



# EDS3000 Device Server User Guide EDS3008/16/32PR EDS3008/16PS

---

## 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* is a registered trademark of Lantronix, Inc. in the United States and other countries.

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](http://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](http://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](http://www.lantronix.com/about/contact).

## Disclaimer

**Note:** *This product has been designed to comply with the limits for a Class B digital device pursuant to Part 15 of FCC and EN55022:1998 Rules when properly enclosed and grounded. These limits are designed to provide reasonable protection against radio interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with this guide, may cause interference to radio communications. See the appendix, [Compliance \(on page 92\)](#).*

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.

## Open Source Software

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

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

You may request a list of the open source components and the licenses that apply to them. Contact your regional Lantronix sales associate. <https://www.lantronix.com/about-us/contact/>

## Revision History

Date	Rev.	Comments
August 2020	A	Initial document.

# Table of Contents

<b>1: About This Guide</b>	<b>12</b>
Chapter and Appendix Summaries	12
Additional Documentation	13
<b>2: Introduction</b>	<b>14</b>
EDS3008PR, EDS3016PR, and EDS3032PR Overview	14
Key Features	15
EDS3008PS and EDS3016PS Overview	16
Key Features	16
Applications	17
Protocol Support	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
<b>3: Installation of EDS3000PR</b>	<b>22</b>
Package Contents	22
User-Supplied Items	22
Identifying Hardware Components	23
Serial Ports	23
Console Port	23
Ethernet Port	23
LEDs	24
Reset Button	24
Power Input	24
Housing	24
Installing the EDS3000PR	25



Finding a Suitable Location	25
Connecting the EDS3000PR	25
<b>4: Using Lantronix Provisioning Manager</b>	<b>26</b>
Installing Lantronix Provisioning Manager	26
Accessing the EDS3000PR Using Lantronix Provisioning Manager	26
<b>5: Configuration Using Web Manager</b>	<b>27</b>
Accessing Web Manager	27
Device Status Page	27
Web Manager Page Components	29
Navigating the Web Manager	30
<b>6: Network Settings</b>	<b>33</b>
Wired Network (eth0)	33
Interface Status and Configuration	33
To Configure Network Interface Settings	36
Link Status and Configuration	36
To Configure Wired Network (eth0) Link Settings	37
Protocol Stack	37
IP Settings	37
To Configure IP Protocol Stack Settings	37
ICMP Settings	38
To Configure ICMP Protocol Stack Settings	38
ARP Settings	38
To Configure ARP Network Stack Settings	38
<b>7: Filesystem</b>	<b>39</b>
File Transfer and Modification	40
To View, Transfer, or Modify Filesystem Files	40
<b>8: Diagnostics</b>	<b>41</b>
DNS	41
Accessing the DNS Settings	41
Hardware	42
To View Hardware Information	42
IP Sockets	42
To View the List of IP Sockets	42
Log	42
To Configure the Diagnostic Log Output	43
Memory	43
To View Memory Usage	43

Ping	43
To Ping a Remote Host	44
Processes	44
To View Process Information	44
Routes	44
Threads	45
To View Thread Information	45
Traceroute	45
To Perform a Traceroute	45

## 9: Administration 46

CLI	46
CLI Status and Configuration	46
To View and Configure Basic CLI Settings	47
Clock	47
To Specify a Clock-Setting Method	48
Discovery	48
To Configure Discovery	48
Email	49
To View, Configure and Send Email	49
FTP	50
To Configure FTP Settings	50
Host	50
To Configure Host Settings	51
HTTP	51
Interface Status, Configuration and Authentication	51
To View or Configure HTTP	53
To Configure HTTP Authentication	53
Line	54
Line Status and Configuration	54
To View and Configure Line Configuration and Command Mode	55
MACH10	56
To Configure MACH10 Client	56
To Configure MACH10 Line 1, Line 2, or Line 3	57
To Configure MACH10	57
RSS	58
To Configure RSS Settings	58
SMTP	58
To Configure SMTP Settings	59
SNMP	59
To Configure SNMP Settings	60
SSH	60
SSH Server: Host Keys	61

SSH Server: Authorized Users	61
SSH Client: Known Hosts	62
SSH Client: Users	62
To Configure SSH Settings	64
SSL	64
Credentials	64
To Create a New Credential	64
To Delete a Credential	65
To Configure an SSL Credential to Use an Uploaded Certificate	66
To Configure an SSL Credential to Use a Self-Signed Certificate	67
Trusted Authorities	67
To Upload an Authority Certificate	67
CSR (Certificate Signing Request)	68
Syslog	69
To Configure Syslog Settings	69
System	69
To access System settings:	71
Terminal	71
To Configure the Terminal Network Connection	72
To Configure the Terminal Line	72
Tunnel	72
Tunnel Statistics	72
To View Tunnel Statistics	73
Serial Settings	73
To Configure Tunnel Serial Settings	73
Packing Mode	74
To Configure Tunnel Packing Mode Settings	74
Accept Mode	75
To Configure Tunnel Accept Mode Settings	77
Connect Mode	77
To Configure Tunnel Connect Mode Settings	80
Connecting Multiple Hosts	80
Host List Promotion	80
Disconnect Mode	81
To Configure Tunnel Disconnect Mode Settings	81
Modem Emulation	81
To Configure Tunnel Modem Emulation Settings	82
User Management	83
To Configure User Management	84
XML	85
To Export Configuration	85
To Export Status	86
To Import Configuration	87

<b>Appendix A: Technical Support</b>	<b>89</b>
<b>Appendix B: Binary to Hexadecimal Conversions</b>	<b>90</b>
Converting Binary to Hexadecimal _____	90
Conversion Table _____	90
Scientific Calculator _____	91
<b>Appendix C: Compliance</b>	<b>92</b>
Emissions and Immunity _____	93
Safety _____	93
RoHS, REACH and WEEE Compliance Statement _____	93
Lithium Battery Notice _____	93
Installationsanweisungen _____	94
Rackmontage _____	94
Energiezufuhr _____	94
Erdung _____	94
Installation Instructions _____	94
Rack Mounting _____	94
Input Supply _____	94
Grounding _____	94
<b>Appendix D: Lantronix Cables and Adapters</b>	<b>95</b>

## List of Figures

Figure 2-1 EDS3008PR Device Server	15
Figure 2-2 EDS3016PR Device Server	15
Figure 2-3 EDS3032PR Device Server	15
Figure 2-4 EDS3008PS Device Server	16
Figure 2-5 EDS3016PS Device Server	16
Figure 2-6 Sample Hardware Address	20
Figure 2-7 EDS3008PR Product Label	21
Figure 3-1 Front View of the EDS3032PR	23
Figure 3-2 Back View of the EDS3032PR	23
Figure 3-3 RJ45 Serial Port	23
Figure 3-5 Example of EDS3032PR Connections	25
Figure 5-1 Prompt for User Name and Password	27
Figure 5-2 Web Manager Home Page	28
Figure 5-3 Components of the Web Manager Page	29
Figure 5-4 Expandable Menu Bar Selections	30
Figure 6-1 Wired Network (eth0) Interface Status	34
Figure 6-2 Wired Network (eth0) Interface Configuration	34
Figure 6-4 Wired Network (eth0) Ethernet Link Status	36
Figure 6-5 Wired Network (eth0) Link Configuration	36
Figure 7-1 Filesystem Statistics	39

## List of Tables

Table 3-4 Back Panel LEDs	24
Table 5-5 Summary of Web Manager Pages	30
Table 6-3 Wired Network (eth0) Interface Configuration	35
Table 6-6 Wired Network (eth0) Link Configuration	36
Table 6-1 IP Protocol Stack Settings	37
Table 6-2 ICMP Protocol Stack Settings	38
Table 6-3 ARP Protocol Stack Settings	38
Table 7-4 Filesystem Statistics	39
Table 7-5 File Modification Settings	39
Table 7-6 File Transfer Settings	40
Table 8-7 DNS Settings	41
Table 8-8 Log Settings	43
Table 8-9 Ping Configuration	43
Table 8-10 Traceroute Settings	45
Table 9-11 CLI Configuration Settings	47
Table 9-12 Clock Settings	47
Table 9-13 Discovery Settings	48
Table 9-14 Email Configuration	49
Table 9-15 FTP Settings	50
Table 9-16 Host Settings	50
Table 9-17 HTTP Configuration	52
Table 9-18 HTTP Authentication	53
Table 9-19 Line Configuration Settings	54
Table 9-20 Line Command Mode Setting	55
Table 9-21 MACH10 Client Configuration	56
Table 9-22 MACH10 Line	57
Table 9-23 RSS	58
Table 9-24 SMTP Settings	59
Table 9-25 SNMP Settings	59
Table 9-26 SSH Server Host Keys	61
Table 9-27 SSH Server Authorized Users	62
Table 9-28 SSH Client Known Hosts	62
Table 9-29 SSH Client Users	63
Table 9-30 Create New Keys	63
Table 9-31 SSL Credential - Upload Certificate	65

Table 9-32 SSL Credential - Create New Self-Signed Certificate	65
Table 9-33 SSL Trusted Authority	67
Table 9-34 SSL CSR (Certificate Signing Request)	68
Table 9-35 Syslog	69
Table 9-36 System Settings	70
Table 9-37 Terminal on Network and Line Settings	71
Table 9-38 Tunnel Serial Settings	73
Table 9-39 Tunnel Packing Mode Settings	74
Table 9-40 Tunnel Accept Mode Settings	75
Table 9-41 Tunnel Connect Mode Settings	78
Table 9-42 Host Settings	79
Table 9-43 Tunnel Disconnect Mode Settings	81
Table 9-44 Tunnel Modem Emulation Settings	82
Table 9-45 Administrator Settings	83
Table 9-46 Current Users List	83
Table 9-47 New User Settings	83
Table 9-48 Current Roles List	84
Table 9-49 New Role Settings	84
Table 9-50 Configuration from Filesystem	87
Table 9-51 Line(s) from single line Settings on the Filesystem	88

# 1: About This Guide

This user guide provides the information needed to configure, use, and update the Lantronix® EDS3000PR, which includes models EDS3008PR, EDS3016PR, and EDS3032PR. It is intended for software developers and system integrators who are installing the EDS in their designs.

## Chapter and Appendix Summaries

A summary of each chapter is provided below.

Chapter	Description
<a href="#">Chapter 2: Introduction</a>	Main features of the product and the protocols it supports. Includes technical specifications.
<a href="#">Chapter 3: Installation of EDS3000PR</a>	Instructions for installing the EDS3008PR, the EDS3016PR, and the EDS3032PR device/terminal server.
<a href="#">Chapter 4: Using Lantronix Provisioning Manager</a>	Instructions for viewing the current configuration using Lantronix Provisioning Manager.
<a href="#">Chapter 5: Configuration Using Web Manager</a>	Instructions for accessing Web Manager and using it to configure settings for the device.
<a href="#">Chapter 6: Network Settings</a>	Instructions for using the web interface to configure Ethernet settings.
<a href="#">Chapter 7: Filesystem</a>	Instructions to view and configure the filesystem.
<a href="#">Chapter 8: Diagnostics</a>	Instructions to view and configure DNS, hardware, IP socket, log, memory, ping, processes, routes, threads, and traceroute information.
<a href="#">Chapter 9: Administration</a>	Instructions to view and configure CLI, clock, discovery, email, FTP, host, HTTP, line, RSS, SMTP, SNMP, SSH, SSL, syslog, system, terminal, tunnel, user management, and XML.
<a href="#">Appendix A: Technical Support</a>	Instructions for contacting Lantronix Technical Support.
<a href="#">Appendix B: Binary to Hexadecimal Conversions</a>	Instructions for converting binary values to hexadecimal.
<a href="#">Appendix C: Compliance</a>	Lantronix compliance information.
<a href="#">Appendix D: Lantronix Cables and Adapters</a>	Lantronix cables and adapters for use with the EDS3000PR devices are listed here according to part number and application.



## Additional Documentation

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

Document	Description
<b><i>EDS3000 Device Server Command Reference</i></b>	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.
<b><i>Lantronix Provisioning Manager Online Help</i></b>	Instructions for using the Lantronix Provisioning Manager application that discovers, configures, upgrades, and manages Lantronix devices.

## 2: Introduction

This chapter introduces the Lantronix EDS3000PR and EDS3000PS family of device servers. It provides an overview of the product, lists the key features, and describes the applications for which they are suited.

The EDS3000PR/EDS3000PS is a unique, hybrid Ethernet terminal and multi-port device server product designed to remotely access and manage virtually all of your IT/networking equipment and servers. It is also designed to provide connectivity for edge devices such as medical equipment, kiosks, POS/retail terminals, security equipment, and more.

The EDS3000PR/EDS3000PS devices contain all the components necessary to deliver full network connectivity to virtually any kind of serial device. It boasts a reliable TCP/IP protocol stack, a variety of remote management capabilities, and an innovative design.

The devices deliver a data center-grade, programmable device computing and networking platform for integrating edge equipment into the enterprise network. Rack-mountable EDS3000PR models are available in 8, 16, and 32 port configurations. The EDS3000PS models can be wall-mounted or place on a desktop and are available in 8 or 16 port configurations.

This chapter contains the following sections:

- ◆ [\*EDS3008PR, EDS3016PR, and EDS3032PR Overview\*](#)
- ◆ [\*Key Features\*](#)
- ◆ [\*Protocol Support\*](#)
- ◆ [\*Additional Features\*](#)
- ◆ [\*Configuration Methods\*](#)
- ◆ [\*Addresses and Port Numbers\*](#)
- ◆ [\*Product Information Label\*](#)

### EDS3008PR, EDS3016PR, and EDS3032PR Overview

The EDS3008PR (8 serial ports), EDS3016PR (16 serial ports), and EDS3032PR (32 serial ports) are compact, easy-to-use, rack-mountable device servers that give you the ability to network-enable asynchronous RS-232 serial devices. They provide fully transparent RS-232 point-to-point connections without requiring modifications to existing software or hardware components in your application.

**Figure 2-1 EDS3008PR Device Server**



**Figure 2-2 EDS3016PR Device Server**



**Figure 2-3 EDS3032PR Device Server**



## Key Features

The key features of the EDS3008PR, EDS3016PR, and EDS3032PR include:

- ◆ Dual-purpose Ethernet terminal server and device server design
- ◆ 8 (EDS3008PR), 16 (EDS3016PR) or 32 (EDS3032PR) serial ports with hardware handshaking signals
- ◆ RS-232 support

- ◆ One RJ45 Ethernet port
- ◆ 4 Gbit (512 Mbyte) NAND flash memory
- ◆ 4 Gbit (512 Mbyte) DRAM
- ◆ A dedicated console port
- ◆ AES, SSH, or SSL secure data encryption
- ◆ Three configuration methods (Web, command line, and XML)

## EDS3008PS and EDS3016PS Overview

The EDS3008PS (8 serial ports) and EDS3016PS (16 serial ports) are compact desktop device servers that give you the ability to network-enable asynchronous RS-232 serial devices. They provide fully transparent RS-232 point-to-point connections without requiring modifications to existing software or hardware in your application.

**Figure 2-4 EDS3008PS Device Server**



**Figure 2-5 EDS3016PS Device Server**



## Key Features

Key features of the EDS3008PS and EDS3016PS include:

- ◆ Dual-purpose Ethernet terminal server and device server design
- ◆ 8 (EDS3008PS) or 16 (EDS3016PS) serial ports with hardware handshaking signals
- ◆ RS-232 support
- ◆ An RJ45 Ethernet port

- ◆ 8 MB Flash memory
- ◆ 32 MB random access memory (RAM)
- ◆ Lantronix Evolution OS software
- ◆ A dedicated console port
- ◆ AES, SSH, or SSL secure data encryption
- ◆ Three convenient configuration methods (Web, command line, and XML)
- ◆ Print server functionality (LPR/LPD)

## Applications

EDS3000PR and EDS3000PS device servers connect 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 EDS3000PR and EDS3000PS device servers contain a full-featured TCP/IP stack. Supported protocols include:

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

## Additional Features

### Modem Emulation

In modem emulation mode, the EDS3000PR/EDS3000PS 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 EDS3000PR/EDS3000PS 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 EDS3000PR/EDS3000PS uses industry-standard tools for configuration, communication, and control. For example, the EDS3000PR/EDS3000PS 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 EDS3000PR 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 EDS3000PR and EDS3000PS devices.

### XML-Based Architecture and Device Control

XML is a fundamental building block for the future growth of M2M networks. The EDS3000PR/EDS3000PS 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 EDS3000PR/EDS3000PS supports Really Simple Syndication (RSS) for streaming and managing on-line content. RSS feeds all the configuration changes that occur on the device. An RSS aggregator then reads (polls) the feed. More powerful than simple email alerts, RSS uses XML as an underlying Web page transport and adds intelligence to the networked device, while not taxing already overloaded email systems.

### Enterprise-Grade Security

The EDS3000PR/EDS3000PS has 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 EDS3000PR/EDS3000PS has robust defenses to hostile Internet attacks such as denial of service (DoS), which can be used to take down the network. Moreover, the EDS3000PR/EDS3000PS cannot be used to bring down other devices on the network.

You can use the EDS3000PR/EDS3000PS 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 EDS3000PR/EDS3000PS 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 EDS3000PR/EDS3000PS offers a comprehensive diagnostic toolset that lets you troubleshoot problems quickly and easily. Available from the Web Manager, CLI, and XML interfaces, the diagnostic tools let you:

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

**Configuration Methods**

After installation, the EDS3000PR 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 EDS3000PR and assigning IP addresses and other configurable settings:

**Lantronix Provisioning Manager:** Obtain basic information about the device such as firmware version, IP address, and serial number. Update the firmware, configure the device using XML files, or upload to the file system. See [Chapter 4: Using Lantronix Provisioning Manager](#).

**Web Manager:** Through a web browser, configure the EDS3000PR settings using the Lantronix Web Manager. See [Chapter 5: 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 *EDS3000PR Device Server Command Reference* for instructions and available commands. Lantronix documentation is available at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation).)

**XML:** The EDS3000PR 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 *EDS3000PR Device Server Command Reference* for instructions and available commands. Lantronix documentation is available at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation).)

**Web API:** The Web APIs are restful APIs that allow access to a subset of device server functions through a standard HTTP request. They can be used to export and import configuration, export status, take a status action, and manipulate the file system. See the EDS3000 Command Reference for details and a list of actions.

## 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 08-04-13, identifying the unit as a Lantronix product. The fourth, fifth, and sixth bytes are unique numbers assigned to each unit.

**Figure 2-6 Sample Hardware Address**  
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 EDS3000PR device server.

- ◆ TCP Port 22: SSH Server (Command Mode configuration)
- ◆ TCP Port 23: Telnet Server (Command Mode configuration)
- ◆ TCP Port 80: HTTP (Web Manager configuration)
- ◆ TCP Port 443: HTTPS (Web Manager configuration)
- ◆ UDP Port 161: SNMP
- ◆ TCP Port 21: FTP
- ◆ UDP Port 69: TFTP
- ◆ UDP Port 514: Syslog



- ◆ UDP Port 30718: LDP (Lantronix Discovery Protocol) port
- ◆ TCP/UDP Port 10001: Tunnel 1
- ◆ TCP/UDP Port 10002: Tunnel 2
- ◆ TCP/UDP Port 10003: Tunnel 3

**Note:** Multi-port products include one or more additional supported ports and tunnels with default sequential numbering, such as TCP/UDP Port 10004: Tunnel 4, TCP/UDP Port 10005: Tunnel 5, etc.

## Product Information Label

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

- ◆ QR Code
- ◆ Model Part Number
- ◆ Revision
- ◆ Manufacturing Date Code
- ◆ Country of Manufacture
- ◆ Hardware Address (MAC address or serial number)
- ◆ Device ID

Figure 2-7 EDS3008PR Product Label



## 3: Installation of EDS3000PR

This chapter describes installing the EDS3008PR, EDS3016PR and EDS3032PR device servers.

### Package Contents

Your EDS package includes the following items:

- ◆ One EDS3000PR unit (EDS3008PR, EDS3016PR or EDS3032PR).
- ◆ One RJ45-to-DB9F serial cable.
- ◆ A printed Quick Start guide.
- ◆ Your package may also include a power supply.

### User-Supplied Items

To complete your EDS3000PR installation, you need the following items:

- ◆ RS-232 serial devices that require network connectivity. Each EDS3000PR serial port supports a directly connected RS-232 serial device.
- ◆ A serial cable for each serial device. All devices attached to the EDS3000PR device ports must support the RS-232C (EIA-232) standard. Category 5 cabling with RJ45 connections is used for the device port connections.

**Note:** To connect an EDS3000PR serial port to a DTE device, you need a DTE cable, such as the one supplied in your EDS3000PR package, or an RJ45 patch cable and DTE adapter. To connect the EDS3000PR serial port to a DCE device, you need a DCE (modem) cable, or an RJ45 patch cable and DTE adapter.

For a list of the Lantronix cables and adapters you can use with the EDS3000PR, see [Appendix D: Lantronix Cables and Adapters](#).

- ◆ An available connection to your Ethernet network and an Ethernet cable.
- ◆ A working power outlet.

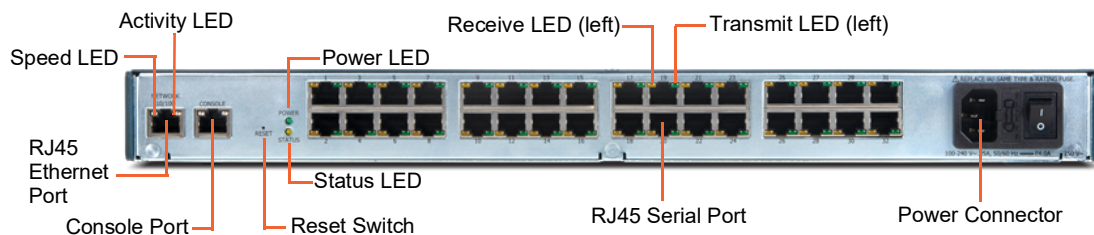
## Identifying Hardware Components

The following two figures show the components on the front and back of the EDS3032PR.

**Figure 3-1 Front View of the EDS3032PR**



**Figure 3-2 Back View of the EDS3032PR**



### Serial Ports

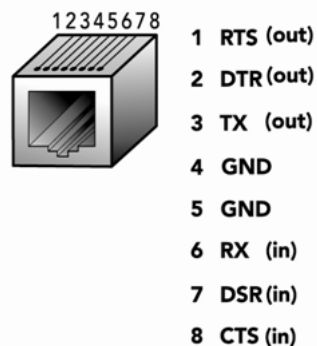
All EDS3000PR serial ports are configured as DTE and support up to 230,400 baud.

- ◆ The EDS3008PR has 8 serial ports.
- ◆ The EDS3016PR has 16 serial ports.
- ◆ The EDS3032PR has 32 serial ports.

### Console Port

The EDS3000PR has an RJ45 Console port configured as DTE and supports up to 230,400 baud.

**Figure 3-3 RJ45 Serial Port**



### Ethernet Port

The EDS3000PR has an RJ45 Ethernet port that supports 10/100/1000Mbps Ethernet.

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

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

## LEDs

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

- ◆ **Front panel.** The front panel has a blue Power LED.
- ◆ **Back panel.** Each serial port has a Transmit and a Receive LED. The Ethernet connector has Speed and Activity LEDs. There is also a Power LED and a Status LED.

The table below describes the LEDs on the back of the EDS3000PR.

**Table 3-4 Back Panel LEDs**

LED	Description
Transmit (green)	Blinking = EDS3000PR is transmitting data on the serial port.
Receive (orange)	Blinking = EDS3000PR is receiving data on the serial port.
Power (green)	On = EDS3000PR is receiving power.
Status (orange)	Fast blink = initial startup (loading OS). Slow blink (once per second) = operating system startup. On = unit has finished booting.
Speed (green)	On = EDS3000PR is connected to a 100 Mbps Fast Ethernet network.
	Off = EDS3000PR is connected to a 10 Mbps Ethernet network.
Activity (green)	Blink = EDS3000PR is sending data to or receiving data from the Ethernet network.

## Reset Button

The reset button is on the back of the EDS3000PR to the left of the power LED.

Pressing this button for 2 to 3 seconds reboots the EDS3000PR and terminates all data activity occurring on the serial and Ethernet ports.

## Power Input

- ◆ 100-240VAC, 50 to 60 Hz IEC-type cord
- ◆ Typical: 10 Watts
- ◆ Maximum: 20 Watts

## Housing

- ◆ Case: Metal enclosure with removable wall mounts
- ◆ Dimensions: (L x W x H): 304.37 x 480.82 x 42.18 mm (11.98 x 18.93 x 1.66 in)
- ◆ Weight: 4.20 kg (9.25 lb) maximum, depending upon model

## Installing the EDS3000PR

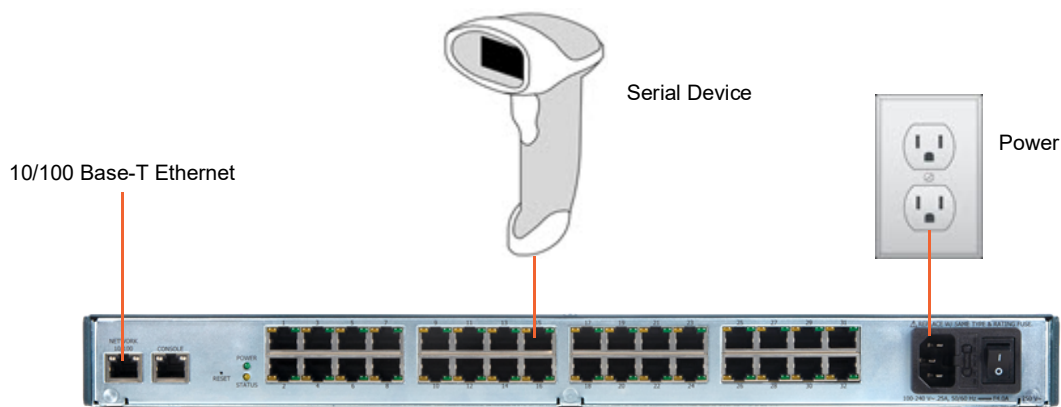
### Finding a Suitable Location

You can install the EDS3000PR either in an EIA-standard 19-inch rack (1U tall) or as a desktop unit. If using AC power, avoid outlets controlled by a wall switch.

### Connecting the EDS3000PR

1. Power off the serial devices that will be connected to the EDS3000PR.
2. Attach a CAT 5 serial cable between the EDS3000PR and your serial device. For a list of cables and adapters you can use with the EDS3000PR, [Appendix D: Lantronix Cables and Adapters](#).
3. Connect an Ethernet cable between the EDS3000PR Ethernet port and your Ethernet network.
4. Insert the power cord into the back of the EDS3000PR. Plug the other end into an AC wall outlet. After power-up, the self-test begins.
5. Power up the serial devices.

Figure 3-5 Example of EDS3032PR Connections



## 4: Using Lantronix Provisioning Manager

This chapter covers the steps for locating a device and viewing its properties and details. Lantronix Provisioning Manager is a free utility program provided by Lantronix that discovers, configures, upgrades, and manages Lantronix devices. It can be downloaded from the Lantronix website at <https://www.lantronix.com/products/lantronix-provisioning-manager/>. For instructions on using the application, see the [Lantronix Provisioning Manager online help](#).

### Installing Lantronix Provisioning Manager

1. Download the latest version of Lantronix Provisioning Manager from <https://www.lantronix.com/products/lantronix-provisioning-manager/>.
2. In most cases, you can simply extract Lantronix Provisioning Manager from the archive and run the executable. For detailed instructions, see the [Lantronix Provisioning Manager online help](#).

### Accessing the EDS3000PR Using Lantronix Provisioning Manager

**Note:** For detailed instructions, see the [Lantronix Provisioning Manager online help](#).

1. Launch Lantronix Provisioning Manager
2. If this is the first time you have launched Lantronix Provisioning Manager, you may need to proceed through an initial setup.
3. Locate the EDS3000PR in the device list. The device's firmware version, serial number, IP address, and MAC address will be shown. Additional information can be obtained by clicking the **three dot menu** and clicking **Get Device Info**.
4. In order to perform operations on the EDS3000PR such as upgrading the firmware, updating the configuration, or uploading to the file system, click the **checkbox** next to the device, click the **menu** button at the top, and select an operation.

## 5: Configuration Using Web Manager

This chapter describes how to configure the EDS3000PR 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. This chapter contains the following sections:

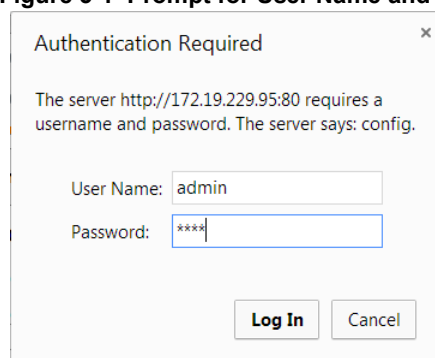
- ◆ [Accessing Web Manager](#)
- ◆ [Web Manager Page Components](#)
- ◆ [Navigating the Web Manager](#)
- ◆ [Summary of Web Manager Pages](#)

### Accessing Web Manager

*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 EDS3000PR unit in the address bar. The IP address may have been assigned automatically by DHCP. If you do not know the IP address, you can use Lantronix Provisioning Manager. See [Chapter 4: Using Lantronix Provisioning Manager](#).

**Figure 5-1 Prompt for User Name and Password**



3. Enter your username and password. The factory-default username is `admin` and the factory-default password is the last eight bytes of the Device ID. The Device Status web page shown in [Figure 5-2](#) 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 5-2](#)).

Figure 5-2 Web Manager Home Page

EDS3032PR

[Help](#)
[admin](#)

Status

Network

Filesystem

Diagnostics

Administration

Device

Network

Lines

Tunnels

MACH10

## Device

### Product Information

Product Type:	Lantronix EDS3032PR (EDS3032PR)
Secure Boot:	Disabled
Firmware Version:	2.0.0.0R5
Build Date:	Thu Feb 13 09:20:08 PST 2020
Serial Number:	0080A3D92B9B
Device ID:	0080A3D92B9B
Uptime:	0 days 00:02:35
Current Date/Time:	Thu Mar 05 23:34:48 UTC 2020
Permanent Config:	Saved

## Network

### Network Settings

Primary DNS:	10.153.90.1
Secondary DNS:	10.167.90.1

### Interface eth0

Link:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)
MAC Address:	00:80:A3:D9:2B:9B
Hostname:	EDS3032PR-0080a3d92b9b
MTU:	1500
IP Address:	172.20.197.113/24 <DHCP>
Network Mask:	255.255.255.0 <DHCP>

[Home](#)

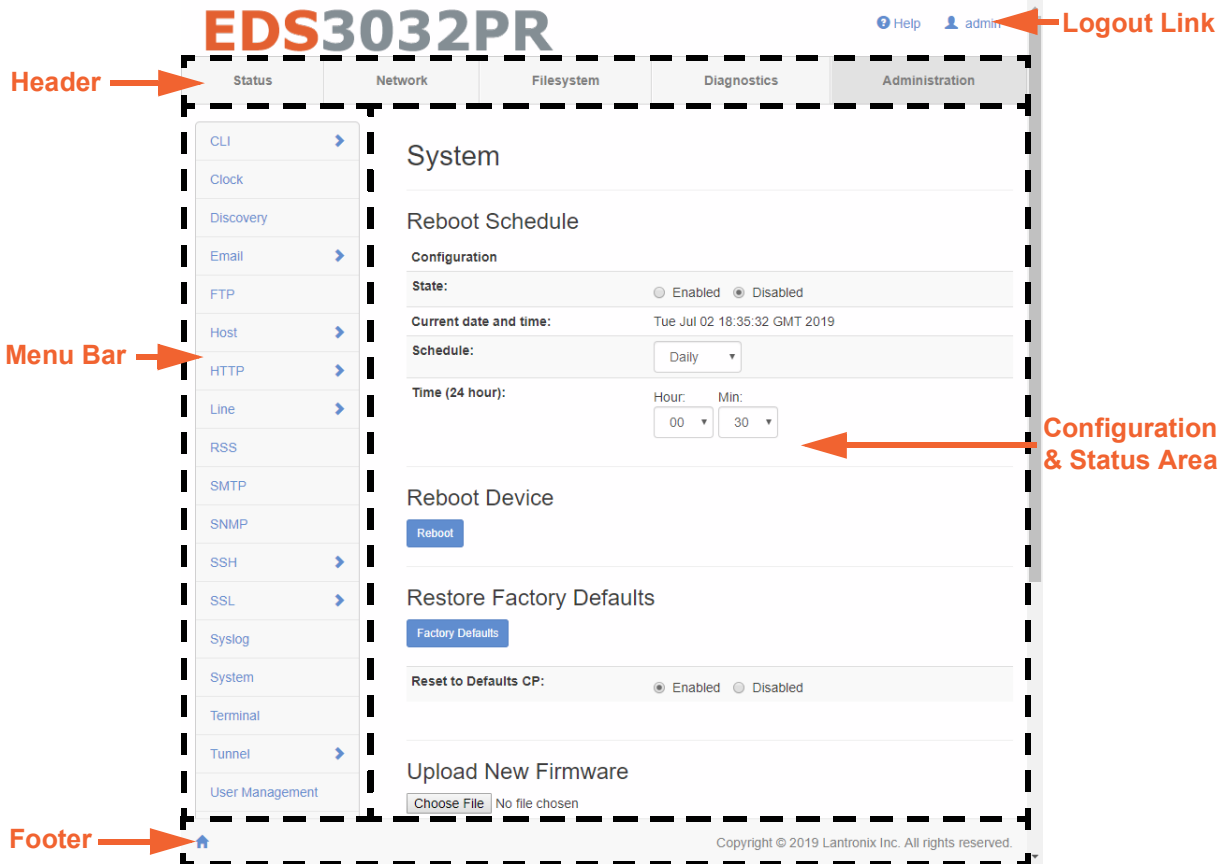
Copyright © 2020 Lantronix Inc. All rights reserved.



## Web Manager Page Components

The layout of a typical Web Manager page is below.

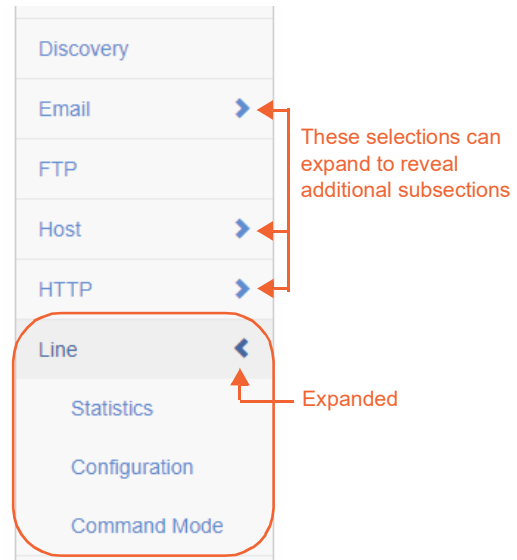
Figure 5-3 Components of the Web Manager Page



### Web Manager pages have these sections:

- ◆ The Status, Network, Filesystem, Diagnostics and Administration tabs located in the header at the top of the page provide direct access to each Web Manager page of the same name. All the functionality is accessible through Web Manager and is divided between these tab/pages.

- ◆ Each Web Manager page accessed through the header tabs reveal a page-specific menu bar on the left side organizing available sections for that page.
- ◆ The menu bar accessed via the Network and Administration tabs contain selections that can further expand to reveal additional subsections. A right-pointing blue arrow indicates a particular selection can be expanded to reveal subsections.
- ◆ Expand or collapse an expandable menu bar section by clicking on it.
- ◆ The main body area of the page contains either view-only Status info or Configuration options according to the tab, menu bar selection or subsection selected.
- ◆ When a parameter is changed on a page, a **Submit** button will appear at the bottom of the page. Click on this button to save the change.
- ◆ A **Logout** link is available at the upper right corner of every Setup and Admin page after clicking the user name. In Chrome or Safari, it is necessary to close out of the browser to completely 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 status page.

**Figure 5-4 Expandable Menu Bar Selections**

## Navigating the Web Manager

The table below provides a shortcut to the various software features available for viewing and configuration through Web Manager.

**Note:** There may be times when you must reboot the EDS3000PR for the new configuration settings to take effect. The chapters that follow indicate when a change requires a reboot.

**Table 5-5 Summary of Web Manager Pages**

Web Manager Page	Description	See Page
<b>Status</b>	Shows product information and network, line, and tunneling settings.	<a href="#">27</a>
<b>CLI</b>	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	<a href="#">46</a>
<b>Clock</b>	Allows you to view and configure date and time for the device by either SNTP or manual settings.	<a href="#">47</a>
<b>Diagnostics</b>	Lets you perform various diagnostic procedures.	<a href="#">41</a>
<b>Discovery</b>	Allows you to view and modify the configuration and statistics for device discovery.	<a href="#">48</a>

Web Manager Page (continued)	Description	See Page
<b>DNS</b>	Shows the current configuration of the DNS subsystem and the DNS cache.	<a href="#">41</a>
<b>Email</b>	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	<a href="#">49</a>
<b>Filesystem</b>	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.	<a href="#">39</a>
<b>FTP</b>	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	<a href="#">50</a>
<b>Hardware</b>	Shows hardware status and configuration options.	<a href="#">42</a>
<b>Host</b>	Lets you view and change settings for a host on the network.	<a href="#">50</a>
<b>HTTP</b>	Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	<a href="#">51</a>
<b>IP Sockets</b>	Shows IP socket status and lets you change hardware configuration.	<a href="#">42</a>
<b>Line</b>	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	<a href="#">54</a>
<b>Log</b>	Shows and allows changes with logs.	<a href="#">42</a>
<b>MACH10</b>	Shows the configuration and status for the MACH10 client.	<a href="#">56</a>
<b>Memory</b>	Shows memory status and lets you change hardware configuration.	<a href="#">43</a>
<b>Network</b>	Shows status and lets you configure the network interface.	<a href="#">33</a>
<b>Ping</b>	Shows how to ping a network host with a DNS hostname or IP address.	<a href="#">43</a>
<b>Processes</b>	Shows the processes currently running on the system.	<a href="#">44</a>
<b>Protocol Stack</b>	Lets you perform lower level network stack-specific activities.	<a href="#">37</a>
<b>Routes</b>	Shows the current system routing table.	<a href="#">44</a>
<b>RSS</b>	Lets you change current Really Simple Syndication (RSS) settings.	<a href="#">58</a>
<b>SMTP</b>	Shows SMTP status and configuration options.	<a href="#">58</a>
<b>SNMP</b>	Lets you change the current Simple Network Management Protocol (SNMP) configuration settings.	<a href="#">59</a>
<b>SSH</b>	Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	<a href="#">60</a>
<b>SSL</b>	Lets you upload an existing certificate or create a new self-signed certificate.	<a href="#">64</a>
<b>Syslog</b>	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	<a href="#">69</a>
<b>System</b>	Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.	<a href="#">69</a>
<b>Terminal</b>	Lets you change current settings for a terminal.	<a href="#">71</a>
<b>Threads</b>	Shows thread ID numbers, names and CPU usage.	<a href="#">45</a>
<b>Traceroute</b>	Shows how to perform a traceroute to a network host.	<a href="#">45</a>
<b>Tunnel</b>	Lets you change the current configuration settings for a tunnel.	<a href="#">72</a>

Web Manager Page (continued)	Description	See Page
User Management	Shows the configuration of users.	<a href="#">83</a>
XML	Lets you export XML configuration and status records, and import XML configuration records.	<a href="#">85</a>

## 6: Network Settings

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

This chapter contains the following sections:

- ◆ [Interface Status and Configuration](#)
- ◆ [Link Status and Configuration](#)

### Wired Network (eth0)

This wired Ethernet network (eth0) is described in this section.

#### Interface Status and Configuration

[Figure 6-1 Wired Network \(eth0\) Interface Status](#) displays the wired network's interface status information. This same information is configurable on the Wired Network (eth0) Interface Configuration page, shown in [Figure 6-2 Wired Network \(eth0\) Interface Configuration](#). [Table 6-3 Wired Network \(eth0\) Interface Configuration](#) describes the configuration information.

Figure 6-1 Wired Network (eth0) Interface Status

## Wired Network (eth0) Interface Status

	Current	After Reboot
Hostname:	EDS3032PR-0080a38aa011	<DHCP>
MTU:	1500	1500
DHCP Client	On <a href="#">Renew</a>	On
IP Address:	10.4.51.53	<DHCP>
Network Mask:	255.255.0.0	<DHCP>
Default Gateway:	10.4.0.1	<DHCP>
Domain:	<None>	<DHCP>
DNS Suffix Search List:	<None>	<None>
DHCP Client ID:	<None>	<None>
Primary DNS:	172.22.1.2	<DHCP>
Secondary DNS:	172.16.1.4	<DHCP>

## Statistics

Received:	769845 bytes
Transmitted:	2142923 bytes

Figure 6-2 Wired Network (eth0) Interface Configuration

## Wired Network (eth0) Interface Configuration

Hostname:	<input type="text"/>
MTU:	<input type="text" value="1500"/>
DHCP Client:	<input checked="" type="radio"/> On <input type="radio"/> Off
IP Address:	<input type="text" value="&lt;None&gt;"/>
Default Gateway:	<input type="text" value="&lt;None&gt;"/>
Domain:	<input type="text"/>
DHCP Client ID:	<input type="text"/>
Primary DNS:	<input type="text" value="&lt;None&gt;"/>
Secondary DNS:	<input type="text" value="&lt;None&gt;"/>

**Table 6-3 Wired Network (eth0) Interface Configuration**

Setting	Description
<b>Hostname</b>	Enter the hostname for the interface. It must begin with a letter or number, continue with a sequence of letters, numbers, or hyphens, and end with a letter or number.  This setting will take effect immediately, but will not register the hostname with a DNS server until the next reboot.
<b>MTU</b>	When DHCP is enabled, the MTU size is (usually) provided with the IP address. When not provided by the DHCP server, or using a static configuration, this value is used. The MTU size can be from 576 to 1500 bytes, the default being 1500 bytes.
<b>DHCP Client</b>	Select to turn On or Off. At boot up, after the physical link is up, the EDS3000PR will attempt to obtain IPv4 settings from a DHCP server and will periodically renew these settings with the server.  <b>Note:</b> Overrides the configured IPv4 address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the EDS3000PR. Within Web Manager, click <b>Renew</b> to renew the DHCP lease.
<b>IP Address</b>	Enter the static IPv4 address to use for the interface. You may enter it alone or in CIDR format.  <b>Note:</b> This setting will be used if Static IP is active (DHCP is Disabled). Changing this value requires you to reboot the EDS3000PR. When DHCP is enabled, the EDS3000PR unit tries to obtain an IPv4 address from a DHCP server. If it cannot, the EDS3000PR generates and uses an Auto IP address in the range of 169.254.xxx.xxx with a network mask of 255.255.0.0.
<b>Default Gateway</b>	Enter the IP address of the router for this network.  <b>Note:</b> This setting will be used if Static IP is active (DHCP is Disabled).
<b>Domain</b>	Enter the domain name suffix for the interface.  <b>Note:</b> This setting will be used when either static IP or auto IP is active, or if DHCP is active and no domain suffix was acquired from the server.
<b>DHCP Client ID</b>	Enter the ID if the DHCP server requires a DHCP client ID option. The DHCP server's lease table shows IP addresses and MAC addresses for devices. The lease table shows the client ID, in hexadecimal notation, instead of the EDS3000PR MAC address.
<b>Primary DNS</b>	Enter the IP address of the primary domain name server (DNS.)  <b>Note:</b> This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.
<b>Secondary DNS</b>	Enter the IP address of the secondary domain name server.  <b>Note:</b> This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.

Some changes to the following settings require a reboot for the changes to take effect:

- ◆ DHCP Client
- ◆ IP Address
- ◆ DHCP Client ID

**Note:** If DHCP 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.

## To Configure Network Interface Settings

### Using Web Manager

- ◆ To view Wired Network (eth0) Interface status, on the **Network** page, select **Wired Network > Interface**.
- ◆ To configure Wired Network (eth0) Interface settings, on the **Network** page, select **Wired Network > Interface > Configuration**.

### Using the CLI

- ◆ To enter the command level: `enable > config > if 1`

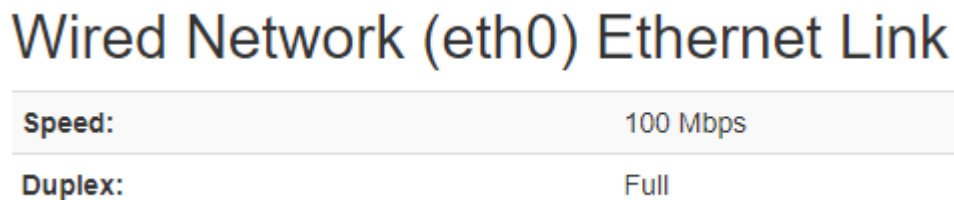
### Using XML

Include in your file: `<configgroup name= "interface" instance="eth0">`

## Link Status and Configuration

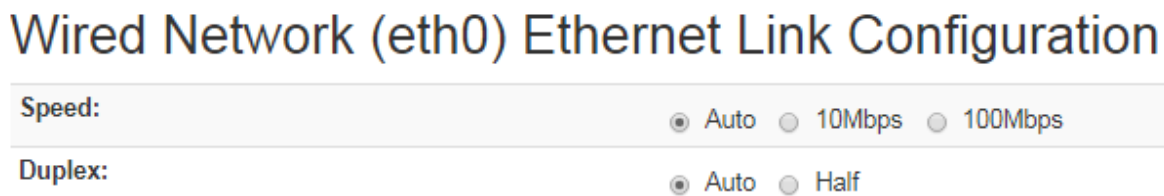
[Figure 6-4 Wired Network \(eth0\) Ethernet Link Status](#) displays the wired network's link status information. This same information is configurable on the Wired Network (eth0) Link Configuration page, shown in [Figure 6-5 Wired Network \(eth0\) Link Configuration](#). [Table 6-6 Wired Network \(eth0\) Link Configuration](#) describes the configuration information.

Figure 6-4 Wired Network (eth0) Ethernet Link Status



Speed:	100 Mbps
Duplex:	Full

Figure 6-5 Wired Network (eth0) Link Configuration



Speed:	<input checked="" type="radio"/> Auto <input type="radio"/> 10Mbps <input type="radio"/> 100Mbps
Duplex:	<input checked="" type="radio"/> Auto <input type="radio"/> Half

Table 6-6 Wired Network (eth0) Link Configuration

Setting	Description
Speed	Select the Ethernet link speed. Choices are Auto, 10Mbps, and 100Mbps. Default is Auto.
Duplex	Select the Ethernet link duplex mode. Choices are Auto, Half, and Full. Default is Auto.

### Notes:

- ◆ When speed is Auto, duplex must be Auto or Half.
- ◆ When speed is not Auto, duplex must be Half or Full.



- ◆ *Fixed-speed Full duplex produces errors when connected to Auto, due to duplex mismatch.*

## To Configure Wired Network (eth0) Link Settings

### Using Web Manager

- ◆ To view Wired Network (eth0) link status, on the **Network** page, select **Wired Network > Link**.
- ◆ To configure Wired Network (eth0) link settings, on the **Network** page, select **Wired Network > Link > Configuration**.

### Using the CLI

- ◆ To enter the command level: `enable > config > if 1 > link`

### Using XML

Include in your file: `<configgroup name= "interface" instance="eth0">`

## Protocol Stack

There are various low level network stack specific items that are available for configuration. This includes settings related to IP, ICMP, and ARP, which are described in the sections below.

### IP Settings

This page contains lower level IP Network Stack specific configuration items.

**Table 6-1 IP Protocol Stack Settings**

IP Settings	Description
<b>IP Time to Live</b>	Enter the number of hops to be transmitted before the packet is discarded. This value typically fills the time to live in the IP header. SNMP refers to this value as "ipDefaultTTL".
<b>Multicast Time to Live</b>	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.

## To Configure IP Protocol Stack Settings

### Using Web Manager

- ◆ To configure IP protocol settings, on the **Network** page, click **Protocol Stack > IP**.

### Using the CLI

- ◆ To enter the command level: `enable > config > ip`

### Using XML

- ◆ Include in your file: `<configgroup name="ip">`

## ICMP Settings

This page contains lower level ICMP Network Stack specific configuration items.

**Table 6-2 ICMP Protocol Stack Settings**

ICMP Settings	Description
<b>State</b>	The State selection is used to turn on/off processing of ICMP messages. This includes both incoming and outgoing messages. Choose <b>Enabled</b> or <b>Disabled</b> .

## To Configure ICMP Protocol Stack Settings

### Using Web Manager

- ◆ To configure ICMP protocol settings, on the **Network** page, click **Protocol Stack > ICMP**.

### Using the CLI

- ◆ To enter the command level: `enable > config > icmp`

### Using XML

- ◆ Include in your file: `<configgroup name="icmp">`

## ARP Settings

This page contains lower level Address Resolution Protocol (ARP) network stack specific configuration items. The ARP cache can be manipulated manually by adding new entries and deleting existing ones. Added entries are static and for test purposes only.

**Table 6-3 ARP Protocol Stack Settings**

ARP Settings	Description
<b>IP Address</b>	Enter the IP address to add the ARP cache.
<b>MAC Address</b>	Enter the MAC address to add to the ARP cache.
<b>Interface</b>	Select the type of interface if adding to the ARP cache.
<b>Add (button)</b>	Click this button to add a new entry (after entering the IP address, MAC address and Interface info for the new entry above.)
<b>Clear</b>	Click the <b>Clear</b> link above all listed addresses to remove all the addresses.
<b>Remove</b>	Click the <b>Remove</b> link beside a specific address to remove it.

## To Configure ARP Network Stack Settings

### Using Web Manager

- ◆ To configure ARP protocol settings, on the **Network** page, click **Protocol Stack > ARP**.

### Using the CLI

- ◆ To enter the command level: `enable > config > arp`

### Using XML

- ◆ Include in your file: `<configgroup name="arp">`

## 7: Filesystem

The Filesystem page provides statistics and current usage information for the flash filesystem. From here you may format the entire filesystem.

- ◆ Directories can be created, deleted, moved, and renamed. A directory must be empty before it can be deleted.
- ◆ Files can be created, deleted, moved, renamed, uploaded via HTTP, and transferred to and from a TFTP server. Newly created files will be empty.

Figure 7-1 Filesystem Statistics

Filesystem Statistics	
Filesystem Size:	225128K
Available Space:	220268K
File & Dir Space Used:	24K
Actions:	<a href="#">Format</a>

Table 7-4 Filesystem Statistics

Field	Description
Filesystem Size	This is the total size of the filesystem.
Available Space	This is the available space in the filesystem.
File & Dir Space Used	This is the amount of used space in the filesystem.
Actions	The Format button will format the filesystem, deleting all existing files in the filesystem.

Table 7-5 File Modification Settings

File Modification Commands	Description
rm	Removes the specified file from the file system.
touch	Creates the specified file as an empty file.
cp	Creates a copy of a file.
mkdir	Creates a directory on the file system.
rmdir	Removes a directory from the file system.
format	Format the file system and remove all data.

## File Transfer and Modification

Files can be transferred to and from the EDS3000PR via the TFTP protocol. This can be useful for saving and restoring XML configuration files. Files can also be uploaded via HTTP.

**Table 7-6 File Transfer Settings**

File Transfer Settings	Description
<b>Create</b>	Type in a <b>Directory</b> name and click the <b>Create</b> button. The newly created Directory will appear above.
<b>Upload File</b>	Click <b>Choose File</b> and select a file to be uploaded via HTTP. Click <b>Upload</b> to upload the chosen file.
<b>Copy File</b>	Enter the <b>Source</b> and <b>Destination</b> name for file to be copied and click the <b>Copy</b> button.
<b>Move</b>	Enter the <b>Source</b> and <b>Destination</b> name for file to be moved and click the <b>Move</b> button.
<b>TFTP</b>	
<b>Action</b>	Select the action that is to be performed via TFTP: <ul style="list-style-type: none"> <li>◆ Get = a “get” command will be executed to store a file locally.</li> <li>◆ Put = a “put” command will be executed to send a file to a remote location.</li> </ul>
<b>Local File</b>	Enter the name of the local file on which the specified “get” or “put” action is to be performed.
<b>Remote File</b>	Enter the name of the file at the remote location that is to be stored locally (“get”) or externally (“put”).
<b>Host</b>	Enter the IP address or name of the host involved in this operation.
<b>Port</b>	Enter the number of the port involved in TFTP operations.
<b>Transfer (button)</b>	Click the <b>Transfer</b> button after entering all TFTP settings.

## To View, Transfer, or Modify Filesystem Files

### Using Web Manager

- ◆ To view current filesystem browser statistics or to format the filesystem, on the **Filesystem** page, click **Statistics**.

**Note:** *Formatting the filesystem will cause existing files on the filesystem to be deleted.*

- ◆ To create a new file or directory, upload an existing file, copy or move a file, on the **Filesystem** page, click **Browse**.

### Using the CLI

- ◆ To enter the Filesystem command level: `enable > filesystem`

### Using XML

- ◆ Not applicable.

## 8: Diagnostics

Diagnostic settings for the EDS3000PR can be viewed and modified under the Diagnostics tab in the Web Manager user interface. This chapter describes the following diagnostic settings:

- ◆ [DNS](#)
- ◆ [Hardware](#)
- ◆ [IP Sockets](#)
- ◆ [Log](#)
- ◆ [Memory](#)
- ◆ [Ping](#)
- ◆ [Processes](#)
- ◆ [Routes](#)
- ◆ [Threads](#)
- ◆ [Traceroute](#)

### DNS

The primary and secondary DNS addresses come from the active interface. DHCP can override the static addresses from the network interface configurations.

To look up either the DNS host name or the IP address for an address, type the address or host name in the field, then click Lookup.

This section describes the active run-time settings for the domain name system (DNS) protocol. The primary and secondary DNS addresses come from the active interface. The static addresses from the Network Interface configuration settings may be overridden by DHCP.

**Table 8-7 DNS Settings**

Field/Button	Description
<b>Lookup</b>	Perform one of the following and click the <b>Lookup</b> button: <ul style="list-style-type: none"> <li>◆ Enter an IP address, and perform a reverse Lookup to locate the host name for that IP address</li> <li>◆ Enter a host name, and perform a forward Lookup to locate the corresponding IP address.</li> </ul>

### Accessing the DNS Settings

#### Using Web Manager

- ◆ To view the current DNS name or IP address, on the **Diagnostics** page, click **DNS**.
- ◆ To configure the DNS Settings, on the **Diagnostics** page, enter the name of a DNS host and click **Lookup**.

**Note:** If DNS information is not supplied by DHCP, configure Wired Network (eth0) internet settings according to instructions at [Wired Network \(eth0\) \(on page 33\)](#).

### *Using CLI*

- ◆ To enter CLI command level: `enable > dns`

### *Using XML*

- ◆ Not applicable.

## Hardware

View the CPU type, CPU speed, RAM size and flash size of the hardware on this Web Manager page.

### **To View Hardware Information**

#### *Using Web Manager*

- ◆ To view hardware information, on the **Diagnostics** page, click **Hardware**.

#### *Using the CLI*

- ◆ To enter the command level: `enable > device, show hardware information`

#### *Using XML*

- ◆ Include in your file: `<statusgroup name= "hardware">`

## IP Sockets

You can view the list of listening and connected IP sockets.

### **To View the List of IP Sockets**

#### *Using Web Manager*

- ◆ To view IP Sockets, on the **Diagnostics** page, click **IP Sockets**.

#### *Using the CLI*

- ◆ To enter the command level: `enable > show ip sockets`

#### *Using XML*

- ◆ Include in your file: `<statusgroup name="ip sockets">`

## Log

Configure a line or disable the diagnostic log on this Web Manager page.

**Table 8-8 Log Settings**

Diagnostics	Log Description
<b>Output</b>	Select a diagnostic log output type: <ul style="list-style-type: none"> <li>◆ Disable - Turn off the logging feature.</li> <li>◆ Line 1 - Directs logging to the selected serial line.</li> <li>◆ Line 2 - Directs logging to the selected serial line.</li> <li>◆ Line 3 - Directs logging to the selected serial line.</li> <li>◆ Line 4 - Directs logging to the selected serial line.</li> </ul>

## To Configure the Diagnostic Log Output

### Using Web Manager

- ◆ To configure the Diagnostic Log output, on the **Diagnostics** page, click **Log**.

### Using the CLI

- ◆ To enter the command level: `enable > config > diagnostics > log`

### Using XML

- ◆ Include in your file: `<configgroup name="diagnostics">`

## Memory

The memory information includes the total, used, and available memory (in kilobytes).

## To View Memory Usage

### Using Web Manager

- ◆ To view memory information, on the **Diagnostics** page, click **Memory**.

### Using the CLI

- ◆ To enter the command level: `enable > device, show memory`

### Using XML

- ◆ Include in your file: `<statusgroup name="memory">`

## Ping

You can use Ping to test connectivity to a remote host.

**Table 8-9 Ping Configuration**

IP Socket	Description
<b>Host</b>	Enter the IP address or host name for the EDS3000PR that you want to ping.
<b>Count</b>	Enter the number of ping packets that the EDS3000PR attempts to send to the Host. The default number of packets is 3.

IP Socket	Description
<b>Timeout</b>	Enter the time in seconds that the EDS3000PR waits for a response from the Host before it times out. The default time is 5 seconds.
<b>Ping (button)</b>	Click the <b>Ping</b> button to ping the host specified.

## To Ping a Remote Host

### Using Web Manager

- ◆ To view memory information, on the **Diagnostics** page, click **Ping**.

### Using the CLI

- ◆ To enter the command level: `ping` or `ping6`

### Using XML

- ◆ Not applicable.

## Processes

The EDS3000PR shows all the processes currently running on the system. It shows the process ID (PID), parent process ID (PPID), user, CPU percentage, percentage of total CPU cycles, and process command line information.

## To View Process Information

### Using Web Manager

- ◆ To view process information, on the **Diagnostics** page, click **Processes**.

### Using the CLI

- ◆ To enter the command level: `enable`, `show processes`

### Using XML

- ◆ Include in your file: `<statusgroup name="processes">`

## Routes

Routing allows one system to find the network path to another system, from a gateway to a destination.

### Using Web Manager

- ◆ To view the current networking routes, on the **Diagnostics** page, click **Routes**.

### Using CLI

- ◆ To enter the command level: `enable`, `show routes`

### Using XML

- ◆ Not applicable.



## Threads

The EDS3000PR threads information shows details of threads in the ltrx\_evo task which can be useful for technical experts in debugging.

### To View Thread Information

#### Using Web Manager

- ◆ To view thread information, on the **Diagnostics** page, click **Threads**.

#### Using the CLI

- ◆ To enter the command level: `enable > auto show processes or show processes`

#### Using XML

- ◆ Not applicable.

## Traceroute

You can use traceroute to trace a packet from the EDS3000PR to an Internet host. A traceroute shows how many hops the packet requires to reach the host and how long each hop takes. This information can be helpful to diagnose delays for a web page that loads slowly.

**Table 8-10 Traceroute Settings**

Traceroute Fields	Description
<b>Host</b>	Enter the IP address or DNS host name of the destination device.
<b>Protocol</b>	Select the protocol that you want to use for the traceroute. <ul style="list-style-type: none"> <li>◆ TCP</li> <li>◆ ICMP</li> <li>◆ UDP</li> </ul>
<b>Traceroute (button)</b>	Click the <b>Traceroute</b> button to perform the traceroute.

### To Perform a Traceroute

#### Using Web Manager

- ◆ To view traceroute information, on the **Diagnostics** page, click **Traceroute**.

#### Using the CLI

- ◆ To enter the command level: `enable > trace route`

#### Using XML

- ◆ Not applicable.

## 9: Administration

Administrative features for the EDS3000PR are organized beneath the Administration tab in the Web Manager user interface. This chapter describes the following administrative settings:

- ◆ [CLI](#)
- ◆ [Clock](#)
- ◆ [Discovery](#)
- ◆ [Email](#)
- ◆ [FTP](#)
- ◆ [Host](#)
- ◆ [HTTP](#)
- ◆ [Line](#)
- ◆ [MACH10](#)
- ◆ [RSS](#)
- ◆ [SMTP](#)
- ◆ [SNMP](#)
- ◆ [SSH](#)
- ◆ [SSL](#)
- ◆ [Syslog](#)
- ◆ [System](#)
- ◆ [Terminal](#)
- ◆ [Tunnel](#)
- ◆ [User Management](#)
- ◆ [XML](#)

### CLI

The command line interface (CLI) settings allow you to control how users connect to and interact with the command line of the EDS3000PR. It is possible to configure access via the Telnet and SSH protocols, in addition to general CLI options.

#### CLI Status and Configuration

View-only status information on the CLI Statistics page displays the current Telnet and SSH server status, uptime, and current connections (if any.)

**Table 9-11 CLI Configuration Settings**

Command Line Interface Configuration Settings	Description
<b>Enable Level Password</b>	Enter the password for access to the Enable level of a CLI session. There is no password by default.
<b>Quit Connect Line</b>	Enter the <b>Quit Connect Line</b> string to be used to terminate a Telnet and SSH session and resume the CLI. Type <control> before the key to be pressed while holding down the <b>[Ctrl]</b> key (example: <control>L)
<b>Inactivity Timeout</b>	Set a time period in which the CLI session should disconnect if no data is received. Enter 0 to disable. Blank the display field to restore the default.
<b>Line Authentication</b>	<b>Enable</b> or <b>Disable</b> authentication for CLI access on the serial lines.
<b>Telnet State</b>	<b>Enable</b> or <b>Disable</b> CLI access via Telnet
<b>Telnet Port</b>	Enter an alternative Telnet Port to override the default used by the CLI server. Blank the field to restore the default.
<b>Telnet Max Sessions</b>	Specify the maximum number of concurrent Telnet sessions that will be allowed.
<b>Telnet Authentication</b>	<b>Enable</b> or <b>Disable</b> authentication for Telnet logins.
<b>SSH State</b>	Select to <b>Enable</b> or <b>Disable</b> CLI access via SSH.
<b>SSH Port</b>	Specify the SSH Port and override the default, as needed. Blank the field to restore the default.
<b>SSH Max Sessions</b>	Specify the maximum number of concurrent SSH sessions that will be allowed.

## To View and Configure Basic CLI Settings

### Using Web Manager

- ◆ To view CLI statistics, on the **Administration** page, click **CLI > Statistics**.
- ◆ To configure basic CLI settings, on the **Administration** page, click **CLI > Configuration**.

### Using the CLI

- ◆ To enter CLI command level: `enable > config > cli`

### Using XML

- ◆ Include in your file: `<configgroup name="cli">`

## Clock

You can view current clock settings at the bottom of the Clock page and can also either manually update or synchronize the clock with an SNTP server. If you select SNTP, you can choose automatic time zone detection.

**Table 9-12 Clock Settings**

Clock Settings	Description
<b>Method</b>	Select <b>Manual</b> or <b>SNTP</b> from the drop-down window.

Clock Settings	Description
<b>Date</b>	If <b>Manual</b> is selected, enter the date using the <b>Year</b> , <b>Month</b> and <b>Day</b> drop-down menus that become available.
<b>Time</b>	If <b>Manual</b> is selected, enter the time using the <b>Hour</b> , <b>Minute (Min)</b> and <b>Second (Sec)</b> drop-down menus that become available.
<b>NTP Server</b>	If <b>SNTP</b> is selected, the clock will keep time synchronized with the NTP Server by default. Enter an alternative NTP server if you wish to use an address other than the default.
<b>Time Zone</b>	Select the desired Time Zone from the drop-down menu based on geographic location. The time zones listed are in Universal Time Coordinated (UTC), formerly known as Greenwich Mean Time (GMT). Syslog and other applications may use UTC. The UTC Offset of the form HHMM (H = hour, M = minute) is applied to the UTC time to get the local time. The EDS3000PR will make seasonal time changes required for Daylight Savings Time.

## To Specify a Clock-Setting Method

### Using Web Manager

- ◆ To view or configure basic Clock settings, on the **Administration** page, click **Clock**.

### Using the CLI

- ◆ To enter Clock command level: `enable > config > clock`

### Using XML

- ◆ Include in your file: `<configgroup name="clock">`

## Discovery

Network discovery allows your computer to locate other computers and devices on the network. This setting also allows other computers to see your computer.

The current statistics and configuration options for device discovery are available for the EDS3000PR.

**Table 9-13 Discovery Settings**

Discovery Settings	Description
<b>Query Port Server State</b>	Select to enable or disable the query port server from responding to autodiscovery messages on port 0x77FE.

## To Configure Discovery

### Using Web Manager

- ◆ To configure Discovery, on the **Administration** page, click **Discovery**.

### Using the CLI

- ◆ To enter Discovery command level: `enable > config > discovery`

### Using XML

- ◆ Include in your file: `<configgroup name="discovery">`

## Email

View and configure email alerts relating to events occurring within the system.

**Table 9-14 Email Configuration**

Email Configuration Settings	Description
<b>From</b>	Click the <b>Configure SMTP</b> link to configure SMTP. See <a href="#">SMTP (on page 58)</a> .
<b>To</b>	Enter the email address to which the email alerts will be sent. Multiple addresses are separated by semicolon (;). Required field if email is to be sent.
<b>CC</b>	Enter the email address to which the email alerts will be copied. Multiple addresses are separated by semicolon (;).
<b>Reply To</b>	Enter the email address to list in the Reply-To field of the email alert.
<b>Subject</b>	Enter the subject for the email alert.  <b>Note:</b> Emails sent as a result of an alarm will display the name of the alarm in the subject of the email, overriding the email subject configured in this field.
<b>Message File</b>	Enter the path of the file to send with the email alert. This file appears within the message body of the email, not as an attachment.
<b>Priority</b>	Select the priority level for the email alert: <ul style="list-style-type: none"> <li>◆ Urgent</li> <li>◆ High</li> <li>◆ Normal</li> <li>◆ Low</li> <li>◆ Very Low</li> </ul>

### To View, Configure and Send Email

**Note:** The following section describes the steps to view and configure Email 1 settings; these steps apply to other emails available for the EDS3000PR.

#### Using Web Manager

- ◆ To view Email statistics, on the **Administration** page, click **Email > Statistics**.
- ◆ To configure basic Email settings and send an email, on the **Administration** page, click **Email > Configuration**.

#### Using the CLI

- ◆ To enter Email command level: `enable > email 1`

#### Using XML

- ◆ Include in your file: `<configgroup name="email" instance="1">`

## FTP

The FTP protocol can be used to upload and download user files as well as upgrade the EDS3000PR firmware. A configurable option is provided to enable or disable access via this protocol.

**Table 9-15 FTP Settings**

FTP Settings	Description
<b>State</b>	Select to enable or disable the FTP server: <ul style="list-style-type: none"> <li>◆ Enabled (default)</li> <li>◆ Disabled</li> </ul>
<b>Port</b>	Enter the Port to be used by FTP server. Entering a Port overrides the default ftp port. Blank the field to restore the default ftp port.
<b>Data Port</b>	Enter the Data Port where the server initiates a data channel to the client. In active mode, the client starts listening for incoming data connections from the server on port M. It sends the FTP command PORT M to inform the server on which port it is listening. The server then initiates a data channel to the client from its Data Port.
<b>Passive Mode Start Port</b>	Define the port range by entering the <b>Passive Mode Start Port</b> and <b>Passive Mode Port</b> . In passive mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server, which the client then uses to open a data connection to the server IP address and server port number received. In situations where the client is behind a firewall and unable to accept incoming TCP connections, passive mode may be used.
<b>Passive Mode Ports</b>	
<b>Submit (button)</b>	Click the <b>Submit</b> button to enter the change of state. The <b>Submit</b> button appears when a new state is selected.

## To Configure FTP Settings

### Using Web Manager

- ◆ To configure FTP, on the **Administration** page, click **FTP**.

### Using the CLI

- ◆ To enter the FTP command level: `enable > config > ftp`

### Using XML

- ◆ Include in your file: `<configgroup name="ftp server">`

## Host

**Table 9-16 Host Settings**

Host Settings	Description
<b>Name</b>	Enter a name for the host. This name appears on the Connect Menu during the CLI login. To leave a host out of the menu, leave this field blank.

Host Settings	Description
<b>Protocol</b>	Select the protocol to use to connect to the host. Choices are: <ul style="list-style-type: none"> <li>◆ Telnet</li> <li>◆ SSH</li> </ul> <p><b>Note:</b> SSH keys must be loaded or created on the SSH page for the SSH protocol to work.</p>
<b>SSH Username</b>	Appears if you selected SSH as the protocol. Enter a username to select a preconfigured 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. <p><b>Note:</b> This configuration option is only available when SSH is selected for Protocol.</p>
<b>Remote Address</b>	Enter an IP address for the host to which the EDS3000PR will connect.
<b>Remote Port</b>	Enter the port on the host to which the EDS3000PR will connect.

## To Configure Host Settings

**Note:** The following section describes the steps to view and configure Host 1 settings; these steps apply to other host instances of the EDS3000PR.

### Using Web Manager

- ◆ To configure a particular Host, on the **Administration** page, click **Host > Configuration**.

### Using the CLI

- ◆ To enter the Host command level: `enable > config > host 1`

### Using XML

- ◆ Include in your file: `<configgroup name="host" instance="1">`

## HTTP

Hypertext Transfer Protocol (HTTP) is a request-response standard protocol between clients and servers. HTTP defines how messages are formatted and transmitted. It also defines the actions Web servers and browsers take in response to different commands. HTTP Authentication enables the requirement of user names and passwords for access to the EDS3000PR.

### Interface Status, Configuration and Authentication

View-only status information on the HTTP Statistics page displays various HTTP server statistics including information on Rx bytes, Tx bytes, error message types, status unknown, work queue full, socket error, memory error, and logs.

See [Table 9-17](#) for the HTTP settings that can be modified on the HTTP Configuration page. See [Table 9-18](#) for the HTTP settings that can be authenticated on the HTTP Authentication page.

Table 9-17 HTTP Configuration

HTTP Settings	Description
<b>State</b>	Select to enable or disable the HTTP server.
<b>Port</b>	Enter the port for the HTTP server to use. The default is <b>80</b> .
<b>HTTPS State</b>	Select to enable or disable.
<b>Secure Port</b>	Enter the port for the HTTPS server to use. The default is <b>443</b> . The HTTP server only listens on the <b>HTTPS Port</b> when an SSL certificate is configured.
<b>Secure Protocols</b>	<p>Select to enable or disable the following protocols:</p> <ul style="list-style-type: none"> <li>◆ <b>SSL3</b> = Secure Sockets Layer version 3</li> <li>◆ <b>TLS1.0</b> = Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF.</li> <li>◆ <b>TLS1.1</b> = Transport Layer Security version 1.1</li> <li>◆ <b>TLS1.2</b> = Transport Layer Security version</li> </ul> <p>The protocols are enabled by default.</p> <p><b>Note:</b> A server certificate and associated private key need to be installed in the <b>SSL</b> configuration section to use <b>HTTPS</b>.</p>
<b>Secure Credentials</b>	Specify the name of the set of RSA and/or DSA certificates and keys to be used for the secure connection.
<b>Max Timeout</b>	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is <b>10</b> seconds.
<b>Max Bytes</b>	<p>Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is <b>40</b> KB (this prevents DoS attacks).</p> <p><b>Note:</b> You may need to increase this number in some cases where the browser is sending data aggressively within TCP Windows size limit, when file (including firmware upgrade) is uploaded from webpage.</p>
<b>Logging State</b>	<p>Select to enable or disable HTTP server logging:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> (default)</li> <li>◆ <b>Disabled</b></li> </ul>
<b>Max Log Entries</b>	Set the maximum number of HTTP server log entries. Only the last <b>Max Log Entries</b> are cached and viewable.
<b>Log Format</b>	<p>Set the log format string for the HTTP server. Follow these <b>Log Format</b> rules:</p> <ul style="list-style-type: none"> <li>◆ <b>%a</b> - remote IP address (could be a proxy)</li> <li>◆ <b>%b</b> - bytes sent excluding headers</li> <li>◆ <b>%B</b> - bytes sent excluding headers (0 = '-')</li> <li>◆ <b>%h</b> - remote host (same as '%a')</li> <li>◆ <b>%{h}i</b> - header contents from request (h = header string)</li> <li>◆ <b>%m</b> - request method</li> <li>◆ <b>%p</b> - ephemeral local port value used for request</li> <li>◆ <b>%q</b> - query string (prepend with '?' or empty '-')</li> <li>◆ <b>%t</b> - timestamp HH:MM:SS (same as Apache '%(H:%M:%S)t' or '%(T)t')</li> <li>◆ <b>%u</b> - remote user (could be bogus for 401 status)</li> <li>◆ <b>%U</b> - URL path info</li> <li>◆ <b>%r</b> - first line of request (same as '%m %U%q &lt;version&gt;')</li> <li>◆ <b>%s</b> - return status</li> </ul>
<b>Authentication Timeout</b>	The timeout period applies if the selected authentication type is either <b>Digest</b> or <b>SSL/Digest</b> . After this period of inactivity, the client must authenticate again.



## To View or Configure HTTP

### Using Web Manager

- ◆ To view HTTP statistics, on the **Administration** page, click **HTTP > Statistics**
- ◆ To configure HTTP, on the **Administration** page, click **HTTP > Configuration**.

### Using the CLI

- ◆ To enter the HTTP command level: `enable > config > http`

### Using XML

- ◆ Include in your file: `<configgroup name="http server">`

The HTTP Server can be configured with many different authentication directives. The authentication is hierarchical in that any URI can be given an authentication directive in order to override a parent URI authentication directive.

**Table 9-18 HTTP Authentication**

HTTP Authentication Settings	Description
<b>URI</b>	Enter the URI. The URI must begin with / to refer to the filesystem.
<b>Authentication Type</b>	<p>Select an HTTP authentication type. The different types offer various levels of security, from the least to most secure:</p> <ul style="list-style-type: none"> <li>◆ <b>None:</b> no authentication necessary</li> <li>◆ <b>Basic:</b> encodes passwords using Base64</li> <li>◆ <b>Digest:</b> encodes passwords using MD5</li> </ul> <p>When changing the parameters of Digest authentication, it is often best to close and reopen the browser to ensure that it does not attempt to use cached authentication information.</p> <p>There is no real reason to create an authentication directive using None unless you want to override a parent directive that uses some other Authentication Type.</p> <p>Click <b>Submit</b> when URI and Authentication Type is entered to submit it.</p>
<b>Delete</b>	Click to delete the existing configuration.

## To Configure HTTP Authentication

### Using Web Manager

- ◆ To configure HTTP authentication, on the **Administration** page, click **HTTP > Authentication**.

### Using the CLI

- ◆ To enter the HTTP command level: `enable > config > http`

### Using XML

- ◆ Include in your file: `<configgroup name="http authentication uri">`

## Line

The EDS3000PR offers 8, 16, or 32 serial ports that use standard RS232 interfaces.

The line settings allow configuration of the serial line.

**Note:** The following section describes the steps to view and configure Line 1 settings; these steps apply to other line instances of the EDS3000PR.

### Line Status and Configuration

View-only status information on the Line - Statistics page displays line statistics including information on bytes, queued bytes, breaks, flow control, parity errors, framing errors, overrun errors, no Rx buffer errors, CTS input, RTS output, DSR input, and DTR output.

See [Table 9-19](#) for the line settings that can be modified on the Line - Configuration page. See [Table 9-20](#) for the line settings that can be established on the Line - Command Mode page.

**Table 9-19 Line Configuration Settings**

Line Settings	Description
<b>Name</b>	Enter a name or short description for the line, if desired. By default, there is no name specified. A name that contains white space must be quoted.
<b>Interface</b>	Interface is set to RS232 and cannot be changed.
<b>State</b>	Select to enable or disable the operational state of the Line. The default is Enabled.
<b>Protocol</b>	Set the operational protocol for the Line. The default is Tunnel. Choices are None and Tunnel.
<b>Baud Rate</b>	Select the desired baud rate from the drop-down menu. The default is 9600.
<b>Parity</b>	Select parity from the drop-down menu. The default is None. Choices are None, Even, and Odd.
<b>Data Bits</b>	Select 7 or 8 data bits from the drop-down menu. The default is 8.
<b>Stop Bits</b>	Select 1 or 2 stop bits from the drop-down menu. The default is 1.
<b>Flow Control</b>	Select None, Hardware or Software flow control from the drop-down menu. The default is None.
<b>Gap Timer</b>	Set the gap timer delay to set the number of milliseconds to pass from the last character received before the driver forwards the received serial bytes. By default, the delay is four character periods at the current baud rate (minimum 1 msec). Gap timer range is 1 to 5000 milliseconds.
<b>Threshold</b>	Set the number of threshold bytes that need to be received in order for the driver to forward received characters. Default value is 56 bytes.

**Table 9-20 Line Command Mode Setting**

Line Command Mode Settings	Description
<b>Mode</b>	<p>Set the Command Mode state of the Line. When in Command Mode, a CLI session operates exclusively on the Line. Choices are:</p> <ul style="list-style-type: none"> <li>◆ Always</li> <li>◆ Use Serial String</li> <li>◆ Disabled</li> </ul> <p><b>Note:</b> In order to enable Command Mode on the Line, Tunneling on the Line must be Disabled. Custom baud rates are not supported in Command Mode.</p>
<b>Wait Time</b>	<p>Enter the amount of time to wait during boot time for the Serial String. This timer starts right after the Signon Message has been sent on the Serial Line and applies only if mode is Use Serial String.</p> <p><b>Note:</b> This field becomes available when Use Serial String is selected for Mode.</p>
<b>Serial String</b>	<p>Enter the Text or Binary string of bytes that must be read on the Serial Line during boot time in order to enable Command Mode. It may contain a time element to specify a required delay in milliseconds x, formed as {x}. Applies only if mode is Use Serial String. It may contain one or more binary characters of the form [x]. For example, use decimal [12] or hex [0xc].</p> <p><b>Note:</b> This field becomes available when Use Serial String is selected for Mode.</p>
<b>Echo Serial String</b>	<p>Select Enable or Disable for Echo Serial String. Applies only if mode is Use Serial String. Select Enable to echo received characters back out on the line while looking for the serial string.</p> <p><b>Note:</b> This field becomes available when Use Serial String is selected for Mode.</p>
<b>Signon Message</b>	<p>Enter the string of bytes to be sent to the Serial Line during boot time. It may contain one or more binary characters of the form [x]. For example, use decimal [12] or hex [0xc]. Click the Submit button after entering the signon message.</p> <p><b>Note:</b> The Submit button will only appear if the Mode is not disabled.</p>

## To View and Configure Line Configuration and Command Mode

### Using Web Manager

- ◆ To view line statistics, on the **Administration** page, click **Line > Statistics** and then select a line number from the **Select Line** drop-down list at the top.
- ◆ To configure a line, on the **Administration** page, click **Line > Configuration** and then select a line number from the **Select Line** drop-down list at the top.
- ◆ To configure line command mode on the **Administration** page, click **Line > Command Mode** and then select a line number from the **Select Line** drop-down list at the top.

### Using the CLI

- ◆ To enter the Line command level: `enable > line <number>`

### Using XML

- ◆ Include in your file: `<configgroup name="line" instance="<number>">`

## MACH10

The EDS3000PR comes integrated with MACH10® cloud platform to allow for the remote management of devices. To set up the MACH10 client, you need to configure the following settings:

- ◆ **MACH10 Client** - to connect to the MACH10 cloud platform.
- ◆ **Line Settings (Line 1, Line 2, or Line 3)** - to enable remote management and data access to your application or device attached on the serial line.

### To Configure MACH10 Client

This page displays the configuration and status for MACH10 client.

**Table 9-21 MACH10 Client Configuration**

MACH10 Client	Description
<b>State</b>	Click to enable or disable the MACH10 client.
<b>Device ID</b>	Read only. Displays the gateway's Device ID. Device ID may be provisioned through Lantronix Provisioning Manager. <i>Note: Device ID can only be provisioned once. It will persist across resets.</i>
<b>Device Key</b>	Read only. Shows whether the gateway's Device Key has been configured. Device Key may be configured through Lantronix Provisioning Manager.
<b>Device Name</b>	Enter the MACH10 Device Name.
<b>Device Description</b>	Enter the MACH10 Device Description.
<b>Status Update Interval</b>	Enter the frequency that the gateway updates the device status to MACH10. The valid range is between 1 minute and 1440 minutes (1 day).
<b>Content Check Interval</b>	Enter the frequency that the gateway checks MACH10 for updates to configuration or firmware. The valid range is between 1 hour and 2160 hours (90 days).
<b>Apply Firmware Updates</b>	Enable to allow firmware updates to be applied via MACH10. Enabled by default.
<b>Apply Configuration Updates</b>	Select when to <b>Apply Configuration Updates</b> from the drop-down menu: <ul style="list-style-type: none"> <li>◆ <b>Never</b>: signifying no configuration updates will be applied.</li> <li>◆ <b>If unchanged</b>: signifying configuration updates will only be applied if no changes have been made locally.</li> <li>◆ <b>Always</b>: signifying configuration updates will always apply.</li> </ul>
<b>Reboot After Update</b>	Automatically reboot device after firmware or configuration update. <i>Note: Setting causes automatic reboot after a firmware update.</i>
<b>Active Connection</b>	Select the connection instance to use when connecting to MACH10. The configuration options for both Connection 1 and Connection 2 are below.
<b>Host</b>	Enter the host name or IP address
<b>Port</b>	Enter the MACH10 port
<b>Secure Port</b>	Click to enable or disable the MACH10 client secure port 443.
<b>Validate Certificates</b>	Click to enable or disable the MACH10 client <b>Validate Certificates</b> .
<b>Local Port</b>	Enter the local port for the SMTP protocol. When configured, a total of 16 consecutive ports will be reserved.
<b>MQTT State</b>	Enable or Disable MQTT.

MACH10 Client	Description
<b>MQTT Host</b>	Hostname or IP address of MQTT server.
<b>MQTT Port</b>	Update the port of MACH10 MQTT server. When configured, a total of 32 consecutive ports will be reserved.
<b>MQTT Security</b>	Enable SSL for MQTT.
<b>MQTT Local Port</b>	Enter the local port of MACH10 MQTT client. When configured, a total of 32 consecutive ports will be reserved.
<b>Use Proxy</b>	Enable or disable the use of a proxy for this connection. Disabled by default.
<b>Proxy Type</b>	Proxy server type. The supported type is SOCKS5.
<b>Proxy Host</b>	Hostname or IP address of the proxy server to be used.
<b>Proxy Port</b>	Port of the proxy server to be used. Default port is <b>80</b> .
<b>Proxy Username</b>	Username for the proxy server.
<b>Proxy Password</b>	Password for the proxy server.
<b>Submit (button)</b>	Click the <b>Submit</b> button to enter the settings. The <b>Submit</b> button appears when new settings are entered.

## To Configure MACH10 Line 1, Line 2, or Line 3

**Note:** The following section describes the steps to view and configure MACH10 Line 1 settings; these steps also apply to Line 2 and Line 3.

This page displays the configuration and status for MACH10 Line client.

**Table 9-22 MACH10 Line**

MACH10 Line	Description
<b>State</b>	Click to enable or disable the MACH10 line client.
<b>Project Tag</b>	Enter the <b>MACH10 Project Tag</b> name.
<b>Status Update Interval</b>	Enter the <b>Status Update Interval</b> in minutes. The status update interval is the frequency in which the gateway will contact the MACH10 server.
<b>Content Check Interval</b>	Enter the <b>Content Check Interval</b> in hours. The content check interval is the frequency in which the gateway contacts the server for new content.
<b>Command Delimiter</b>	Enter the Command Delimiter for attached serial devices. <b>Note:</b> Send delimiter before command and after response is received.
<b>Local Port</b>	Enter the local port for the MACH10 client. When configured, a total of 16 consecutive ports will be reserved.
<b>Submit (button)</b>	Click the <b>Submit</b> button to enter the settings. The <b>Submit</b> button appears when new settings are entered.

## To Configure MACH10

### Using Web Manager

- ◆ To configure MACH10 Client, on the **Administration** page, click **MACH10 > Client**.
- ◆ To configure MACH10 Line 1, on the **Administration** page, click **MACH10 > Line 1**.
- ◆ To configure MACH10 Line 2, on the **Administration** page, click **MACH10 > Line 2**.

- ◆ To configure MACH10 Line 3, on the **Administration** page, click **MACH10 > Line 3**.

#### Using the CLI

- ◆ To enter the command level: `enable > config > mach10`

#### Using XML

- ◆ Include in your file: `<configgroup name="mach10">`

## RSS

An RDF Site Summary (RSS) syndication feed is served by the HTTP Server. This feed contains up-to-date information regarding the configuration changes that occur on the EDS3000PR.

Specifying the RSS Feed to be Persistent results in the data being stored on the filesystem. The file used is `/cfg_log.txt`. This allows feed data to be available across reboots (or until the factory defaults are set).

Each RSS Feed entry contains a standard timestamp in its `<pubDate>` field.

The RSS Feed is a scrolling feed in that only the last Max Entries entries are cached and viewable.

Simply register the RSS Feed within your favorite RSS aggregator and you will automatically be notified of any configuration changes that occur.

**Table 9-23 RSS**

RSS Settings	Description
<b>RSS Feed</b>	Click to select whether to turn the RSS Feed <b>On</b> or <b>Off</b> .
<b>Persistent</b>	Click to select whether to turn Persistent mode for the RSS Feed <b>On</b> or <b>Off</b> .
<b>Max Entries</b>	Enter the numerical value of maximum RSS feed entries to be cached and viewable. Default is 100.
<b>Data</b>	<ul style="list-style-type: none"> <li>◆ Click <b>View</b> to view existing RSS data.</li> <li>◆ Click <b>Clear</b> to clear accumulated RSS data.</li> </ul>

## To Configure RSS Settings

#### Using Web Manager

- ◆ To configure RSS settings, on the **Administration** page, click **RSS**.

#### Using the CLI

- ◆ To enter the command level: `enable > config > rss`

#### Using XML

- ◆ Include in your file: `<configgroup name="rss">`

## SMTP

Configure Simple Mail Transfer Protocol (SMTP) settings including addresses, port, user name, password, overriding domain information and local port.

**Table 9-24 SMTP Settings**

SMTP Settings	Description
<b>From Address</b>	Enter the From Address here. This is an email address and is required. If you wish to direct outbound email messages through a mail server, put your client email address here.
<b>Server Address</b>	Enter the Server Address to direct outbound email messages through a mail server.
<b>Server Port</b>	Enter the SMTP server port number. The default is 25
<b>Username</b>	Enter a Username to direct outbound email messages through a mail server.
<b>Password</b>	Enter a Password to direct outbound email messages through a mail server.
<b>Overriding Domain</b>	Enter the domain name to override the current domain name in EHLO (Extended Hello).
<b>Local Port</b>	Enter the local port for the SMTP protocol. The local port is the source port for the SMTP client.

## To Configure SMTP Settings

### Using Web Manager

- ◆ To configure SMTP protocol settings, on the **Administration** page, click **SMTP** in the menu.

### Using the CLI

- ◆ To enter the command level: `enable > config > smtp`

### Using XML

- ◆ Include in your file: `<configgroup name="smtp">`

## SNMP

Simple Network Management Protocol (SNMP) settings may be viewed and configured in this section.

**Table 9-25 SNMP Settings**

SNMP Settings	Description
<b>SNMP Agent</b>	
<b>State</b>	Select to enable or disable the SNMP agent state.
<b>Port</b>	Set the port of the SNMP agent.
<b>Version</b>	Select the SNMP version used by the SNMP agent. Choices are SNMPv1, SNMPv2c, and SNMPv3.
<b>Read Community</b>	Specify the read community used by the agent (defaults to public community).
<b>Write Community</b>	Specify the write community used by the agent (defaults to private community).
<b>System MIB</b>	
<b>System Contact</b>	Specify the system contact.

SNMP Settings	Description
<b>System Name</b>	Update the system name, as necessary.
<b>System Description</b>	Update the system description, as necessary. The default system information includes the manufacturer name, model name, version and the serial number of the EDS3000PR.
<b>System Location</b>	Specify a system location for the SNMP setting.
<b>MIB</b>	
<b>Lantronix MIB File</b>	Click the Lantronix MIB file name to save and load it into the MIB browser and trap receiver. This is the base MIB file for Lantronix products. Load or compile this file first.
<b>MIB File</b>	Click the MIB file name to save and load it into the MIB browser and trap receiver. This is the product specific MIB file. Load or compile this after the Lantronix MIB File.
<b>SNMP Traps</b>	
<b>Primary Destination</b>	Enter the Primary Destination. <i>Note: SNMP Traps fields become available when SNMP Agent State is enabled.</i>
<b>Primary Destination Port</b>	Enter the Primary Destination port. <i>Note: SNMP Traps fields become available when SNMP Agent State is enabled.</i>
<b>Secondary Destination</b>	Enter the Secondary Destination. <i>Note: SNMP Traps fields become available when SNMP Agent State is enabled.</i>
<b>Secondary Destination Port</b>	Enter the Secondary Destination port. <i>Note: SNMP Traps fields become available when SNMP Agent State is enabled.</i>

## To Configure SNMP Settings

### Using Web Manager

- ◆ To configure SNMP, on the **Administration** page, click **SNMP** in the menu.

### Using the CLI

- ◆ To enter the SNMP command level: `enable > config > snmp`

### Using XML

- ◆ Include in your file: `<configgroup name="snmp">`

## SSH

The SSH Server Host Keys are used by all applications that play the role of an SSH Server during Tunneling in Accept Mode. These keys can be created elsewhere and uploaded to the EDS3000PR or automatically generated on the gateway.

Configuration is required when the EDS3000PR is either (1) the SSH server or (2) 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 EDS3000PR 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 EDS3000PR SSH server.

### SSH Server: Host Keys

The SSH Server Host Keys are used by all applications that play the role of an SSH Server during Tunneling in Accept Mode. These keys can be created elsewhere and uploaded to the device or automatically generated on the gateway.

If uploading existing keys, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

**Note:** Some SSH Clients require RSA Host Keys to be at least 1024 bits in size.

**Table 9-26 SSH Server Host Keys**

SSH Settings	Description
<b>Private Key</b>	Click the <b>Choose File</b> button to navigate to the existing private key you want to upload. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
<b>Public Key</b>	Click the <b>Choose File</b> button to navigate to the existing public key you want to upload.
<b>Submit (button)</b>	Click the <b>Submit</b> button after changes are made in the above Upload Keys fields.
<b>Key Type</b>	Select a key type to use for the new key: <ul style="list-style-type: none"> <li>◆ RSA</li> <li>◆ DSA</li> </ul>
<b>Bit Size</b>	Select a bit length for the new key: <ul style="list-style-type: none"> <li>◆ 512</li> <li>◆ 768</li> <li>◆ 1024</li> <li>◆ 2048</li> <li>◆ 4096</li> </ul>
<b>Submit (button)</b>	Click the <b>Submit</b> button after changes are made in the above Create New Keys fields.

**Note:** SSH Keys from other programs may be converted to the required EDS3000PR format. Use Open SSH to perform the conversion.

### SSH Server: Authorized Users

The SSH Server Authorized Users are used by all applications that play the role of an SSH Server during Tunneling in Accept Mode. Every user account must have a Password.

The user's Public Keys are optional and only necessary if public key authentication is wanted. Using public key authentication will allow a connection to be made without the password being asked at that time.

**Note:** When uploading the security keys, ensure the keys are not compromised in transit.

**Table 9-27 SSH Server Authorized Users**

SSH Settings	Description
<b>Username</b>	Enter a new username or edit an existing one.
<b>Password</b>	Enter a new password or edit an existing one.
<b>Public RSA Key</b>	Click the <b>Choose File</b> button to browse to the existing public RSA key you want to use with this user. If authentication is successful with the key, no password is required.
<b>Public DSA Key</b>	Click the <b>Choose File</b> button to browse to the existing public DSA key you want to use with this user. If authentication is successful with the key, no password is required.
<b>Add/Edit (button)</b>	Click the <b>Add/Edit</b> button after changes are made in the above SSH Server: Authorized Users fields.

### SSH Client: Known Hosts

The SSH Client Known Hosts are used by all applications that play the role of an SSH Client. Specifically in Connect Mode. Configuring these public keys are optional, but if they exist another layer of security is offered which helps prevent Man-in-the-Middle (MITM) attacks.

**Table 9-28 SSH Client Known Hosts**

SSH	Settings Description
<b>Server</b>	Specify either a DNS Hostname or IP Address when adding public host keys for a Server. This Server name should match the name used as the Remote Address in Connect Mode Tunneling.
<b>Public RSA Key</b>	Click the <b>Choose File</b> button to browse to the existing public RSA key you want to use with this user. If authentication is successful with the key, no password is required.
<b>Public DSA Key</b>	Click the <b>Choose File</b> button to browse to the existing public DSA key you want to use with this user. If authentication is successful with the key, no password is required.
<b>Submit (button)</b>	Click the <b>Submit</b> button after changes are made in the above SSH Server: Known Hosts fields.

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

### SSH Client: Users

The SSH Client Users are used by all applications that play the role of an SSH Client during Tunneling in Connect Mode. To configure the EDS3000PR as an SSH client, an SSH client user must be both configured and also exist on the remote SSH server.

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 EDS3000PR or automatically generated on the device.

If uploading existing Keys, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

The default Remote Command is '<Default login shell>' which tells the SSH Server to execute a remote shell upon connection. This can be changed to anything the SSH Server on the remote host can execute.

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

**Table 9-29 SSH Client Users**

SSH Settings	Description
<b>Username</b>	Enter the name that the EDS3000PR uses to connect to an SSH server.
<b>Password</b>	Enter the password associated with the username.
<b>Remote Command</b>	Enter the command that can be executed remotely. Default is shell, which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.
<b>Private Key</b>	Click the <b>Choose File</b> button to browse to the existing private key you want to upload. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
<b>Public Key</b>	Click the <b>Choose File</b> button to browse to the existing public key you want to upload.
<b>Key Type</b>	Select a key type: <ul style="list-style-type: none"> <li>◆ RSA</li> <li>◆ DSA</li> </ul>
<b>Add/Edit (button)</b>	Click the <b>Add/Edit</b> button after changes are made in the above SSH Client: Users fields.

**Table 9-30 Create New Keys**

SSH Setting	Description
<b>Username</b>	Enter the <b>Username</b> for the new key.
<b>Key Type</b>	Select a key type for the new key: <ul style="list-style-type: none"> <li>◆ RSA</li> <li>◆ DSA</li> </ul>
<b>Bit Size</b>	Select the bit length of the new key: <ul style="list-style-type: none"> <li>◆ 512</li> <li>◆ 768</li> <li>◆ 1024</li> <li>◆ 2048</li> <li>◆ 4096</li> </ul> <p>Using a larger bit size takes more time to generate the key. Approximate times are:</p> <ul style="list-style-type: none"> <li>◆ 1 second for a 512 bit RSA key</li> <li>◆ 1 second for a 768 bit RSA key</li> <li>◆ 1 second for a 1024 bit RSA key</li> <li>◆ 2 seconds for a 512 bit DSA key</li> <li>◆ 2 seconds for a 768 bit DSA key</li> <li>◆ 20 seconds for a 1024 bit DSA key</li> </ul> <p><b>Note:</b> Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 2048 bits long.</p>

SSH Setting	Description
<b>Submit (button)</b>	Click the <b>Submit</b> button after changes are made in the above Create New Keys fields.

## To Configure SSH Settings

### Using Web Manager

- ◆ To configure SSH, on the **Administration** page, click **SSH** in the menu and then click either **SSH Server: Host Keys**, **SSH Server: Authorized Users**, **SSH Client: Known Hosts**, or **SSH Client: Users**.

### Using the CLI

- ◆ To enter the SSH command level: `enable > ssh`

### Using XML

- ◆ Include in your file: `<configgroup name="ssh">`
- ◆ Include in your file: `<configgroup name="ssh client">`
- ◆ Include in your file: `<configgroup name="ssh server">`

## SSL

Secure Sockets Layer (SSL) is a protocol that creates an encrypted connection between devices. It also provides authentication and message integrity services. SSL is used widely for secure communication to a Web server, and also for wireless authentication.

SSL certificates identify the EDS3000PR to peers and are used with some methods of wireless authentication. Provide a name at upload time to identify certificates on the EDS3000PR.

You can upload Certificate and Private key combinations, obtained from an external Certificate Authority (CA), to the EDS3000PR. The EDS3000PR can also generate self-signed certificates with associated private keys.

### Credentials

The EDS3000PR can generate self-signed certificates and their associated keys for both RSA and DSA certificate formats. When you generate certificates, assign them a credential name to help identify them on the EDS3000PR. Once you create your credentials, then configure them with the desired certificates.

## To Create a New Credential

### Using Web Manager

1. In Web Manager, click the **Administration** tab in the header.
2. Click **SSL**.
3. Click **Credentials**.
4. Type the name for your credential in the **Create new credential** field.
5. Click **Submit**. The new SSL credential appears in the list.

**Using the CLI**

- ◆ To enter the SSL command level: `enable > ssl`

**Using XML**

- ◆ Include in your file: `<configgroup name="ssl"`

**To Delete a Credential****Using Web Manager**

1. In the Web Manager, click the **Administration** tab.
2. Click **SSL**.
3. Click **Credentials**.
4. Click **X** beside the existing credential you wish to delete.
5. To confirm the delete, click **OK**.

**Using CLI**

- ◆ To enter the SSL command level: `enable > ssl`

**Using XML**

- ◆ Include in your file: `<configgroup name="ssl"`

**Table 9-31 SSL Credential - Upload Certificate**

Upload Certificate Settings	Description
<b>New Certificate</b>	Click the <b>Choose File</b> button to browse to the SSL certificate to be uploaded. RSA or DSA certificates are allowed.
<b>New Certificate Type</b>	Select the certificate type to upload: <ul style="list-style-type: none"> <li>◆ PEM</li> <li>◆ PKCS7</li> <li>◆ PKCS12</li> </ul>
<b>New Private Key</b>	Click the <b>Choose File</b> button to browse to the SSL private key to be uploaded. The key must belong to the entered certificate.
<b>New Key Type</b>	Select the key type being uploaded: <ul style="list-style-type: none"> <li>◆ PEM</li> <li>◆ Encrypted PEM</li> <li>◆ PKCS12</li> </ul>
<b>Submit (button)</b>	Click the <b>Submit</b> button to enter the settings. The <b>Submit</b> button appears when new settings are entered.

**Table 9-32 SSL Credential - Create New Self-Signed Certificate**

Field	Description
<b>Country (2 Letter code)</b>	Enter the 2 letter code for the country where the organization is located. This is a two-letter ISO code (e.g., "US" for the United States).
<b>State/Province</b>	Enter the state or province where the organization is located.

Field	Description
<b>Locality (City)</b>	Enter the city where the organization is located.
<b>Organization</b>	Enter the organization name to which the EDS3000PR belongs.
<b>Organization Unit</b>	Enter the organization unit which specifies the department or organization to which the EDS3000PR belongs.
<b>Common Name</b>	Enter a network name for the EDS3000PR when installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the EDS3000PR with a web browser without the prefix <code>http://</code> . In case the name given here and the actual network name differ, the browser will pop up a security warning when the EDS3000PR is accessed using HTTPS.
<b>Expires</b>	Type the date that the self-signed certificate expires in <b>mm/dd/yyyy</b> format.
<b>Type</b>	Select <b>RSA</b> , <b>DSA</b> , or <b>ECDSA</b> .
<b>Key length</b>	Select the key length: <ul style="list-style-type: none"> <li>◆ 512</li> <li>◆ 768</li> <li>◆ 1024</li> <li>◆ 2048</li> <li>◆ 4096</li> </ul>
<b>ECDSA curve</b>	Select the ECDSA curve: <ul style="list-style-type: none"> <li>◆ 256 bit</li> <li>◆ 384 bit</li> <li>◆ 521 bit</li> </ul>

## To Configure an SSL Credential to Use an Uploaded Certificate

1. In the Web Manager, click the **Administration** tab.
  2. Click **SSL**.
  3. Click **Credentials**.
  4. Under the **View or Edit** heading, click the credential that you want to modify to access the information page for that credential.
  5. To upload a **New Certificate** to assign to the credential, click **Choose File** beside **New Certificate**, locate the valid certificate, then double-click the file to select it.
  6. Identify the **New Certificate Type** selected.
    - ◆ If you select SSL authority, RSA, or DSA certificates, select **PEM** or **PKCS7**.
    - ◆ If the Web Manager determines that the certificate is an Authority Certificate type, the New Certificate Type field updates to **PKCS12** automatically. For PKCS12 certificates, enter a password.
- Note:** Ensure that the certificate is formatted properly with a valid open and close tag. Also ensure that the Private Key is associated to the selected certificate and that it is formatted properly with a valid open and close tag.
7. To locate the associated valid **New Private Key** for this certificate, click **Choose File** to browse to and select the file.
  8. Select the **New Key Type** from the drop-down menu.
  9. Click **Submit**.

## To Configure an SSL Credential to Use a Self-Signed Certificate

1. In the Web Manager, click the **Administration** tab.
2. Click **SSL**.
3. Click **Credentials**.
4. Under **View or Edit**, click the credential you wish to modify to access the information page for that credential.
5. Enter the details for a new self-signed certificate for this credential. Reference [Table 9-32 SSL Credential - Create New Self-Signed Certificate on page 65](#).
6. Click **Submit**. The process to create a self-signed certificate can take up to 30 seconds, depending on the length of the key.

## Trusted Authorities

One or more authority certificates are used to verify the identity of a peer. Authority certificates are used with some wireless authentication methods. These certificates do not require a private key.

**Table 9-33 SSL Trusted Authority**

Trusted Authorities Settings	Description
<b>Authority</b>	Click the <b>Choose File</b> button to browse to an existing SSL authority certificate. RSA or DSA certificates are allowed.  The format of the authority certificate can be PEM or PKCS7. PEM files must start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----". Some certificate authorities add comments before and/or after these lines. Those comments must be deleted before upload.
<b>New Certificate Type</b>	Select the certificate type through the drop-down list.  This field may automatically update, depending upon extension of the certificate entered.
<b>Delete All</b>	To delete all existing certificate authorities as listed, click the <b>Delete ALL</b> button.
<b>Delete</b>	To delete an existing certificate authority, click the <b>Delete</b> button beside the specific authority listed under <b>Current Certificate Authorities</b> .

## To Upload an Authority Certificate

You can upload SSL authority, RSA, or DSA certificates.

### To upload a trusted authority certificate:

1. In the Web Manager, click the **Administration** tab.
2. Click **SSL**.
3. Click **Trusted Authorities**.
4. Click **Choose File** to browse to and select an authority certificate.
5. Select the **New Certificate Type** from the drop-down window:
  - ◆ If you select SSL authority, RSA, or DSA certificates, select **PEM** or **PKCS7**.
  - ◆ If the Web Manager determines that the certificate is an authority certificate type, the field updates to **PKCS12** automatically. For PKCS12 certificates, type a **Password**.

**Notes:**

- ◆ Ensure that the certificate is formatted properly with a valid open and close tag.
- ◆ Ensure that the Private Key is associated to the selected certificate and that it is formatted properly with a valid open and close tag.
- ◆ If the New Certificate field is set to **None**, the certificate is not supported.

6. Click **Submit**.

## CSR (Certificate Signing Request)

The EDS3000PR uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the EDS3000PR has to expose its identity to a client using a cryptographic certificate. Upon leaving the factory this certificate and the underlying secret key is the same for all EDS3000PR devices and will not match the network configuration where it is installed. The certificate's underlying secret key is also used for securing the SSL handshake. Leaving the default certificate unmodified is all right in most circumstances and is necessary only if the network facility is vulnerable to man-in-the-middle attacks.

It is possible to generate and install a new base64 encoded x.509 certificate that is unique for a particular EDS3000PR unit. The EDS3000PR is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA).

To create and install an SSL certificate, perform the following steps.

1. On the **Administration** page, click **SSL > CSR (Certificate Signing Request)**. The Certificate Signing Request page displays.
2. Modify the following fields:

**Table 9-34 SSL CSR (Certificate Signing Request)**

Field	Description
<b>Country (2 Letter code)</b>	Enter the two-letter ISO code (e.g., US for the United States) for the country where the organization is located.
<b>State/Province</b>	Enter the state or province where the organization is located.
<b>Locality (City)</b>	Enter the city where the organization is located.
<b>Organization</b>	Enter the organization name to which the EDS3000PR belongs.
<b>Organization Unit</b>	Enter the department within the organization to which the EDS3000PR belongs.
<b>Common Name</b>	Enter the network name of the EDS3000PR once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the EDS3000PR with a web browser without the prefix http://. In case the name given here and the actual network name differ, the browser will pop up a security warning when the EDS3000PR is accessed using HTTPS.
<b>Key length</b>	Select the key length of <b>2048</b> or <b>4096</b> .

3. Click **Submit** to initiate the Certificate Signing Request generation. After a few moments, the CSR file created will appear.
4. Click the CSR file to download it if desired.



## Syslog

The system log (Syslog) provides information that shows the current configuration and statistics of the Syslog. You can configure the Syslog host and set the severity level for events to log.

**Note:** The system log is saved to local storage, but is not retained through reboots unless diagnostics logging to the file system is enabled. To allow the administrator to save the complete system log, save the system log to a server that supports remote logging services. For details, refer to RFC 3164. The default port is 514.

**Table 9-35 Syslog**

Field	Description
<b>State</b>	Enable or disable the Syslog.
<b>Host</b>	Enter the IP address of the remote server that stores the logs.
<b>Remote Port</b>	Enter the port number for the remote host that supports logging services. The default port is 514.
<b>Local Port</b>	Enter the local port to use for Syslog.
<b>Severity Log Level</b>	Enter the department within the organization to which the EDS3000PR belongs.
<b>Common Name</b>	Select the minimum level message type that should be logged.
<b>Submit (button)</b>	Click the <b>Submit</b> button to enter the settings. The <b>Submit</b> button appears when new settings are entered.

### To Configure Syslog Settings

#### Using Web Manager

- ◆ In the Web Manager, click the **Administration** tab and then click **Syslog** in the menu.

#### Using CLI

- ◆ To enter the Syslog command level: `enable > configure > syslog`

#### Using XML

- ◆ Include in your file: `<configgroup name="syslog"`

## System

The EDS3000PR settings allow for reboot, restoring factory defaults, uploading new firmware and updating a system's reboot schedule, short name, and long name.

**Note:** Anytime you reboot the unit, this operation will take some time to complete. Please wait a minimum of 10-20 seconds after rebooting the unit before attempting to make any subsequent connections.

Table 9-36 System Settings

System Settings	Description
<b>State</b>	<p>Select to enable or disable the reboot schedule.</p> <p><b>Warning:</b> Use extreme caution when using scheduled reboots. The EDS3000PR will automatically reboot as scheduled. Any configuration changes not saved to flash memory will be lost. CLI/Web sessions and network traffic will be interrupted. To avoid frequent reboots, device will not be rebooted if it was started or configured less than 30 minutes from the current date/time.</p>
<b>Schedule</b>	Select the reboot schedule interval: <b>Daily</b> or <b>Interval</b>
<b>Time (24 hour)</b>	<p>Set the time to reboot by selecting the <b>Hour</b> and <b>Min</b> (Minute) in the drop-down menus.</p> <p><b>Note:</b> This configuration option appears when the <b>Daily</b> schedule is selected.</p>
<b>Interval</b>	<p>Enter the interval number in the field. Then select the type of interval from the drop-down menu:</p> <ul style="list-style-type: none"> <li>◆ Hours</li> <li>◆ Days</li> <li>◆ Weeks</li> <li>◆ Months</li> </ul> <p><b>Note:</b> This configuration option appears when the <b>Interval</b> schedule is selected.</p>
<b>Submit (button)</b>	Click the <b>Submit</b> button after settings are made in the above Reboot Schedule fields.
<b>Reboot Device</b>	<p>Click the <b>Reboot</b> button to reboot the EDS3000PR. When rebooted, your browser should be refreshed and redirected to the main status page after 30 seconds.</p> <p><b>Note:</b> The redirect will not work as expected if the IP Address of the EDS3000PR changes after reboot.</p>
<b>Restore Factory Defaults</b>	Click the <b>Factory Defaults</b> button to restore the EDS3000PR to the original factory settings. All configuration will be lost. The EDS3000PR automatically reboots upon setting back to the defaults. After setting the configuration back to the factory defaults, the device will automatically be rebooted.
<b>Reset to Defaults CP</b>	Choose to enable or disable reset to factory default function via the CP that may be accessible to walk-up users.
<b>Upload New Firmware</b>	<p>Click <b>Choose File</b> to browse to and select the firmware file. If Secure Boot is enabled, only authorized software is allowed to run on the EDS3000PR. Secure Boot requires that the firmware is signed by Lantronix or the authorized OEM. To check if Secure Boot is enabled, click <b>Status</b> in the header and check the status of Secure Boot under Device. Uploading new firmware writes the new firmware file to firmware.rom on the EDS3000PR. The gateway automatically reboots upon the installation of new firmware. See the section <a href="#">FTP on page 50</a>.</p> <p><b>Caution:</b> Do not to power off or reset the EDS3000PR while uploading new firmware. Once the upload has completed and the new firmware has been verified and flashed to memory, the EDS3000PR will automatically be rebooted.</p>
<b>Short Name</b>	Enter a short name for the system name. A maximum of 32 characters is allowed.
<b>Long Name</b>	Enter a long name for the system name. A maximum of 64 characters is allowed.

## To access System settings:

### Using Web Manager

- ◆ To access System settings with options to set up a reboot schedule, reboot, restore factory defaults, upload new firmware, reboot the standalone firmware installer, update the system name (long or short names) or to view the current configuration, on the **Administration** page, click **System**.

### Using the CLI

- ◆ To reboot or restore factory defaults, enter the System command level: `enable`
- ◆ To setup a reboot schedule, update the system name (long or short names), enter the Device command level: `enable > device`

### Using XML

- ◆ Include in your file: `<configgroup name="xml import control">`
- ◆ Include in your file: `<configgroup name="reboot schedule">`
- ◆ Include in your file: `<configgroup name="device">`

## Terminal

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.

**Table 9-37 Terminal on Network and Line Settings**

Terminal on Network and Line Settings	Description
<b>Terminal Type</b>	Enter text to describe the type of terminal. The text will be sent to a host via IAC. <i>Note:</i> IAC means, "interpret as command." It is a way to send commands over the network such as <b>send break</b> or <b>start echoing</b> . IAC is only supported in Telnet.
<b>Login Connect Menu</b>	Select the interface to display when the user logs in. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = shows the Login Connect Menu.</li> <li>◆ <b>Disabled</b> = shows the CLI (default)</li> </ul>
<b>Exit Connect Menu</b>	Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = a choice allows the user to exit to the CLI.</li> <li>◆ <b>Disabled</b> = there is no exit to the CLI (default)</li> </ul>
<b>Send Break</b>	Enter the Send Break control character received from the network on its way to a serial line which would cause the line output to be forced inactive. Example setting: <code>&lt;Ctrl&gt; Y</code> Blank the field to set to <code>&lt;None&gt;</code> . <i>Note:</i> This field is not available for terminal network configuration.
<b>Break Duration</b>	Specify the length in milliseconds of the spacing condition placed on the line when a break is sent. <i>Note:</i> This field is not available for terminal network configuration.

Terminal on Network and Line Settings	Description
<b>Echo</b>	<p>Select whether to enable echo:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b></li> <li>◆ <b>Disabled</b></li> </ul> <p><i><b>Note:</b> Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable <b>Echo</b> if your terminal echoes, in which case you will see double of each character typed. Default is enabled.</i></p>

## To Configure the Terminal Network Connection

### Using Web Manager

- ◆ To configure the Terminal on Network, on the **Administration** page, click **Terminal** and then select **Network** from the **Select Terminal on** drop-down list at the top.

### Using the CLI

- ◆ To enter the Terminal Network command level: `enable > config > terminal network`

### Using XML

- ◆ Include in your file: `<configgroup name="terminal" instance="network">`

## To Configure the Terminal Line

**Note:** The following section describes the steps to view and configure terminal line 1 settings; these steps apply to terminal line 2 and terminal line 3 of the EDS3000PR.

### Using Web Manager

- ◆ To configure a particular Terminal Line, on the **Administration** page, click **Terminal** and then select a line from the **Select Terminal on** drop-down list at the top..

### Using the CLI

- ◆ To enter the Terminal Line command level: `enable > config > terminal <number>`

### Using XML

- ◆ Include in your file: `<configgroup name="terminal" instance="<number>">`

## Tunnel

Tunneling allows serial devices to communicate over a network without 'being aware' of the devices that establish the network connection between them. Tunneling parameters are configured using the Tunnel menu and submenus. The Tunnel settings allow you to configure how the Serial-Network tunneling operates. Tunneling is available on all serial lines. The connections on one serial line are separate from these on another serial port.

### Tunnel Statistics

Tunnel statistics contains data counters, error counters, connection time, and connection information. Statistics are available at each individual connection and aggregated across all connections.

## To View Tunnel Statistics

### Using Web Manager

- ◆ To view statistics for a specific tunnel, on the **Administration** page, click **Tunnel > Statistics** and then select a tunnel number from the **Select Tunnel** drop-down list at the top.

### Using the CLI

- ◆ To view tunnel statistics: `enable > tunnel <number>, show statistics`

### Using XML

- ◆ Include in your file: `<statusgroup name="tunnel" instance="<number>">`

## Serial Settings

These serial settings for the tunnel apply to the Serial Line interface. The Line Settings and Protocol are displayed for informational purposes and must be configured from the Line settings.

**Table 9-38 Tunnel Serial Settings**

Terminal Serial Settings	Description
Line Settings	Line Settings information here is display only. Go to the section, <a href="#">To Configure the Terminal Line</a> to modify these settings.
Protocol	Protocol information here is display only. Go to the section, <a href="#">To Configure the Terminal Line</a> to modify these settings.
DTR	Select the conditions in which the Data Terminal Ready (DTR) control signal on the serial line are asserted. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Unasserted</b></li> <li>◆ <b>TruPort</b> = the DTR is 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.</li> <li>◆ <b>Asserted while connected</b> = the DTR is asserted whenever either a connect or an accept mode tunnel connection is active.</li> <li>◆ <b>Continuously asserted</b></li> </ul>

## To Configure Tunnel Serial Settings

### Using Web Manager

- ◆ To configure the Serial Settings for a specific tunnel, on the **Administration** page, click **Tunnel > Serial Settings** and then select a tunnel number from the **Select Tunnel** drop-down list at the top.

### Using the CLI

- ◆ To enter the tunnel command level: `enable > tunnel <number> > serial`

### Using XML

- ◆ Include in your file: `<configgroup name="tunnel serial" instance="<number>">`

## Packing Mode

With Packing, data from the serial Line is not sent over the network immediately. Instead, data is queued and sent in segments, when either the timeout or byte threshold is reached. Packing applies to both Accept and Connect Modes.

**Table 9-39 Tunnel Packing Mode Settings**

Tunnel Packing Mode Settings	Description
<b>Mode</b>	Configure the Tunnel Packing Mode. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Disable</b> = Data not packed.</li> <li>◆ <b>Timeout</b> = data sent after timeout occurs.</li> <li>◆ <b>Send Character</b> = data sent when the Send Character is read on the Serial Line.</li> </ul>
<b>Threshold</b>	Set the threshold (byte count). If the received serial data reaches this threshold, then the data will be sent on the network. Valid range is 100 to 1450 bytes. Default is 512.  <i>Note: This configuration option appears when Timeout mode or Send Character mode is selected.</i>
<b>Timeout</b>	Set the timeout value, in milliseconds, after the first character is received on the serial line, before data is sent on the network. Valid range is 1 to 30000 milliseconds. Default is 1000. This setting becomes available when the Timeout mode is selected.  <i>Note: This configuration option appears when Timeout mode is selected.</i>
<b>Send Character</b>	Enter Control Characters in any of the following forms: <ul style="list-style-type: none"> <li>◆ &lt;control&gt;J</li> <li>◆ 0xA (hexadecimal)</li> <li>◆ \10 (decimal)</li> </ul> If used, the Send Character is a single printable character or a control character that, when read on the Serial Line, forces the queued data to be sent on the network immediately.  <i>Note: This configuration option appears when Send Character mode is selected.</i>
<b>Trailing Character</b>	Enter Control Characters in any of the following forms: <ul style="list-style-type: none"> <li>◆ &lt;control&gt;J</li> <li>◆ 0xA (hexadecimal)</li> <li>◆ \10 (decimal).</li> </ul> If used, the Trailing Character is a single printable character or a control character that is injected into the outgoing data stream right after the Send Character. Disable the Trailing Character by blanking the field (setting it to <None>).  <i>Note: This configuration option appears when Send Character mode is selected.</i>

## To Configure Tunnel Packing Mode Settings

### Using Web Manager

- ◆ To configure the Packing Mode for a specific tunnel, on the **Administration** page, click **Tunnel > Packing Mode** and then select a tunnel number from the **Select Tunnel** drop-down list at the top.

### Using the CLI

- ◆ To enter the Tunnel Packing command level: `enable > tunnel <number> > packing`

### Using XML

- ◆ Include in your file: `<configgroup name="tunnel packing" instance="<number>">`

## Accept Mode

In Accept Mode, the EDS3000PR listens (waits) for incoming connections from the network. A remote node on the network initiates the connection. The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. Supported serial lines and associated local port numbers progress sequentially in matching value. For instance, the default local port is 10001 for serial line 1 and the default local port for serial line 2 is 10002, and so on for the number of serial lines supported. Serial data can still be received while waiting for a network connection, keeping in mind serial data buffer limitations.

**Table 9-40 Tunnel Accept Mode Settings**

Tunnel Accept Mode Settings	Description
<b>Mode</b>	Set the method used to start a tunnel in Accept mode. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Disable</b> = do not accept an incoming connection.</li> <li>◆ <b>Always</b> = accept an incoming connection (<i>default</i>).</li> <li>◆ <b>Any Character</b> = start waiting for an incoming connection when any character is read on the serial line.</li> <li>◆ <b>Start Character</b> = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line.</li> <li>◆ <b>Modem Control Asserted</b> = 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.</li> <li>◆ <b>Modem Emulation</b> = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.</li> </ul>
<b>Local Port</b>	Set the port number for use as the network local port. The default local port number for each supported serial line number progresses sequentially in equal value so that Tunnel X: 1000X. For example: <ul style="list-style-type: none"> <li>◆ Tunnel 1: 10001</li> <li>◆ Tunnel 2: 10002</li> </ul>
<b>Protocol</b>	Select the protocol type for use with Accept Mode: <ul style="list-style-type: none"> <li>◆ SSH</li> <li>◆ SSL</li> <li>◆ TCP (default protocol)</li> <li>◆ TCP AES</li> <li>◆ Telnet</li> </ul>
<b>TCP Keep Alive</b>	Enter the time, in milliseconds, the EDS3000PR waits during a silent TCP connection before the first Keep Alive probe is sent to the remote host in order to keep the TCP connection up during idle transfer periods. Set to 0 to disable TCP Keep Alive, and blank the field to restore the default.
<b>TCP Keep Alive Interval</b>	Enter the time, in milliseconds, to wait between Keep Alive probes in order to keep the TCP connection up during idle transfer periods. Blank the display field to restore the default.

Tunnel Accept Mode Settings (continued)	Description
<b>TCP Keep Alive Probes</b>	Enter the number of TCP Keep Alive probes to send before closing the connection if no response is received. The probes are sent after the initial TCP Keep Alive probe is sent. Valid values are between 1 and 16. Blank the field to restore the default.
<b>Initial Send</b>	<p>Enter the <b>Initial Send</b> data to be sent out the network upon connection establishment before any data from the Line. It may contain one or more <b>Directives</b> of the form %&lt;char&gt;.</p> <p>The Initial Send string can be entered in <b>Text</b> or <b>Binary</b> form. The Binary form allows square braces [ ] to enclose one or more character designations separated by commas. Use straight decimal numbers up to 255 or hexadecimal numbers prefixed with 0x up to 0xFF within the square braces. To specify an open brace in binary mode, use two in a row. Example (in Binary mode): AB [255, 0xFF] C [ [D] Results in a string containing binary values where the dots appear: AB · · C [D]</p> <p><b>Directives</b></p> <ul style="list-style-type: none"> <li>◆ %i local IP address</li> <li>◆ %m MAC address</li> <li>◆ %n network interface name</li> <li>◆ %p local port</li> <li>◆ %s serial number</li> <li>◆ %% %</li> </ul>
<b>Flush Serial</b>	<p>Set whether the serial line data buffer is flushed upon a new network connection. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = serial data buffer is flushed on network connection</li> <li>◆ <b>Disabled</b> = serial data buffer is not flushed on network connection (<i>default</i>)</li> </ul>
<b>Block Serial</b>	<p>Set whether Block Serial is enabled for debugging purposes. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = if Enabled, incoming characters from the serial line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the serial line if hardware or software flow control is configured.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.</li> </ul>
<b>Block Network</b>	<p>Set whether Block Network is enabled for debugging purposes. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = if Enabled, incoming characters from the network will not be forwarded to the Serial Line. Instead, they will be buffered and will eventually flow off the network side.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.</li> </ul>
<b>Password</b>	<p>Enter a password. This password can be up to 31 characters in length and must contain only alphanumeric characters and punctuation. When set, clients must send the correct password string to the unit within 30 seconds from opening network connection in order to enable data transmission. The password sent to the unit must be terminated with one of the following:</p> <ul style="list-style-type: none"> <li>◆ 0A (Line Feed)</li> <li>◆ 00 (Null)</li> <li>◆ 0D 0A (Carriage Return/Line Feed)</li> <li>◆ 0D 00 (Carriage Return/Null)</li> </ul> <p>If, <b>Prompt for Password</b> is set to <b>Enabled</b> and a password is provided, the user will be prompted for the password upon connection.</p>



Tunnel Accept Mode Settings (continued)	Description
Email on Connect	Select an email profile number to which an email notification will be sent upon the establishment of an accept mode tunnel.
Email on Disconnect	Select an email profile number to which an email notification will be sent upon the disconnection of an accept mode tunnel.

## To Configure Tunnel Accept Mode Settings

### Using Web Manager

- ◆ To configure the Accept Mode for a specific tunnel, on the **Administration** page, click **Tunnel > Accept Mode** and then select a tunnel number from the **Select Tunnel** drop-down list at the top.

### Using the CLI

- ◆ To enter Tunnel Accept Mode command level: `enable > tunnel <number> > accept`

### Using XML

- ◆ Include in your file: `<configgroup name="tunnel accept" instance="<number>">`

## Connect Mode

In Connect Mode, the EDS3000PR continues to attempt an outgoing connection on the network until established (based on which connection method is selected in the configuration described in [Table 9-41](#)). If the connection attempt fails or the connection drops, then it retries after a timeout. The remote node on the network must listen for the Connect Mode's connection.

For Connect Mode to function, it must be enabled, have a remote station (node) configured, and a remote port configured (TCP or UDP). When established, Connect Mode is always on. Enter the remote station as an IPv4 or IPv6 address or DNS name. The EDS3000PR will not make a connection unless it can resolve the address. For Connect Mode using UDP, the EDS3000PR accepts packets from any device on the network. It will send packets to the last device that sent it packets.

**Note:** *The port in Connect Mode is not the same port configured in Accept Mode. The TCP keepalive time is the time in which probes are periodically sent to the other end of the connection. This ensures the other side is still connected.*

**Table 9-41 Tunnel Connect Mode Settings**

Tunnel Connect Mode Settings	Description
<b>Mode</b>	<p>Set the method to be used to attempt a connection to a remote host or device. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Disable</b> = an outgoing connection is never attempted. (<i>default</i>)</li> <li>◆ <b>Always</b> = a connection is attempted until one is made. If the connection gets disconnected, the EDS3000PR retries until it makes a connection.</li> <li>◆ <b>Any Character</b> = a connection is attempted when any character is read on the serial line.</li> <li>◆ <b>Start Character</b> = a connection is attempted when the start character for the selected tunnel is read on the serial line.</li> <li>◆ <b>Modem Control Asserted</b> = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made.</li> <li>◆ <b>Modem Emulation</b> = a connection is attempted when triggered by modem emulation AT commands.</li> </ul>
<b>Local Port</b>	<p>Enter an alternative Local Port. The Local Port is set to &lt;Random&gt; by default but can be overridden. Blank the field to restore the default.</p>
<b>Host 1</b>	<p>Click on the displayed information to expand it for editing. Complete the Host fields that appear according to <a href="#">Table 9-42</a>.</p> <p>If &lt;None&gt; is displayed, clicking it will allow you to configure a new host. At least one Host is required to enable Connect Mode as this information is necessary to connect to that host. Once you start to edit Host 1, a box for Host 2 will show up. Editing Host 2 will cause a Host 3 box to appear. Up to 32 hosts are available.</p>
<b>Reconnect Timer</b>	<p>Set the value of the reconnect timeout (in milliseconds) for outgoing connections established by the EDS3000PR. Valid range is 1 to 65535 milliseconds. Default is 15000.</p>
<b>Flush Serial Data</b>	<p>Set whether the serial Line data buffer is flushed upon a new network connection. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = serial data buffer is flushed on network connection</li> <li>◆ <b>Disabled</b> = serial data buffer is not flushed on network connection (<i>default</i>)</li> </ul>
<b>Block Serial</b>	<p>Set whether Block Serial is enabled for debugging purposes. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = If Enabled, incoming characters from the Serial Line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the Serial Line if hardware or software flow control is configured.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.</li> </ul>
<b>Block Network</b>	<p>Set whether Block Network is enabled for debugging purposes. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = If Enabled, incoming characters from the network will not be forwarded to the Serial Line. Instead, they will be buffered and will eventually flow off the network side.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.</li> </ul>
<b>Email on Connect</b>	<p>Select an email profile number to which an email notification will be sent upon the establishment of an connect mode tunnel.</p>
<b>Email of Disconnect</b>	<p>Select an email profile number to which an email notification will be sent upon the disconnection of an connect mode tunnel.</p>

**Table 9-42 Host Settings**

Host Field	Description
<b>Address</b>	Enter the address for the remote host connection. Either a DNS address or an IP address may be provided.
<b>Port</b>	Designate the TCP or UDP port on the remote host for connection.
<b>Protocol</b>	Select the desired security protocol. Choices are SSH, SSL, TCP, TCP AES, Telnet, UDP, and UDP AES. SSH is recommended for circumstances with high security concerns. When using SSH, both the SSH server host keys and the SSH server authorized users must be configured.
<b>SSH Username</b>	Enter a Username. This configuration field becomes available when the SSH Protocol is selected.
<b>Credentials</b>	Select an existing credential from the drop-down list. This configuration field becomes available when the SSL protocol is selected. Credentials can be created, viewed or edited at the <a href="#">SSL &gt; Credentials</a> page.
<b>Validate Certificate</b>	Select to enable or disable. This configuration field becomes available when the SSL protocol is selected.
<b>TCP Keep Alive</b>	Enter the time, in milliseconds, the EDS3000PR waits during a silent TCP connection before the first Keep Alive probe is sent to the remote host in order to keep the TCP connection up during idle transfer periods. Set to 0 to disable TCP Keep Alive, and blank the field to restore the default.
<b>TCP Keep Alive Interval</b>	Enter the time, in milliseconds, to wait between Keep Alive probes in order to keep the TCP connection up during idle transfer periods. Blank the display field to restore the default.
<b>TCP Keep Alive Probes</b>	Enter the number of TCP Keep Alive probes to send before closing the connection if no response is received. The probes are sent after the initial TCP Keep Alive probe is sent. Valid values are between 1 and 16. Blank the field to restore the default.
<b>TCP User Timeout</b>	Specify the amount of time the TCP segments will be retransmitted before the connection is closed.
<b>AES Encrypt Key</b>	Enter the AES Encrypt Key and select <b>Text</b> or <b>Hexadecimal</b> to indicate format. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
<b>AES Decrypt Key</b>	Enter the AES Decrypt Key and select <b>Text</b> or <b>Hexadecimal</b> to indicate format. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
<b>Initial Send</b>	Enter the Initial Send character and select either <b>Text</b> or <b>Binary</b> format. This configuration field becomes available when the SSH, TCP, UDP, or UDP AES protocol is selected.

**Notes:**

- ◆ *If the keep alive time expires, the user timeout is expired, and there are probes in flight, the connection will be reset. For this reason, it is recommended that if keep alive is used in conjunction with the user timeout, the keep alive timeouts be larger than the user timeout. If it is smaller, what will typically be seen is that the initial probe will be sent, then at the interval where the next probe would normally be sent, the connection will be reset, with no additional probes sent. Also note that in these cases: if the keep alive timer is significantly smaller than the user timeout, probes will continue to be sent for an unreachable host until the user timeout expires.*

- ◆ *If there is data in flight when the TCP retransmission timeout kicks in, the user timeout is checked as a limiting condition only when the timer expirations would normally be checked during RTO handling. In other words, the user timeout will not be an exact limit; in practice, it will always take somewhat longer for the connection to be closed. The longer the user timeout is, the more likely it will expire between exponentially slower retransmissions, and the connection will not experience an error until the next retransmission timeout is checked. Also note that the user timeout expiration during retransmission returns an error to the application; it does not automatically reset the connection as happens with keep alive timeout. It is up to the application (e.g., tunneling) to close the connection (this happens almost immediately with tunneling).*

## To Configure Tunnel Connect Mode Settings

### Using Web Manager

- ◆ To configure the Connect Mode for a specific tunnel, on the **Administration** page, click **Tunnel > Connect Mode** and then select a tunnel number from the **Select Tunnel** drop-down list at the top.

### Using the CLI

- ◆ To enter the Tunnel Connect Mode command level: `enable > tunnel <number> > connect`

### Using XML

- ◆ Include in your file: `<configgroup name="tunnel connect" instance="<number>">`

## 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 the EDS3000PR, the Connect Mode supports up to 32 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 80](#)). Sequential is the default Host Mode.
- ◆ **Simultaneous** – A tunnel will connect to all hosts accepting a connection. Simultaneous connections occur at the same time to all listed hosts. The EDS3000PR can support a maximum of 64 total aggregate connections.

## 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.

## Disconnect Mode

Disconnect Mode specifies the optional conditions for disconnecting any Accept Mode or Connect Mode connection that may be established. If any of these conditions are selected but do not occur and the network disconnects to the EDS3000PR, a Connect Mode connection will attempt to reconnect. However, if none of these conditions are selected, a closure from the network is taken as a disconnected host. The gateway can support a maximum of 64 total aggregate connections.

**Table 9-43 Tunnel Disconnect Mode Settings**

Tunnel Disconnect Mode Settings	Description
<b>Stop Character</b>	Enter the Stop Character which, when received on the Serial Line, disconnects the tunnel. The Stop Character may be designated as a single printable character or as a control character. Control characters may be input in any of the following forms: <control>J or 0xA(hexadecimal) or \10 (decimal). Disable the Stop Character by blanking the field to set it to <None>.
<b>Modem Control</b>	Set whether Modem Control enables disconnect when the Modem Control pin is not asserted on the Serial Line. Choices are: ♦ <b>Enabled</b> ♦ <b>Disabled</b> (default)
<b>Timeout</b>	Enter the number of milliseconds a tunnel may be idle before disconnection. The value of zero disables the idle timeout.
<b>Flush Serial Data</b>	Set whether to flush the Serial Line when the Tunnel is disconnected. Choices are: ♦ <b>Enabled</b> ♦ <b>Disabled</b> (default)

## To Configure Tunnel Disconnect Mode Settings

### Using Web Manager

- ♦ To configure the Disconnect Mode for a specific tunnel, on the **Administration** page, click **Tunnel > Disconnect Mode** and then select a tunnel number from the **Select Tunnel** drop-down list at the top.

### Using the CLI

- ♦ To enter the Tunnel Disconnect command level: `enable > tunnel <number> > disconnect`

### Using XML

- ♦ Include in your file: `<configgroup name="tunnel disconnect" instance="<number>">`

## Modem Emulation

Some older equipment is designed to attach to a serial port and dial into a network with a modem. This equipment uses AT commands to control the connection. For compatibility with these older devices on modern networks, the EDS3000PR mimics the behavior of the modem.

**Table 9-44 Tunnel Modem Emulation Settings**

<b>Tunnel Modem Emulation Settings</b>	<b>Description</b>
<b>Echo Pluses</b>	Set whether the pluses will be echoed back during a "pause +++ pause" escape sequence on the Serial Line. Choices are: ◆ <b>Enabled</b> ◆ <b>Disabled</b> (default)
<b>Echo Commands</b>	Set whether characters read on the Serial Line will be echoed, while the Line is in Modem Command Mode. Choices are: ◆ <b>Enabled</b> (default) ◆ <b>Disabled</b>
<b>Verbose Response</b>	Set whether Modem Response Codes are sent out on the Serial Line. Choices are: ◆ <b>Enabled</b> (default) ◆ <b>Disabled</b>
<b>Response Type</b>	Select a representation for the Modem Response Codes sent out on the Serial Line. Choices are: ◆ <b>Text</b> (ATV1) (default) ◆ <b>Numeric</b> (ATV0)
<b>Error Unknown Commands</b>	Set whether the Error Unknown Commands is enabled (ATU0) and ERROR is returned on the Serial Line for unrecognized AT commands. Otherwise (ATU1) OK is returned for unrecognized AT commands. Choices are: ◆ <b>Enabled</b> ◆ <b>Disabled</b> (default)
<b>Incoming Connection</b>	Set how and if requests are answered after an incoming RING (ATS0=2). Choices are: ◆ <b>Disabled</b> (default) ◆ <b>Automatic</b> ◆ <b>Manual</b>
<b>Connect String</b>	Enter the customized Connect String sent to the Serial Line with the Connect Modem Response Code.
<b>Display Remote IP</b>	Set whether the Display Remote IP is enabled so that the incoming RING sent on the Serial Line is followed by the IP address of the caller. Choices are: ◆ <b>Enabled</b> ◆ <b>Disabled</b> (default)

## To Configure Tunnel Modem Emulation Settings

### Using Web Manager

- ◆ To configure the Modem Emulation for a specific tunnel, on the **Administration** page, click **Tunnel > Modem Emulation** and then select a tunnel number from the **Select Tunnel** drop-down list at the top.

### Using the CLI

- ◆ To enter the Tunnel Modem command level: `enable > tunnel <number> > modem`

### Using XML

- ◆ Include in your file: `<configgroup name="tunnel modem" instance="<number>">`

## User Management

This page displays the configuration of users. The Admin Password is used for initial login access from the Telnet port, SSH port, FTP, HTTP, and serial line.

**Table 9-45 Administrator Settings**

The Admin user can modify their username and/or password here. The Admin Username and Admin Password is used for initial login access from the Telnet port, SSH port, FTP, HTTP, or any serial Line.

Administrator Settings	Description
<b>Username</b>	View and modify the Administrator <b>Username</b> as desired. The default Username is admin.
<b>Password</b>	Modify the Administrator <b>Password</b> as desired. The default Password is the last 8 characters of the Device ID.
<b>Submit</b>	Click <b>Submit</b> to submit changes <b>Username</b> and/or <b>Password</b> . The <b>Submit</b> button appears when either or both Username and Password are modified.

**Table 9-46 Current Users List**

Users created by the original Admin user will be listed here for editing and deletion.

Current Users	Description
<b>Delete</b>	Click the check box besides a specific user to be deleted and click the <b>Submit</b> button which appears (or click Cancel to cancel the deletion). Click <b>OK</b> in the confirmation window which appears to delete indicated user.
<b>Name</b>	Name of User. Click a specific user name to edit the user information ( <b>Username</b> , <b>Password</b> , and <b>Role</b> ) on the <b>Edit User</b> page.
<b>Role</b>	The Role assigned to the user.

**Table 9-47 New User Settings**

Create new user login, password and roles here. Admin-created users can be deleted or altered in the Current Users list ([Table 9-46](#)). Up to 8 user accounts can be created to access the EDS3000PR.

New User Settings	Description
<b>Username</b>	Enter the <b>Username</b> of the new user. Must be between 4 and 15 characters.
<b>Password</b>	Enter the <b>Password</b> of the new user. Must be between 4 and 15 characters.
<b>Role</b>	Click the <b>Role</b> field to select a role for this user: <ul style="list-style-type: none"> <li>◆ Administrator</li> <li>◆ Technician</li> <li>◆ User</li> </ul>
<b>Add</b>	Click <b>Add</b> to submit the new user. Click <b>OK</b> in the confirmation window which appears to add the user.

**Table 9-48 Current Roles List**

The system-defined default roles that come with the EDS3000PR along with any Admin-created user roles are listed here. Admin-created custom roles can be deleted or altered.

Current Role	Description
<b>Delete</b>	Click the check box beside a specific custom role to be deleted and click the <b>Submit</b> button which appears (or click <b>Cancel</b> to cancel the deletion). Click <b>OK</b> in the confirmation window which appears to delete indicated user.
<b>Name</b>	Name of Role. Click a specific custom role to edit the role information ( <b>Role</b> , <b>Configuration Groups</b> , and <b>Actions</b> ) on the <b>Edit Role</b> page. <b>Administrator</b> , <b>Technician</b> and <b>User</b> roles are system-defined and cannot be deleted or altered.
<b>Configuration Groups</b>	Displays the <b>Configuration Groups</b> accessible by the role. Configuration Group access can be modified for custom-created roles.
<b>Actions</b>	Displays the <b>Actions</b> accessible by the role. Actions can be modified for custom-created roles.

**Table 9-49 New Role Settings**

Create a custom role here. Admin-created custom roles can be deleted or altered in the Current Roles list ([Table 9-48](#)). Up to 8 custom roles can be created.

New Role Settings	Description																																							
Name	Enter the name of a new role to be created.																																							
Actions	Check the <b>Actions</b> that the new role will have access to, if any: <ul style="list-style-type: none"><li>◆ Device Reboot</li><li>◆ Factory Reset</li><li>◆ Firmware Upgrade</li></ul>																																							
Configuration Groups	Check the Configuration Groups the new role will have access to configuring, if any: <table><tr><td>◆ ARP</td><td>◆ HTTP</td><td>◆ SSH server</td></tr><tr><td>◆ CLI</td><td>◆ ICMP</td><td>◆ SSL</td></tr><tr><td>◆ Clock</td><td>◆ Interface</td><td>◆ Syslog</td></tr><tr><td>◆ CP Functions</td><td>◆ IP</td><td>◆ Telnet</td></tr><tr><td>◆ Device</td><td>◆ Line</td><td>◆ Terminal</td></tr><tr><td>◆ Diagnostics</td><td>◆ Reboot schedule</td><td>◆ Tunnel Accept</td></tr><tr><td>◆ Discovery</td><td>◆ RSS</td><td>◆ Tunnel Connect</td></tr><tr><td>◆ Email</td><td>◆ Serial Command Mode</td><td>◆ Tunnel Disconnect</td></tr><tr><td>◆ Wired Network</td><td>◆ SMTP</td><td>◆ Tunnel Modem</td></tr><tr><td>◆ Filesystem</td><td>◆ SNMP</td><td>◆ Tunnel Packing</td></tr><tr><td>◆ FTP Server</td><td>◆ SSH</td><td>◆ Tunnel Serial</td></tr><tr><td>◆ Host</td><td>◆ SSH client</td><td>◆ User Management</td></tr><tr><td>◆ HTTP Authentication</td><td></td><td></td></tr></table>	◆ ARP	◆ HTTP	◆ SSH server	◆ CLI	◆ ICMP	◆ SSL	◆ Clock	◆ Interface	◆ Syslog	◆ CP Functions	◆ IP	◆ Telnet	◆ Device	◆ Line	◆ Terminal	◆ Diagnostics	◆ Reboot schedule	◆ Tunnel Accept	◆ Discovery	◆ RSS	◆ Tunnel Connect	◆ Email	◆ Serial Command Mode	◆ Tunnel Disconnect	◆ Wired Network	◆ SMTP	◆ Tunnel Modem	◆ Filesystem	◆ SNMP	◆ Tunnel Packing	◆ FTP Server	◆ SSH	◆ Tunnel Serial	◆ Host	◆ SSH client	◆ User Management	◆ HTTP Authentication		
◆ ARP	◆ HTTP	◆ SSH server																																						
◆ CLI	◆ ICMP	◆ SSL																																						
◆ Clock	◆ Interface	◆ Syslog																																						
◆ CP Functions	◆ IP	◆ Telnet																																						
◆ Device	◆ Line	◆ Terminal																																						
◆ Diagnostics	◆ Reboot schedule	◆ Tunnel Accept																																						
◆ Discovery	◆ RSS	◆ Tunnel Connect																																						
◆ Email	◆ Serial Command Mode	◆ Tunnel Disconnect																																						
◆ Wired Network	◆ SMTP	◆ Tunnel Modem																																						
◆ Filesystem	◆ SNMP	◆ Tunnel Packing																																						
◆ FTP Server	◆ SSH	◆ Tunnel Serial																																						
◆ Host	◆ SSH client	◆ User Management																																						
◆ HTTP Authentication																																								
Add	Click <b>Add</b> to submit the new role. Click <b>OK</b> in the confirmation window which appears to add the role.																																							

## To Configure User Management

### Using Web Manager

- ◆ To configure User Management, on the **Administration** page, click **User Management**.

### Using the CLI

- ◆ To enter the User Management command level: `enable > config > user management`



### Using XML

Include in your file: `<configgroup name="user management">`

## XML

This page is used to clone the current system configuration. The generated file can be imported at a later time to restore the configuration.

**Caution:** *The 'User Management', 'HTTP Authentication', and SSL groups must be imported with secrets manually filled in (e.g., passwords and private key) before import.*

The exported file can be modified and imported to update the configuration on this EDS3000PR or another.

XML records can also be exported to browser window or to a download link on the EDS3000PR.

Notice that by default, all Groups to Export are checked except some pertaining to the network configuration; this is so that if you later 'paste' the entire clone configuration, it will not break your network connectivity. You may check or uncheck any group to include or omit that group from export.

Selection of Lines to Export filters instances to be exported are in the line, relay, serial, terminal, and groups.

### To Export Configuration

By default, all settings groups are checked.

#### Using Web Manager

1. In the Web Manager, click the **Administration** tab.
2. Click **XML**.
3. Click **Export Configuration**.
4. Select where to send exported status information:
  - ◆ **Export to browser** sends the information into a separate web window which appears.
  - ◆ **Export to local file** sends information into a new locally saved file. A file name must be specified in field provided if this option is selected.
5. Select **Download (from link)** to download this content as a file, or click **Export to browser** to open a web browser with this content.
6. To include descriptive comments in the XML file, check **Comments**.
7. For **Lines to Export**, check the lines and/or the network that you want to export to the XML configuration file.
  - ◆ Clicking the **Clear All** button will uncheck all checkboxes.
  - ◆ Clicking the **Select All** button will check all checkboxes.
8. Click the desired **Groups to Export**. Several checkboxes are available.
  - ◆ Clicking the **Clear All** button will uncheck all checkboxes.

- ◆ Clicking the **Select All but Networking** button will check all checkboxes except `Interface:etho`.

**Note:** Ensure that the group list is comma delimited and encased in double-quotes. To view the list of available groups, use the **xcr list** command.

#### 9. Click **Export**.

**Note:** Though keys are not exported with XML objects and variables, there is a placeholder value included in the XML variable that would need to be populated with the correct key value when using an exported configuration for an import operation.

#### Using the CLI

- ◆ To enter the XML command level: `enable > xml`

#### Using XML

- ◆ Include in your file: `<configgroup name="xml">`

### To Export Status

You can export the current status in XML format. By default, all groups are exported, or you can select a subset of groups to export.

#### Using Web Manager

1. In the Web Manager, click the **Administration** tab.
2. Click **XML**.
3. Click **Export Status**.
4. Select where to send exported status information:
  - ◆ **Export to browser** sends the information into a separate web window which appears.
  - ◆ **Export to local file** sends information into a new locally saved file. A file name must be specified in field provided if this option is selected.
5. For **Lines to Export**, check the lines and/or the network that you want to export to the XML configuration file.
  - ◆ Clicking the **Clear All** button will uncheck all checkboxes.
  - ◆ Clicking the **Select All** button will check all checkboxes.
6. Click the desired **Groups to Export**. Several checkboxes are available.
  - ◆ Clicking the **Clear All** button will uncheck all checkboxes.
  - ◆ Clicking the **Select All** button will check all checkboxes.

#### Notes:

- ◆ Ensure that the group list is comma delimited and encased in double-quotes.
- ◆ To view the list of available groups, use the **xcr list** command.

#### 7. Click **Export**.

#### Using the CLI

- ◆ To enter the XML command level: `enable > xml`

### Using XML

- ◆ Include in your file: `<configgroup name="xml">`

### To Import Configuration

To import system XML configuration file that you saved previously, use Import Configuration.

### Using Web Manager

1. In the Web Manager, click the **Administration** tab.
2. Click **XML**.
3. Click **Import Configuration**.
4. Select where to import configuration information:
  - ◆ **Configuration from External file** picks up all the settings from the external file. For this option, click **Choose File** to locate and select the XML configuration file that you wish to import. The name of the file will appear in the Web Manager screen. Click **Import**.
  - ◆ **Configuration from Filesystem** picks up settings from the selected Groups, Lines and Instances. Make selections in form which appears (see [Table 9-50](#)) and click **Import**.
  - ◆ **Line(s) from single line Settings on the Filesystem** copies lines settings from an the input file containing only one Line instance to all of the selected Lines. Make selections in form which appears (see [Table 9-51](#)) and click **Import**.

### Using the CLI

- ◆ To enter the XML command level: `enable > xml`

### Using XML

- ◆ Include in your file: `<configgroup name="xml import control">`

**Table 9-50 Configuration from Filesystem**

Setting	Description
<b>Filename</b>	Enter the name of the file on the EDS3000PR (local to its filesystem) that contains XCR data.
<b>Lines to Import</b>	Select filter instances to be imported in the line, serial, tunnel and terminal groups. This affects both Whole Groups to Import and Text List selections. Click <b>Clear All</b> to clear all checkmarks, or <b>Select All</b> to check all checkmarks.
<b>Whole Groups to Import</b>	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group. Click <b>Clear All</b> to clear all checkmarks, or <b>Select All but Networking</b> to check all checkmarks except Networking.
<b>Text List</b>	Enter the string to import specific instances of a group. The textual format of this string is: <code>&lt;g&gt;:&lt;i&gt;;&lt;g&gt;:&lt;i&gt;;...</code> Each group name <code>&lt;g&gt;</code> is followed by a colon and the instance value <code>&lt;i&gt;</code> and each <code>&lt;g&gt;:&lt;i&gt;</code> value is separated by a semi-colon. If a group has no instance then only the group name <code>&lt;g&gt;</code> should be specified.
<b>Import (button)</b>	Click the <b>Import</b> button when the Configuration from Filesystem fields are completed above.

**Table 9-51 Line(s) from single line Settings on the Filesystem**

Setting	Description
<b>Filename</b>	Enter the name of the file on the EDS3000PR (local to its filesystem) that contains XCR data.
<b>Lines to Import</b>	Select filter instances to be imported in the line, serial, tunnel and terminal groups. This affects both Whole Groups to Import and Text List selections. Click <b>Clear All</b> to clear all checkmarks, or <b>Select All</b> to check all checkmarks.
<b>Whole Groups to Import</b>	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group. Click <b>Clear All</b> to clear all checkmarks, or <b>Select All but Networking</b> to check all checkmarks except Networking.
<b>Import (button)</b>	Click the <b>Import</b> button when the Line(s) from single line Settings on the Filesystem fields are completed above.

## Appendix A: Technical Support

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

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

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

## Appendix B: Binary to Hexadecimal Conversions

Many of the unit's configuration procedures require you to assemble a series of options (represented as bits) into a complete command (represented as a byte).

The resulting binary value must be converted to a hexadecimal representation.

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

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

### Converting Binary to Hexadecimal

#### Conversion Table

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

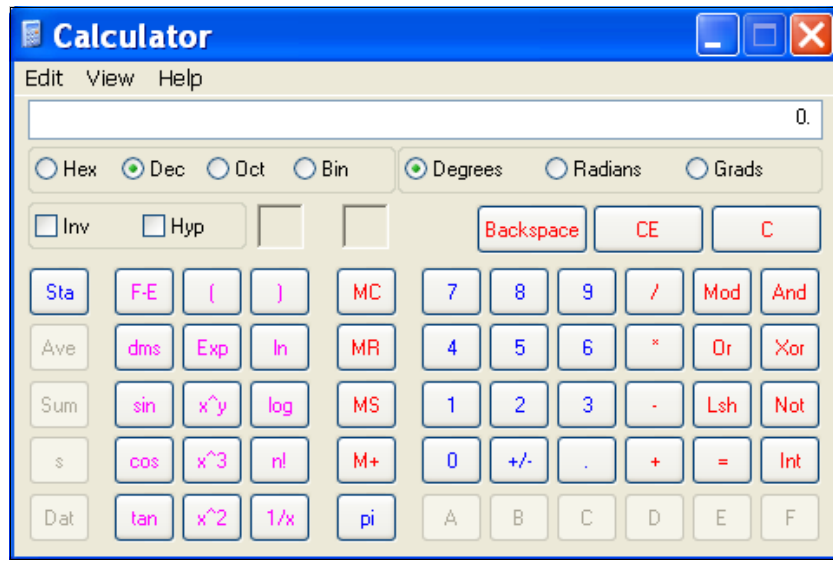
**Table B-1 Binary to Hexadecimal Conversion Table**

Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

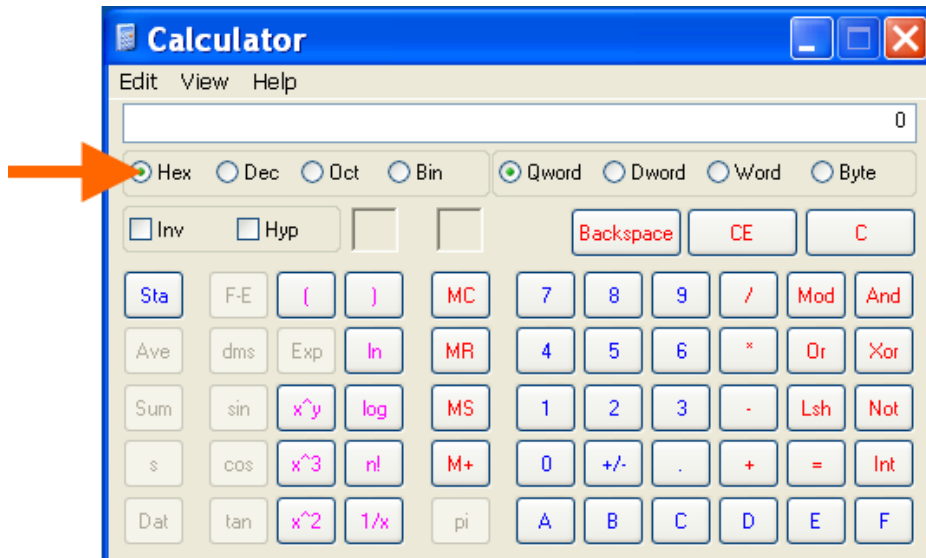
## Scientific Calculator

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, search for Calculator and run the application.
2. In versions with the View menu, select **Scientific** from the menu. In versions with the menu button in the top left, click the menu button and select **Programmer**.
3. Click **Bin** (Binary), and type the number you want to convert.



4. Click **Hex**. The hexadecimal value appears.



## Appendix C: Compliance

### EU Declaration of Conformity for EDS3008PR, 3016PR, 3032PR



#### EU DECLARATION OF CONFORMITY (DoC) No. CERT-00155

We,  
Company Name: LANTRONIX, INC.  
Postal address: 7535 Irvine Center Dr. Suite 100, Irvine, CA 92618  
Telephone number: 949 453-3990

**Declare that the DoC is issued under our sole responsibility and belongs to the following product:**

Apparatus model/Product: EDS3008PR, EDS3016PR, EDS3032PR / Ethernet Terminal and Device Server

**Object of the declaration** The product provides secure, remote management and monitoring of serial devices in a rack mount form factor. Indoor Use.

**The object of the declaration described above is in conformity with the relevant Union harmonization legislation:**

- Low Voltage Directive (LVD), 2014/35/EU
- Electromagnetic Compatibility (EMC) Directive, 2014/30/EU
- Restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS) Directive, 2011/65/EU

**The following harmonized standards and technical specifications have been applied**

**Low Voltage Directive:**

- EN 60950-1: 2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
- EN 62368-1:2014

**EMC Directive:**

**Emissions**

- EN 55024: 2010
- EN 55032:2015 + AC:2016

**Immunity**

- EN 61000-3-2:2014
- EN 61000-3-3:2013

**ROHS**

- EN 50581:2012

**Signed for and on behalf of:**

Place of Issue: Irvine, CA USA

Date of issue: 11/4/2019

Fathi Hakam, VP of Engineering:

A handwritten signature in blue ink, appearing to be "Fathi Hakam", written over a horizontal line.

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

800.526.8766

lantronix.com



## EU Declaration of Conformity for EDS3008PS, 3016PS

Planned compliance. To be updated when compliance is complete.

## Emissions and Immunity

FCC 47 CFR PART 15 SUBPART B, Class B

ICES-003 ISSUE 6:2016, Class B

VCCI-CISPR 32:2016, Class B

AS/NZS CISPR 32:2015, Class B

EN 55032:2015 + AC:2016, Class B

EN 55024:2010

EN 61000-3-2:2014

EN 61000-3-3:2013

## Safety

EN/IEC 60950-1 + A2:2013

EN/IEC 62368-1:2014 + A11:2017

UL 60950-1, 2<sup>nd</sup> Edition 2019-05-09

CAN/CSA C.22.2 No. 60950-1-07, 2<sup>nd</sup> Edition, 2014-10

UL 62368-1, 2<sup>nd</sup> Edition, 2014-12-01

CAN/CSA C22.2 No. 62368-1-14, 2<sup>nd</sup> Edition

## RoHS, REACH and WEEE Compliance Statement

Please visit <http://www.lantronix.com/legal/rohs/> for Lantronix's statement about RoHS, REACH and WEEE compliance.

## Lithium Battery Notice

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

**ACHTUNG:** WIRD BEIM BATTERIEWECHSEL EINE FALSCH E BATTERIE EINGESETZT, BESTEHT EXPLOSIONSGEFAHR. SETZEN SIE NUR EINE BATTERIE DES GLEICHEN ODER EINES ENTSPRECHENDEN, VOM HERSTELLER EMPFOHLENEN TYP S EIN. ENTSORGEN SIE VERBRAUCHTE BATTERIEN GEMÄSS DEN ANWEISUNGEN DES HERSTELLERS.

---

## Installationsanweisungen

### Rackmontage

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

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

### Energiezufuhr

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

### Erdung

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

## Installation Instructions

### Rack Mounting

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

- ◆ The ambient conditions within the rack may be greater than the room conditions. Installation should be so that the amount of air flow required for safe operation is not compromised. The maximum temperature for the equipment in this environment is 50°C. Consideration should be given to the maximum rated ambient conditions.
- ◆ Installation should be so that a hazardous stability condition is not achieved due to uneven loading.

### Input Supply

Check nameplate ratings to assure there is no overloading of supply circuits that have an effect on over current protection and supply wiring.

### Grounding

Reliable earthing of this equipment must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than direct connections to the branch circuit strips.

## Appendix D: Lantronix Cables and Adapters

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

Lantronix P/N	Description	Applications
500-103-R	6' RJ45-to DB9F	Included with EDS3008/3016/3032PR for setup or device connectivity. Connects the RJ45 RS232 serial ports of EDS3008/3016/3032PR to a DB9M DTE interface of a PC or serial device.
200.2062	Cable Ethernet CAT5; RJ45, 2 m (6.6 ft)	Connects the EDS3008/3016/3032PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS3008/3016/3032PR to another. Connects the EDS3008/3016/3032PR serial RJ45 RS232 ports to a device using one of the adapters listed below.
200.2063	Cable Ethernet CAT5; RJ45, 5 m (16.4 ft)	Connects the EDS3008/3016/3032PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS3008/3016/3032PR to another. Connects the EDS3008/3016/3032PR serial RJ45 RS232 ports to a device using one of the below listed adapters.
200.2064	Cable Ethernet CAT5; RJ45, 10 m (32.8 ft)	Connects the EDS3008/3016/3032PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS3008/3016/3032PR to another. Connects the EDS3008/3016/3032PR serial RJ45 RS232 ports to a device using one of the adapters listed below.
200.2065	Cable Ethernet CAT5; RJ45, 15 m (49.2 ft)	Connects the EDS3008/3016/3032PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS3008/3016/3032PR to another. Connects the EDS3008/3016/3032PR serial RJ45 RS232 ports to a device using one of the adapters listed below.
200.2066A	Adapter RJ45-to-DB25M	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR RJ45 serial ports to the DB25F DTE interface of a serial device.
200.2067A	Adapter RJ45-to-DB25F	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR RJ45 serial ports to the DB25M DTE interface of a serial device.
200.2069A	Adapter RJ45-to-DB9M	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR RJ45 serial ports to the DB9F DTE interface of a serial device.
200.2070A	Adapter RJ45-to-DB9F	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR to the DB9M DTE interface of a PC or serial device.
200.2071	Adapter RJ45-to-DB9M DCE	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR RJ45 serial ports to the DB9F DCE interface of a serial device.
200.2072	Adapter RJ45-to-DB9F DCE	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR RJ45 serial ports to the DB9M DCE interface of a serial device.
200.2073	Adapter RJ45-to-DB25M	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR RJ45 serial ports to the DB25F DCE interface of a serial device.

---

200.2074	Adapter RJ45-to-DB25F	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR RJ45 serial ports to the DB25M DCE interface of a serial device.
ADP010104-01	Adapter "Rolled" RJ45-to-RJ45	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR to an RJ45 console port on products from Cisco and other manufacturers.