr>
<td>Query Port</td>
<td>112</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>113</td>
</tr>
<tr>
<td>Hardware</td>
<td>113</td>
</tr>
<tr>
<td>MIB-II Statistics</td>
<td>114</td>
</tr>
<tr>
<td>IP Sockets</td>
<td>115</td>
</tr>
<tr>
<td>Ping</td>
<td>115</td>
</tr>
<tr>
<td>Traceroute</td>
<td>116</td>
</tr>
<tr>
<td>Log</td>
<td>117</td>
</tr>
<tr>
<td>Memory</td>
<td>118</td>
</tr>
<tr>
<td>Buffer Pools</td>
<td>119</td>
</tr>
<tr>
<td>Processes</td>
<td>119</td>
</tr>
<tr>
<td>System Settings</td>
<td>121</td>
</tr>
<tr>
<td><strong>14: Advanced Settings</strong></td>
<td>123</td>
</tr>
<tr>
<td>Email Settings</td>
<td>123</td>
</tr>
<tr>
<td>Email Statistics</td>
<td>123</td>
</tr>
<tr>
<td>Email Configuration</td>
<td>125</td>
</tr>
<tr>
<td>Command Line Interface Settings</td>
<td>127</td>
</tr>
<tr>
<td>CLI Statistics</td>
<td>127</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>127</td>
</tr>
<tr>
<td>XML Settings</td>
<td>129</td>
</tr>
<tr>
<td>XML: Export Configuration</td>
<td>130</td>
</tr>
<tr>
<td>XML: Export Status</td>
<td>131</td>
</tr>
<tr>
<td>XML: Import Configuration</td>
<td>133</td>
</tr>
<tr>
<td><strong>15: Branding the EDS1100/2100 Unit</strong></td>
<td>138</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>16: Updating Firmware</td>
<td>139</td>
</tr>
<tr>
<td>Obtaining Firmware</td>
<td>139</td>
</tr>
<tr>
<td>Loading New Firmware</td>
<td>139</td>
</tr>
<tr>
<td>A: Technical Support</td>
<td>140</td>
</tr>
<tr>
<td>B: Binary to Hexadecimal Conversions</td>
<td>141</td>
</tr>
<tr>
<td>Converting Binary to Hexadecimal</td>
<td>141</td>
</tr>
<tr>
<td>Conversion Table</td>
<td>141</td>
</tr>
<tr>
<td>Scientific Calculator</td>
<td>142</td>
</tr>
<tr>
<td>C: Compliance</td>
<td>143</td>
</tr>
<tr>
<td>RoHS, REACH and WEEE Compliance Statement</td>
<td>144</td>
</tr>
<tr>
<td>Index</td>
<td>145</td>
</tr>
</tbody>
</table>
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1</td>
<td>Sample Hardware Address</td>
<td>20</td>
</tr>
<tr>
<td>2-2</td>
<td>Product Label</td>
<td>21</td>
</tr>
<tr>
<td>3-1</td>
<td>EDS1100 DB25 (Female) Serial Port</td>
<td>23</td>
</tr>
<tr>
<td>3-2</td>
<td>EDS1100 RS-232 Pinouts</td>
<td>23</td>
</tr>
<tr>
<td>3-3</td>
<td>EDS1100 RS-422 (4-wire) Pinouts</td>
<td>23</td>
</tr>
<tr>
<td>3-4</td>
<td>EDS1100 RS-485 (2-wire) Pinouts</td>
<td>24</td>
</tr>
<tr>
<td>3-5</td>
<td>EDS1100 Back Panel</td>
<td>24</td>
</tr>
<tr>
<td>3-6</td>
<td>EDS1100 Top LEDs</td>
<td>25</td>
</tr>
<tr>
<td>3-8</td>
<td>EDS1100 Connections</td>
<td>26</td>
</tr>
<tr>
<td>4-1</td>
<td>EDS2100 Male DB9 DTE Serial Ports</td>
<td>28</td>
</tr>
<tr>
<td>4-2</td>
<td>EDS2100 Pinout Configuration for RS-232</td>
<td>28</td>
</tr>
<tr>
<td>4-3</td>
<td>EDS2100 Pinout Configuration for RS-422 (4-wire)</td>
<td>28</td>
</tr>
<tr>
<td>4-4</td>
<td>EDS2100 Pinout Configuration for RS-485 (2-wire)</td>
<td>29</td>
</tr>
<tr>
<td>4-5</td>
<td>EDS2100 Ethernet RJ45 Port, Reset Button, and Power Plug</td>
<td>29</td>
</tr>
<tr>
<td>4-6</td>
<td>EDS2100 Top LEDs</td>
<td>30</td>
</tr>
<tr>
<td>4-8</td>
<td>EDS2100 Connections</td>
<td>32</td>
</tr>
<tr>
<td>6-1</td>
<td>Prompt for User Name and Password</td>
<td>35</td>
</tr>
<tr>
<td>6-2</td>
<td>Web Manager Home Page</td>
<td>36</td>
</tr>
<tr>
<td>6-3</td>
<td>Components of the Web Manager Page</td>
<td>37</td>
</tr>
<tr>
<td>7-1</td>
<td>Network 1 (eth0) Interface Status</td>
<td>40</td>
</tr>
<tr>
<td>7-2</td>
<td>Network 1 (eth0) Interface Configuration</td>
<td>41</td>
</tr>
<tr>
<td>7-4</td>
<td>Network 1 Ethernet Link</td>
<td>43</td>
</tr>
<tr>
<td>8-1</td>
<td>Line 1 Statistics</td>
<td>44</td>
</tr>
<tr>
<td>8-2</td>
<td>Line 1 Configuration</td>
<td>45</td>
</tr>
<tr>
<td>8-4</td>
<td>Line 1 Command Mode</td>
<td>47</td>
</tr>
<tr>
<td>8-6</td>
<td>Tunnel 1 Statistics</td>
<td>50</td>
</tr>
<tr>
<td>8-7</td>
<td>Tunnel 1 Serial Settings</td>
<td>51</td>
</tr>
<tr>
<td>8-9</td>
<td>Tunnel 1 Packing Mode (Mode = Disable)</td>
<td>52</td>
</tr>
<tr>
<td>8-10</td>
<td>Tunnel 1 Packing Mode (Mode = Timeout)</td>
<td>53</td>
</tr>
<tr>
<td>8-11</td>
<td>Tunnel 1 Packing Mode (Mode = Send Character)</td>
<td>53</td>
</tr>
<tr>
<td>8-13</td>
<td>Tunnel 1 Accept Mode</td>
<td>55</td>
</tr>
<tr>
<td>8-15</td>
<td>Tunnel 1 - Connect Mode</td>
<td>58</td>
</tr>
<tr>
<td>8-17</td>
<td>Host 1, Host 2, Host 3 Exchanged</td>
<td>61</td>
</tr>
<tr>
<td>8-18</td>
<td>Tunnel 1 Disconnect Mode</td>
<td>62</td>
</tr>
<tr>
<td>8-21</td>
<td>Tunnel 1 Modem Emulation</td>
<td>65</td>
</tr>
<tr>
<td>9-1</td>
<td>Terminal on Network Configuration</td>
<td>66</td>
</tr>
</tbody>
</table>
List of Tables

Table 3-7 EDS1100 LEDs and Descriptions ........................................................................ 25
Table 4-7 EDS2100 LEDs and Descriptions .................................................................... 30
Table 5-1 Device Details Summary .................................................................................. 34
Table 6-4 Summary of Web Manager Pages ..................................................................... 38
Table 7-3 Network 1 (eth0) Interface Configuration .......................................................... 41
Table 7-5 Network 1 Ethernet Link ...................................................................................... 43
Table 8-3 Line Configuration ............................................................................................... 46
Table 8-5 Line Command Mode ......................................................................................... 47
Table 8-8 Tunnel - Serial Settings ...................................................................................... 51
Table 8-12 Tunnel Packing Mode ....................................................................................... 53
Table 8-14 Tunnel Accept Mode ......................................................................................... 56
Table 8-16 Tunnel Connect Mode ....................................................................................... 59
Table 8-19 Tunnel Disconnect Mode .................................................................................. 63
Table 8-20 Modem Emulation Commands and Descriptions ............................................. 63
Table 8-22 Tunnel Modem Emulation .................................................................................. 65
Table 9-2 Terminal on Network Configuration .................................................................... 67
Table 9-4 Terminal on Line 1 Configuration ....................................................................... 68
Table 9-6 Host Configuration .............................................................................................. 69
Table 10-3 PPP Configuration .............................................................................................. 72
Table 10-5 SNMP ................................................................................................................ 74
Table 10-7 FTP Settings ...................................................................................................... 75
Table 10-9 TFTP Server ....................................................................................................... 75
Table 10-11 Syslog .............................................................................................................. 77
Table 10-14 HTTP Configuration ....................................................................................... 79
Table 10-16 HTTP Authentication ...................................................................................... 81
Table 10-18 RSS ................................................................................................................... 83
Table 10-21 LPD Configuration ......................................................................................... 85
Table 11-2 SSH Server Host Keys Settings - Upload Keys Method .................................... 88
Table 11-3 SSH Server Host Keys Settings - Upload Keys Method .................................... 88
Table 11-4 SSH Server Host Keys Settings - Create New Keys Method ............................. 89
Table 11-6 SSH Server Authorized User Settings .............................................................. 90
Table 11-8 SSH Client Known Hosts .................................................................................. 91
Table 11-10 SSH Client Users ........................................................................................... 93
Table 11-11 Supported Cipher Suites ............................................................................... 94
Table 11-13 SSL .................................................................................................................. 98
Table 12-1 6 Byte Header of Modbus Application Protocol ................................................. 100
1: **About This Guide**

This user guide provides the information needed to configure, use, and update the Lantronix® EDS1100/2100 device server. It is intended for software developers and system integrators who are installing the EDS1100/2100 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 EDS1100</td>
<td>Instructions for installing the EDS1100.</td>
</tr>
<tr>
<td>Chapter 4: Installation of EDS2100</td>
<td>Instructions for installing the EDS2100.</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>
<tr>
<td>Chapter 12: Modbus</td>
<td>Instructions for using the web interface to configure Modbus.</td>
</tr>
<tr>
<td>Chapter 13: Maintenance and Diagnostics Settings</td>
<td>Instructions for using the web interface to maintain the device, view statistics, files, and logs, and to diagnose problems.</td>
</tr>
<tr>
<td>Chapter 14: Advanced Settings</td>
<td>Instructions for using the web interface to configure email, CLI, and XML settings.</td>
</tr>
<tr>
<td>Chapter 15: Branding the EDS1100/2100 Unit</td>
<td>Instructions for customizing the device.</td>
</tr>
<tr>
<td>Chapter 16: Updating Firmware</td>
<td>Instructions for obtaining the latest firmware and updating the device.</td>
</tr>
<tr>
<td>B: Binary to Hexadecimal Conversions</td>
<td>Instructions for converting binary values to hexadecimals.</td>
</tr>
<tr>
<td>C: Compliance</td>
<td>Lantronix compliance information.</td>
</tr>
</tbody>
</table>
Additional Documentation

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

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDS1100/2100 Device Server Quick Start Guide</td>
<td>Instructions for getting the EDS1100/2100 configured and up and running.</td>
</tr>
<tr>
<td>EDS1100/2100 Device Server Command Reference</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>DeviceInstaller Online Help</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>Com Port Redirector Quick Start and Online Help</td>
<td>Instructions for using the Lantronix Windows based utility to create virtual com ports.</td>
</tr>
<tr>
<td>Secure Com Port Redirector User Guide</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 EDS1100/2100 device server. 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, 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.

The EDS device server is a complete network-enabling solution. The EDS1100 and EDS2100 provide the same solution and differ only in the number of serial ports. The EDS1100 has one serial port supported via a DB25 connector. The EDS2100 has two serial ports supported via 2 DB9 connectors.

This chapter contains the following sections:

- Key Features
- Protocol Support
- Evolution OS™ Application
- Additional Features
- Configuration Methods
- Addresses and Port Numbers
- Product Information Label

Key Features

- **Power Supply:** Regulated 9 - 30 VDC input required. There is a step-down converter to 1.5V for the processor core. All voltages have LC filtering to minimize noises and emissions.
- **Controller:** A Lantronix FX 32-bit microprocessor, running at 166 MHz internal bus and 83 MHz external bus.
- **Memory:** 8 MB flash and 8 MB SDRAM. Please contact your sales representative if you need larger memory sizes.
- **Temperature Range:** Operates over an extended temperature range of -40°C to +85°C.
- **Ethernet:** 10/100 megabits per second (Mbps) Ethernet transceiver
- **Serial Ports:** RS232/422/485 high-speed serial port with all hardware handshaking signals. Baud rate is software selectable (300 bps to 921600 bps).

The EDS1100/2100 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 EDS1100/2100 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, PPP, 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 EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 devices.

XML-Based Architecture and Device Control
XML is a fundamental building block for the future growth of M2M networks. The EDS1100/2100 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 EDS1100/2100 supports Really Simple Syndication (RSS) for streaming and managing online 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 EDS1100/2100 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 EDS1100/2100 has robust defenses to hostile Internet attacks such as denial of service (DoS), which can be used to take down the network. Moreover, the EDS1100/2100 cannot be used to bring down other devices on the network.

You can use the EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100, including CPU utilization and total stack space available.

**Configuration Methods**

After installation, the EDS1100/2100 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 EDS1100/2100 and assigning IP addresses and other configurable settings:

- **DeviceInstaller:** Configure the IP address and related settings and view current settings on the EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 Device Server Command Reference for instructions and available commands. Lantronix documentation is available at www.lantronix.com/support/documentation.)

XML: The EDS1100/2100 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 EDS1100/2100 Device Server Command Reference for instructions and available commands. Lantronix documentation is available at 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 2-1 Sample Hardware Address
00-20-4A-14-01-18 or 00:20:4A:14:01:18
08-04-13-14-01-18 or 08:04:13:14:01:18

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 EDS1100/2100.

- 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 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
- Part Number
- Country of Manufacture
- Revision
- Date of Manufacture
- Device ID
- Hardware Address (MAC address or serial number)

Figure 2-2 Product Label
3: **Installation of EDS1100**

This chapter describes how to install the EDS1100 device server. It contains the following sections:

- **Package Contents**
- **User-Supplied Items**
- **Hardware Components**
- **Installing the EDS1100**

**Package Contents**

- The EDS1100 package includes the following items:
  - One EDS1100 device
  - One DB25M-to-DB9F serial cable
  - Power Cube, 100-240 VAC with international adapters
  - Power cord restraint
  - Printed *Quick Start Guide*

**User-Supplied Items**

To complete your installation, you need the following items:

- RS-232/422/485 serial device that requires network connectivity.
- A serial cable, as in the following list, for your serial device. One end of the cable must have a male DB25 connector for the serial port.
  - A null modem cable to connect the serial port to a DCE device.
  - A straight-through modem cable, such as the one supplied in the package, to connect the serial port to a DTE device.
- 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.
Hardware Components

The EDS1100 has a female DB25 serial port that supports RS-232, RS-422, and RS-485 serial devices. The default serial port settings are 9600 baud, 8 bits, no parity, 1 stop bit, no flow control. *Figure 3-1* shows the front panel.

*Figure 3-1* EDS1100 DB25 (Female) Serial Port

*Figure 3-2* shows the RS-232 pinout configuration.

*Figure 3-2* EDS1100 RS-232 Pinouts

*Figure 3-3* shows the RS-422 (4-wire) pinout configuration.

*Figure 3-3* EDS1100 RS-422 (4-wire) Pinouts

*Figure 3-4* shows the RS-485 (2-wire) pinout configuration.

*Figure 3-4* shows the RS-485 (2-wire) pinout configuration.
Back Panel

On the EDS1100 back panel, there is a power plug, reset button, and an RJ45 (10/100) Ethernet port as shown in Figure 3-5.

The Ethernet port has two LEDs that indicate the status of the connection.

- **Left LED**
  - Green ON 100Mbps Link
  - Green Blink 100Mbps Activity
  - Orange ON 10Mbps Link
  - Orange Blink 10Mbps Activity

- **Right LED**
  - Green ON Full Duplex
  - OFF Half Duplex

The Ethernet port can connect to an Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) network.

Reset Button

You can reset the EDS1100 to factory defaults, including clearing the network settings. The IP address, gateway, and netmask are set to 00s.

To reset the unit to factory defaults, perform the following steps.

1. Place the end of a paper clip or similar object into the reset opening (back panel) and press for a minimum of 3 seconds.

2. Remove the paper clip to release the button. The firmware restores factory default settings to the configuration and reboots the unit.
Top LEDs

*Figure 3-6* shows the top of the EDS1100 and *Table 3-7* lists and describes the LEDs that are on the top of the device.

*Figure 3-6  EDS1100 Top LEDs*

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power (blue)</td>
<td>ON—EDS is receiving power</td>
</tr>
<tr>
<td>TX Serial (green)</td>
<td>Blinking—EDS is transmitting data on the serial port</td>
</tr>
<tr>
<td>RX Serial (yellow)</td>
<td>Blinking—EDS is receiving data on the serial port</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>ON—EDS firmware has completed booting</td>
</tr>
<tr>
<td></td>
<td>Blinking 1x/sec—EDS firmware is booting</td>
</tr>
<tr>
<td></td>
<td>Blinking 2x/sec—EDS is writing a file to flash</td>
</tr>
<tr>
<td></td>
<td>Blinking 4x/sec—EDS is compacting the file system</td>
</tr>
<tr>
<td></td>
<td>Blinking 5x/sec—EDS is restoring factory defaults</td>
</tr>
</tbody>
</table>

Installing the EDS1100

Be sure to place the device on a flat horizontal or vertical surface. The device comes with mounting brackets for mounting the device vertically, for example on a wall. If using AC power, avoid outlets controlled by a wall switch.

Observe the following guidelines when connecting the serial devices:
The EDS1100 serial ports support RS-232/422/485 devices.

- The null modem cable is the best cable to connect the serial port to a DCE device. The straight-through (modem) cable is the best cable to connect the serial port to a DTE device.
- Power-up the device by using the barrel-power connector only. The barrel-power connector supports a power range of 9 to 30 VDC.

**Note:** As soon as you plug the device into power, the device powers up automatically, the self-test begins, and Evolution OS™ starts.

Perform the following steps to install your device. The steps are shown in *Figure 3-8*.

1. Connect a serial device to your unit.
2. Connect an Ethernet cable between the EDS1100 RJ45 port and your Ethernet network.
3. Plug the EDS1100 into the power outlet by using the power supply that was included in the packaging. The required input voltage is 9-30 VDC (center +) with 1.5W maximum power required.
4. Power up the serial device.
4: Installation of EDS2100

This chapter describes how to install the EDS2100 device server. It contains the following sections:

- Package Contents
- User-Supplied Items
- Hardware Components
- Installing the EDS2100

Package Contents

The EDS2100 package includes the following items:

- One EDS2100 device
- One DB9F-to-DB9F serial null modem cable
- Power Cube, 100-240 VAC with international adapters
- Power cord restraint
- Printed Quick Start Guide

User-Supplied Items

To complete your installation, you need the following items:

- RS-232/422/485 serial devices that require network connectivity.
- A serial cable, as listed below, for each serial device. One end of the cable must have a female DB9 connector for the serial port.
  - A null modem cable, such as the one supplied in your EDS2100 package, to connect the serial port to another DTE device.
  - A straight-through modem cable to connect the serial port to a DCE device.
- 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.
Hardware Components

The EDS2100 has two male DB9 serial ports that support RS-232/422/485. Figure 4-1 shows the front of the device. The default serial port settings are 9600 baud, 8 bits, no parity, 1 stop bit, no flow control.

![Figure 4-1 EDS2100 Male DB9 DTE Serial Ports](image)

The RS-232 pinout configuration is shown in Figure 4-2.

![Figure 4-2 EDS2100 Pinout Configuration for RS-232](image)

Figure 4-3 shows the pinout configuration for RS-422 (4-wire).

![Figure 4-3 EDS2100 Pinout Configuration for RS-422 (4-wire)](image)

Figure 4-4 shows the pinout configuration for RS-485 (2-wire).
Back Panel

On the EDS2100 back panel, there is a power plug, reset button, and an RJ45 (10/100) Ethernet port as shown in Figure 4-5.

The Ethernet port has two LEDs that indicate the status of the connection as follows:

- **Left LED**
  - Green ON 100Mbps Link
  - Green Blink 100Mbps Activity
  - Orange ON 10Mbps Link
  - Orange Blink 10Mbps Activity.

- **Right LED**
  - Green ON Full Duplex.
  - OFF Half Duplex

The Ethernet port can connect to an Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) network.

Reset Button

You can reset the EDS2100 to factory defaults, including clearing the network settings. The IP address, gateway, and netmask are set to 00s. To reset the unit to factory defaults, perform the following steps.

1. Place the end of a paper clip or similar object into the reset opening and press for a minimum of 3 seconds.
2. Remove the paper clip to release the button. The firmware restores factory default settings to the configuration and reboots the unit.
Top LEDs

*Figure 4-6* shows the top of the EDS2100. *Table 4-7* lists and describes the LEDs.

*Figure 4-6  EDS2100 Top LEDs*

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power (blue)</td>
<td>ON—EDS is receiving power</td>
</tr>
<tr>
<td>TX Serial 1 (green)</td>
<td>Blinking—EDS is transmitting data on serial port 1</td>
</tr>
<tr>
<td>RX Serial 1 (yellow)</td>
<td>Blinking—EDS is receiving data on serial port 1</td>
</tr>
<tr>
<td>TX Serial 2 (green)</td>
<td>Blinking—EDS is transmitting data on serial port 2</td>
</tr>
<tr>
<td>RX Serial 2 (yellow)</td>
<td>Blinking—EDS is receiving data on serial port 2</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>ON—EDS firmware has completed booting</td>
</tr>
<tr>
<td></td>
<td>Blinking 1x/sec—EDS firmware is booting</td>
</tr>
<tr>
<td></td>
<td>Blinking 2x/sec—EDS is writing a file to flash</td>
</tr>
<tr>
<td></td>
<td>Blinking 4x/sec—EDS is compacting the file system</td>
</tr>
<tr>
<td></td>
<td>Blinking 5x/sec—EDS is restoring factory defaults</td>
</tr>
</tbody>
</table>
Installing the EDS2100

Be sure to place the device on a flat horizontal or vertical surface. The device comes with mounting brackets for mounting the device vertically, for example on a wall. If using AC power, avoid outlets controlled by a wall switch.

Observe the following guidelines when connecting the serial devices:

- The EDS2100 serial ports support RS-232/422/485 devices.
- The null modem cable is the best cable to connect the serial port to another DTE device. The straight-through (modem) cable is the best cable to connect the serial port to a DCE device.
- Power-up the device by using the Barrel-power connector only. The barrel-power connector supports a power range of 9 to 30 VDC.

Note: As soon as you plug the device into power, the device powers up automatically, the self-test begins, and Evolution OS™ starts.

Perform the following steps to install your device which are numbered in Figure 4-8 also.

1. Connect a serial device to your unit.
2. Connect an Ethernet cable between the EDS2100 RJ45 port and your Ethernet network.
3. Plug the EDS2100 into the power outlet by using the power supply that was included in the packaging. The required input voltage is 9-30 VDC (center +) with 1.5W maximum power required.
4. Power up the serial devices.
Figure 4-8  EDS2100 Connections

Serial Devices

1

Cat5 Ethernet Cable

2

10/100BASE-T Ethernet

3
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 EDS1100/2100 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 EDS1100/2100 devices appear.
4. Select the EDS1100/2100 unit by expanding its entry and clicking on its hardware (MAC) or IP address to view its configuration.
5. On the right page, click the Device Details tab. The current EDS1100/2100 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><strong>Name</strong></td>
<td>Name identifying the EDS1100/2100 device server.</td>
</tr>
<tr>
<td><strong>DHCP Device Name</strong></td>
<td>Shows the name associated with the current IP address, if the IP address was obtained dynamically.</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>Configurable field. Enter a group to categorize the EDS1100/2100 device server. Double-click the field, type in the value, and press <strong>Enter</strong> 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><strong>Comments</strong></td>
<td>Configurable field. Enter comments for the EDS1100/2100 device server. Double-click the field, type in the value, and press <strong>Enter</strong> 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><strong>Device Family</strong></td>
<td>Shows the EDS1100/2100 device family type as “EDS”.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Shows the specific device type, such as “EDS1100” or “EDS2100”.</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>Shows the EDS1100/2100 ID embedded within the unit.</td>
</tr>
<tr>
<td><strong>Hardware Address</strong></td>
<td>Shows the EDS1100/2100 hardware (MAC) address.</td>
</tr>
<tr>
<td><strong>Firmware Version</strong></td>
<td>Shows the firmware currently installed on the EDS1100/2100.</td>
</tr>
<tr>
<td><strong>Extended Firmware Version</strong></td>
<td>Provides additional information on the firmware version.</td>
</tr>
<tr>
<td><strong>Online Status</strong></td>
<td>Shows the EDS1100/2100 status as <strong>Online</strong>, <strong>Offline</strong>, <strong>Unreachable</strong> (if the EDS1100/2100 is on a different subnet), or <strong>Busy</strong> (if the EDS1100/2100 is currently performing a task).</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Shows the EDS1100/2100 device’s current IP address. To change the IP address, click the <strong>Assign IP</strong> button on the DeviceInstaller menu bar.</td>
</tr>
<tr>
<td><strong>IP Address was Obtained</strong></td>
<td>Displays <strong>Dynamically</strong> if the EDS1100/2100 automatically received an IP address (e.g., from DHCP). Displays <strong>Statically</strong> if the IP address was configured manually.</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Shows the subnet mask specifying the network segment on which the EDS1100/2100 resides.</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td>Shows the IP address of the router of this network. There is no default.</td>
</tr>
<tr>
<td><strong>Number of Serial Ports</strong></td>
<td>Shows the number of serial ports on this EDS1100/2100 unit.</td>
</tr>
<tr>
<td><strong>Supports Configurable Pins</strong></td>
<td>Shows <strong>False</strong>, indicating configurable pins are available on the EDS1100/2100 unit.</td>
</tr>
<tr>
<td><strong>Supports Email Triggers</strong></td>
<td>Shows <strong>True</strong>, indicating email triggers are available on the EDS1100/2100 unit.</td>
</tr>
<tr>
<td><strong>Telnet Supported</strong></td>
<td>Indicates whether Telnet is enabled on this EDS1100/2100 unit. Shows <strong>True</strong>.</td>
</tr>
<tr>
<td><strong>Telnet Port</strong></td>
<td>Shows the EDS1100/2100 port for Telnet sessions.</td>
</tr>
<tr>
<td><strong>Web Port</strong></td>
<td>Shows the EDS1100/2100 port for Web Manager configuration.</td>
</tr>
<tr>
<td><strong>Firmware Upgradable</strong></td>
<td>Shows <strong>True</strong>, indicating the EDS1100/2100 firmware is upgradable as newer versions become available.</td>
</tr>
</tbody>
</table>
6: Configuration Using Web Manager

This chapter describes how to configure the EDS1100/2100 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 EDS1100/2100 unit in the address bar. The IP address may have been assigned manually using the DeviceInstaller application (see Chapter 5: Using DeviceInstaller EDS1100/2100) 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.

Figure 6-3 Components of the Web Manager Page

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 EDS1100/2100 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>36</td>
</tr>
<tr>
<td>CLI</td>
<td>Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.</td>
<td>127</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Lets you perform various diagnostic procedures.</td>
<td>113</td>
</tr>
<tr>
<td>DNS</td>
<td>Shows the current configuration of the DNS subsystem and the DNS cache.</td>
<td>70</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>123</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>103</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>74</td>
</tr>
<tr>
<td>Host</td>
<td>Lets you view and change settings for a host on the network.</td>
<td>68</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>77</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>111</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>44</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>LPD</td>
<td>Shows LPD (Line Printer Daemon) Queue statistics and lets you configure the LPD and print a test page.</td>
<td>83</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.</td>
<td>100</td>
</tr>
<tr>
<td>Network</td>
<td>Shows status and lets you configure the network interface.</td>
<td>40</td>
</tr>
<tr>
<td>PPP</td>
<td>Lets you configure a network link using Point-to-Point Protocol (PPP) over a serial line.</td>
<td>71</td>
</tr>
<tr>
<td>Protocol Stack</td>
<td>Lets you perform lower level network stack-specific activities.</td>
<td>106</td>
</tr>
<tr>
<td>Query Port</td>
<td>Lets you change configuration settings for the query port.</td>
<td>112</td>
</tr>
<tr>
<td>RSS</td>
<td>Lets you change current Really Simple Syndication (RSS) settings.</td>
<td>82</td>
</tr>
<tr>
<td>SNMP</td>
<td>Lets you change the current Simple Network Management Protocol (SNMP) configuration settings.</td>
<td>73</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>86</td>
</tr>
<tr>
<td>SSL</td>
<td>Lets you upload an existing certificate or create a new self-signed certificate.</td>
<td>94</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>76</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>121</td>
</tr>
<tr>
<td>Terminal</td>
<td>Lets you change current settings for a terminal.</td>
<td>66</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>75</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Lets you change the current configuration settings for a tunnel.</td>
<td>48</td>
</tr>
<tr>
<td>XML</td>
<td>Lets you export XML configuration and status records, and import XML configuration records.</td>
<td>129</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><strong>BOOTP Client</strong></td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td><strong>DHCP Client</strong></td>
<td>On [Renew]</td>
<td>On</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>172.19.100.199 (DHCP)</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>Network Mask</strong></td>
<td>255.255.0.0 (DHCP)</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>172.19.0.1 (DHCP)</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>&lt;None&gt;</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>eng.lantronix.com (DHCP)</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>DNS Suffix Search List</strong></td>
<td>eng.lantronix.com, int.lantronix.com, lantronix.com</td>
<td>&lt;DHCP&gt;</td>
</tr>
<tr>
<td><strong>DHCP Client ID</strong></td>
<td>[0x0d, 0x01]</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td><strong>MTU</strong></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.

![Network 1 (eth0) Interface Configuration](image)

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Network 1 (eth0) Interface Configuration Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| BOOTP Client: | Select **On** or **Off**. At boot up, the device will attempt to obtain an IP address from a BOOTP server. **Notes:**
| | ◆ **Overides the configured IP address, network mask, gateway, hostname, and domain.**
| | ◆ **When DHCP is On, the system automatically uses DHCP, regardless of whether BOOTP Client is On.**

Table 7-3  Network 1 (eth0) Interface Configuration
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.

Figure 7-4  Network 1 Ethernet Link

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 7-5  Network 1 Ethernet Link

<table>
<thead>
<tr>
<th>Network 1-Ethernet Link Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Select the Ethernet link speed. Default is Auto.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Select the Ethernet link duplex mode. Default is Auto.</td>
</tr>
</tbody>
</table>

3. Click Submit. The changes take effect immediately.

Note: The following section describes the steps to view and configure Line 1 settings; these steps apply to other line instances of the device.
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**

**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.

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.
3. Select **Statistics**. The Line Statistics page for the selected line appears.
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.

Note: The Interface option is only supported in XPort Pro, EDS4100, EDS1100 and EDS2100.

Note: The Buffer option is only supported in EDS1100 and EDS2100.
4. Enter or modify the following settings:

<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 66 for related configuration information.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface type from the drop-down menu. The default is RS232. Note: 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. Note: 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>
<tr>
<td>Buffer</td>
<td>Enter the buffer in Kbytes. Specifies the buffer size allocation in RAM that will be used in Tunnel Accept and Tunnel Connect mode connection/session. Buffer range is 16 to 1200 Kbytes.</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 8-5 Line Command Mode

<table>
<thead>
<tr>
<th>Line – Command Mode Settings</th>
<th>Description</th>
</tr>
</thead>
</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 \x and each decimal byte value starts with \\. |
| Echo Serial String           | Select Yes to enable echoing of the serial string at boot-up. |
5. 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.*

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 35)](#) or the [Command Reference](#) for the full list of commands.

The EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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**

---

<table>
<thead>
<tr>
<th>Line – Command Mode Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Signon Message** | Enter the boot-up signon message. Select a string type.  
  - **Text** = string of bytes sent on the serial line during boot time.  
  - **Binary** = one or more byte values separated by commas. Each byte value may be decimal or hexadecimal. Start hexadecimal values with 0x.  
    
  *Note: This string will be output on the serial port at boot, regardless of whether command mode is enabled or not.* |
8: Line and Tunnel Settings

- **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 EDS1100/2100 logs statistics for tunneling. The **Dropped** statistic shows connections ended by the remote location. The **Disconnects** statistic shows connections ended by the EDS1100/2100 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.
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>
<thead>
<tr>
<th>Tunnel - Serial Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol (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>- <strong>Unasserted</strong> = never asserted</td>
</tr>
<tr>
<td></td>
<td>- <strong>TruPort</strong> = 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>- <strong>Asserted while connected</strong> = asserted whenever either a connect or an accept mode tunnel connection is active.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Continuously asserted</strong> = 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.

![Figure 8-9 Tunnel 1 Packing Mode (Mode = Disable)](image)

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.
4. Enter or modify the following settings:

**Table 8-12 Tunnel Packing Mode**

<table>
<thead>
<tr>
<th>Tunnel - Packing Mode Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Mode                           | - **Select Disable** to disable Packing Mode completely.  
- **Select Timeout** to send data after the specified time has elapsed.  
- **Select Send Character** to send the queued data when the send character is received. |
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 EDS1100/2100 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 EDS1100/2100 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**

- **AES encryption over TCP**

- **Telnet**
  The EDS1100/2100 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:**

- **Disabled**
  Never accepts a connection.

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

- **Active**
  (If it receives any character from the serial port.)
8: Line and Tunnel Settings

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

- **Modem control signal**
  (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.

![Figure 8-13 Tunnel 1 Accept Mode](image)

**Tunnel 1 - Accept Mode**

- **Mode:** Always
- **Local Port:** 10001
- **Protocol:** TCP
- **TCP Keep Alive:** 45000 milliseconds
- **Flush Serial:** Enabled
- **Block Serial:** Disabled
- **Block Network:** Disabled
- **Password:** <None>
- **Email on Connect:** <None>
- **Email on Disconnect:** <None>
- **CP Output:**

**Note:** The **CP Output** option is only supported in XPort Pro and XPort AR.

4. Enter or modify the following settings:
8: Line and Tunnel Settings

Table 8-14 Tunnel Accept Mode

<table>
<thead>
<tr>
<th>Tunnel - Accept Mode Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Mode                        | Select the method used to start a tunnel in Accept mode. Choices are:  
  - **Disable** = do not accept an incoming connection.  
  - **Always** = accept an incoming connection *(default)*  
  - **Any Character** = start waiting for an incoming connection when any character is read on the serial line.  
  - **Start Character** = start waiting for an incoming connection when the start character for the specific tunnel is read on the serial line.  
  - **Modem Control Asserted** = 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.  
  - **Modem Emulation** = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation. |
| Local Port                  | Enter the port number for use as the local port. The defaults are port 10001 for Tunnel 1. Additional tunnels, if supported, increase sequentially. |
| Protocol                    | 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. |
| TCP Keep Alive              | 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. |
| Flush Serial Data           | Select Enabled to flush the serial data buffer on a new connection. |
| Block Serial Data           | Select On to block, or not tunnel, serial data transmitted to the device. |
| Block Network               | Select On to block, or not tunnel, network data transmitted to the device. |
| Password                    | Enter a password that clients must send to the device within 30 seconds from opening a network connection to enable data transmission.  
  The password can have up to 31 characters and must contain only alphanumeric characters and punctuation. When set, the password sent to the device must be terminated with one of the following: (a) 0x0A (LF), (b) 0x00, (c) 0x0D 0x0A (CR LF), or (d) 0x0D 0x00. |
| Email on Connect            | Select whether the device sends an email when a connection is made. Select None if you do not want to send an email. Otherwise, select the Email profile to use for sending. |
| Email on Disconnect         | Select whether the device sends an email when a connection is closed. Select None if you do not want to send an email. Otherwise, select the Email profile to use for sending. |

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 EDS1100/2100 device will make a connection only if it can resolve the address. For DNS names, the EDS1100/2100 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 EDS1100/2100 unit is the SSH client. Ensure the EDS1100/2100 SSH client username is configured on the remote SSH server before using it with the EDS1100/2100.
- **SSL**
- **UDP**
  - Is only available in Connect Mode because it is a connectionless protocol. For Connect Mode using UDP, the EDS1100/2100 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.
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:

   - **Note**: The **Host Mode** options is supported in all products except the XPort AR.

   - **Note**: The **CP Output** option is only supported in MatchPort b/g Pro, XPort Pro and XPort AR device servers.
### Table 8-16 Tunnel Connect Mode

<table>
<thead>
<tr>
<th>Tunnel – Connect Mode Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>Select the method to be used to attempt a connection to a remote host or device. Choices are:</td>
</tr>
<tr>
<td>◆ <strong>Disable</strong> = an outgoing connection is never attempted.</td>
<td></td>
</tr>
<tr>
<td>◆ <strong>Always</strong> = a connection is attempted until one is made. If the connection gets disconnected, the EDS1100/2100 retries until it makes a connection. (default)</td>
<td></td>
</tr>
<tr>
<td>◆ <strong>Any Character</strong> = a connection is attempted when any character is read on the serial line.</td>
<td></td>
</tr>
<tr>
<td>◆ <strong>Start Character</strong> = a connection is attempted when the start character for the specific tunnel is read on the serial line.</td>
<td></td>
</tr>
<tr>
<td>◆ <strong>Modem Control Asserted</strong> = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made.</td>
<td></td>
</tr>
<tr>
<td>◆ <strong>Modem Emulation</strong> = a connection is attempted when triggered by modem emulation AT commands.</td>
<td></td>
</tr>
<tr>
<td><strong>Local Port</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>Click &lt;None&gt; in the Host field to configure the Host parameters.</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</strong> and <strong>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/AES 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.
8: Line and Tunnel Settings

<table>
<thead>
<tr>
<th>Tunnel – Connect Mode Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnect Timer</td>
<td>Enter the reconnect time in milliseconds. The device attempts to reconnect after this amount of time after failing a connection or exiting an existing connection. This behavior depends upon the Disconnect Mode.</td>
</tr>
</tbody>
</table>

**Note:**
- **When you configure Tunnel - Connect Mode**, you can specify a number of milliseconds to attempt to reconnect after a dropped connection has occurred. The default is 1500 milliseconds.
- **The Reconnect Timer only applies if a Disconnect Mode is configured.** With a Disconnect Mode set, the device server maintains a connection until the disconnect mode condition is met (at which time the device server closes the connection). If the tunnel is dropped due to conditions beyond the device server, the device server attempts to re-establish a failed connection when the specified reconnect interval reaches its limit.
- **Any network-side disconnect is considered an error and a reconnect is attempted without regard to the Connect Mode settings.** Simultaneous Connect Mode connections require some Disconnect Mode configurations or the connections will never terminate. See To configure Connect Mode for a specific tunnel: on page 58 for more information about the parameters.
- **If Disconnect Mode is disabled and the network connection is dropped, then the re-establishment of a tunnel connection is governed by the configured Connect Mode settings.**

<table>
<thead>
<tr>
<th>Flush Serial Data</th>
<th>Select whether to flush the serial line when a connection is made. Choices are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>◆ <strong>Enabled</strong> = flush the serial line when a connection is made.</td>
</tr>
<tr>
<td></td>
<td>◆ <strong>Disabled</strong> = do not flush the serial line. (default)</td>
</tr>
</tbody>
</table>

| Block Serial                             | Select **Enabled** to block (not tunnel) serial data transmitted to the device. This is a debugging tool that causes serial data sent to the device to be ignored. |
|                                          | Select **Disabled** to block (not tunnel) serial data transmitted to the device. This is a debugging tool that causes serial data sent to the device to be ignored. |

| Email on Connect                         | Select whether the device sends an email when a connection is made. Select None if you do not want to send an email. Otherwise, select the Email profile to use. |
|                                          | Select whether the device sends an email when a connection is closed. Select None if you do not want to send an email. Otherwise, select the Email profile to use. |

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. EDS1100/2100 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 EDS1100/2100, 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 62). 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 8-17  Host 1, Host 2, Host 3 Exchanged*

*Note:* The Host Mode options is supported in all products except the XPort AR.

*Note:* The CP Output option is only supported in MatchPort b/g Pro, XPort Pro and XPort AR device servers.
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 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 EDS1100/2100 unit shuts down the specific tunnel connection gracefully.

The following settings end a specific tunnel connection:

- The EDS1100/2100 receives the stop character.
- The timeout period has elapsed and no activity is going in or out of the EDS1100/2100 device. Both Accept Mode and Connect Mode must be idle for the time frame.
- The EDS1100/2100 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.

4. Enter or modify the following settings:
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 EDS1100/2100, an “OK” message is sent (but the command is silently ignored).

The EDS1100/2100 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 8-20 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>
<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>
</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 EDS1100/2100 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 EDS1100/2100 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>
<thead>
<tr>
<th>Command (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>

**Table 8-20  Modem Emulation Commands and Descriptions (continued)**
4. Enter or modify the following settings:

**Table 8-22 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 EDS1100/2100 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:
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.

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:

![Figure 9-5 Host Configuration](image)

<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. <strong>Note:</strong> 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>Appears if you selected SSH as the protocol. 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.</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
- Point-to-Point (PPP) 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 EDS1100/2100 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.

Point-to-Point (PPP) Settings

Point-to-Point Protocol establishes a direct connection between two nodes. It defines a method for data link connectivity between devices using physical layers (such as serial lines).

The EDS1100/2100 device server supports two types of PPP authentication: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both of these authentication methods require the configuration of a username and password. The EDS1100/2100 device server also supports the authentication scheme of “None” when no authentication is required during link negotiation.

PAP authentication offers a straightforward method for the peer to determine its identity. Upon the link establishment, the user ID and password are repeatedly sent to the authenticator until it is acknowledged or the connection is terminated. However, PAP is not a strong authentication process. There is no protection against trial-and-error attacks. The peer is responsible for the frequency of the authentication communication attempts.

CHAP is a more secure method than PAP. It works by sending a challenge message to the connection requestor. Using a one-way hash function, the requestor responds with its value. If the value matches the server’s own calculations, authentication is provided. Otherwise, the connection is terminated.

Note: RFC1334 defines both CHAP and PAP.

The EDS1100/2100 device server also supports authentication scheme of “None” when no authentication is required during link negotiation.

Since the EDS1100/2100 unit does not support Network Address and Port Translation (NAPT), static routing table entries must be added to the serial-side and network-side devices (both of which are external devices).

Use the EDS1100/2100 Web Manager or CLI to configure a network link using PPP over a serial line. Turn off Connect Mode, Accept Mode, and Command mode before enabling PPP. The EDS1100/2100 device acts as the server side of the PPP link; it can require authentication and assign an IP address to the peer. Upon PPP configuration, IP packets are routed between Ethernet and PPP interfaces.

Note: The EDS1100/2100 device server does not perform network address translation (NAT) between the serial-side network interface and the Ethernet/WLAN network interface. Therefore, to pass packets through the EDS1100/2100 unit, a static route must be configured on both the PPP Peer device and the remote device it wishes to communicate with. The static route in the PPP Peer device must use the PPP Local IP.
Address as its gateway, and the static route in the remote device must use the network interface IP Address of the EDS1100/2100 device server as its gateway.

The following section describes the steps to configure PPP 1 (PPP on serial line 1); these steps also apply to any line instance of the device. Since the EDS1100/2100 unit does not support NAPT (Network Address and Port Translation), static routing table entries must be added to both the serial-side and network-side devices (both of which are external to the EDS1100/2100 device server).

To configure PPP:
1. Select PPP on the menu bar. The PPP web page appears.
2. Select a line number at the top of the page. The PPP Configuration page for the selected line number appears.

![Figure 10-2 PPP Configuration Settings](image)

3. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>PPP Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local IP Address</td>
<td>Enter the IP address assigned to the device’s PPP interface.</td>
</tr>
<tr>
<td>Peer IP Address</td>
<td>Enter the IP address assigned to the peer (when requested during negotiation).</td>
</tr>
</tbody>
</table>
| Authentication Mode       | Choose the authentication mode:  
  - None = no authentication is required  
  - PAP = Password Authentication Protocol  
  - CHAP = Challenge Handshake Authentication Protocol  
  - MS-CHAP = Microsoft Challenge-Handshake Authentication Protocol  
  - MS-CHAPV2 = Microsoft Challenge-Handshake Authentication Protocol Version 2 |
| Username                  |             |
| Password                  |             |

Submit
4. Click **Submit**.

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

### 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 10-4 SNMP Configuration](image)

**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><strong>State</strong></td>
<td>Select <strong>Enabled</strong> to enable SNMP.</td>
</tr>
<tr>
<td><strong>Read Community</strong></td>
<td>Enter the SNMP read-only community string.</td>
</tr>
<tr>
<td><strong>Write Community</strong></td>
<td>Enter the SNMP read/write community string.</td>
</tr>
<tr>
<td><strong>System Contact</strong></td>
<td>Enter the name of the system contact.</td>
</tr>
<tr>
<td><strong>System Name</strong></td>
<td>Enter the system name.</td>
</tr>
<tr>
<td><strong>System Description</strong></td>
<td>Enter the system description.</td>
</tr>
<tr>
<td><strong>System Location</strong></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. The Cold Start trap is sent on device boot up, and the Linkdown trap is sent when the device is rebooted from software control.</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 10-6 FTP Configuration](image)

2. Enter or modify the following settings:
### 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 10-8 TFTP Configuration](image)

2. Enter or modify the following settings:

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

2. Enter or modify the following settings:
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 EDS1100/2100 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.

---

**Table 10-11 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**.
Figure 10-12 HTTP Statistics

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

![HTTP Configuration](image)

<table>
<thead>
<tr>
<th>HTTP Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select Enabled to enable the HTTP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port for the HTTP server to use. The default is 80.</td>
</tr>
<tr>
<td>Secure Port</td>
<td>Enter the port for the HTTPS server to use. The default is 443. The HTTP server only listens on the HTTPS Port when an SSL certificate is configured.</td>
</tr>
</tbody>
</table>
3. Click **Submit**.
HTTP Authentication

HTTP Authentication enables you to require usernames and passwords to access specific web pages or directories on the EDS1100/2100' 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.

2. Enter or modify the following settings:

   **Table 10-16 HTTP Authentication**

<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>Realm</td>
<td>Enter the domain, or realm, used for HTTP. Required with the URI field.</td>
</tr>
</tbody>
</table>

   **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".

Figure 10-15 HTTP Authentication
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 EDS1100/2100 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 EDS1100/2100 configuration changes, RSS feeds permit viewing only relevant and new information regarding changes made to the EDS1100/2100 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.
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. <strong>Note:</strong> It may be necessary to remove authentication from RSS access to view data entries on certain web browsers. Go to HTTP Authentication on page 81 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 EDS1100/2100 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:
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.
3. Select **Print Test Page**. A popup window appears.
4. Enter the numbers to print in the popup window.
5. Click OK.
11: Security Settings

The EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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.
   ```shell
   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.

   ![SSH Server: Host Keys (Upload Keys)](image)

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 89).
   ```
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 11-3  SSH Server Host Keys Settings - Upload Keys Method

<table>
<thead>
<tr>
<th>SSH Server: Host Keys Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Key</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>Public Key</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 EDS1100/2100 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 11-4  SSH Server Host Keys Settings - Create New Keys Method

<table>
<thead>
<tr>
<th>SSH Server: Host Keys Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Type</td>
<td>Select a key type to use:</td>
</tr>
<tr>
<td></td>
<td>◆ RSA = use this key with SSH1 and SSH2 protocols.</td>
</tr>
<tr>
<td></td>
<td>◆ DSA = use this key with the SSH2 protocol.</td>
</tr>
<tr>
<td></td>
<td>Note: RSA is more secure.</td>
</tr>
<tr>
<td>Bit Size</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></td>
<td>Using a larger bit size takes more time to generate the key. Approximate times are:</td>
</tr>
<tr>
<td></td>
<td>◆ 10 seconds for a 512 bit RSA Key</td>
</tr>
<tr>
<td></td>
<td>◆ 15 seconds for a 768 bit RSA Key</td>
</tr>
<tr>
<td></td>
<td>◆ 1 minute for a 1024 bit RSA Key</td>
</tr>
<tr>
<td></td>
<td>◆ 30 seconds for a 512 bit DSA Key</td>
</tr>
<tr>
<td></td>
<td>◆ 1 minute for a 768 bit DSA Key</td>
</tr>
<tr>
<td></td>
<td>◆ 2 minutes for a 1024 bit DSA Key</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

3. Click Submit.

Note: SSH Keys from other programs may be converted to the required EDS1100/2100 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 EDS1100/2100 device server that can be used to log into the EDS1100/2100 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 11-6  SSH Server Authorized User 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 <strong>Choose File</strong> 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 <strong>Choose File</strong> 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.

   ![Figure 11-7 SSH Client: Known Hosts](image)

   **Figure 11-7 SSH Client: Known Hosts**

2. Enter or modify the following settings:

<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 EDS1100/2100 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.
2. Enter or modify the following settings:

<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 <code>shell</code>, 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 <code>Choose File</code> button to select the key.</td>
</tr>
</tbody>
</table>
| Public Key                  | Enter the path and name of the existing public key you want to use with this SSH client user or use the `Choose File` button to select the key. **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>Username</th>
<th>Enter the name of the user associated with the new key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Type</td>
<td>Select the key type to be used for the new key. Choices are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RSA</td>
<td>= use this key with the SSH1 and SSH2 protocols.</td>
</tr>
<tr>
<td></td>
<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>
<td></td>
</tr>
<tr>
<td></td>
<td>512</td>
<td></td>
</tr>
<tr>
<td></td>
<td>768</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1024</td>
<td></td>
</tr>
</tbody>
</table>

Using a larger Bit Size takes more time to generate the key. Approximate times are:

- 10 seconds for a 512 bit RSA Key
- 15 seconds for a 768 bit RSA Key
- 1 minute for a 1024 bit RSA key
- 30 seconds for a 512 bit DSA key
- 1 minute for a 768 bit DSA key
- 2 minutes for a 1024 bit DSA key

**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 95).

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 EDS1100/2100 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 EDS1100/2100 unit supports SSLv3 and its successors, TLS1.0 and TLS1.1.

Note: An incoming SSLv2 connection attempt is answered with an SSLv3 response. If the initiator also supports SSLv3, SSLv3 handles the rest of the connection.

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>
<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>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.

When using HTTPS, SSL Tunneling in Accept mode, and/or EAP-TLS, the EDS1100/2100 unit needs a personal certificate with a matching private key to identify itself and sign its messages. When using SSL Tunneling in Connect mode and/or EAP-TLS, EAP-TTLS or PEAP, the EDS1100/2100 device server needs the authority certificate that can authenticate users with which it wishes to communicate.

SSL RSA

As mentioned above, the certificates contain a public key. Different key exchange methods require different public keys and therefore different certificate styles. The EDS1100/2100 device server supports key exchange methods that require an RSA-style certificate. The RSA key exchange method can work with this style if an RSA certificate is stored in the EDS1100/2100 unit.

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 EDS1100/2100 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 EDS1100/2100 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 EDS1100/2100 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:

```
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:

```
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 EDS1100/2100 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:

```
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 EDS1100/2100 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 Diagram](image-url)
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>Upload Certificate</strong></td>
<td></td>
</tr>
<tr>
<td><strong>New Certificate</strong></td>
<td>This certificate identifies the device to peers. It is used for HTTPS and SSL Tunneling. Enter the path and name of the certificate you want to upload, or use the <strong>Choose File</strong> button to select the certificate. RSA certificates with 1024 or 2048 bit public keys are allowed. The format of the file must be <strong>PEM</strong>. 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. <strong>Note:</strong> Supported RSA Certificates include MD5, SHA1, SHA256, SHA384, and SHA512.</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 <strong>Choose File</strong> button to select the private key. The key needs to belong to the certificate entered above. The format of the file must be <strong>PEM</strong>. 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></td>
</tr>
<tr>
<td><strong>Authority</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. Enter the path and name of the certificate you want to upload, or use the <strong>Choose File</strong> button to select the certificate. RSA certificates with 1024 or 2048 bit public keys are allowed. The format of the file must be <strong>PEM</strong>. 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></td>
</tr>
<tr>
<td><strong>Country (2 Letter Code)</strong></td>
<td>Enter the 2-letter country code to be assigned to the new self-signed certificate. <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. <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. <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>
### SSL Settings (continued) | Description
--- | ---
**Common Name** | Enter the same name that the user will enter when requesting your web site.  
**Example:** If a user enters [http://www.widgets.abccompany.com](http://www.widgets.abccompany.com) to access your web site, the **Common Name** would be [www.widgets.abccompany.com](http://www.widgets.abccompany.com).

| **Expires** | Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate.  
**Example:** An expiration date of May 9, 2020 is entered as 05/09/2020.

| **Key length** | Select the bit size of the new self-signed certificate.  
♦ **1024 bits**  
The larger the bit size, the longer it takes to generate the key. Approximate times are:  
♦ 1 minute for a 1024-bit RSA key |

| **Type** | Select the type of key:  
♦ **RSA** = Public-Key Cryptography algorithm based on large prime numbers, invented by Rivest Shamir and Adleman. Used for encryption and signing. |

3. Click **Submit**.
12: Modbus

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 12-1  6 Byte Header of Modbus Application Protocol**

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

*Note: Reference the Modbus Protocol User Guide for additional information. Lantronix documentation is available at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation).*

**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 12-2  Modbus Transmission Modes**

<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>

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>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>State:</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>Port:</td>
<td>502</td>
<td></td>
</tr>
<tr>
<td>Last Connection:</td>
<td>local 502 &lt; 172.19.205.10:3903</td>
<td></td>
</tr>
<tr>
<td>Uptime:</td>
<td>0 days 02:38:20</td>
<td></td>
</tr>
<tr>
<td>Total PDUs In:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total PDUs Out:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total Connections:</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Current Connections:</td>
<td>local 502 &lt; 172.19.205.10:3903</td>
<td>Kill</td>
</tr>
<tr>
<td></td>
<td>Uptime: 0 days 02:38:48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PDUs In: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PDUs Out: 0</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Local Slave</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total PDUs In:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total PDUs Out:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Exception Count:</td>
<td>0</td>
<td></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 44 for details.
13: Maintenance and Diagnostics 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 EDS1100/2100 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.
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.

![Filesystem Browser](image)
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 Create.</td>
</tr>
<tr>
<td>Directory</td>
<td>Enter the name of the directory you want to create, and then click Create.</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 Choose File button to select the file, and then click Upload.</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 Copy 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 Move 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>• Get = a &quot;get&quot; command will be executed to store a file locally.</td>
</tr>
<tr>
<td>Put</td>
<td>• Put = 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>• ASCII</td>
</tr>
<tr>
<td>Binary</td>
<td>• Binary</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 Transfer 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 13-5 TCP Protocol Settings

<table>
<thead>
<tr>
<th>Protocol Stack TCP Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Send RSTs                   | Click **Enabled** to send RSTs or **Disabled** 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.  
**Note:** Setting the RSTs may pose a security risk. |
| Ack Limit                   | 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 Ack Limit to 1 packet improves performance by forcing immediate acknowledgements. |
| Send Data                   | The **Send Data** selection governs when data may be sent into the network. The **Standard** implementation waits for an ACK before sending a packet less than the maximum length. Select **Expedited** to send data whenever the window allows it. |
4. Click Submit.

**IP Settings**

*To configure the network protocol settings for IP:*

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

![Figure 13-6 IP Protocol]

3. Modify the following settings:

*Table 13-7 IP Protocol Settings*

<table>
<thead>
<tr>
<th>Protocol Stack IP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Time to Live</strong></td>
<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>
<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</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Settings</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 13-11 ARP Settings**

<table>
<thead>
<tr>
<th>Protocol Stack ARP Settings</th>
<th>Description</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</strong>, <strong>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>
13: Maintenance and Diagnostics 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**.

![Figure 13-12 SMTP](image)

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 EDS1100/2100 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 EDS1100/2100 unit. You will have to then access the EDS1100/2100 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 33).

To configure the query port server:

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

   ![Figure 13-16 Query Port Configuration]

   **Figure 13-16 Query Port Configuration**

   - Query Port Server: On
   - Current Configuration and Statistics:
     - Query Port Status: On (running)
     - In Valid Queries: 135
     - In Unknown Queries: 124
     - In Erroneous Packets: 0
     - Out Query Replies: 135
     - Out Errors: 0
     - Last Connection: 172.19.229.60:28883

2. Select On to enable the query port server.

3. Click Submit.
Diagnostics

The EDS1100/2100 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.

![Figure 13-17 Diagnostics: Hardware](image-url)
**MIB-II Statistics**

The MIB-II Network Statistics page shows the various SNMP-served Management Information Bases (MIBs) available on the EDS1100/2100 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 13-19 Requests for Comments (RFCs)

<table>
<thead>
<tr>
<th>RFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1213</td>
<td>Original MIB-II definitions.</td>
</tr>
<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>
```

Figure 13-18  MIB-II Network Statistics
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>255.255.255.255</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.191:21</td>
<td>255.255.255.255</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.190:29</td>
<td>255.255.255.255</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.195:514</td>
<td>172.19.23.514</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.196:80</td>
<td>255.255.255.255</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.197:30716</td>
<td>172.19.230:32770</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>4</td>
<td>172.19.100.198:80</td>
<td>172.19.250.1944</td>
<td>ESTABLISHED</td>
</tr>
</tbody>
</table>

Ping

EDS1100/2100 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:
Table 13-22 Diagnostics: Ping

<table>
<thead>
<tr>
<th>Diagnostics: Ping Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the IP address or host name for the device to ping.</td>
</tr>
<tr>
<td>Count</td>
<td>Enter the number of ping packets the device should attempt to send to the Host. The default is 3.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Enter the time, in seconds, for the device to wait for a response from the host before timing out. The default is 5 seconds.</td>
</tr>
</tbody>
</table>

3. Click Submit. The results of the ping display in the page.

**Traceroute**

Here you can trace a packet from the EDS1100/2100 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](image)

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

![Figure 13-26 Diagnostics: Log (Filesystem)](image)
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 EDS1100/2100 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>Buffer Pools</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>256</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>
```

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.
### Figure 13-30 Processes

<table>
<thead>
<tr>
<th>PID</th>
<th>CPU %</th>
<th>Stack/Size</th>
<th>Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>99.43%</td>
<td>392/2048</td>
<td>Idle Task</td>
</tr>
<tr>
<td>3</td>
<td>0.19%</td>
<td>428/4000</td>
<td>LED</td>
</tr>
<tr>
<td>4</td>
<td>0.16%</td>
<td>364/2048</td>
<td>Timeout Server</td>
</tr>
<tr>
<td>5</td>
<td>0.44%</td>
<td>956/4006</td>
<td>Event Server</td>
</tr>
<tr>
<td>6</td>
<td>0.00%</td>
<td>976/5008</td>
<td>Log</td>
</tr>
<tr>
<td>7</td>
<td>0.00%</td>
<td>264/2048</td>
<td>DNS Cache</td>
</tr>
<tr>
<td>8</td>
<td>0.01%</td>
<td>484/4096</td>
<td>Ethernet Manager</td>
</tr>
<tr>
<td>9</td>
<td>0.00%</td>
<td>448/3008</td>
<td>Snmp Agent</td>
</tr>
<tr>
<td>11</td>
<td>0.00%</td>
<td>324/2048</td>
<td>FTP Server</td>
</tr>
<tr>
<td>12</td>
<td>0.00%</td>
<td>460/3072</td>
<td>TFTP Server</td>
</tr>
<tr>
<td>13</td>
<td>0.00%</td>
<td>1812/5120</td>
<td>Syslog</td>
</tr>
<tr>
<td>14</td>
<td>0.00%</td>
<td>2760/13008</td>
<td>Http1</td>
</tr>
<tr>
<td>15</td>
<td>0.00%</td>
<td>2636/13008</td>
<td>Http2</td>
</tr>
<tr>
<td>16</td>
<td>0.00%</td>
<td>2644/13008</td>
<td>Http3</td>
</tr>
<tr>
<td>17</td>
<td>0.00%</td>
<td>644/2512</td>
<td>Http0</td>
</tr>
<tr>
<td>18</td>
<td>0.00%</td>
<td>848/3072</td>
<td>Query Port (77FE)</td>
</tr>
<tr>
<td>19</td>
<td>0.00%</td>
<td>736/6512</td>
<td>Network-&gt;Serial Daemon Port 1</td>
</tr>
<tr>
<td>20</td>
<td>0.10%</td>
<td>1204/8000</td>
<td>Serial-&gt;Network Daemon Port 1</td>
</tr>
<tr>
<td>21</td>
<td>0.04%</td>
<td>668/8000</td>
<td>Accept Mode Daemon Port 1</td>
</tr>
<tr>
<td>22</td>
<td>0.00%</td>
<td>252/9216</td>
<td>Connect Mode Daemon Port 1</td>
</tr>
<tr>
<td>23</td>
<td>0.00%</td>
<td>710/8192</td>
<td>SMTP Client</td>
</tr>
<tr>
<td>24</td>
<td>0.00%</td>
<td>664/5120</td>
<td>LPD Daemon</td>
</tr>
<tr>
<td>25</td>
<td>0.00%</td>
<td>304/2512</td>
<td>Telnet CLI Server</td>
</tr>
<tr>
<td>26</td>
<td>0.00%</td>
<td>304/2512</td>
<td>SSH CLI Server</td>
</tr>
<tr>
<td>27</td>
<td>0.00%</td>
<td>264/10000</td>
<td>Serial Command Interpreter Port 1</td>
</tr>
</tbody>
</table>

**Total processor load: 0.57%**

CPU Load (3 second snapshots)
System Settings

The EDS1100/2100 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.

![System Settings](image)

2. Configure the following settings:

<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>
</tbody>
</table>
| Upload New Firmware   | 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.  
  
  *Note: Close and reopen the web manager browser upon a firmware update.* |
Name

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.

**Note:** Additional information about long and short name customization is available in [Short and Long Name Customization on page 138 of Chapter 15: Branding the EDS1100/2100 Unit](#).

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 EDS1100/2100 allows you to view and configure email alerts relating to the events occurring within the system. Please see SMTP Settings on page 110 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

<table>
<thead>
<tr>
<th>Email 1</th>
<th>Email 2</th>
<th>Email 3</th>
<th>Email 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistics</td>
<td>Configuration</td>
<td>Send Email</td>
<td></td>
</tr>
</tbody>
</table>

**Email 1 - Statistics**

- Sent successfully: 1
- Retries: 0
- Not sent due to excessive errors: 0
- In transmission queue: 0

**Log [Clear]**

```
120:15:49 220 SMTP International.com Microsoft ESMTP MAIL Service, Version: 6.0.2
120:15:49 EHLO ens.iamtronix.com
120:15:49 250-2smtp.int.iamtronix.com Helo [172.19.100.123]
120:15:49 250-EXTN
120:15:49 250-UTF8
120:15:49 250-EPHEMERAL
120:15:49 250-PSN
120:15:49 250-ENHANCEDSTATUSCODES
120:15:49 250-UBIXTIME
120:15:49 250-RESTARTTIME
120:15:49 250-CHUNKING
120:15:49 250-REQUEST-TIMEOUT
120:15:49 250-EDITOR
120:15:49 250-SESSION-ID
120:15:49 250-AUTH-LOGIN
120:15:49 250-X-LINKSTATE
120:15:49 250-X-GENERAL
120:15:49 250 X-CHUNK
120:15:49 MAIL FROM: <skuppusswamy@iamtronix.com>
120:15:49 RCPT TO: <skuppusswamy@iamtronix.com>...Sender OK
120:15:49 DATA
120:15:49 DATA
120:15:49 DATA
120:15:49 Data Start mail input; end with <CR>
120:15:49
120:15:49 250 OK
120:15:49 QUIT
```
Email Configuration

The EDS1100/2100 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:

| 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>
</tbody>
</table>

Note: The Trigger Email Send option is only supported in XPort Pro and XPort AR devices.
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.

<table>
<thead>
<tr>
<th>Email – Configuration Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From</strong></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><strong>Reply-To</strong></td>
<td>Enter the email address to list in the Reply-To field of the email alert.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>Enter the subject for the email alert.</td>
</tr>
<tr>
<td><strong>Message File</strong></td>
<td>Enter the path of the file to send with the email alert. This file appears within the message body of the email.</td>
</tr>
<tr>
<td><strong>Overriding Domain</strong></td>
<td>Enter the domain name to override the current domain name in EHLO (Extended Hello).</td>
</tr>
<tr>
<td><strong>Server Port</strong></td>
<td>Enter the SMTP server port number. The default is port <strong>25</strong>.</td>
</tr>
<tr>
<td><strong>Local Port</strong></td>
<td>Enter the local port to use for email alerts. The default is a random port number.</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Select the priority level for the email alert.</td>
</tr>
</tbody>
</table>
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:


<table>
<thead>
<tr>
<th>Figure 14-3 CLI Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Line Interface Statistics</td>
</tr>
<tr>
<td>Telnet</td>
</tr>
<tr>
<td>Server Status:</td>
</tr>
<tr>
<td>Last Connection:</td>
</tr>
<tr>
<td>Uptime:</td>
</tr>
<tr>
<td>Total Bytes In:</td>
</tr>
<tr>
<td>Total Bytes Out:</td>
</tr>
<tr>
<td>Current Connections:</td>
</tr>
<tr>
<td>SSH</td>
</tr>
<tr>
<td>Server Status:</td>
</tr>
<tr>
<td>Last Connection:</td>
</tr>
<tr>
<td>Uptime:</td>
</tr>
<tr>
<td>Total Bytes In:</td>
</tr>
<tr>
<td>Total Bytes Out:</td>
</tr>
<tr>
<td>Current Connections:</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 |
2. Enter or modify the following settings:

**Table 14-5 CLI Configuration**

<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>Select to enable or disable. The login string state controls the display of a device-specific string when SSH or Telnet connection is established to the CLI.</td>
</tr>
<tr>
<td>Login String</td>
<td>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.

| Telnet State                                   | Select **Disabled** to disable Telnet access. Telnet is enabled by default. |
| Telnet Port                                    | Enter the Telnet port to use for Telnet access. The default is **23**. |
| Telnet Max Sessions                            | Maximum number of simultaneous Telnet sessions. The default is 3 and the maximum is 10. |
| SSH State                                      | Select **Disabled** to disable SSH access. SSH is enabled by default. |
| SSH Port                                       | Enter the SSH port to use for SSH access. The default is **22**. |
| SSH Max Sessions                               | Maximum number of simultaneous SSH sessions. The default is 3 and the maximum is 10. |

3. Click **Submit**.
XML Settings

An EDS1100/2100 device server allows for the configuration of devices by using XML configuration records (XCRs). You can export an existing configuration for use on other EDS1100/2100 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 EDS1100/2100 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.

---

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

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, PPP, 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.

2. Click one of the following radio buttons:
   - Configuration from External file. See Import Configuration from External File on page 133.
   - Configuration from Filesystem. See Import Configuration from the Filesystem on page 134.
   - Line(s) from single line Settings on the Filesystem. See Import Line(s) from Single Line Settings on the Filesystem on page 136.

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.
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](image)
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 <strong>Select All</strong> link to select all the serial lines and the network lines. Click the <strong>Clear All</strong> 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, PPP, 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:  

\[ <g>:\langle i\rangle;<g>:\langle i\rangle;... \]

Each group name \(<g>\) is followed by a colon and the instance value \(<i>\) and each \(<g>:\langle i\rangle\) 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**:

![XML: Import Line(s) from Single Line Settings on the Filesystem](image)

**XML: Import Configuration**

Import Line(s) from single line settings on the filesystem:

- **Filename**

- **Lines to Import**: [Clear All] [Select All]
  - 1
  - network

- **Whole Groups to Import**: [Clear All] [Select All but Networking]
  - arg
  - device
  - ethernet
  - ftp server
  - http server
  - ip
  - ipcl
  - ppp
  - serial command mode
  - ssh
  - ssl
  - telnet
  - tunnel accept
  - tunnel modems
  - vip
  - cli
  - diagnostics
  - execute
  - exit cli
  - host
  - icmp
  - ip filter
  - manage line
  - query port
  - smtp
  - ssh client
  - syslog
  - terminal
  - tunnel connect
  - tunnel disconnect
  - tunnel packing
  - tunnel serial
  - xml import control

- **Import**
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><strong>Filename</strong></td>
<td>Provide the name of the file on the device (local to its file system) that contains XCR data.</td>
</tr>
<tr>
<td><strong>Lines to Import</strong></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>
</tbody>
</table>
   | **Whole Groups to Import** | Select the configuration groups to import from the XML configuration record.  
   
   **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. |

2. Click **Import**.
15: Branding the EDS1100/2100 Unit

This chapter describes how to brand your EDS1100/2100 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 EDS1100/2100 device server file system.

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

1. FTP to the EDS1100/2100 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 EDS1100/2100 (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.

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 EDS1100/2100 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 EDS1100/2100 device server over a FTP or TFTP connection.
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)
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>
<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.
C: Compliance

(According to ISO/IEC Guide 17050-1, 17050-2 and EN 45014)

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

Product Name Model: EDS1100/2100 Device Server

Conform to the following standards or other normative documents:

Radiated and Conducted Emissions
FCC Part 15 Subpart B
Industry Canada ICES-003 Issue 4 2004
CISPR 22: 2005 Information Technology Equipment
VCCI V-3/2009.04
AS/NZS CISPR 22: 2006
EN55022: 2006
EN61000-3-2: 2006

Immunity

Direct & Indirect ESD
EN61000-4-2: 1995 + A2:2001

RF Electromagnetic Field Immunity

Electrical Fast Transient/Burst Immunity
EN61000-4-4: 2004

Surge Immunity
EN61000-4-5: 2006

RF Common Mode Conducted Susceptibility
EN61000-4-6: 2007

Power Frequency Magnetic Field Immunity
EN61000-4-8: 1994 +A1: 2001

Voltage Dips and Interrupts
EN61000-4-11: 2004

Safety
UL 60950-1
CAN/CSA-C22.2 No. 60950-1-03
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
Index

A
Accept Mode 48
Accept Mode 54
Additional Documentation 15
Additional TCP Server Port 102
Address
  Ethernet 20
  Hardware 20, 21
  IP 20
  MAC 20, 21
Advanced Settings
  Email Configuration 125
  XML Configuration 129
Advanced Settings 123
AES 17
Allow Firmware Update 76
Allow TFTP File Creation 75
Allow XCR Import 76
ARP 17
ARP Settings 109, 110
ASCII 100
Auth Type 82
Authentication Mode 72
Authentication Type 82
Authority 98
AutoIP 17

B
Banner 85
Bar Code 21
Bin 142
Binary 85, 141
Binary to Hexadecimal Conversions 141
Block Network 56, 60
Block Serial 60
Block Serial Data 56
BOOTP 17, 41
Branding 138
  Web Manager Customization 138
Break Duration 68

C
Challenge Handshake Authentication Protocol 71
CHAP 71
CLI 18
CLI Configuration 127

CLI Statistics 127
Command Line Interface Settings 127
Command Mode 19
Command-Line Interface 18
Common Name 99
Compliance 143
Configuration Methods 19
Configuration Settings 70
Connect Mode 48
Connect Mode 56
Controller 16
Convert Newlines 85
Count 116
Create New Keys 93
Create New Self-Signed Certificate 98

D
DB25 Connector 22
DB25M-to-DB9F Serial Cable 22
DB9F-to-DB9F Serial Null Modem Cable 27
Default Gateway 42
Default Server Port Numbers 20
Device Control 18
Device Details 33
Device Details Summary 33
Device Management 19
Device Status 36
DeviceInstaller 33
DeviceInstaller 33
DHCP 17, 42
Diagnostic Toolset 19
Diagnostics 113
  Buffer Pools 119
  Hardware 113
  IP Sockets 115
  Memory 118
  MIB-II Statistics 114
  Ping 115
  Processes 119
Diagnostics Log 117
Diagnostics Settings 103
Disconnect Mode 48
Disconnect Mode 62
DNS 17, 42
DNS Settings 70
DTE Device 22

E
Echo 67, 68
EDS1100 installation 22
Lines to Export 131, 132
Lines to Import 135, 137
Loading New Firmware 139
Local IP Address 72
Local Port 56, 59
Login Connect Menu 67, 68
Login Password 128
Logout 37
LPD
    Configuration Page 84, 85
    Settings 83
    LPD Statistics 83

M
MAC Address 20, 21
Maintenance and Diagnostics Settings
    Protocol Stack 106
Maintenance Settings 103
Manufacturer’s Name & Address 143
Max Entries 83
Memory 16
Modbus Configuration 102
Modbus Statistics 101
Modbus 100
Mode 59
Modem Emulation 18
Modem Emulation 63
MTU 42
Multiple Hosts 61

N
Name 122
NAT 71
Network 1 (eth0) Interface Configuration 41
Network 1 Ethernet Link 43
Network Address Translation 71
Network Settings
    Network 1 Interface Configuration 41
    Network 1 Interface Status 40
Network Settings 40
New Certificate 98
New Private Key 98

O
Obtaining Firmware 139
Organization Unit 98

P
Packing Mode 52
PAP 71
Part Number 21
Password 56, 73, 93
Password Authentication Protocol 71
PBX 19
Peer IP Address 72
Persistent 83
Point-to-Point Protocol 71
Port 105
Port Numbers 20
Ports
    Serial and Telnet 20
Power Cube 22, 27
Power Supply 16
PPP 17
PPP Peer Device 71
PPP Settings 71
Private Branch Exchange 19
Private Key 88, 93
Product Information Label 21
Product Name Model 143
Product Revision 21
Protocol 56, 69
Protocol Support 17
Public Key 88, 93

Q
Query Port 112
Queue Name 85
Quick Start Guide 22, 27
Quit Connect Line 128

R
Radiated and Conducted Emissions 143
Read Community 74
Really Simple Syndication 18
Reboot Device 121
Reconnect Timer 60
Remote Address 69
Remote Command 93
Remote Port 69
Response Timeout 102
Restore Factory Defaults 121
RFC1334 71
RS232 16
RS-232/422/485 Serial Device 22
RS-232/422/485 serial device 22
RS-232/422/485 Serial Devices 27
RSS 17, 18
RSS Feed 83
RSS Settings 82
RSS Trace Input 102
RTU 100

S
Scientific 142
Scientific Calculator 142
SCPR 19
Secure Com Port Redirector 19
Secure Shell 86
Secure Sockets Layer 86, 94
Security
   Enterprise-Grade 18
   Settings 86
Security Settings 86
   SSL Certificates and Private Keys 95
   SSL Cipher Suites 94
   SSL RSaor DSA 95
   SSL Utilities 96
Send Break 68
Send Character 54
Serial Port 16
Serial Settings 51
Serial Transmission Mode 100
Services Settings 70
   CHAP Authentication 71
   LPD 83
Short and Long Name Customization 138
SMTP 17
SNMP 17
SNMP Configuration 73
SNMP Management 18
SOJ String 85
SSH 17, 86
   Client Known Hosts 91
   Server Authorized Users 89
   Server Host Keys 87
   Settings 86
SSH Client Known Hosts 91
SSH Client User Configuration 92
SSH Max Sessions 128
SSH Port 128
SSH Server Authorized Users 89
SSH Server Host Keys 87
SSH State 128
SSH Username 69
SSL 17, 86, 94
   Settings 94
   SSL Certificates 95
SSL Cipher Suites 94
SSL Configuration 97
SSL Utilities 96
Start of Job 85
State 108
Steel Belted RADIUS 96
Syslog 17
Syslog Configuration 76
System Contact 74
System Description 74
System Location 74
System Name 74
System Settings 121

T
TCP 17
TCP Keep Alive 56
TCP Server State 102
TCP Settings 106
TCP/IP 100
Technical Support 140
Telnet 17
Telnet Max Sessions 128
Telnet Port 128
Telnet State 128
Terminal
   Server 19
   Settings 66
Terminal Type 67, 68
Text List 135
TFTP 17, 139
TFTP Configuration 75
Threshold 54
Timeout 54, 116
TLS 17
Traceroute 116
Trailing Character 54
Traps Primary Destination 74
Traps Secondary Destination 74
Traps State 74
Troubleshooting 19
Troubleshooting Capabilities 19
Tunnel – Accept Mode 54
Tunnel – Connect Mode 56
Tunnel – Disconnect Mode 62
Tunnel – Packing Mode 52
Tunnel 1 – Statistics 49
Tunnel Settings
   Connect Mode 56
   Modem Emulation
   Command Mode 63
   Packing Mode 52

EDS1100/2100 Device Server User Guide  148
Tunnel Settings  48
Type 99

U
UDP 17
Uniform Resource Identifier 81
Updating Firmware 139
Upload Authority Certificate 98
Upload Certificate 98
Upload New Firmware 121
URI 81
Username 73, 93

W
Web Manager
  Device Status Web Page 36
  Navigating 38
  Page Components 37
  Page Summary 38
Web Manager Customization 138
Web Manager 35
Web-Based Configuration 18
Whole Groups to Import 135, 137
WLAN
  Settings
    Network 1 Ethernet Link 43
Write Community 74

X
XML 20
  Export Configuration 130
  Export Status 131
  Import System Configuration 133
XML-Based Architecture 18