LANTRONIX®





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

Part Number PMD-00010
Revision D November 2026

Intellectual Property

© 2026 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 Edge are registered trademarks of the Microsoft Corporation. *Mozilla* and *Firefox* are registered trademarks of the Mozilla Foundation. *Chrome* is a trademark of Google Inc. *Safari* is a registered trademark of Apple Inc. *Opera* is a registered trademark of Opera Software ASA Corporation Norway. All other trademarks and trade names are the property of their respective holders.

Warranty

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

Contacts

Lantronix, Inc. Corporate Headquarters

48 Discovery, Suite 250
Irvine, CA 92618, USA
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: www.lantronix.com/technical-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-us/contact.

Open Source Software

Some applications are Open Source software licensed under the Berkeley Software Distribution (BSD) license, the GNU General Public License (GPL) as published by the Free Software Foundation (FSF), and the Python Software Foundation (PSF) License Agreement for Python 2.7.6 (Python License). Lantronix grants you no right to receive source code to the Open Source software. 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 https://www.python.org/download/releases/2.7/license/.Your use of each Open Source component or software is subject to the terms of the applicable license.

Openssl : http://openssl.org/source/license.html

Busybox: http://busybox.net/license.html

VSFTPD: https://security.appspot.com/vsftpd.html#about

Bootstrap: https://github.com/twbs/bootstrap/blob/master/LICENSE

Python: https://www.python.org/download/releases/2.7/license/

Linux kernel version 3.6.5.

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

Disclaimer & Revisions

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

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

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

User Information

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

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

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

Revision History

Date	Rev.	Comments
August 2020	A	Initial document.
February 2021	B	Updated to firmware version 2.0.0.0R7. ◆ Updated installation and compliance information. ◆ Added TLS1.3 support
April 2023	C	Updated to firmware version 2.2.0.0R2: ◆ Added Audit Log enable and disable option to Percepxion client ◆ Added IP Address Filter support. ◆ Added 1000Mbps option to Wired Network (eth0) Link Configuration. ◆ Updated SNMP configuration settings.
November 2026	D	◆ ConsoleFlow is renamed to Percepxion. ◆ Accept mode and FTP are disabled by default. ◆ Telnet Authentication is enabled by default.

Table of Contents

1: About This Guide 12

Chapter and Appendix Summaries 12
Additional Documentation 13

2: Introduction 14

EDS3008PR, EDS3016PR, and EDS3032PR Overview 14
EDS3008PS and EDS3016PS Overview 15
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

3: Installation of EDS3000PR/EDS3000PS 22

Package Contents 22
User-Supplied Items 22
Identifying Hardware Components 23
- Serial Ports 24
- Console Port 24
- Ethernet Port 24
- LEDs 24
- Reset Button 25
- Power Input 26
- Housing 26

Installing the EDS3000PR Devices 26
- Finding a Suitable Location 26

Connecting the EDS3000PR Devices 26
Installing the EDS3000PS Devices 27
Finding a Suitable Location 27
Connecting the EDS3000PS Devices 27

4: Using Lantronix Provisioning Manager 29

Installing Lantronix Provisioning Manager 29
Accessing the EDS3000 Device Using Lantronix Provisioning Manager 29

5: Configuration Using Web Manager 30

Accessing Web Manager 30
Device Status Page 31
Web Manager Page Components 32
Navigating the Web Manager 33

6: Network Settings 36

Wired Network (eth0) 36
Interface Status and Configuration 36
To Configure Network Interface Settings 39
Link Status and Configuration 39
To Configure Wired Network (eth0) Link Settings 40
Protocol Stack 40
IP Settings 40
To Configure IP Protocol Stack Settings 40
ICMP Settings 41
To Configure ICMP Protocol Stack Settings 41
ARP Settings 41
To Configure ARP Network Stack Settings 41

7: Filesystem 42

File Transfer and Modification 43
To View, Transfer, or Modify Filesystem Files 43

8: Diagnostics 44

DNS 44
Accessing the DNS Settings 44
Hardware 45
To View Hardware Information 45
IP Sockets 45
To View the List of IP Sockets 45
Log 46
To Configure the Diagnostic Log Output 46

Memory 46
To View Memory Usage 46
Ping 47
To Ping a Remote Host 47
Processes 47
To View Process Information 48
Routes 48
Threads 48
To View Thread Information 48
Traceroute 49
To Perform a Traceroute 49

9: Administration 50

CLI 51
CLI Status and Configuration 51
To View and Configure Basic CLI Settings 51
Clock 52
To Specify a Clock-Setting Method 52
Percepxion 53
Configure Percepxion Client 53
Configure Percepxion Line 55
To Configure Percepxion 55
Discovery 56
To Configure Discovery 56
Email 56
To View, Configure and Send Email 57
FTP 58
To Configure FTP Settings 58
Host 59
HTTP 59
Interface Status, Configuration and Authentication 60
To View or Configure HTTP 61
To Configure HTTP Authentication 62
IP Address Filter 63
IP Address Filter Statistics and Configuration 63
Line 64
Line Status and Configuration 64
To View and Configure Line Configuration and Command Mode 65
RSS 66
To Configure RSS Settings 66
SMTP 67
To Configure SMTP Settings 67
SNMP 67

To Configure SNMP Settings 70
SSH 70
SSH Server: Host Keys 70
SSH Server: Authorized Users 71
SSH Client: Known Hosts 72

SSH Client: Users 72
To Configure SSH Settings 73
SSL 74
Credentials 74
To Create a New Credential 74
To Delete a Credential 74
To Configure an SSL Credential to Use an Uploaded Certificate 76
To Configure an SSL Credential to Use a Self-Signed Certificate 76
Trusted Authorities 77
To Upload an Authority Certificate 77
CSR (Certificate Signing Request) 78
Syslog 79
To Configure Syslog Settings 79
System 80
To access System settings 81
Terminal 81
To Configure the Terminal Network Connection 82
To Configure the Terminal Line 82
Tunnel 83
Tunnel Statistics 83
To View Tunnel Statistics 83
Serial Settings 83
To Configure Tunnel Serial Settings 84
Packing Mode 84
To Configure Tunnel Packing Mode Settings 85
Accept Mode 85

To Configure Tunnel Accept Mode Settings 87
Connect Mode 88
To Configure Tunnel Connect Mode Settings 91
Connecting Multiple Hosts 91
Host List Promotion 91
Disconnect Mode 92
To Configure Tunnel Disconnect Mode Settings 92
Modem Emulation 92
To Configure Tunnel Modem Emulation Settings 93

User Management 94

To Configure User Management 96
XML 96
To Export Configuration 97
To Export Status 98
To Import Configuration 99

Appendix A: Technical Support 101

Appendix B: Binary to Hexadecimal Conversions 102
Converting Binary to Hexadecimal 102
Conversion Table 102
Scientific Calculator 103

Appendix C: Compliance 104
Emissions and Immunity 106
Safety 106
NDAA, RoHS, REACH and WEEE Compliance Statement 106
Lithium Battery Notice 106
Installationsanweisungen 107
Rackmontage nur für EDS3000PR 107
Energiezufuhr 107
Erdung 107
Installation Instructions 107
Rack Mounting for EDS3000PR only 107
Input Supply 107
Grounding 107

Appendix D: Lantronix Cables and Adapters 108

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 Front View of the EDS3016PS 23
Figure 3-4 Back View of the EDS3016PS 23
Figure 3-5 RJ45 Serial Port 24
Figure 3-9 Example of EDS3032PR Connections 27
Figure 3-10 Example of EDS3016PS Connections 28
Figure 5-1 Prompt for User Name and Password 30
Figure 5-2 Web Manager Home Page 31
Figure 5-3 Components of the Web Manager Page 32
Figure 5-4 Expandable Menu Bar Selections 33
Figure 6-1 Wired Network (eth0) Interface Status 37
Figure 6-2 Wired Network (eth0) Interface Configuration 37
Figure 6-4 Wired Network (eth0) Ethernet Link Status 39
Figure 6-5 Wired Network (eth0) Link Configuration 39
Figure 7-1 Filesystem Statistics 42

List of Tables

Table 3-6 Back Panel LEDs for EDS3000PR 24
Table 3-7 Front Panel LEDs of EDS3000PS 25
Table 3-8 Back Panel LEDs of EDS3000PS 25
Table 5-5 Summary of Web Manager Pages 33
Table 6-3 Wired Network (eth0) Interface Configuration 38
Table 6-6 Wired Network (eth0) Link Configuration 39
Table 6-1 IP Protocol Stack Settings 40
Table 6-2 ICMP Protocol Stack Settings 41
Table 6-3 ARP Protocol Stack Settings 41
Table 7-4 Filesystem Statistics 42
Table 7-5 File Modification Settings 42
Table 7-6 File Transfer Settings 43
Table 8-7 DNS Settings 44
Table 8-8 Log Settings 46
Table 8-9 Ping Configuration 47
Table 8-10 Traceroute Settings 49
Table 9-11 CLI Configuration Settings 51
Table 9-12 Clock Settings 52
Table 9-13 Percepxion Client Configuration 53
Table 9-14 Percepxion Line 55
Table 9-15 Discovery Settings 56
Table 9-16 Email Configuration 56
Table 9-17 FTP Settings 58
Table 9-18 Host Settings 59
Table 9-19 HTTP Configuration 60
Table 9-20 HTTP Authentication 61
Table 9-21 IP Address Filter. 63
Table 9-22 Line Configuration Settings 64
Table 9-23 Line Command Mode Setting 65
Table 9-24 RSS 66
Table 9-25 SMTP Settings 67
Table 9-26 SNMP Settings 68
Table 9-27 SSH Server Host Keys 70
Table 9-28 SSH Server Authorized Users 71
Table 9-29 SSH Client Known Hosts 72

Table 9-30 SSH Client Users 72
Table 9-31 Create New Keys 73
Table 9-32 SSL Credential - Upload Certificate 75
Table 9-33 SSL Credential - Create New Self-Signed Certificate 75
Table 9-34 SSL Trusted Authority 77
Table 9-35 SSL CSR (Certificate Signing Request) 78
Table 9-36 Syslog 79
Table 9-37 System Settings 80
Table 9-38 Terminal on Network and Line Settings 81
Table 9-39 Tunnel Serial Settings 83
Table 9-40 Tunnel Packing Mode Settings 84
Table 9-41 Tunnel Accept Mode Settings 85
Table 9-42 Tunnel Connect Mode Settings 88
Table 9-43 Host Settings 89
Table 9-44 Tunnel Disconnect Mode Settings 92
Table 9-45 Tunnel Modem Emulation Settings 93
Table 9-46 Administrator Settings 94
Table 9-47 Current Users List 94
Table 9-48 New User Settings 94
Table 9-49 Current Roles List 95
Table 9-50 New Role Settings 95
Table 9-51 Configuration from Filesystem 99
Table 9-52 Line(s) from single line Settings on the Filesystem 100

1: About This Guide

This user guide provides the information needed to configure, use, and update the Lantronix® EDS3000 devices, which includes models EDS3008PR/EDS3008PS, EDS3016PR/EDS3016PS, and EDS3032PR. It is intended for software developers and system integrators who are installing the EDS3000 devices in their designs.

Chapter and Appendix Summaries

A summary of each chapter is provided below.

Chapter	Description
Chapter 2: Introduction	Main features of the product and the protocols it supports. Includes technical specifications.
Chapter 3: Installation of EDS3000PR/ EDS3000PS	Instructions for installing the EDS3000devices/terminal server.
Chapter 4: Using Lantronix Provisioning Manager	Instructions for viewing the current configuration using Lantronix Provisioning Manager.
Chapter 5: Configuration Using Web Manager	Instructions for accessing Web Manager and using it to configure settings for the device.
Chapter 6: Network Settings	Instructions for using the web interface to configure Ethernet settings.
Chapter 7: Filesystem	Instructions to view and configure the filesystem.
Chapter 8: Diagnostics	Instructions to view and configure DNS, hardware, IP socket, log, memory, ping, processes, routes, threads, and traceroute information.
Chapter 9: Administration	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.
Appendix A: Technical Support	Instructions for contacting Lantronix Technical Support.
Appendix B: Binary to Hexadecimal Conversions	Instructions for converting binary values to hexadecimals.
Appendix C: Compliance	Lantronix compliance information.
Appendix D: Lantronix Cables and Adapters	Lantronix cables and adapters for use with the EDS3000 devices are listed here according to part number and application.

Additional Documentation

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

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

2: Introduction

This chapter introduces the Lantronix EDS3000 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 EDS3000 devices are a unique, hybrid Ethernet terminal and multi-port device server product, which 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*
- *EDS3008PS and EDS3016PS Overview*
- *Key Features*
- *Applications*
- *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



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

The key features of the EDS3000 devices includes:

- Dual-purpose Ethernet terminal server and device server design
- 8 (EDS3008PR/PS), 16 (EDS3016PR/PS) 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
- Multiple configuration methods (Web, command line, and XML)

Applications

EDS3000 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 EDS3000 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, HTTP, and HTTPS for firmware upgrades and uploading files.

Additional Features

Modem Emulation

In modem emulation mode, the EDS3000 devices 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 EDS3000 devices enable 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 EDS3000 devices use industry-standard tools for configuration, communication, and control. For example, the EDS3000 devices 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 EDS3000 devices support 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 EDS3000 devices.

XML-Based Architecture and Device Control

XML is a fundamental building block for the future growth of M2M networks. The EDS3000 devices support 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 EDS3000 devices support 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 EDS3000 devices have 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 EDS3000 devices have robust defenses to hostile Internet attacks such as a denial of service (DoS), which can be used to take down the network. Moreover, the EDS3000 devices cannot be used to bring down other devices on the network.

You can use the EDS3000 devices 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 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 could 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 EDS3000 devices easily attach 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 EDS3000 devices offers a comprehensive diagnostic tool set 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 EDS3000, including CPU utilization and total stack space available.

Configuration Methods

After installation, the EDS3000 devices requires configuration. For the unit to operate correctly on a network, it must have a unique IP address on the network. The following methods are available for logging into the EDS3000 devices 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 EDS3000 devices 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 *EDS3000 Device Server Command Reference* for instructions and available commands. Lantronix documentation is available at www.lantronix.com/support/documentation.)

XML: The EDS3000 devices 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 *EDS3000 Device Server Command Reference* for instructions and available commands. Lantronix documentation is available at 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 Device Server 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 EDS3000 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/EDS3000PS

This chapter describes installing the EDS3000PR/EDS3000PS family of device servers.

Package Contents

Each EDS3000 serial port includes the following items:

- One EDS3000PR unit or one EDS3000PS unit (EDS3008PR, EDS3016PR, EDS3032PR, or EDS3008PS, EDS3016PS).
- One RJ45-to-DB9F serial cable.
- A printed Quick Start guide.

User-Supplied Items

To complete your EDS3000 device installation, you need the following items:

- RS-232 serial devices that require network connectivity. Each EDS3000 serial port supports a directly connected RS-232 serial device.
- A serial cable for each serial device. All devices attached to the EDS3000 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 EDS3000 serial port to a DTE device, you need a DTE cable, such as the one supplied in your EDS3000PR/EDS3000PS package, or an RJ45 patch cable and DTE adapter. To connect the EDS3000 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/EDS3000PS devices, see *Appendix D: Lantronix Cables and Adapters*.

- An available connection to your Ethernet network and an CAT5E Ethernet cable.
- A working power outlet.

Identifying Hardware Components

The following figures show the components on the front and back of the EDS3032PR and EDS3016PS.

Figure 3-1 Front View of the EDS3032PR



Figure 3-2 Back View of the EDS3032PR

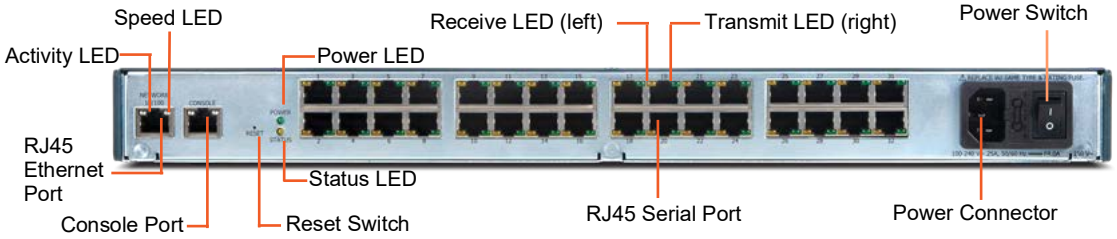


Figure 3-3 Front View of the EDS3016PS

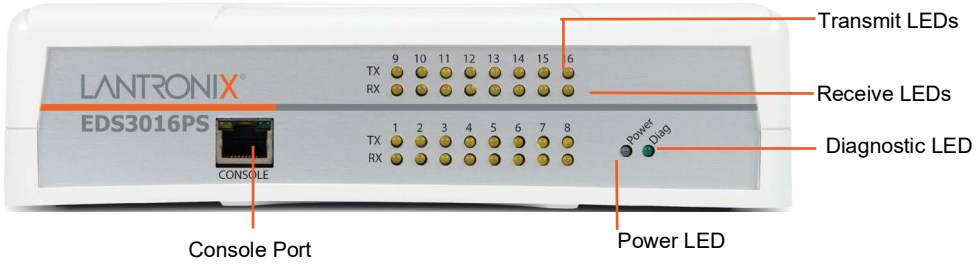
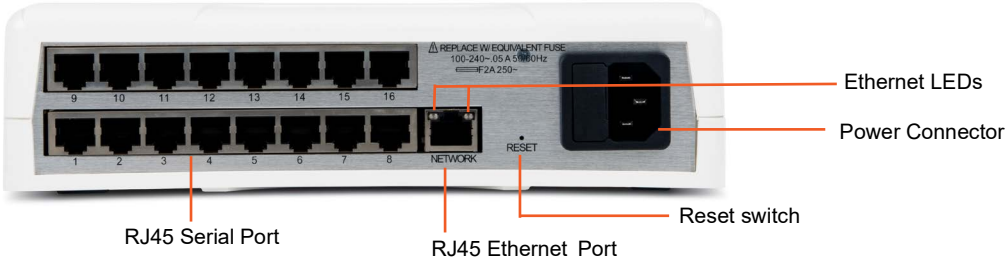


Figure 3-4 Back View of the EDS3016PS



Serial Ports

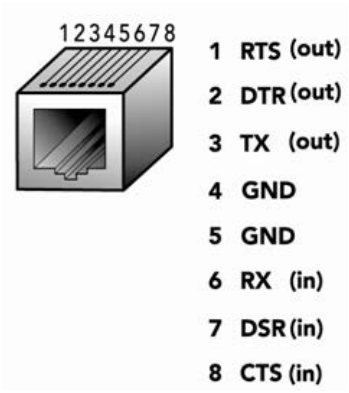
All EDS3000 serial ports are configured as DTE and support up to 230,400 baud.

- The EDS3008PR/EDS3008PS has 8 serial ports.
- The EDS3016PR/EDS3016PS has 16 serial ports.
- The EDS3032PR has 32 serial ports.

Console Port

The EDS3000PR/EDS3000PS has an RJ45 Console port configured as DTE and supports up to 230,400 baud.

Figure 3-5 RJ45 Serial Port



Ethernet Port

The EDS3000 devices have an RJ45 Ethernet port that supports 10/100/1000 Mbps Ethernet.

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

You can configure the EDS3000PR/EDS3000PS 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.

For EDS3000PR

- **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 3-6 Back Panel LEDs for EDS3000PR

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 1000 Mbps Fast Ethernet network. Off = EDS3000PR is connected to a 10/100 Mbps Ethernet network.
Activity (green)	Blink = EDS3000PR is sending data to or receiving data from the Ethernet network.

For EDS3000PS

- **Front panel.** The front panel has a blue Power LED, Status LED, Transmit and a Receive LED for each serial port.
- **Back panel.** The Ethernet connector has Speed and Activity LEDs on right and left sides.

The table below describes the LEDs on the front of the EDS3000PS.

Table 3-7 Front Panel LEDs of EDS3000PS

LED	Description
Transmit (green)	Blinking = EDS3000PS is transmitting data on the serial port.
Receive (orange)	Blinking = EDS3000PS is receiving data on the serial port.
Power (blue)	On = EDS3000PS is receiving power.
Status (green)	Fast blink = initial startup (loading OS). Slow blink (once per second) = operating system startup. On = unit has finished booting.

The table below describes the LEDs on the back of the EDS3000PS.

Table 3-8 Back Panel LEDs of EDS3000PS

LED	Description
Speed (green)	On = EDS3000PS is connected to a 1000 Mbps Fast Ethernet network. Off = EDS3000PS is connected to a 10/100 Mbps Ethernet network.
Activity (green)	Blink = EDS3000PS is sending data to or receiving data from the Ethernet network

Reset Button

For EDS3000PR

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

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

For EDS3000PS

The reset button is on the back of the EDS3000PS device to the left of the Power connector.

Pressing this button for 2 to 3 seconds reboots the EDS3000PS device and terminates all data activity occurring on the serial and Ethernet ports.

Power Input

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

Housing

For EDS3000PR

- 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

For EDS3000PS

- Dimensions: (L x W x H): 12.8 x 22.7 x 6 cm (5.02 x 8.92 x 2.36 in.)
- Weight: 0.616 kg (1.36lbs)

Installing the EDS3000PR Devices

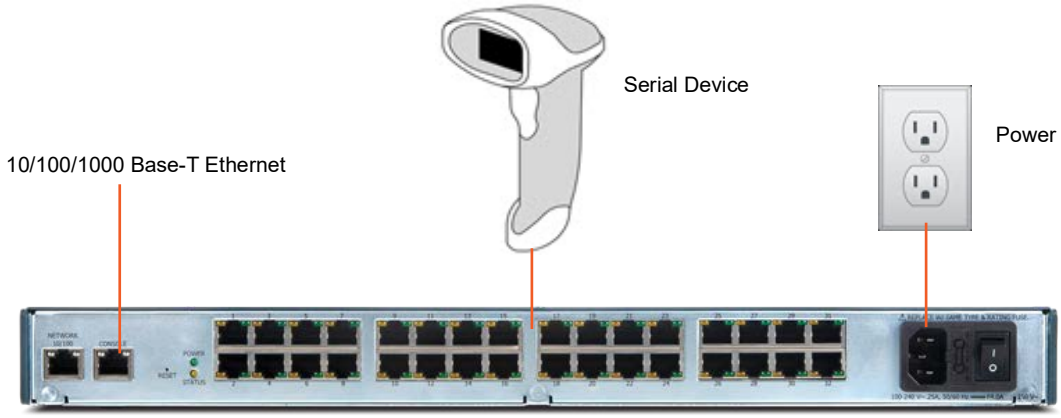
Finding a Suitable Location

You can install the EDS3000PR device 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 Devices

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

Figure 3-9 Example of EDS3032PR Connections



Installing the EDS3000PS Devices

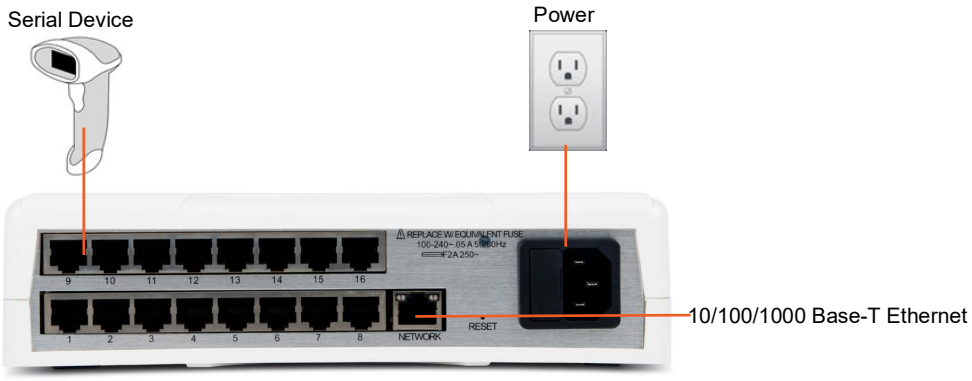
Finding a Suitable Location

You can install the EDS3000PS device as a desktop unit or it can be mounted to existing wall brackets (not provided) using mounting holes located on the bottom of the EDS3000PS. If using AC power, avoid outlets controlled by a wall switch.

Connecting the EDS3000PS Devices

1. Power off the serial devices that will be connected to the EDS3000PS device.
2. Attach a serial cable between the EDS3000PS device and your serial device. For a list of cables and adapters you can use with the EDS3000PS device, refer to *Appendix D: Lantronix Cables and Adapters*.
3. Connect an Ethernet cable between the EDS3000PS device Ethernet port and your Ethernet network.
4. Insert the power cord into the back of the EDS3000PS device. Plug the other end into an AC wall outlet. After power-up, the self-test begins.
5. Power up the serial devices.

Figure 3-10 Example of EDS3016PS 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 EDS3000 Device 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 EDS3000 device 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. To perform operations on the EDS3000 device, 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:

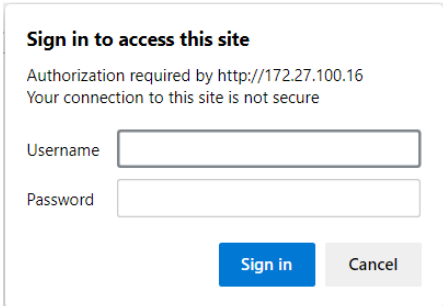
- *Accessing Web Manager*
- *Web Manager Page Components*
- *Navigating the Web Manager*
- *Summary of Web Manager Pages*

Accessing Web Manager

To access Web Manager, perform the following steps:

1. Open a standard web browser. Lantronix supports the latest version of Microsoft EdgeMozilla Firefox, Apple Safari, Google 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 Percepxion information.

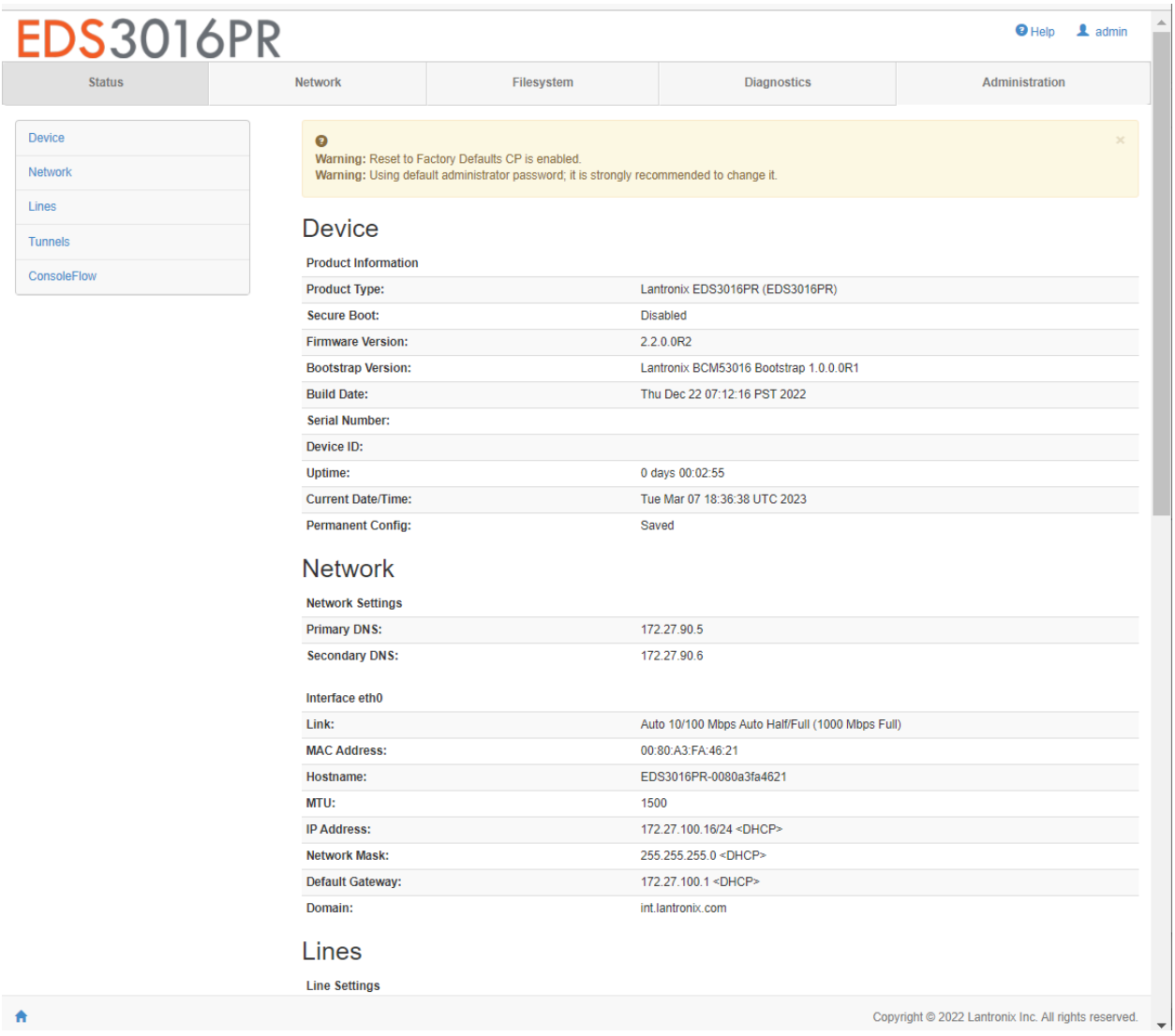
Note: *The admin/Logout button is available on the upper right of any web page. Logging out of the web page forces re-authentication to take place the next time the web page is accessed. Click the Help icon to display context-sensitive help information.*

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*).

Warning: ***Using default administrator password; it is strongly recommended to change it.***

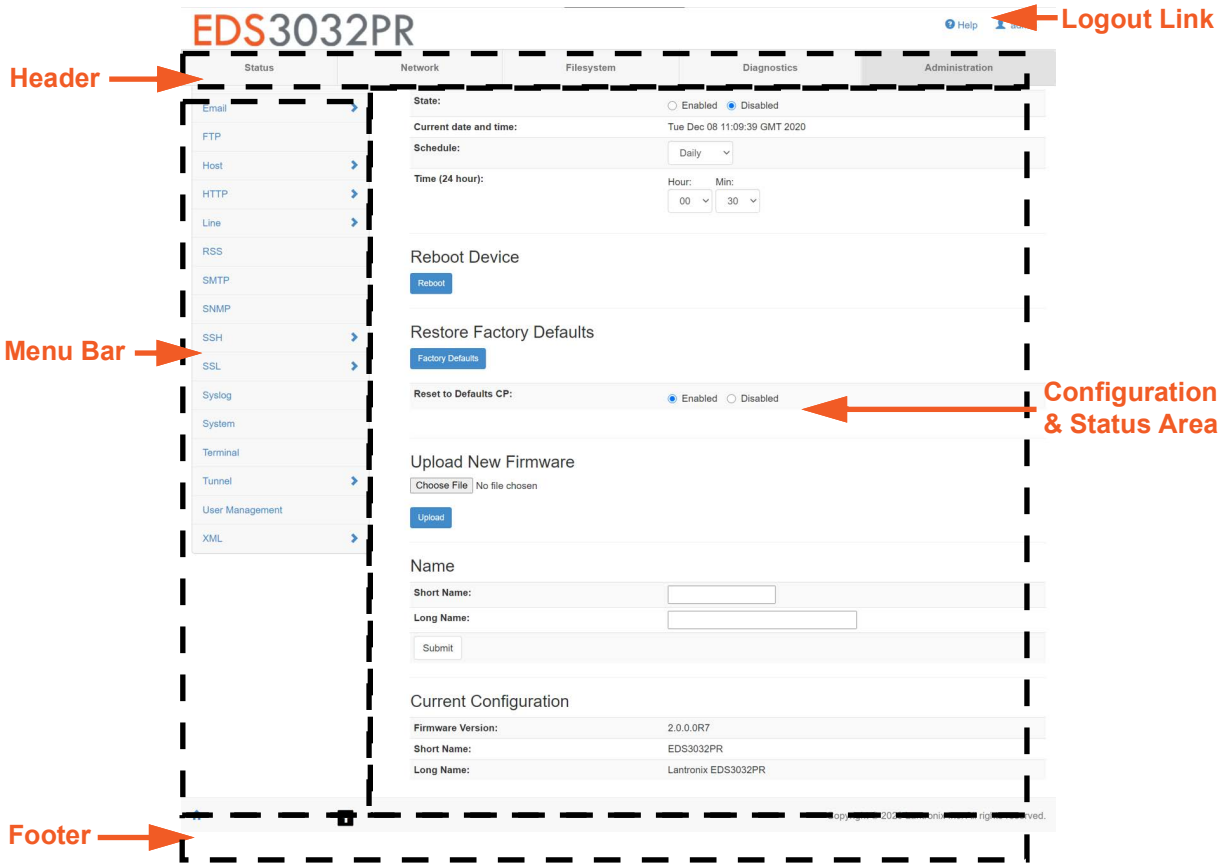
Figure 5-2 Web Manager Home Page



Web Manager Page Components

The layout of a typical Web Manager page is below.

Figure 5-3 Components of the Web Manager Page

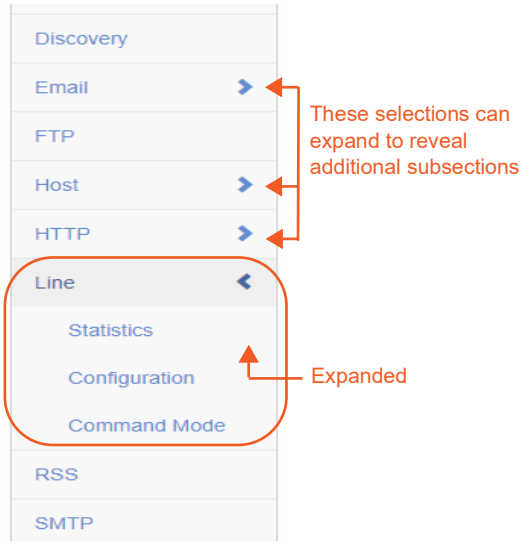


Web Manager pages have these sections:

- 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.

Figure 5-4 Expandable Menu Bar Selections



- 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.

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
Status	Shows device information and network, line, tunneling and Percepxion settings.	*31*
CLI	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	*51*
Clock	Allows you to view and configure date and time for the device by either SNTP or manual settings.	*52*
Percepxion	Shows the configuration and status for the Percepxion client.	*53*
Diagnostics	Lets you perform various diagnostic procedures.	*44*

Web Manager Page (continued)	Description	See Page
Discovery	Allows you to view and modify the configuration and statistics for device discovery.	56
DNS	Shows the current configuration of the DNS subsystem and the DNS cache.	44
Email	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	56
Filesystem	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.	42
FTP	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	58
Hardware	Shows hardware status and configuration options.	45
Host	Lets you view and change settings for a host on the network.	59
HTTP	Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	59
IP Sockets	Shows IP socket status and lets you change hardware configuration.	45
Line	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	63
Log	Shows and allows changes with logs.	46
Memory	Shows memory status and lets you change hardware configuration.	46
Network	Shows status and lets you configure the network interface.	36
Ping	Shows how to ping a network host with a DNS hostname or IP address.	47
Processes	Shows the processes currently running on the system.	47
Protocol Stack	Lets you perform lower level network stack-specific activities.	40
Routes	Shows the current system routing table.	48
RSS	Lets you change current Really Simple Syndication (RSS) settings.	66
SMTP	Shows SMTP status and configuration options.	67
SNMP	Lets you change the current Simple Network Management Protocol (SNMP) configuration settings.	67
SSH	Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	70
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	74
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	79
System	Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.	80
Terminal	Lets you change current settings for a terminal.	81
Threads	Shows thread ID numbers, names and CPU usage.	48
Traceroute	Shows how to perform a traceroute to a network host.	49

Web Manager Page (continued)	Description	See Page
Tunnel	Lets you change the current configuration settings for a tunnel.	*83*
User Management	Shows the configuration of users.	*94*
XML	Lets you export XML configuration and status records, and import XML configuration records.	*96*

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

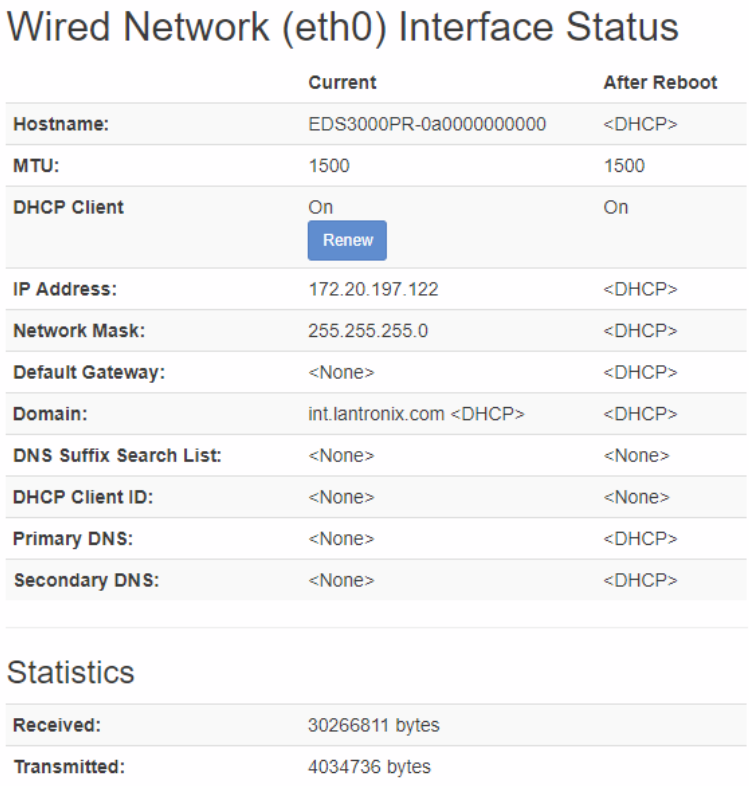


Figure 6-2 Wired Network (eth0) Interface Configuration

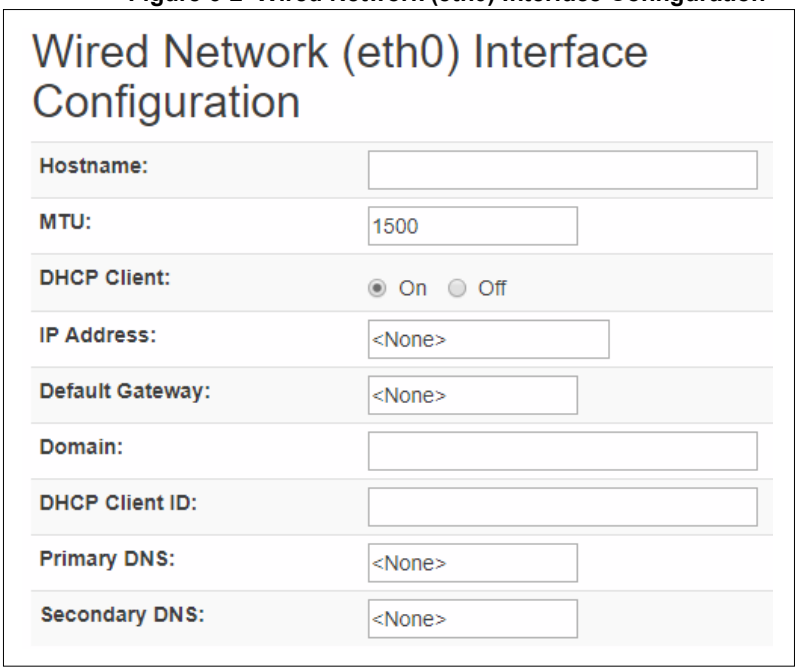


Table 6-3 Wired Network (eth0) Interface Configuration

Setting	Description
Hostname	Enter the host name 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 host name with a DNS server until the next reboot.
MTU	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.
DHCP Client	Select to turn On or Off At boot up, after the physical link is up, the EDS3000 will attempt to obtain IPv4 settings from a DHCP server and will periodically renew these settings with the server. ***Note:*** *Overrides the configured IPv4 address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the EDS3000PR/EDS3000PS. Within Web Manager, click* ***Renew*** *to renew the DHCP lease.*
IP Address	Enter the static IPv4 address to use for the interface. You may enter it alone or in CIDR format. ***Note:*** *This setting will be used if Static IP is active (DHCP is Disabled). Changing this value requires you to reboot the EDS3000PR/EDS3000PS. When DHCP is enabled, the tries to obtain an IPv4 address from a DHCP server. If it cannot, the EDS3000 generates and uses an Auto IP address in the range of 169.254.xxx.xxx with a network mask of 255.255.0.0.*
Default Gateway	Enter the IP address of the router for this network. ***Note:*** *This setting will be used if Static IP is active (DHCP is Disabled).*
Domain	Enter the domain name suffix for the interface. ***Note:*** *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.*
DHCP Client ID	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 MAC address.
Primary DNS	Enter the IP address of the primary domain name server (DNS.) ***Note:*** *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.*
Secondary DNS	Enter the IP address of the secondary domain name server. ***Note:*** *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

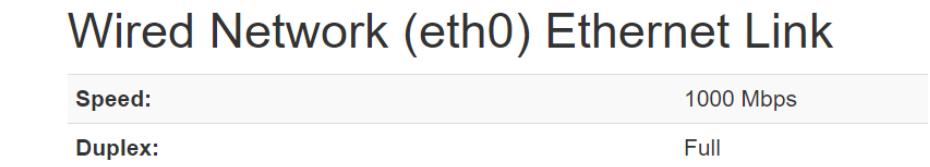


Figure 6-5 Wired Network (eth0) Link Configuration

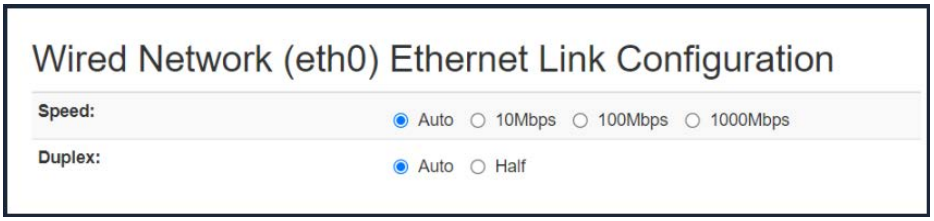


Table 6-6 Wired Network (eth0) Link Configuration

Setting	Description
Speed	Select the Ethernet link speed. Choices are Auto, 10Mbps, 100Mbps, and 1000Mbps. 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
IP Time to Live	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 “IP Default TTL”.
Multicast Time to Live	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

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

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
IP Address	Enter the IP address to add the ARP cache.
MAC Address	Enter the MAC address to add to the ARP cache.
Interface	Select the type of interface if adding to the ARP cache.
Add (button)	Click this button to add a new entry (after entering the IP address, MAC address and Interface info for the new entry above.)
Clear	Click the **Clear** link above all listed addresses to remove all the addresses.
Remove	Click the **Remove** 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 or HTTPS, and transfered to and from a TFTP server. Newly created files will be empty. Some filesystems may contain a 'lost+found' directory.
- Extra internal storage, if available, will list under filesystem as Internal_Storage. The internal storage cannot be unmounted or deleted.

Figure 7-1 Filesystem Statistics

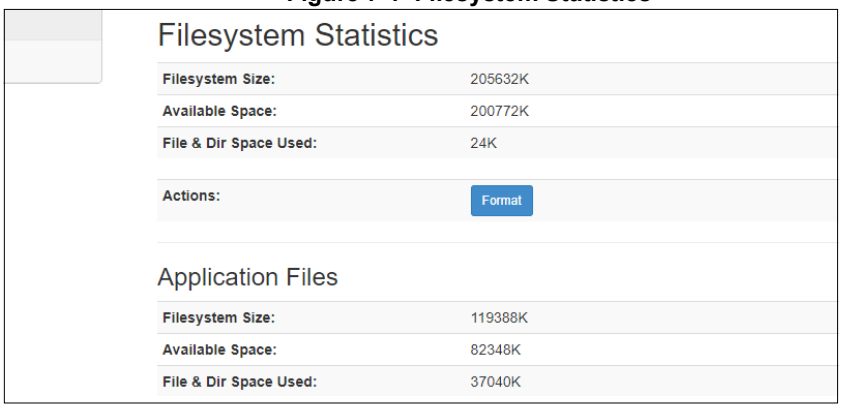


Table 7-4 Filesystem Statistics

Field	Description
Filesystem Size	This is the total size of the Filesystem or Application Files.
Available Space	This is the available space in the Filesystem or Application Files.
File & Dir Space Used	This is the amount of used space in the filesystem or Application Files.
Actions	The Format button will format the filesystem, deleting all existing files in the filesystem. Formatting the filesystem will delete all files on it and Internal_Storage (if available).

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 EDS3000 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
Create	Type in a **Directory** name and click the **Create** button. The newly created Directory will appear above.
Upload File	Click and select a file to be uploaded via HTTP. Click **Upload** to upload the chosen file.
Copy File	Enter the **Source** and **Destination** name for file to be copied and click the **Copy** button.
Move	Enter the **Source** and **Destination** name for file to be moved and click the **Move** button.
TFTP	
Action	Select the action that is to be performed via TFTP: ◆ Get = A “get” command will be executed to store a file locally. ◆ Put = A “put” command will be executed to send a file to a remote location.
Local File	Enter the name of the local file on which the specified “get” or “put” action is to be performed.
Remote File	Enter the name of the file at the remote location that is to be stored locally (“get’) or externally (“put”).
Host	Enter the IP address or name of the host involved in this operation.
Port	Enter the number of the port involved in TFTP operations.
Transfer (button)	Click the **Transfer** 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 devices 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 or BOOTP.

Table 8-7 DNS Settings

Field/Button	Description
Lookup	Perform one of the following and click the **Lookup** button: ◆ Enter an IP address, and perform a reverse Lookup to locate the host name for that IP address ◆ Enter a host name, and perform a forward Lookup to locate the corresponding IP address.

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 36)**.*

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 sockets and connected IP sockets and Reserved Ports.

Note: *For a TCP socket in LISTEN state the LocalAddr and RemoteAddr will be 0.0.0.0 to indicate that the application is listening on all local interfaces. A UDP socket will not have a state.*

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. This page lists the diagnostic log records. The Output selection optionally directs logging to the filesystem.

If Filesystem is selected, the output goes into /log.txt. Use Max Length to limit the size in Kbytes that /log.txt will be allowed to grow to. If this size is exceeded, the file will be reinitialized using the 100 most recent messages.

Table 8-8 Log Settings

Diagnostics	Log Description
Output	Select a diagnostic log output type: ◆ Disable - Turn off the logging feature. ◆ Filesystem - Directs logging to the EDS3000 Filesystem. ◆ Line 1 - Directs logging to the selected serial line. ◆ Line 2 - Directs logging to the selected serial line. ◆ Line 3 - Directs logging to the selected serial line. ◆ Line 4 - Directs logging to the selected serial line.
Max Length	Select the maximum diagnostic log length. The default is 50 Kbytes.

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 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
Host	Enter the IP address or host name for the devices that you want to ping.
Count	Enter the number of ping packets that the EDS3000 attempts to send to the Host. The default number of packets is 3.
Timeout	Enter the time in seconds that the EDS3000 waits for a response from the Host before it times out. The default time is 5 seconds.
Ping (button)	Click the **Ping** 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

This page shows all the processes currently running on the system. It shows the process ID (PID), parent process ID (PPID), user, State, CPU percentage, percentage of total CPU cycles, process name and total processor load .

The %CPU column displays the share of elapsed CPU time expressed as a percentage of total CPU time. The STATE column displays the process state. The Process State Codes include:

D: uninterruptible sleep (usually IO)

R: runnable (on run queue)

S: sleeping

T: traced or stopped

Z: a defunct ('zombie') process

Additional letters may be displayed:

W: has no resident pages

<: high-priority process

N: low-priority task

L: has pages locked into memory (for real-time and custom IO)

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 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 EDS3000 to an Internet host. A traceroute shows how much time it takes in milliseconds to reach the host. This information can be helpful to diagnose delays for a web page that loads slowly.

Table 8-10 Traceroute Settings

Traceroute Fields	Description
Host	Enter the IP address or DNS host name of the destination device.
Protocol	Select the protocol that you want to use for the traceroute. ◆ TCP ◆ ICMP ◆ UDP
Traceroute (button)	Click the **Traceroute** 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 EDS3000 devices are organized beneath the Administration tab in the Web Manager user interface. This chapter describes the following administrative settings:

- *CLI*
- *Clock*
- *Percepxion*
- *Discovery*
- *Email*
- *FTP*
- *Host*
- *HTTP*
- *IP Address Filter*
- *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 EDS3000 devices. 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). The EDS3000 initially uses the default Logon password; you may want to change it. Note that by default non-secure Telnet State is enabled. Device is vulnerable to Cleartext transmission of sensitive information. Setup and verify SSH, then disable Telnet.

Table 9-11 CLI Configuration Settings

Command Line Interface Configuration Settings	Description
Enable Level Password	Enter the password for access to the Enable level of a CLI session. There is no password by default.
Quit Connect Line	Enter the **Quit Connect Line** string to be used to terminate a connect line, telnet or SSH session and resume the CLI. Type <control> before the key to be pressed while holding down the **[Ctrl]** key (example: **<control>L**).
Inactivity Timeout	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.
Line Authentication	**Enable** or **Disable** authentication for CLI access on the serial lines.
Telnet State	**Enable** or **Disable** CLI access via Telnet.
Telnet Port	Enter an alternative Telnet Port to override the default used by the CLI server. Blank the field to restore the default.
Telnet Max Sessions	Specify the maximum number of concurrent Telnet sessions that will be allowed (1-10).
Telnet Authentication	**Enable** or **Disable** authentication for Telnet logins. Enabled by default.
SSH State	Select to **Enable** or **Disable** CLI access via SSH.
SSH Port	Specify the SSH Port and override the default, as needed. Blank the field to restore the default.
SSH Max Sessions	Specify the maximum number of concurrent SSH sessions that will be allowed (1-10).

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
Method	Select **Manual** or **SNTP** from the drop-down window.
Date	If **Manual** is selected**,** enter the date using the **Year**, **Month** and **Day** drop-down menus that become available.
Time	If **Manual** is selected**,** enter the time using the **Hour**, **Minute (Min)** and **Second (Sec)** drop-down menus that become available.
NTP Server	If **SNTP** 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.
Time Zone	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 EDS3000 device 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">`

Percepxion

The EDS3000 devices come integrated with the Percepxion cloud platform to allow for the remote management of devices. To set up the Percepxion client, you need to configure the following settings:

- **Percepxion Client** - To connect to the Percepxion cloud platform.
- **Line Settings** (number of lines varies by EDS3000 model) - To enable remote management and data access to your application or device attached on the serial line.

Configure Percepxion Client

This page displays the configuration and status for Percepxion client.

Table 9-13 Percepxion Client Configuration

Percepxion Client	Description
State	Click to enable or disable the Percepxion client.
Device ID	Read only. Displays the gateway's Device ID. Device ID may be provisioned through Lantronix Provisioning Manager. ***Note:*** *Device ID can only be provisioned once. It will persist across resets.*
Device Key	Read only. Shows whether the gateway's Device Key has been configured. Device Key may be configured through Lantronix Provisioning Manager.
Device Name	Enter the Percepxion Device Name.
Device Description	Enter the Percepxion Device Description.
Status Update Interval	Enter the frequency that the gateway updates the device status to Percepxion. The valid range is between 1 minute and 1440 minutes (1 day).
Content Check Interval	Enter the frequency that the gateway checks Percepxion for updates to configuration or firmware. The valid range is between 1 hour and 2160 hours (90 days).
Apply Firmware Updates	Enable to allow firmware updates to be applied via Percepxion. Enabled by default.
Apply Configuration Updates	Select when to **Apply Configuration Updates** from the drop-down menu: ◆ **Never**: signifying no configuration updates will be applied. ◆ **If unchanged**: signifying configuration updates will only be applied if no changes have been made locally. ◆ **Always**: signifying configuration updates will always apply.
Reboot After Update	Automatically reboot device after firmware or configuration update. ***Note:*** *Setting causes automatic reboot after a firmware update.*
Audit Log	Enable or Disable the Audit Log. The default is Disabled.
Allow Remote Connections	Enable / Disable remote access from Percepxion. The default is Disabled.
Remote Access Local Port	Local port for Percepxion Remote Access. When configured, a total of 16 consecutive ports will be reserved. The default is <Random>.
Active Connection	Select the connection instance to use when connecting to Percepxion. The configuration options for both Connection 1 and Connection 2 are below.
Connection 1	Connection 1 settings.
Host	Enter the host name or IP address.

Percepxion Client	Description
Connect To	At the dropdown select Cloud or On-Premise as the Percepxion connection method for this connection. The default is Cloud connection.
Port	Enter the Percepxion port.
Secure Port	Click to enable or disable the Percepxion client secure port 443.
Validate Certificates	Click to enable or disable the Percepxion client **Validate Certificates**.
Local Port	Enter the local port for the SMTP protocol. When configured, a total of 16 consecutive ports will be reserved. Remote Access Local Port range is from 1024 to 65504.
MQTT State	Enable or Disable MQTT.
MQTT Host	Hostname or IP address of MQTT server.
MQTT Port	Update the port of Percepxion MQTT server. When configured, a total of 32 consecutive ports will be reserved.
MQTT Security	Enable SSL for MQTT.
MQTT Local Port	Enter the local port of Percepxion MQTT client. When configured, a total of 32 consecutive ports will be reserved.
Use Proxy	Enable or disable the use of a proxy for this connection. Disabled by default.
Proxy Type	Proxy server type. The supported type is SOCKS5.
Proxy Host	Hostname or IP address of the proxy server to be used.
Proxy Port	Port of the proxy server to be used. Default port is **80**.
Proxy Username	Username for the proxy server.
Proxy Password	Password for the proxy server.
Connection 2	Connection 2 settings are identical to connection 1 settings.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

Configure Percepxion Line

This page displays the configuration and status for Percepxion Line client. The number of configurable lines will be 8, 16, or 32 , depending on your EDS3000 device model.

Table 9-14 Percepxion Line

Percepxion Line	Description
Select	Select the Percepxion line to be configured. The number of lines depends on the EDS3000 model number.
State	Click to enable or disable the Percepxion line client.
Project Tag	Enter the **Percepxion Project Tag** name.
Status Update Interval	Enter the **Status Update Interval** in minutes (0-65535). The status update interval is the frequency in which the gateway will contact the Percepxion server.
Content Check Interval	Enter the **Content Check Interval** in hours (0-65535). The content check interval is the frequency in which the gateway contacts the server for new content.
Command Delimiter	Enter the Command Delimiter for attached serial devices. ***Note:*** *Send delimiter before command and after response is received.*
Local Port	Enter the local port for the Percepxion client. When configured, a total of 16 consecutive ports will be reserved. Local Port range is from 1024 to 65504.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure Percepxion

Using Web Manager

- To configure Percepxion Client, on the **Administration** page, click **Percepxion > Client**.
- To configure Percepxion Line, on the **Administration** page, click **Percepxion > Line**.

Using the CLI

- To enter the command level: `enable > config > percepxion`

Using XML

- Include in your file: `<configgroup name=”percepxion”>`

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 EDS3000 devices.

Table 9-15 Discovery Settings

Discovery Settings	Description
Query Port Server State	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 9-16 Email Configuration

Email Configuration Settings	Description
From	Click the **Configure SMTP** link to configure SMTP. See *SMTP (on page 67)*.
To	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.
CC	Enter the email address to which the email alerts will be copied. Multiple addresses are separated by semicolon (;).
Reply To	Enter the email address to list in the Reply-To field of the email alert.
Subject	Enter the subject for the email alert. ***Note:*** *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.*
Message File	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.

Email Configuration Settings (continued)	Description
Priority	Select the priority level for the email alert: ◆ Urgent ◆ High ◆ Normal ◆ Low ◆ Very Low

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 EDS3000 devices.*

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 EDS3000 devices firmware. A configurable option is provided to enable or disable access via this protocol.

FTP may run in Active or Passive mode, which determines how the data connection is established. In both cases, the client creates a TCP control connection to the FTP server command port.

Table 9-17 FTP Settings

FTP Settings	Description
State	Select to enable or disable the FTP server: ◆ Enabled ◆ Disabled (default)
Port	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.
Data Port	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. FTP Passive mode start port range is from 1024 to 65535.
Passive Mode Start Port **Passive Mode Ports**	Define the port range by entering the Passive Mode Start Port and Passive Mode Port. 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.
Submit (button)	Click the **Submit** button to enter the change of state. The **Submit** 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

This page displays and changes the current HTTP Configuration settings.

Table 9-18 Host Settings

Host Settings	Description
Name	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.
Protocol	Select the protocol to use to connect to the host. Choices are: ◆ Telnet ◆ SSH ***Note:*** *SSH keys must be loaded or created on the SSH page for the SSH protocol to work.* *If Protocol is SSH, either supply a value in SSH Username to select a pre-configured Username / Password / Key (at SSH Client: Users) or leave it blank to be prompted for Username and Password at connect time.*
SSH Username	Appears if you selected SSH as the protocol. Enter a username to select a pre-configured Username/Password/Key (configured on the SSH: Client Users page), or leave it blank to be prompted for a username and password at connect time. ***Note:*** *This configuration option is only available when SSH is selected for Protocol.*
Remote Address	Enter either an IP address or a DNS address for the host to which the EDS3000 devices will connect.
Remote Port	Enter the port on the host to which the EDS3000 devices will connect.

To Configure Host Settings

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 EDS3000 devices.

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 9-19* for the HTTP settings that can be modified on the HTTP Configuration page. See *Table 9-20* for the HTTP settings that can be authenticated on the HTTP Authentication page.

Table 9-19 HTTP Configuration

HTTP Settings	Description
State	Select to enable or disable the HTTP server.
Port	Enter the port for the HTTP server to use. The default is **80**. The Port can be overridden. Blank the display to restore the default HTTP port. Zero the display to disable listening on HTTP port.
HTTPS State	Select to enable or disable the HTTPS Server.
Secure Port	Enter the port for the HTTPS server to use. The default is **443**. The HTTP server only listens on the **HTTPS Port** when an SSL certificate is configured. The Secure Port (SSL) can be overridden. Blank the display to restore the default HTTPS port. Zero the display to disable listening on HTTPS port.
Secure Protocols	Select to enable or disable the following protocols: ◆ **SSL3** = Secure Sockets Layer version 3 ◆ **TLS1.0** = Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF. ◆ **TLS1.1** = Transport Layer Security version 1.1 ◆ **TLS1.2** = Transport Layer Security version 1.2 ◆ **TLS1.3** = Transport Layer Security version 1.3 The protocols are enabled by default. ***Note:*** *A server certificate and associated private key need to be installed in the **SSL** configuration section to use **HTTPS**.*
Secure Credentials	Specify the name of the set of RSA and/or DSA certificates and keys to be used for the secure connection. ***Note:*** *SHA1, MD5 ciphers are disabled. By default, non-secure HTTP Server Port is configured, so the EDS3000 device is vulnerable to cleartext transmission of sensitive information. Setup and verify your Secure Port and Secure Credential, then set HTTP Server Port to 0 to disable the non-secure port.*
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is **10** seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is **40** KB (this prevents DoS attacks). ***Note:*** *You may need to increase this number in some cases where the browser is sending data aggressively within TCP Windows size limit, when a file (including firmware upgrade) is uploaded from web page.*
Logging State	Select to enable or disable HTTP server logging: ◆ **Enabled** (default) ◆ **Disabled**
Max Log Entries	Set the maximum number of HTTP server log entries. Only the last **Max Log Entries** are cached and viewable.

HTTP Settings	Description
Log Format	Set the log format string for the HTTP server. Follow these **Log Format** rules: ◆ **% a** - remote IP address (could be a proxy) ◆ **% b** - bytes sent excluding headers ◆ **% B** - bytes sent excluding headers (0 = '-') ◆ **% h** - remote host (same as '% a') ◆ **% {h}i** - header contents from request (h = header string) ◆ **% m** - request method ◆ **% p** - ephemeral local port value used for request ◆ **% q** - query string (prepend with '?' or empty '-') ◆ **% t** - timestamp HH:MM:SS (same as Apache '% (% H:% M:% S)t' or '% (% T) t') ◆ **% u** - remote user (could be bogus for 401 status) ◆ **% U** - URL path info ◆ **% r** - first line of request (same as '% m % U% q <version>') ◆ **% s** - return status
Authentication Timeout	The timeout period applies if the selected authentication type is either **Digest** or **SSL/ Digest**. After this period of inactivity, the client must authenticate again.

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 9-20 HTTP Authentication

HTTP Authentication Settings	Description
URI	Enter the URI. The URI must begin with / to refer to the filesystem.
Authentication Type	Select an HTTP authentication type. The different types offer various levels of security, from the least to most secure: ◆ **None:** no authentication necessary ◆ **Basic:** encodes passwords using Base64 ◆ **Digest:** encodes passwords using MD5 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. 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. Click **Submit** when URI and Authentication Type is entered to submit it.

HTTP Authentication Settings	Description
Delete	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">`

Please shut down any open browsers entirely and restart or refresh so it will use the updated web pages.

IP Address Filter

The EDS3000 devices support setting and viewing the IP Address Filtering configuration.

IP Address Filter Statistics and Configuration

The IP Address Filter Statistics page displays the statistics for the IP Address Filter. It shows the IP Address Filter State (Enabled or Disabled), the Default IP Address Filter Policy(Accept or Drop). The IP Address Filters Statistics page displays the current setting or the message “No IP Address filters are defined”.

The IP Address Filter Configuration page allows you to configure the IP Address Filter settings.

Table 9-21 IP Address Filter.

IP Address Filter Settings	Description
IP Address filter	Accept or Drop traffic based on sender or destination IP addresses. Select from: Accept, signifying that traffic to and from all IP addresses other than those with 'DROP' action will be accepted (IP blacklist) and Drop, signifying that traffic to and from all IP addresses other than those with 'ACCEPT' action will be dropped (IP whitelist).
Default IP Address Filter Policy	Sets the default IP Address filter policy.
IP Address	Enter the new IP address and select the Action to be taken. Select either: **ACCEPT**, signifying that traffic to and from all IP addresses other than those with 'DROP' action will be accepted (IP blacklist) or **DROP**, signifying that traffic to and from all IP addresses other than those with 'ACCEPT' action will be dropped (IP whitelist).
Add	Click the button to add the configured instance.

Line

The EDS3000PR offers 8, 16, or 32 serial port serial lines and EDS3000PS offers 8, or 16 serial ports serial lines 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 EDS3000 devices.*

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 9-22* for the line settings that can be modified on the Line - Configuration page. See *Table 9-23* for the line settings that can be established on the Line - Command Mode page.

Table 9-22 Line Configuration Settings

Line Settings	Description
Select Line	Select Console or Line 1 - Line 16. The default is Line 1.
Name	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.
Interface	Set the interface type for the Line. The default is RS232. Choices are: Interface is set to RS232 and cannot be changed.
State	Select to enable or disable the operational state of the Line. The default is Enabled.
Protocol	Set the operational protocol for the Line. The default is Tunnel . Choices are None, Tunnel and Managed Device. A change in line protocol will take effect on the next reboot.
Baud Rate	Set the Baud Rate (speed) of the Line. The default is 9600. Any set speed between 300 and 921600 may be selected: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400. When selecting a Custom baud rate, you may manually enter any value between 300 and 230400. ***Note:*** *Custom baud rates are not supported when a line is configured for Command Mode.*
Parity	Set the Parity of the Line to None, Even, or Odd. The default is None.
Data Bits	Set the number of data bits for the Line to 7 or 8. The default is 8.
Stop Bits	Set the number of stop bits for the Line to 1 or 2. The default is 1.
Flow Control	Set the flow control for the Line. The selections are None, Hardware, and Software. The default is None. ***Note:*** *This field becomes available if RS232 is selected under Interface above.*
Xon Char	Set Xon Char to be used when Flow Control is set to Software. Prefix decimal with \ or prefix hexadecimal with 0x or prefix a single control character <control>. ***Note:*** *This field becomes available for configuration when Software is selected under Flow Control.*
Xoff Char	Set Xoff Char to be used when Flow Control is set to Software. Prefix decimal with \ or prefix hexadecimal with 0x or prefix a single control character <control>. ***Note:*** *This field becomes available for configuration when Software is selected under Flow Control.*

Line Settings	Description
Baud Rate	Select the desired baud rate from the drop-down menu. The default is 9600.
Parity	Select parity from the drop-down menu. The default is None. Choices are None, Even, and Odd.
Data Bits	Select 7 or 8 data bits from the drop-down menu. The default is 8.
Stop Bits	Select 1 or 2 stop bits from the drop-down menu. The default is 1.
Flow Control	Select None, Hardware or Software flow control from the drop-down menu. The default is None.
Gap Timer	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.
Threshold	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 9-23 Line Command Mode Setting

Line Command Mode Settings	Description
Mode	Set the Command Mode state of the Line. When in Command Mode, a CLI session operates exclusively on the Line. Choices are: ◆ Always ◆ Use Serial String ◆ Disabled ***Note:*** *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.*
Wait Time	Enter the amount of time to wait during boot time for the Serial String. This timer starts right after the Sign on Message has been sent on the Serial Line and applies only if mode is Use Serial String. ***Note:*** *This field becomes available when Use Serial String is selected for Mode.*
Serial String	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]. ***Note:*** *This field becomes available when Use Serial String is selected for Mode.*
Echo Serial String	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. ***Note:*** *This field becomes available when Use Serial String is selected for Mode.*
Signon Message	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. ***Note:*** *The Submit button will only appear if the Mode is not disabled.*

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>">`

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 EDS3000 devices.

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 9-24 RSS

RSS Settings	Description
RSS Feed	Click to select whether to turn the RSS Feed **On** or **Off**.
Persistent	Click to select whether to turn Persistent mode for the RSS Feed **On** or **Off**.
Max Entries	Enter the numerical value of maximum RSS feed entries to be cached and viewable. Default is 100.
Data	◆ Click **View** to view existing RSS data. ◆ Click **Clear** to clear accumulated RSS data.

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 9-25 SMTP Settings

SMTP Settings	Description
From Address	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.
Server Address	Enter the Server Address to direct outbound email messages through a mail server.
Server Port	Enter the SMTP server port number. The default is 25.
Username	Enter a Username to direct outbound email messages through a mail server.
Password	Enter a Password to direct outbound email messages through a mail server.
Overriding Domain	Enter the domain name to override the current domain name in EHLO (Extended Hello). The Overriding Domain is used to forge the sender Domain Name in the outgoing Email message. This might be necessary, for example, if this device is located behind a firewall whose IP Address resolves to a different Domain Name than this device. For SPAM protection, many SMTP servers perform reverse lookups on the sender IP Address to ensure the Email message is really from who it says it is from.
Local Port	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 9-26 SNMP Settings

SNMP Settings	Description
SNMP Agent	
State	Select to enable or disable the SNMP agent state.
Port	Set the port of the SNMP agent.
Version	Select the SNMP version used by the SNMP agent. Choices are SNMPv1, SNMPv2c, and SNMPv3.
Read Community	Specify the read community used by the agent (defaults to public community).
Write Community	Specify the write community used by the agent (defaults to private community).
Username	For both a Read/Write User and a Read-Only User, enter the SNMPv3 username to be used by trap.
Security	At the dropdown select either No Authentication and No Privacy, or Authentication but No Privacy, or Authentication and Privacy.
Authentication Protocol	At the dropdown select either MD5 or SHA as the Auth protocol to use. The default is SHA
Authentication Password	Enter a valid Auth password.
Privacy Protocol	At the dropdown select either DES (Data Encryption Standard) or AES (Advanced Encryption Standard) as the Priv protocol to use. The default is DES.
Privacy Password	Enter a valid Priv password.
System MIB	
System Contact	Specify the system contact.
System Name	Update the system name, as necessary.
System Description	Update the system description, as necessary. The default system information includes the manufacturer name, model name, version and the serial number of the EDS3000 devices.
System Location	Specify a system location for the SNMP setting.
MIB	
Lantronix MIB File	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.
MIB File	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.
SNMP Traps	
Primary Destination	Enter the Primary Destination. ***Note:*** *SNMP Traps fields become available when SNMP Agent State is enabled.*
Primary Destination Port	Enter the Primary Destination port. ***Note:*** *SNMP Traps fields become available when SNMP Agent State is enabled.*
Secondary Destination	Enter the Secondary Destination. ***Note:*** *SNMP Traps fields become available when SNMP Agent State is enabled.*
Secondary Destination Port	Enter the Secondary Destination port. ***Note:*** *SNMP Traps fields become available when SNMP Agent State is enabled.*
Version	At the dropdown select SNMPv1, SNMPv2c, or SNMPv3 for SNMP Traps.

SNMP Settings	Description
Username	Enter a user name for SNMP Traps.
Security	At the dropdown select either No Authentication and No Privacy, or Authentication but No Privacy, or Authentication and Privacy for SNMP Traps.
Authentication Protocol	At the dropdown select either MD5 or SHA as the Auth protocol to use for SNMP Traps. The default is SHA
Authentication Password	Enter a valid Auth password. SNMP Trap Authentication Password must be at least 8 characters.

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 EDS3000 devices or automatically generated on the device.

Configuration is required when the EDS3000 devices are 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 used for tunneling in Connect Mode.

To configure the EDS3000 devices 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 EDS3000 devices 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 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.

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

Table 9-27 SSH Server Host Keys

SSH Settings	Description
Private Key	Click the **Choose File** 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.
Public Key	Click the **Choose File** button to navigate to the existing public key you want to upload.
Submit (button)	Click the **Submit** button after changes are made in the above Upload Keys fields.

SSH Settings	Description
Key Type	Select a key type to use for the new key: ◆ RSA ◆ DSA
Bit Size	Select a bit length for the new key: ◆ 512 ◆ 768 ◆ 1024 ◆ 2048 ◆ 4096
Submit (button)	Click the **Submit** button after changes are made in the above Create New Keys fields.

Note: *SSH Keys from other programs may be converted to the required EDS3000 devices 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 9-28 SSH Server Authorized Users

SSH Settings	Description
Username	Enter a new username or edit an existing one.
Password	Enter a new password or edit an existing one.
Public RSA Key	Click the **Choose File** 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.
Public DSA Key	Click the **Choose File** 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.
Add/Edit (button)	Click the **Add/Edit** 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 9-29 SSH Client Known Hosts

SSH	Settings Description
Server	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.
Public RSA Key	Click the **Choose File** 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.
Public DSA Key	Click the **Choose File** 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.
Submit (button)	Click the **Submit** 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 EDS3000 devices 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 EDS3000 devices 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 9-30 SSH Client Users

SSH Settings	Description
Username	Enter the name that the EDS3000 devices uses to connect to an SSH server.
Password	Enter the password associated with the username.
Remote Command	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.

SSH Settings	Description
Private Key	Click the **Choose File** 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.
Public Key	Click the **Choose File** button to browse to the existing public key you want to upload.
Key Type	Select a key type: ◆ RSA ◆ DSA
Add/Edit (button)	Click the **Add/Edit** button after changes are made in the above SSH Client: Users fields.

Table 9-31 Create New Keys

SSH Setting	Description
Username	Enter the **Username** for the new key.
Key Type	Select a key type for the new key: ◆ RSA ◆ DSA
Bit Size	Select the bit length of the new key: ◆ 512 ◆ 768 ◆ 1024 ◆ 2048 ◆ 4096 Using a larger bit size takes more time to generate the key. Approximate times are: ◆ 1 second for a 512 bit RSA key ◆ 1 second for a 768 bit RSA key ◆ 1 second for a 1024 bit RSA key ◆ 2 seconds for a 512 bit DSA key ◆ 2 seconds for a 768 bit DSA key ◆ 20 seconds for a 1024 bit DSA key ***Note:*** *Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 2048 bits long.*
Submit (button)	Click the **Submit** 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 EDS3000 devices to peers and are used with some methods of wireless authentication. Provide a name at upload time to identify certificates on the EDS3000 devices.

You can upload Certificate and Private key combinations, obtained from an external Certificate Authority (CA), to the EDS3000 devices. The EDS3000 devices can also generate self-signed certificates with associated private keys.

Credentials

The EDS3000 devices 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 EDS3000 devices. 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 9-32 SSL Credential - Upload Certificate

Upload Certificate Settings	Description
New Certificate	Click the **Choose File** button to browse to the SSL certificate to be uploaded. RSA or DSA certificates are allowed.
New Certificate Type	Select the certificate type to upload: ◆ PEM ◆ PKCS7 ◆ PKCS12
New Private Key	Click the **Choose File** button to browse to the SSL private key to be uploaded. The key must belong to the entered certificate.
New Key Type	Select the key type being uploaded: ◆ PEM ◆ Encrypted PEM ◆ PKCS12
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

Table 9-33 SSL Credential - Create New Self-Signed Certificate

Field	Description
Country (2 Letter code)	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).
State/Province	Enter the state or province where the organization is located.
Locality (City)	Enter the city where the organization is located.
Organization	Enter the organization name to which the EDS3000 devices belongs.
Organization Unit	Enter the organization unit which specifies the department or organization to which the EDS3000 devices belongs.
Common Name	Enter a network name for the EDS3000 devices 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 EDS3000 devices 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 EDS3000 devices is accessed using HTTPS.
Expires	Type the date that the self-signed certificate expires in **mm/dd/yyyy** format.
Type	Select **RSA**, **DSA**, or **ECDSA**.

Field	Description
Key length	Select the key length: ◆ 512 bit ◆ 768 bit ◆ 1024 bit ◆ 2048 bit ◆ 4096 bit
ECDSA curve	Select the ECDSA curve: ◆ 256 bit ◆ 384 bit ◆ 521 bit

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 9-33 SSL Credential - Create New Self-Signed Certificate on page 75*.
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 9-34 SSL Trusted Authority

Trusted Authorities Settings	Description
Authority	Click the **Choose File** button to browse to an existing SSL authority certificate. RSA or DSA certificates are allowed. The format of the authority certificate can be PEM, PKCS7, or PKCS12. 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.
New Certificate Type	Select the certificate type through the drop-down list. This field may automatically update, depending upon extension of the certificate entered.
Password	If the field is PKCS12, then corresponding password should be entered in the Password field. An option displays to Show Password as it is typed.
Delete All	To delete all existing certificate authorities as listed, click the **Delete ALL** button.
Delete	To delete an existing certificate authority, click the **Delete** button beside the specific authority listed under **Current Certificate Authorities**.

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 EDS3000 devices uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the EDS3000 devices 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 EDS3000 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 EDS3000 device. The EDS3000 device 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 9-35 SSL CSR (Certificate Signing Request)

Field	Description
Country (2 Letter code)	Enter the two-letter ISO code (e.g., **US** for the United States) for the country where the organization is located.
State/Province	Enter the state or province where the organization is located.
Locality (City)	Enter the city where the organization is located.
Organization	Enter the organization name to which the EDS3000 devices belongs.
Organization Unit	Enter the department within the organization to which the EDS3000 devices belongs.
Common Name	Enter the network name of the EDS3000 devices 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 EDS3000 devices 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 EDS3000 devices is accessed using HTTPS.
Type	Select either **RSA** or **ECDSA**.
Key length	Select the key length of **2048** or **4096** bits.
ECDSA curve	Select 256 bit, 384 bit, or 521 bit.

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 9-36 Syslog

Field	Description
State	Enable or disable the Syslog.
Host	Enter the IP address of the remote server that stores the logs.
Remote Port	Enter the port number for the remote host that supports logging services. The default port is 514.
Local Port	Enter the local port to use for Syslog.
Severity Log Level	Select the minimum syslog severity level that should be logged.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** 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 EDS3000 devices 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 9-37 System Settings

System Settings	Description
State	Select to enable or disable the reboot schedule. ***Warning:*** ***Use extreme caution when using scheduled reboots. The EDS3000 devices 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.***
Schedule	Select the reboot schedule interval: **Daily** or **Interval.**
Time (24 hour)	Set the time to reboot by selecting the **Hour** and **Min** (Minute) in the drop-down menus. ***Note:*** *This configuration option appears when the* ***Daily*** *schedule is selected.*
Interval	Enter the interval number in the field. Then select the type of interval from the drop-down menu: ◆ Hours ◆ Days ◆ Weeks ◆ Months ***Note:*** *This configuration option appears when the* ***Interval*** *schedule is selected.*
Submit (button)	Click the **Submit** button after settings are made in the above Reboot Schedule fields.
Reboot Device	Click the **Reboot** button to reboot the EDS3000 devices. When rebooted, your browser should be refreshed and redirected to the main status page after 30 seconds. ***Note:*** *The redirect will not work as expected if the IP Address of the EDS3000 devices changes after reboot.*
Restore Factory Defaults	Click the **Factory Defaults** button to restore the EDS3000 devices to the original factory settings. All configuration will be lost. The EDS3000 device automatically reboots upon setting back to the defaults. After setting the configuration back to the factory defaults, the device will automatically be rebooted.
Reset to Defaults CP	Choose to enable or disable reset to factory default function via the CP that may be accessible to walk-up users. ***Note:*** *The factory reset pin is not supported.*

System Settings	Description
Upload New Firmware	Click **Choose File** to browse to and select the firmware file. If Secure Boot is enabled, only authorized software is allowed to run on the EDS3000 devices. Secure Boot requires that the firmware is signed by Lantronix or the authorized OEM. To check if Secure Boot is enabled, click **Status** 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 EDS3000 devices. The device automatically reboots upon the installation of new firmware. See the section *FTP on page 58*. ***Caution:*** ***Do not to power off or reset the EDS3000PR devices while uploading new firmware. Once the upload has completed and the new firmware has been verified and flashed to memory, the EDS3000 devices will automatically be rebooted.***
Short Name	Enter a short name for the system name. A maximum of 32 characters is allowed.
Long Name	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 9-38 Terminal on Network and Line Settings

Terminal on Network and Line Settings	Description
Terminal Type	Enter text to describe the type of terminal. The text will be sent to a host via IAC. ***Note:*** *IAC means, “interpret as command.” It is a way to send commands over the network such as* **send break** *or* **start echoing**. *IAC is only supported in Telnet.*

Terminal on Network and Line Settings (continued)	Description
Login Connect Menu	Select the interface to display when the user logs in. Choices are: ◆ **Enabled** = shows the Login Connect Menu. ◆ **Disabled** = shows the CLI (default)
Exit Connect Menu	Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are: ◆ **Enabled** = a choice allows the user to exit to the CLI. ◆ **Disabled** = there is no exit to the CLI (default)
Send Break	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: `<Ctrl> Y` Blank the field to set to `<None>`. ***Note:*** *This field is not available for terminal network configuration.*
Break Duration	Specify the length in milliseconds of the spacing condition placed on the line when a break is sent. ***Note:*** *This field is not available for terminal network configuration.*
Echo	Select whether to enable echo: ◆ **Enabled** ◆ **Disabled** ***Note:*** *Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable **Echo** if your terminal echoes, in which case you will see double of each character typed. Default is enabled.*

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 all terminal line instances of EDS3000 devices.*

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 sub-menus. 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 those 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 9-39 Tunnel Serial Settings

Terminal Serial Settings	Description
Line Settings	Line Settings information here is display only. Go to the section, *To Configure the Terminal Line* to modify these settings.
Protocol	Protocol information here is display only. Go to the section, *To Configure the Terminal Line* 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: ◆ **Unasserted** ◆ **TruPort** = 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. ◆ **Asserted while connected** = The DTR is asserted whenever either a connect or an accept mode tunnel connection is active. ◆ **Continuously asserted**

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 Packed (queued) and sent in segments, when either the timeout or byte threshold is reached. Packing applies to both Accept and Connect Modes.

Table 9-40 Tunnel Packing Mode Settings

Tunnel Packing Mode Settings	Description
Mode	Configure the Tunnel Packing Mode. Choices are: ◆ **Disable** = Data not packed. ◆ **Timeout** = Data sent after timeout occurs. ◆ **Send Character** = Data sent when the Send Character is read on the Serial Line.
Threshold	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. ***Note:*** *This configuration option appears when Timeout mode or Send Character mode is selected.*
Timeout	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. ***Note:*** *This configuration option appears when Timeout mode is selected.*
Send Character	Enter Control Characters in any of the following forms: ◆ `<control>J` ◆ `0xA` (hexadecimal) ◆ `\10` (decimal) 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. ***Note:*** *This configuration option appears when Send Character mode is selected.*

Tunnel Packing Mode Settings (continued)	Description
Trailing Character	Enter Control Characters in any of the following forms: ◆ <control>J ◆ 0xA (hexadecimal) ◆ \10 (decimal). 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>). ***Note:*** *This configuration option appears when Send Character mode is selected.*

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 EDS3000 device 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 9-41 Tunnel Accept Mode Settings

Tunnel Accept Mode Settings	Description
Mode	Set the method used to start a tunnel in Accept mode. Choices are: ◆ **Disable** = Do not accept an incoming connection. This is the default mode. ◆ **Always** = Accept an incoming connection. ◆ **Any Character** = Start waiting for an incoming connection when any character is read on the serial line. ◆ **Start Character** = Start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. ◆ **Modem Control Asserted** = Start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made. ◆ **Modem Emulation** = Start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.

Tunnel Accept Mode Settings (continued)	Description
Local Port	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: 1000+X. For example: ◆ Tunnel 1: 10001 ◆ Tunnel 2: 10002
Protocol	Select the protocol type for use with Accept Mode: ◆ SSH ◆ SSL ◆ TCP (default protocol) ◆ TCP with AES ◆ Telnet
TCP Keep Alive	Enter the time, in milliseconds, the EDS3000 device 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.
TCP Keep Alive Interval	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.
TCP Keep Alive Probes	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.
TCP User Timeout	Specify how long TCP segments will be retransmitted before the connection is closed. The default is **0** milliseconds.
Initial Send	Enter the **Initial Send** data to be sent out the network upon connection establishment before any data from the Line. It may contain one or more **Directives** of the form `%<char>`. The Initial Send string can be entered in **Text** or **Binary** 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]` **Directives** ◆ `%i` local IP address ◆ `%m` MAC address ◆ `%n` network interface name ◆ `%p` local port ◆ `%s` serial number ◆ `%%` %
Flush Serial	Set whether the serial line data buffer is flushed upon a new network connection. Flush Serial applies at the time when a connection is accepted from the network. Choices are: ◆ **Enabled** = Serial data buffer is flushed on network connection ◆ **Disabled** = Serial data buffer is not flushed on network connection (*default*)

Tunnel Accept Mode Settings (continued)	Description
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ◆ **Enabled** = 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. ◆ **Disabled** = This is the default setting; incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: ◆ **Enabled** = 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. ◆ **Disabled** = This is the default setting; incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.
Password	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: ◆ 0A (Line Feed) ◆ 00 (Null) ◆ 0D 0A (Carriage Return/Line Feed) ◆ 0D 00 (Carriage Return/Null) If **Prompt for Password** is set to **Enabled** and a password is provided, the user will be prompted for the password upon connection.
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 Connect comes into play when an Accept mode tunnel is established. If an Email profile number has been selected, an email notification based on that profile will then be sent.
Email on Disconnect	Select an email profile number to which an email notification will be sent upon the disconnection of an accept mode tunnel. Email on Disconnect comes into play when an Accept mode tunnel is disconnected. If an Email profile number has been selected, an email notification based on that profile will then be sent.

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 EDS3000 device continues to attempt an outgoing connection on the network until established (based on which connection method is selected in the configuration described in
Table 9-42). 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 address or DNS name. The EDS3000 device will not make a connection unless it can resolve the address. For Connect Mode using UDP, the EDS3000 devices 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 keep alive 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 9-42 Tunnel Connect Mode Settings

Tunnel Connect Mode Settings	Description
Mode	Set the method to be used to attempt a connection to a remote host or device. Choices are: ◆ **Disable** = an outgoing connection is never attempted. (*default*) ◆ **Always** = a connection is attempted until one is made. If the connection gets disconnected, the EDS3000 device retry until it makes a connection. ◆ **Any Character** = A connection is attempted when any character is read on the serial line. ◆ **Start Character** = A connection is attempted when the start character for the selected tunnel is read on the serial line. ◆ **Modem Control Asserted** = A connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made. ◆ **Modem Emulation** = A connection is attempted when triggered by modem emulation AT commands.
Local Port	Enter an alternative Local Port. The Local Port is set to <Random> by default but can be overridden. Blank the field to restore the default.
Host 1	Click on the displayed information to expand it for editing. Complete the Host fields that appear according to *Table 9-43*. If <None> 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.
Reconnect Timer	Set the value of the reconnect timeout (in milliseconds) for outgoing connections established by the EDS3000 device. Valid range is 1 to 65535 milliseconds. Default is 15000.
Flush Serial Data	Set whether the serial Line data buffer is flushed upon a new network connection. Choices are: ◆ **Enabled** = Serial data buffer is flushed on network connection ◆ **Disabled** = Serial data buffer is not flushed on network connection (*default*)

Tunnel Connect Mode Settings (continued)	Description
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ◆ **Enabled** = 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. ◆ **Disabled** = This is the default setting; incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: ◆ **Enabled** = 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. ◆ **Disabled** = This is the default setting; incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.
Email on Connect	Select an email profile number to which an email notification will be sent upon the establishment of a connect mode tunnel.
Email on Disconnect	Select an email profile number to which an email notification will be sent upon the disconnection of a connect mode tunnel.

Table 9-43 Host Settings

Host Field	Description
Address	Enter the address for the remote host connection. Either a DNS address or an IP address maybe provided.
Port	Designate the TCP or UDP port on the remote host for connection.
Protocol	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.
SSH Username	Enter a Username. This configuration field becomes available when the SSH Protocol is selected.
Credentials	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 *SSL* > *Credentials* page.
Validate Certificate	Select to enable or disable. This configuration field becomes available when the SSL protocol is selected.
TCP Keep Alive	Enter the time, in milliseconds, the EDS3000 device 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.
TCP Keep Alive Interval	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.
TCP Keep Alive Probes	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.
TCP User Timeout	Specify the amount of time the TCP segments will be retransmitted before the connection is closed.

Host Field	Description
AES Encrypt Key	Enter the AES Encrypt Key and select **Text** or **Hexadecimal** to indicate format. This configuration field becomes available when the TCP AES or UDP AES protocol is selected. Host AES Encrypt key length must be 16, 24, or 32 bytes.
AES Decrypt Key	Enter the AES Decrypt Key and select **Text** or **Hexadecimal** to indicate format. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
Initial Send	Enter the Initial Send character and select either **Text** or **Binary** 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 EDS3000 device, the Connect Mode supports up to 16 hosts. Hosts may be accessed sequentially or simultaneously:

- **Sequential** – A 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 91*). 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 EDS3000 devices 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:

Click the  icon in the desired Host field; for example Host 2 and Host 3.

5. The selected Host(s) exchanges its place with the Host above it.
6. 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 from the EDS3000 device, a Connect Mode connection will attempt to reconnect. However, if none of these conditions are selected, closure from the network is taken as a disconnected host. The EDS3000 can support a maximum of 64 total aggregate connections.

Table 9-44 Tunnel Disconnect Mode Settings

Tunnel Disconnect Mode Settings	Description
Stop Character	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`(hexadercimal) or `\10` (decimal). Disable the Stop Character by blanking the field to set it to `<None>`.
Modem Control	Set whether Modem Control enables disconnect when the Modem Control pin is not asserted on the Serial Line. Choices are: ◆ **Enabled** ◆ **Disabled** (default)
Timeout	Enter the number of milliseconds a tunnel may be idle before disconnection. The value of zero disables the idle timeout. The valid range is 0 - 4294967295 milliseconds.
Flush Serial Data	Set whether to flush the Serial Line when the Tunnel is disconnected. Choices are: ◆ **Enabled** ◆ **Disabled** (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 EDS3000 devices mimic the modem's behavior.

Table 9-45 Tunnel Modem Emulation Settings

Tunnel Modem Emulation Settings	Description
Echo Pluses	Set whether the pluses will be echoed back during a “pause +++ pause” escape sequence on the Serial Line. Choices are: ◆ **Enabled** ◆ **Disabled** (default)
Echo Commands	Set whether characters read on the Serial Line will be echoed, while the Line is in Modem Command Mode. With Echo Commands enabled (ATE1), characters read on the Serial Line will be echoed while the Line is in Modem Command mode. Choices are: ◆ **Enabled** (default) ◆ **Disabled**
Verbose Response	Set whether Modem Response Codes are sent out on the Serial Line. With Verbose Response enabled (ATQ0), Modem Response Codes are sent out on the Serial Line. Choices are: ◆ **Enabled** (default) ◆ **Disabled**
Response Type	Select a representation for the Modem Response Codes sent out on the Serial Line. Choices are: ◆ **Text** (ATV1) (default) ◆ **Numeric** (ATV0)
Error Unknown Commands	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: ◆ **Enabled** ◆ **Disabled** (default)
Incoming Connection	Set how and if requests are answered after an incoming RING (ATS0=2). Incoming Connection requests may be disabled (ATS0=0), answered automatically (ATS0=1), or answered manually via the ATA command after an incoming RING (ATS0=2). Choices are: ◆ **Disabled** (default) ◆ **Automatic** ◆ **Manual**
Connect String	Enter the customized Connect String sent to the Serial Line with the Connect Modem Response Code.
Display Remote IP	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: ◆ **Enabled** ◆ **Disabled** (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 9-46 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
Username	View and modify the Administrator **Username** as desired. The default Username is `admin`.
Password	Modify the Administrator **Password** as desired. The default Password is the last 8 characters of the Device ID.
Submit	Click **Submit** to submit changes **Username** and/or **Password**. The **Submit** button appears when either or both Username and Password are modified.

Table 9-47 Current Users List

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

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

Table 9-48 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 9-47*). In addition to the built-in Admin account, up to 8 user accounts can be created to access the EDS3000 devices.

New User Settings	Description
Username	Enter the **Username** of the new user. Must be between 4 and 15 characters.
Password	Enter the **Password** of the new user. Must be between 4 and 15 characters. Password can contain a combination of uppercase letters, lowercase letters, numbers, and symbols (punctuation marks).

New User Settings	Description
Role	Click the **Role** field to select a role for this user: ◆ Administrator ◆ Technician ◆ User
Add	Click **Add** to submit the new user. Click **OK** in the confirmation window which appears to add the user.

Table 9-49 Current Roles List

The system-defined default roles that come with the EDS3000 devices along with any Admin-created user roles are listed here. Admin-created custom roles can be deleted or altered.

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

Table 9-50 New Role Settings

Create a custom role here. Admin-created custom roles can be deleted or altered in the Current Roles list (*Table 9-49*). 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 **Actions** that the new role will have access to, if any: ◆ Device Reboot ◆ Factory Reset ◆ Firmware Upgrade

New Role Settings	Description
Configuration Groups	Check the Configuration Groups the new role will have access to configuring, if any: ◆ ARP ◆ CLI ◆ Clock ◆ Percepxion ◆ Percepxion Line ◆ CP Functions ◆ Device ◆ Diagnostics ◆ Discovery ◆ Email ◆ FTP Server ◆ Host ◆ HTTP Authentication ◆ HTTP ◆ ICMP ◆ Interface ◆ IP ◆ IP address filters ◆ Line ◆ Reboot schedule ◆ RSS ◆ Serial Command Mode ◆ SMTP ◆ SNMP ◆ SSH ◆ SSH client ◆ SSH server ◆ SSL ◆ Syslog ◆ Telnet ◆ Terminal ◆ Tunnel Accept ◆ Tunnel Connect ◆ Tunnel Disconnect ◆ Tunnel Modem ◆ Tunnel Packing ◆ Tunnel Serial ◆ User Management ◆ Wired Networking
Add	Click **Add** to submit the new role. Click **OK** 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 EDS3000 devices or another.

XML records can also be exported to a browser window or to a download link on the EDS3000 devices.

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 terminal 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:eth0.`

  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 9-51*) and click **Import**.
   - **Line(s) from single line Settings on the Filesystem** copies lines settings from an input file containing only one Line instance to all of the selected Lines. Make selections in form which appears (see *Table 9-52*) 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 9-51 Configuration from Filesystem

Setting	Description
Filename	Enter the name of the file on the EDS3000 device (local to its file system) that contains XCR data.
Lines to Import	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 **Clear All** to clear all check marks, or **Select All** to check all check marks.
Whole Groups to Import	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group. Click **Clear All** to clear all check marks, or **Select All but Networking** to check all check marks except Networking.
Text List	Enter the string to import specific instances of a group. The textual format of this string is: `<g>:<i>;<g>:<i>;...` Each group name <g> is followed by a colon and the instance value <i> and each <g>:<i> value is separated by a semi-colon. If a group has no instance then only the group name <g> should be specified.
Import (button)	Click the **Import** button when the Configuration from Filesystem fields are completed above.

Table 9-52 Line(s) from single line Settings on the Filesystem

Setting	Description
Filename	Enter the name of the file on the EDS3000 device (local to its file system) that contains XCR data.
Lines to Import	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 **Clear All** to clear all check marks, or **Select All** to check all check marks.
Whole Groups to Import	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group. Click **Clear All** to clear all check marks, or **Select All but Networking** to check all check marks except Networking.
Import (button)	Click the **Import** 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 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 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 EDS3000 configuration procedures require you to assemble a series of options (represented as bits) into a complete command (represented as a byte).
The resulting binary value must be converted to a hexadecimal representation.

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

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

Converting Binary to Hexadecimal

Conversion Table

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

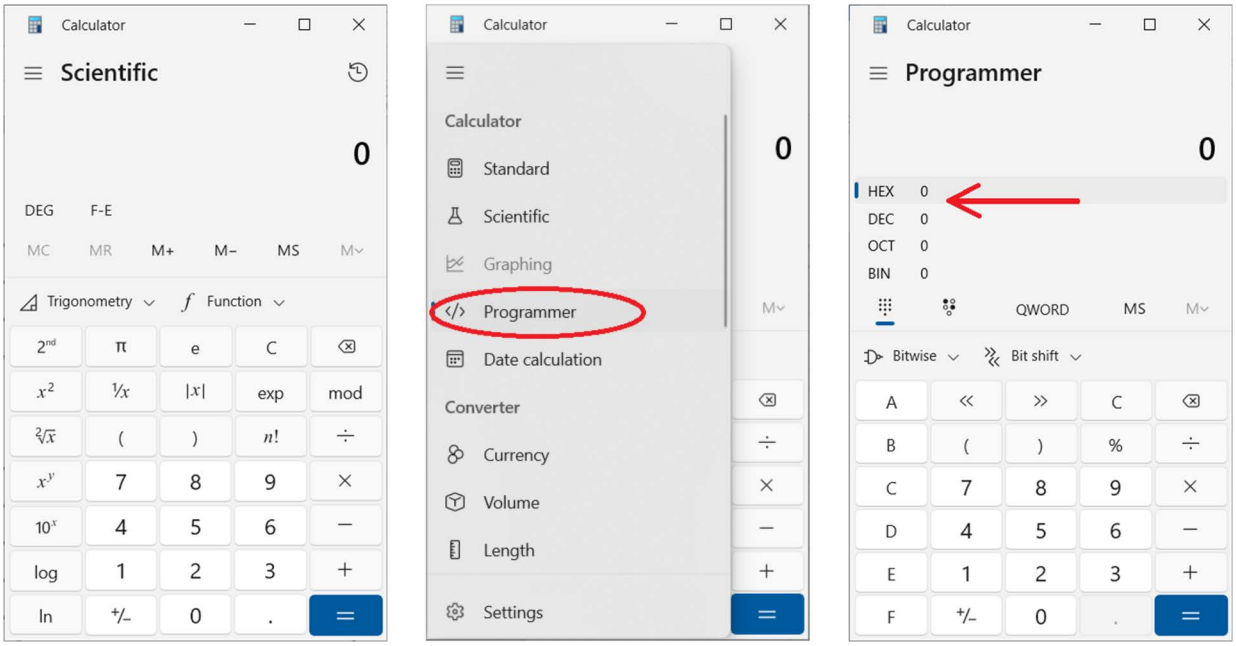
Table B-1 Binary to Hexadecimal Conversion Table

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 then click the = sign**. The hexadecimal value appears.

Appendix C: Compliance

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

LANTRONIX

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: _____

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

EU Declaration of Conformity for EDS3008PS, 3016PS

UK DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 USA
Product Type: Ethernet router
Product Family: EDS3008PS / EDS3016PS
Rated: 100-240Vac, 50-60Hz, 0.5A
Intended use: Commercial installations, indoor use

Manufacturer's Quality System:

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Electrical Equipment Regulations 2016

- **IEC 62368-1:2018**

Electromagnetic Compatibility Regulations 2016

- **EN 55032:2015, Class A**
- **EN 55035:2017**
- **EN 61000-3-2:2014, Class A**
- **EN 61000-3-3:2013**
- **EN 61000-4-2:2009**
- **EN 61000-4-3:2006 +A1:2008 +A2:2010**
- **EN 61000-4-4:2012**
- **EN 61000-4-5:2014**
- **EN 61000-4-6:2014**
- **EN 61000-4-8:2009**
- **EN 61000-4-11:2004 +A1:2017**

UK SI 2012 No. 3032 for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I and 6(c).
1) 2011/65/EU Restriction of the use of Hazardous Substances in EEE (RoHS)
2) 2015/863/EU Change of Annex II from 2011/65/EU
3) Directive 2018/736/EU[7(c)-I] and 2018/741/EU[6(c)]
BS EN IEC 63000 : 2018

Statement of Conformity: The product specified above meets the test requirements of the relevant legislation of United Kingdom, including the application of sound engineering practice.

Signature: _____ Date: November 7, 2022

Name: Fathi Hakam Title: VP of Engineering

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, 2nd Edition 2019-05-09

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

UL 62368-1, 2nd Edition, 2014-12-01

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

NDAA, RoHS, REACH and WEEE Compliance Statement

Please visit http://www.lantronix.com/legal/rohs/ for Lantronix's statement about NDAA, 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 FALSCHE BATTERIE EINGESETZT, BESTEHT EXPLOSIONSGEFAHR. SETZEN SIE NUR EINE BATTERIE DES GLEICHEN ODER EINES ENTSPRECHENDEN, VOM HERSTELLER EMPFOHLENEN TYPS EIN. ENTSORGEN SIE VERBRAUCHTE BATTERIEN GEMÄSS DEN ANWEISUNGEN DES HERSTELLERS.

Installationsanweisungen

Rackmontage nur für EDS3000PR

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 for EDS3000PR only

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/EDS3008/16PS for setup or device connectivity. Connects the RJ45 RS232 serial ports of EDS3008/3016/3032PR/ EDS3008/16PS to a DB9M DTE interface of a PC or serial device.
200.2066A	Adapter RJ45-to-DB25M	Allows a standard straight-pinned CAT5 cable to connect the EDS3008/3016/3032PR/EDS3008/16PS RJ45 serial ports to the DB25F DTE interface of a serial device.
200.2067A	Adapter RJ45-to-DB25F	Allows a standard straight-pinned cable to connect the EDS3008/ 3016/3032PR/EDS3008/16PS RJ45 serial ports to the DB25M DTE interface of a serial device.
200.2069A	Adapter RJ45-to-DB9M	Allows a standard straight-pinned cable to connect the EDS3008/ 3016/3032PR/EDS3008/16PS RJ45 serial ports to the DB9F DTE interface of a serial device.
200.2070A	Adapter RJ45-to-DB9F	Allows a standard straight-pinned cable to connect the EDS3008/ 3016/3032PR/EDS3008/16PS to the DB9M DTE interface of a PC or serial device.
200.2071	Adapter RJ45-to-DB9M DCE	Allows a standard straight-pinned cable to connect the EDS3008/ 3016/3032PR/EDS3008/16PS RJ45 serial ports to the DB9F DCE interface of a serial device.
200.2072	Adapter RJ45-to-DB9F DCE	Allows a standard straight-pinned cable to connect the EDS3008/ 3016/3032PR/EDS3008/16PS RJ45 serial ports to the DB9M DCE interface of a serial device.
200.2073	Adapter RJ45-to-DB25M	Allows a standard straight-pinned cable to connect the EDS3008/ 3016/3032PR/EDS3008/16PS RJ45 serial ports to the DB25F DCE interface of a serial device.
200.2074	Adapter RJ45-to-DB25F	Allows a standard straight-pinned cable to connect the EDS3008/ 3016/3032PR/EDS3008/16PS RJ45 serial ports to the DB25M DCE interface of a serial device.
ADP010104-01	Adapter “Rolled” RJ45-to-RJ45	Allows a standard straight-pinned cable to connect the EDS3008/ 3016/3032PR/EDS3008/16PS to an RJ45 console port on products from Cisco and other manufacturers.