EDS5000 Series Device Server

EDS5008, EDS5016, and EDS5032

User Guide

Part Number PMD-00226
Revision A July 2024

Intellectual Property

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

Patented: www.lantronix.com/legal/patents/. Additional patents pending.

Warranty

For details on the Lantronix warranty policy, go to www.lantronix.com/technical-support/warranty/.

Contacts

Lantronix, Inc.
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free: 800-526-8766
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 Contact Us | Lantronix

Disclaimer

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

Revision History

Rev	Date	Description
A	7/2/24	Initial release at FW v 2.0.0.0R2. See the Release Notes for more information.

Contents

1. About This Manual

Purpose

This guide provides the information needed to install, configure, and use the Lantronix EDS5000 Series Device Server using the web interface. This user guide provides the information needed to configure, use, and update the Lantronix® EDS5000 devices, which includes models EDS5008, EDS5016, and EDS5032. It is intended for software developers and system integrators who are installing the EDS5000 devices in their designs.

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
Chapter 2: Introduction	Describes the features of the product and its applications, SKUs, and hardware components.
Chapter 3: Installation	Instructions for installing the EDS5000 series device servers. List of Package Contents for the EDS5000.
Chapter 4: Using LPM (Lantronix Provisioning Manager)	Instructions for using Lantronix Provisioning Manager to locate and configure the EDS5000.
Chapter 5: Web Admin interface	Login instructions and Web Admin interface page control descriptions. Instructions for accessing the web administration interface and using it to configure settings for the EDS5000 series device servers. Key components on the web admin interface, logging in, changing passwords, and logging out.
Chapter 6: Quick Setup	Instructions for configuring WAN, Percepxion Client, SSH Access, and Time Synchronization.
Chapter 7: Status	View System, Percepxion, and Memory settings. View WAN interface status and Active Connections information, view ARP and Active IPv4 Routes information, view syslog and kernel log messages. View running system processes and their status and perform actions on running processes. View IPv6 routes and IPv6 neighbors.
Chapter 8: System	Instructions for how to perform system (timezone, logging, time synchronization), admin (password, SSH access, SSH keys), software (view free space and filter, download, upload and install software packages.), and perform backup, flash firmware, and reboot functions.
Chapter 9: Services	Instructions for configuring SNMPd, SNMPTRAPd, Service Actions, and uHTTPd services.

Chapter	Description
Chapter 10: Network	Instructions for configuring Interfaces, Host Names, Diagnostics, Protocol Stack, and FTP settings.
Chapter 11: Discovery	Instructions for configuring query port status and statistics and configuring response to auto-discovery messages. Instructions for enabling discovery on query port 0x77FE.
Chapter 12: Email	Instructions for configuring email messages and for viewing email statistics.
Chapter 13: Filesystem	Information on the Filesystem; the internal filesystem of the EDS5000. Instructions for viewing available and free filesystem space and for performing formatting.
Chapter 14: IP Address Filter	Instructions to enable or disable IP Address filters and set Default IP Address Filter Policies.
Chapter 15: Percepxion	Instructions for configuring Percepxion client and line settings for centralized device management.
Chapter 16: Serial	Instructions for configuring serial line settings and viewing receive and transmit statistics.
Chapter 17: SMTP	Instructions for configuring the Simple Mail Transfer Protocol data transmission format used to send and receive email.
Chapter 18: SSH	Instructions for configuring Secure Shell (SSH) Server and SSH Client.
Chapter 19: SSL	Instructions for creating SSL credentials, uploading SSL certificates and private keys from a CA or self-signed, generating self-signed certificates, and uploading trusted authority certificates.
Chapter 20: Tunnel	Instructions for configuring and enabling serial Tunnel connections. Configure Tunnel Accept, Connect host, Disconnect tunnel, Packing, Serial (DTR), Modem Emulation, and Modbus RTU to Modbus TCP settings. Displays current tunnel statistics.
Appendix A: Troubleshooting	Provides troubleshooting steps and information.
Appendix B: Compliance	Provides regulatory agency compliance information.
Appendix C: Cables	Provides information about accessories, cabling, and connectors.
Appendix D: Glossary	Provides a glossary of relevant acronyms and protocols.

Chapter	Description
Appendix E: Commands	Provides information on Bash commands, opkg (open package management) commands, and UCI (Unified Configuration Interface) commands.
Appendix F: Lantronix Technical Support	Provides instructions for contacting Lantronix Technical Support.

Additional Documentation

Visit the EDS5000 Series product page for the latest specifications, resources and part numbers for this product series.

Document	Description
EDS5000 Series Quick Start Guide	Provides hardware installation instructions, directions to connect the EDS5000 device server, and network IP configuration information.
EDS5000 Series Product Brief	Provides EDS5000 device server product overview information and specifications.
Lantronix Provisioning Manager Online Help	For instructions for using the Lantronix Provisioning Manager application that discovers, configures, upgrades, and manages Lantronix devices see: https://www.lantronix.com/products/lantronix-provisioning-manager/.

Additional Information

See the links below for the additional documentation for this product series.

Document	Description
SNMP documentation	net-snmp System Information: http://www.net-snmp.org/docs/man/snmpd.conf.html net-snmp Process Monitoring: http://www.net-snmp.org/docs/man/snmpd.conf.html net-snmp Disk Usage Monitoring: http://www.net-snmp.org/docs/man/snmpd.conf.html net-snmp System Load Monitoring: http://www.net-snmp.org/docs/man/snmpd.conf.html net-snmp Log File Monitoring: http://www.net-snmp.org/docs/man/snmpd.conf.html
SNMPd documentation	Download the Lantronix-SNMPD File for information on each field from the current EDS5000 IP address; for example from https://172.27.100.21/luci-static/resources/view/snmpd/lantronix-snmpd.pdf. Download the SNMPD master daemon/agent for SNMP from the net-snmp project: http://www.net-snmp.org/
Command links (bash, opkg, UCI)	bash commands: https://www.busybox.net/downloads/BusyBox.html opkg commands: https://openwrt.org/docs/guide-user/additional-software/opkg UCI commands: https://openwrt.org/docs/guide-user/base-system/uci

2. Introduction

The EDS5000 Series is the next-generation, rack-mountable device server that supports 8, 16, and 32 serial ports to Ethernet (10/100/1000BASE-T or 100/1000 SFP) for easy remote access and management of virtually any serial-based equipment such as security equipment, medical devices, or POS terminals with data access speeds of up to 921.6 kbps baud rate.

EDS5000 device servers deliver an unprecedented level of intelligence and safety with SSL/TLS and SSH security protocols as well as AES encryption. The EDS Series provides enterprise level security, allowing safe remote Ethernet access and management to your serial equipment from practically anywhere.

Setup is easy with Windows-based Lantronix Provisioning Manager, which can be used locally or remotely with the Lantronix Percepxion™ device management platform. Additionally, the EDS5000 family can be managed via a web browser or command line interface.

The Percepxion™ Centralized Device Management Platform lets you monitor, manage, and control your devices from anywhere, anytime, with the ready-to-use software platform. The Percepxion platform provides software-defined automation across all your devices and the capture of device telemetry data for event management and analytics.

The EDS5000 series offers three distinct models that differ mainly in serial port count. Model differences are noted in this manual where they exist.

Ordering Information

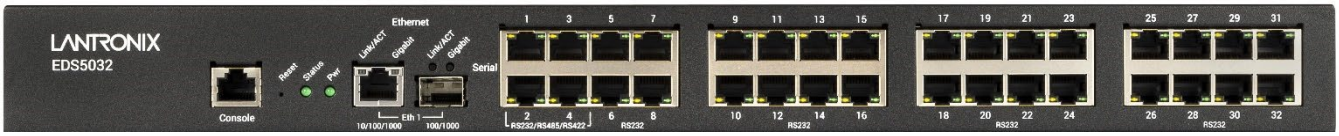
Part Number	Description
EDS5008	Ethernet to serial device server, (1) combo 10/100/1000 Mbps copper or 100/1000 Mbps SFP Ethernet port, 8 total serial device management ports consisting of (4) RS-232/422/485 software selectable and (4) RS232 only RJ-45 serial ports, (1) RJ-45 console port, 100-240 VAC, 60/60Hz input.
EDS5016	Ethernet to serial device server, (1) combo 10/100/1000 Mbps copper or 100/1000 Mbps SFP Ethernet port, 16 total serial device management ports consisting of (4) RS-232/422/485 software selectable and (12) RS232 only RJ-45 serial ports, (1) RJ-45 console port, 100-240 VAC, 60/60Hz input.
EDS5032	Ethernet to serial device server, (1) combo 10/100/1000 Mbps copper or 100/1000 Mbps SFP Ethernet port, 32 total serial device management ports consisting of (4) RS-232/422/485 software selectable and (28) RS232 only RJ-45 serial ports, (1) RJ-45 console port, 100-240 VAC, 60/60Hz input.

Accessories (sold separately)

Accessories Number	Description
25131	DC Power Supply
SFP Modules	Check out our full portfolio of SFPs on Lantronix.com

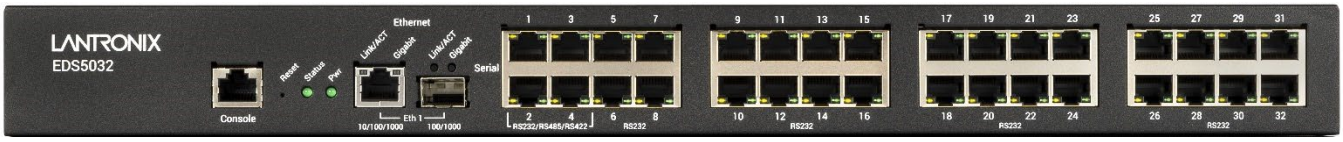
EDS5008, EDS5016, and EDS5032 Hardware Overview

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.



EDS5008 Device Server

EDS50016 Device Server



EDS5032 Device Server

Features

Device Server Features

- Supports RS232, RS422 and RS485
- Tunnel Accept (TCP, SSH, SSL, TCP-AES, UDP, UDP-AES, Telnet)
- Tunnel Connect (TCP, SSH, SSL, TCP-AES, UDP, UDP-AES, Telnet)
- Tunnel TruPort (IETF RFC 2217)
- Tunnel Packing Mode
- Tunnel Disconnect Mode
- Combo Ethernet port via 10/100/1000 copper RJ45 or 100/1000 SFP
- Redundant power inputs; supports AC input, DC input or both
- 1RU rack mount or desktop mount design
- Extended operating temperature of -10°C to +60°C

Diagnostic Features

- Ping, Traceroute, NSLookup
- DNS, IP Socket, Log, Memory Routes
- E-mail

Percepxion Features

- Device status
- Device Firmware and Configuration updates
- Device Reboot, Reset and Shutdown
- Device Telemetry and Dashboard
- Remote Access
- Configuration Management

Specifications

Specifications

Specification	Description
Hardware	CPU: NuMicro MA35DA 4 Gbit (512 MB) Flash On-board memory: 256MB Flash
Serial Interface	Supports standard data rates from 2400 to 921.6K Baud Data bits 5,6,7,8 Parity: Odd, Even, None Stop Bits: 1 or 2 Modem Control Signals: CTS, RTS, DTR, DCD Flow Control: XON/XOFF (software), CTS/RTS (hardware), None
Serial Signals	RS-232: TxD, RxD, RTS, CTS, DTR, DSR RS-422: Tx+, Tx-, Rx+, Rx-, GND RS-485-4W: Tx+, Tx=, Rx+, Rx-, GND RS-485-2W: Data+, Data-, GND
Interface Type	Combo Ethernet port: 1 - 10/100/1000 Mbps Copper **or** 1 - 100/1000 Mbps SFP Both ports are present, but only 1 can be used. If using SFP, copper port is disabled. If using copper port, SFP is disabled. By default it is set to copper.
Speed	10/100/1000 Mbps Copper 100/1000 Mbps SFP
Port Types	RS232 (all ports; default) RS485 Full-Duplex (ports 1-4) RS485 Half-Duplex (ports 1-4) RS422 Full-duplex (ports 1-4)
Baud Rates	2400 to 921.6K Baud; supports standard baud rates (unit=bps): 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230.4k, 460.8k, 921.6k. Note: only ports 1-4 support RS-485/RS422.
Security/Encryption	SSL 3, TLS 1.2, TLS 1.3 MD5,SHA-1,SHA-2 RSA-1024,2048,4096, DSA and ECDHE Password protection IP address filtering SNMP v2/v3 HTTPS AES128, AES256 Data traffic encryption Based on open SSL
NTP	NTP (Network Time Protocol) support

Specification	Description
Management	♦ IPv4 and IPv6 ♦ Internal web server, SNMP v1, SNMP v2, SNMP v3, Serial Login ♦ Telnet SSH login, XML ♦ Percepxion secure cloud and on-premise platform for remote device management ♦ Device status, device firmware and configuration updates, device reboot/reset/ shutdown, device telemetry and dashboard, remote access, CLI commands, Configuration Management, Mobile App ♦ Upgradeable FW via Web Manager, Lantronix Provisioning Manager or Percepxion
Dimensions	443.00 mm W x 175.00 mm D x 43.60 mm H 17.44 “ W x 6.89 “ D x 1.71 “ H (1RU)
Material	Aluminum
Mounting	Rack mount ears for 19 inch rack/cabinet; Rubber feet for desktop
Reset	One recessed front panel Reset button.
LEDs	Power LED TX/RX for serial ports Activity/Link for Ethernet ports
AC	100-240 VAC, 50/60 Hz on back panel
DC	24VDC - 48VDC terminal block on back panel (Negative DC voltage not supported)
Operating Temperature	-10°C to +60°C
Storage Temperature	-40°C to +80°C
Humidity	95% non-condensing
IP Rating	IP30
Protection	8KV Contact Discharge; 15KV Air Discharge
Power	100-240VAC, 50/60 Hz IEC-type cord; 24-48VDC, 1.0.A min.; 20 Watts
Weight	4.54 Kg (10 Lbs.)
Real Time Clock (RTC)	The EDS5000 series of products will retain the set time for a brief period in the event of a power loss if using local timing mode and not Network Time Protocol (NTP).
Warranty	Hardware: 5 year; Software: 1 year
MTBF (years)	Telcordia SR332 Issue 2: Environment: Ground Benign, Controlled. EDS5008 @ 30 °C = 42.07 EDS5008 @ 85 °C = 5.7 EDS5016 @ 30 °C = 39.89 EDS5016 @ 85 °C = 4.62 EDS5032 @ 30 °C = 36.25 EDS5032 @ 85 °C = 2.72

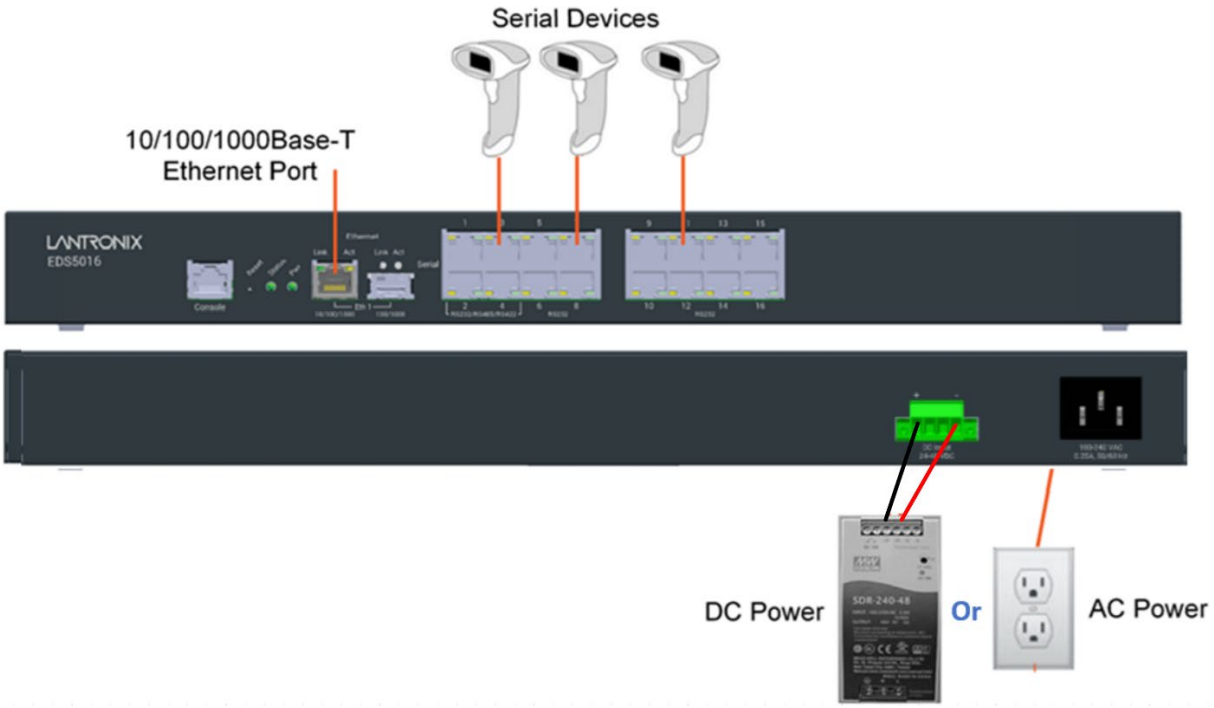
Applications

EDS5000 device servers connect serial devices 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

A sample EDS5000 application scenario is shown below:

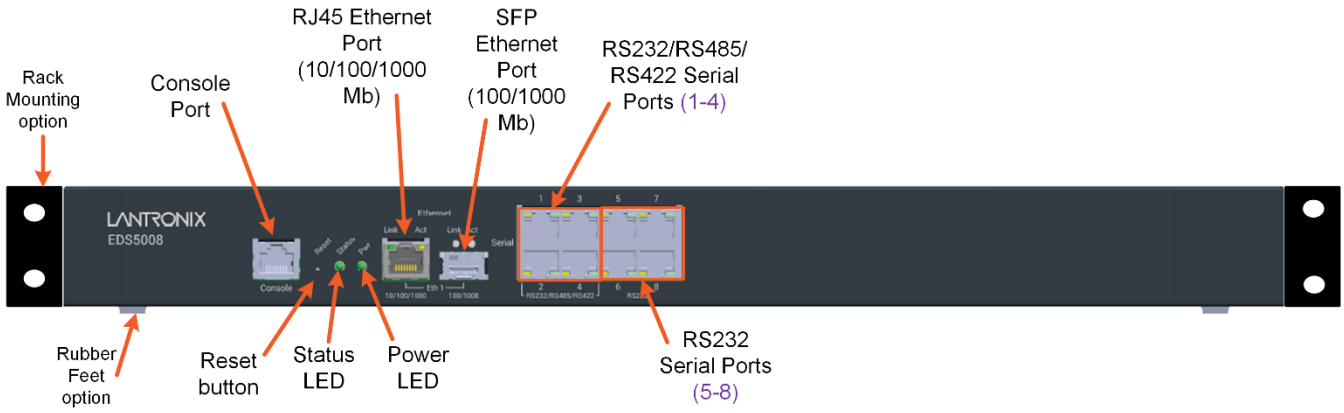
Application Example



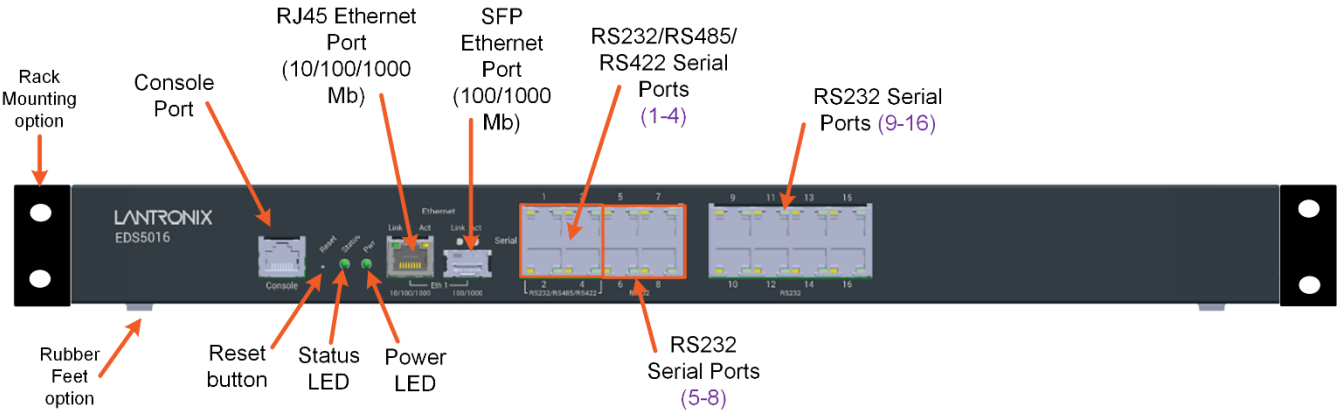
Hardware Components

Front Panels

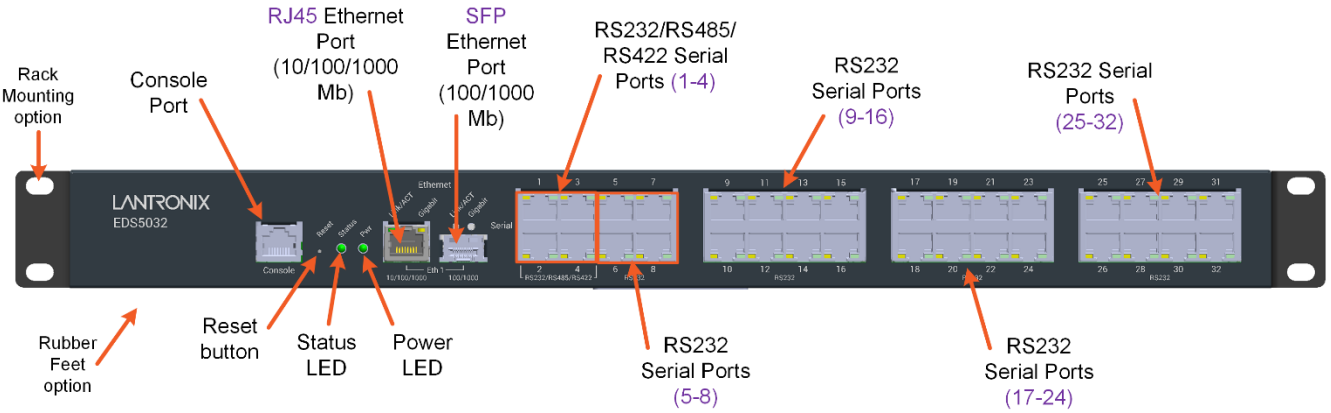
The EDS5008, EDS5016 and EDS5032 front panels are shown and described below.



EDS5008 Front Panel



EDS5016 Front Panel



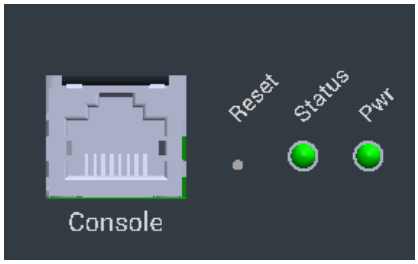
EDS5032 Front Panel

Reset button

The EDS5000 has a physical Reset button which can be used to reset the system without serial or SSH access. The recessed Reset button is located to the right of the Console port on the front panel of the EDS5000. **Note**: Always back up your configuration before performing resets when possible, as the reset process will erase custom settings.

To reboot the device using the Reset button:

1. Using a paper clip or similar object to carefully poke through the Reset hole, press and hold the Reset button for:
   - 0 - 2 seconds = Accidental press, no action
   - 2 - ~10 seconds - Software reboot
   - 11 - ~15 seconds = Factory reset
   - > 16 seconds = Hardware reboot
2. Release the Reset button. The device will perform as described in step 1 above. This operation may take a few minutes to complete.

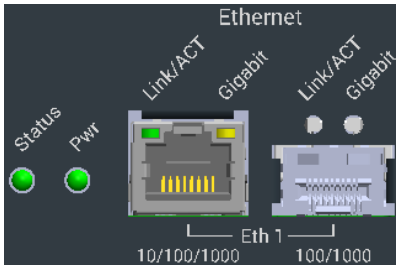


Status LEDs

The front panel LEDs show status information.

The EDS5000 has two front panel LEDs: one green LED for power on and one green LED for diagnostic indication.

Each RJ-45 port has one green LINK LED (left) and one Yellow Link ACTivity LED (right).



Status LEDs

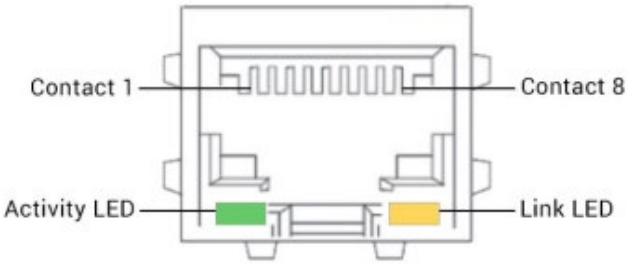
Setting	Description
Status (green)	Fast blink = initial startup (loading OS). Slow blink (once per second) = operating system startup. On = unit has finished booting.
Pwr (Power) (green)	On = EDS5000 is receiving power.
Eth 1 RJ-45 port	Speed (green) On = EDS5000PS is connected to a 1000 Mbps Fast Ethernet network. Speed (green) Off = EDS5000PS is connected to a 10/100 Mbps Ethernet network. Activity (green) Blink = EDS5000PS is sending data to or receiving data from the Ethernet network.

Green LED: Link / Act. **Orange LED: Gigabit.** LED behavior is defined below:

	Link/ACT (RJ-45) LED0	**Gigabit** (RJ-45) LED2	**Link/Act** (Fiber) LED1	**Gigabit** (Fiber) LED3
100M/Fiber			Green LED Lit	
1G/Fiber			Green LED Lit	
100M & 10M/RJ45	Green LED Lit			Yellow LED Lit
1G/RJ45	Green LED Lit	Yellow LED Lit		

Ethernet Port

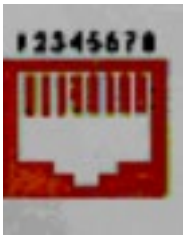
Ethernet Port



Ethernet RJ45 Connector Pin Assignment and LEDs

Pin	Signal Name
1	ETX+
2	ETX-
3	ERX+
4	-
5	-
6	ERX-
7	-
8	-
Left LED (Green)	RX/TX Activity Flashing on: Activity Off: No activity
Right LED (Amber)	Link On: Link Off: No link

Serial Ports

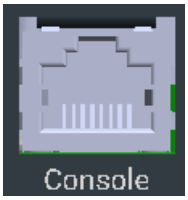


All EDS5000 RS-232 serial ports are configured as DTE and support up to 921600 baud. serial port pin numbering is shown below. **Note**: only ports 1-4 support RS-485/RS-422.

- The EDS5008 has 8 serial ports.
- The EDS5016 has 16 serial ports.
- The EDS5032 has 32 serial ports.

Pin Number	RS-232	RS-485/422 Full	RS-485 Half
1	RTS		
2	DTR	R1-INB(-)	
3	TX	R2-INA(+)	
4	GND	GND	GND
5	GND	GND	GND
6	RX	T1_OUTA(+)	R1_INA
7	DSR	T2_OUTB(-)	R2_INB
8	CTS		

Console Port



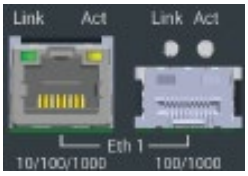
The EDS5000 front panel has one RJ-45 console port for Command Line Interface (CLI) connection. See Appendix E. Commands for more CLI information.

The EDS5000 has an RJ45 Console port configured as DTE and supports 115200 baud.

Combo Network Port (RJ-45 or SFP)

The EDS5000 provides a front panel “Combo” port copper and SFP port interface. Only one port will work at a time (either Copper or SFP but not both). You can change from SFP to copper operation and vice versa in run time.

The device gets the same DHCP IP address after switching from copper to SFP if both are from same DHCP server. If the copper and SFP ports are on different networks they will get different DHCP IP addresses after switching from copper to SFP.



If you switch from copper to SFP using the device IP, the device may lose connectivity to network while switching from copper to SFP depending on the network. If you have both SFP and copper connected, if the copper link goes down it will not automatically switch to SFP depending on your configuration. If you perform a factory default, the Copper port is active.

Ethernet Port: The EDS5000 RJ45 Ethernet port supports 10/100/1000 Mbps Ethernet. The port’s Speed LED shows the connection speed of the connected Ethernet network. You can configure the EDS5000 to operate at a fixed Ethernet speed and duplex mode (half- or full-duplex) or auto-negotiate the connection to the Ethernet network. **Note**: If an unsupported SFP is connected and you switch to SFP mode, the EDS5000 may go to unreachable state and require recovery by performing a factory reset.

Back Panel

The back panel/housing is common across EDS5000 models.

Dimensions

The dimensions are common across EDS5000 models:

- 443.00 mm W x 175.00 mm D x 43.60 mm H
- 17.44” W x 6.89” D x 1.71” H

Configuration Methods

After installation, the EDS5000 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 EDS5000 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 on page 31.
- **Web Admin interface**: Through a web browser, configure the EDS5000 devices settings using the Lantronix Web Admin interface. See chapter 5. Web Administration Interface on page 32.
- **Command Mode**: There are two methods for accessing Command Mode (CLI): making an SSH connection or connecting a terminal (or a PC running a terminal emulation program) to the unit's serial port. See Appendix E. Commands for more information.

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.

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 to 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, an SSH server commonly uses port number 22.

Below is a list of the default server port numbers running on the EDS5000 device server.

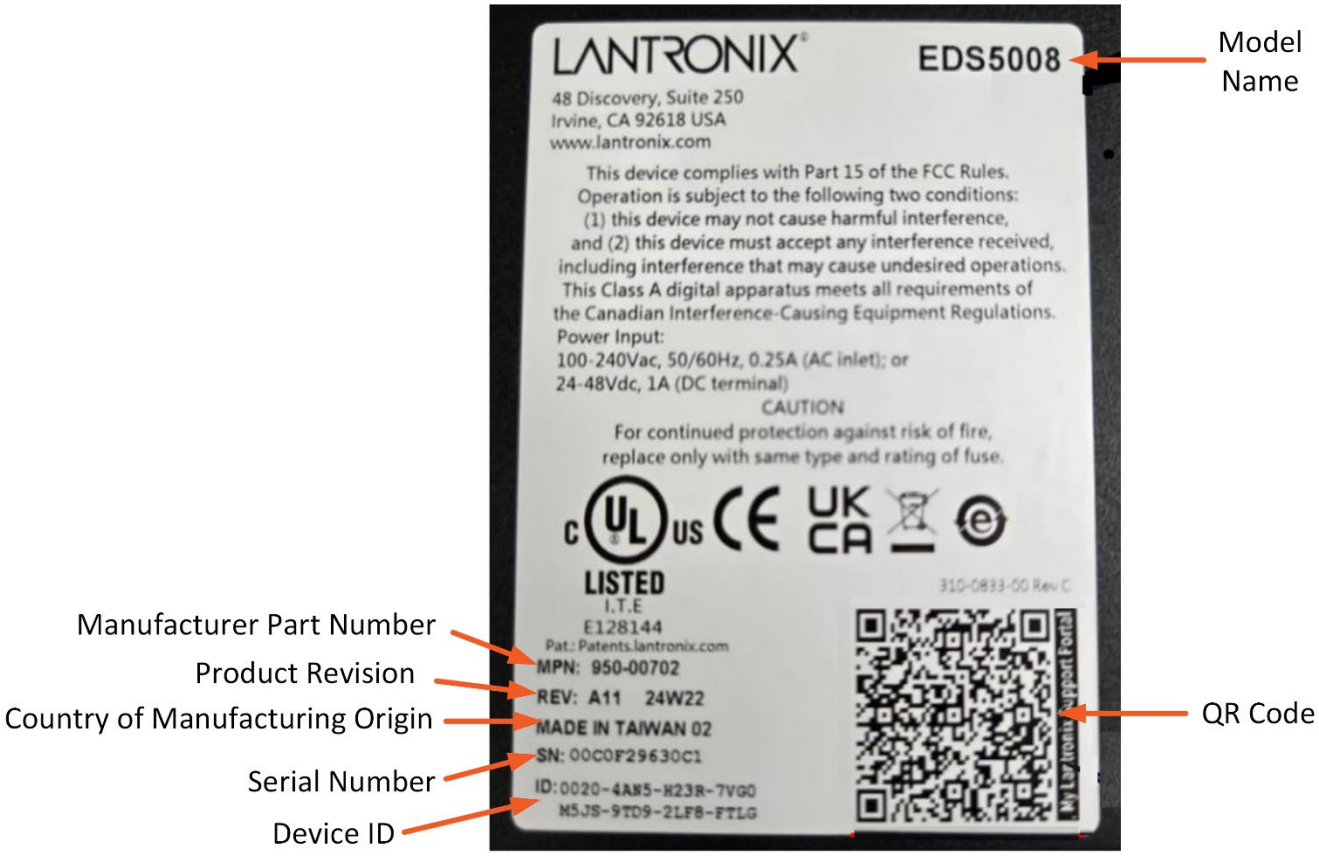
- TCP Port 22: SSH Server
- TCP Port 80: HTTP (Web Admin interface configuration)
- TCP Port 443: HTTPS (Web Admin interface configuration)
- UDP Port 161: SNMP
- TCP Port 21: FTP
- UDP Port 514: Syslog
- UDP Port 30718: LDP (Lantronix Discovery Protocol) port
- TCP/UDP Port 10001: Tunnel 1
- TCP/UDP 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 Label

The product label can provide information valuable to the Technical Support Engineer when contacting Lantronix Technical Support.

Product Label (EDS5008)



The QR code on the product label contains product specific information from the factory including the serial number, Device ID, ICCID, etc. and it points to MyLantronix

When read by a QR scanner via a camera, it brings up MyLantronix, where once you have logged in, that product information is saved to your MyLantronix account so that the product can be easily registered or provisioned.

3. Installation

This chapter describes how to install the EDS5000 device server, including these sections:

- Package Contents
- Safety Information
- Preparing to Install
- Installing EDS5000 Hardware
- Connecting EDS5000 Ports
- Power Source Information

Package Contents

Carefully unpack the contents. Verify that you have received the following items. Contact your sales representative if any item is damaged or missing. Please save the packaging for possible future use.

- One EDS50xx unit (EDS5008, EDS5016, or EDS5032)
- Two Rack Mount Ears: 110-973-00
- Four Rubber feet for bottom of unit for desktop mounting: 120-008-R
- AC Power cord: 500-0282-00 (AC power only)
- Console port cable: ACC-500-103-R
- Percepxion flyer: 900-0811-R
- Errata sheet: 900-569
- One printed Quick Start Guide: 895-0071-002

***Note**: A DC power supply is supported and must be ordered separately. Other accessories must be purchased separately. The Ethernet cable and serial cable can be acquired from various vendors.*

***Note**: If Class I power supply is used, the power cord shall be connected to a socket outlet with earthing connection.*

Additional Items

Not shipped but may be required: ESD-preventive cord with wrist strap, wire and wire crimper for DC power connection, Ethernet cables, a ratcheting torque flathead screwdriver that exerts up to 15 in-lb. (1.69 N-m) of pressure, and a #1 and a #2 Phillips screwdriver.

Safety Information

Review the following Cautions and Warnings before starting to install the EDS5000. Note that not all Cautions and Warnings apply to every device server environment and application.

Cautions and Warnings

Cautions indicate that there is the possibility of poor equipment performance or potential damage to the equipment. Warnings indicate that there is the possibility of injury to person.

Cautions and Warnings appear here and may appear throughout this manual where appropriate. Failure to read and understand the information identified by this symbol could result in poor equipment performance, damage to the equipment, or injury to persons.

Warning*: Do not open the chassis - No field serviceable parts.*

Caution: While installing or servicing the device server, wear a grounding device and observe all electrostatic discharge precautions. Failure to observe this caution could result in damage to or failure of the EDS5000.

Warning: Do not connect the device server to an external power source before installing it into its cabinet or mounting location. Failure to observe this warning could result in an electrical shock, even death.

Warning: A readily accessible, suitable National Electrical Code (NEC) or local electrical code approved disconnect device and branch-circuit protector must be part of the building's installed wiring to accommodate permanently connected equipment. Failure to observe this warning could result in an electric shock, even death.

Warning: Turn any external power source OFF and ensure that the EDS5000 is disconnected from the external power source before performing any maintenance. Failure to observe this warning could result in an electrical shock, even death.

Warning: Ensure that the disconnect device for the external power source is OPEN (turned OFF) before disconnecting or connecting the power leads to the EDS5000. Failure to observe this warning could result in an electric shock, even death.

Warning: Equipment grounding is vital to ensure safe operation. The installer must ensure that the EDS5000 is properly grounded during and after installation. Failure to observe this warning could result in an electric shock, even death.

Warning: Because invisible radiation might be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.

General Laser Safety Guidelines: When working around ports that support optical transceivers, observe the following safety guidelines to prevent eye injury:

- Do not look into unterminated ports or at fibers that connect to unknown sources.
- Do not examine unterminated optical ports with optical instruments.
- Avoid direct exposure to the beam.

High Risk Activities Disclaimer: Components, units, or third-party products used in the product described herein are NOT fault-tolerant and are NOT designed, manufactured, or intended for use as on-line control equipment in the following hazardous environments requiring fail-safe controls: the operation of Nuclear Facilities, Aircraft Navigation or Aircraft Communication Systems, Air Traffic Control, Life Support, or Weapons Systems ("High Risk Activities"). Lantronix and its supplier(s) specifically disclaim any expressed or implied warranty of fitness for such High Risk Activities.

Recycling / Disposal: Do not discard electronic products in household trash! All waste electronics equipment should be recycled according to local regulations. **Information for the recycler**: chassis are made of aluminum.

Preparing to Install

Before starting installation, gather the necessary hardware, accessories, and documentation. Review and follow the safety information above.

Ensure that the computer used to access the web admin interface for EDS5000 configuration is equipped with the following:

- Ethernet port and Internet service
- Web browser with recently updated version (e.g., Chrome, Safari, Firefox, Edge)
- DHCP client is enabled on the computer

Enabling DHCP Client on Your Computer

The DHCP client must be enabled on your computer to obtain a valid IP address from the network.

To enable DHCP on Windows 8 or 10:

1. Go to Windows Start > Control Panel > Network and Internet > Network and Sharing Center.
2. Click the active network connection. The Network Connection Status box appears.
3. Click Properties and then select IPv4 (TCP/IPv4) and click Properties. The Internet Protocol Version 4 (TCP/IP) Properties will appear.
4. On the General tab, select the following options:
   a) Obtain an IP address automatically
   b) Obtain DNS server address automatically
5. Click OK to close the dialog.

To enable DHCP on Mac OS:

1. Launch System Preferences, and then choose Network.
2. Select Ethernet from the adapters list on the left.
3. Set the Configure IPv4 list to “Using DHCP.”

To enable DHCP on Windows 11:

1. Use Windows + R to launch the Run utility.
2. Execute the ncpa.cpl command to open the Network Connections window.
3. Right-click on your network connection (Ethernet) and choose Properties.
4. In the Networking tab, double-click the Internet Protocol Version 4 (TCP/IPv4).
5. Once a new dialogue box launches, choose these options: **Obtain an IP address automatically** and **Obtain DNS server address automatically**.
6. Press the Ok button to save the changes.
7. Repeat the same for Internet Protocol Version 6 (TCP/IPv6), and once that’s done, press OK.

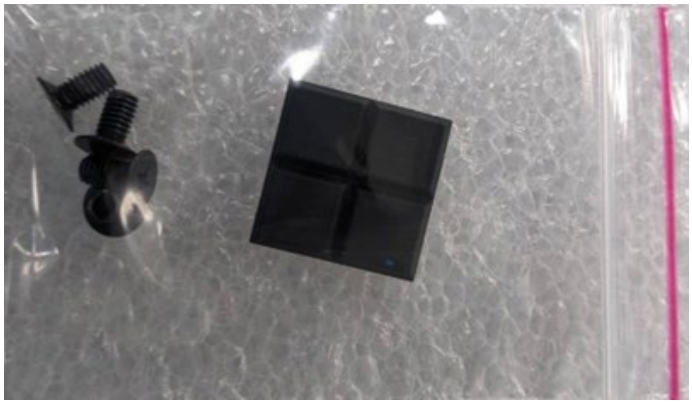
Installing EDS5000 Hardware

Finding a Suitable Location

You can install the EDS5000 device as a desktop unit or it can be rack mounted.

Desktop Installation

Place the provided four Rubber feet on the bottom of unit for desktop mounting.



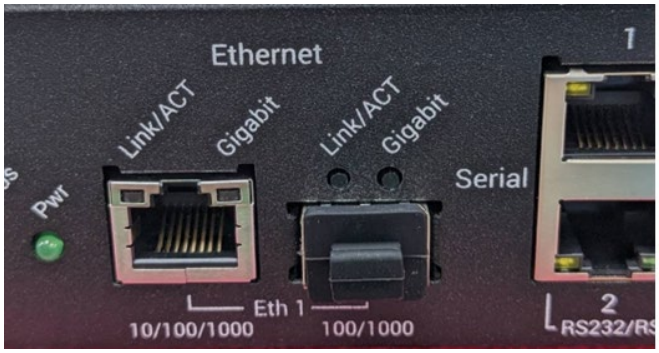
Rack Mounting the EDS5000

Use the two Rack Mount Ears (110-973-00) and provided screws to mount the EDS5000 in a 19” rack.

If rack mounted units are installed in a closed or multi-unit rack assembly, 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. 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.

Connecting EDS5000 Ports

1. Power off the serial devices that will be connected to the EDS5000.
2. Attach a serial cable between the EDS5000 and each serial device. For a list of cables and adapters you can use with the EDS5000, refer to Appendix C. Cables.
3. Connect the EDS5000 Combo Eth1 port to your Ethernet network. Connect an Ethernet cable between the EDS5000 Ethernet port and your 10/100/1000 Ethernet network.
4. Connect the RJ-45 end of the Console port cable to the EDS5000 Console port, and connect the DB9 female end to your computer (either directly or using a DB-9 male to USB adapter).
5. Power up the attached serial devices.



Combo Ethernet Eth 1 Ports

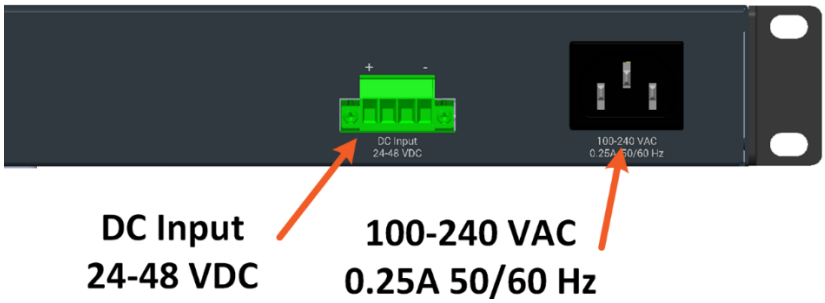
Power Source Information

There are three power source inputs to the EDS5000:

1. AC-DC power source (100-240 VAC input, 12VDC output)
2. Optional DC power supply 25131 (48V)

Connecting the EDS5000 to Power

The EDS5000 back panel provides both AC and DC power connections:



AC and DC Power Connections

Power Connection Rules

1. A 1 DC and 1 AC Power Supply configuration is supported. Both inputs can be the primary (one for AC and one for DC power). When one of the power supplies fails, the other power supply will continue to provide power. If the fault is not caused by the power supply, it may stop customer traffic.
2. A single DC power supply is supported with 24VDC - 48VDC input.
3. A 2 DC Power Supplies configuration is not supported.
4. Negative DC voltage is not supported.
5. There is no grounding lug.
6. For AC: Power cord shall be connected to a socket-outlet with earthing connection.
7. For DC:
   a. The equipment is intended to be supplied by a Listed Power Supply which output is complied with SELV/ES1, output rating 24-48Vdc, 1A, ambient temperature 60 °C minimum.
   b. The wiring for the input terminal block shall be installed by a skilled or qualified persons. Use wire type: Cu, FW2, 20-12 AWG and 3.5 lb-in torque value.

Connecting the EDS5000 to AC Power

AC power connection is made via the 100-240 VAC power plug using the provided AC Power cord PN 500-041-R. When using AC power, avoid outlets controlled by a wall switch.

1. Insert the power cord plug into the back of the EDS5000 device.
2. Plug the other end of the power cord into an AC wall outlet. The PWR LED should light.
3. After power-up, the self-test begins.

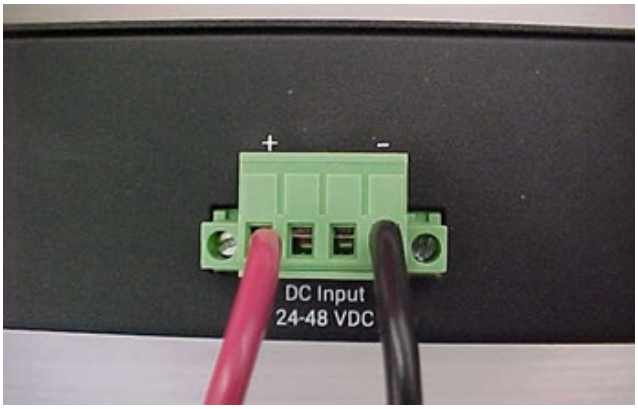
AC Power Cord PN 500-041-R

Connecting the EDS5000 to DC Power

After the EDS5000 is mounted, connected, and grounded, use the 24-48VDC Terminal Block (Euro Block) to provide DC Power. For 25131 Power Supply details refer to PN SDR-75-48 at https://www.meanwell.com/Upload/PDF/SDR-120/SDR%20DIN%20rail.pdf.

Caution: Connect the wires to the Terminal Block before connecting to the optional power supply.

1. Insert the negative/positive DC wires into the **+** and **-** terminals, respectively.
2. To keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.
3. Plug the DC power supply into a live AC outlet.
4. Check the EDS5000 front panel Pwr LED. If it is ON, the power connection is correct.



DC Power Input - Terminal Block

4. Using Lantronix Provisioning Manager

This chapter covers the steps for locating a device and viewing its properties and details. Lantronix Provisioning Manager (LPM) is a free utility program provided by Lantronix that discovers, configures, upgrades, and manages Lantronix devices. LPM v 7.2.4 and above support the EDS5000.

It can be downloaded from the Lantronix website from the Lantronix Provisioning Manager product page.

Installing LPM

Download the latest version of Lantronix Provisioning Manager from https://www.lantronix.com/products/lantronix-provisioning-manager/.

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 EDS5000 Using Lantronix Provisioning Manager

To discover a device on the local network:

1. Launch Lantronix Provisioning Manager (lpm).
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 EDS5000 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 EDS5000 such as upgrading the firmware, updating the configuration, or uploading to the file system, click the checkbox next to the device and select the appropriate operation from the menu.

5. Web Administration Interface

This chapter covers the steps to access the Web manager and the Web Admin interface page components, controls, and messages.

Accessing Web Admin interface

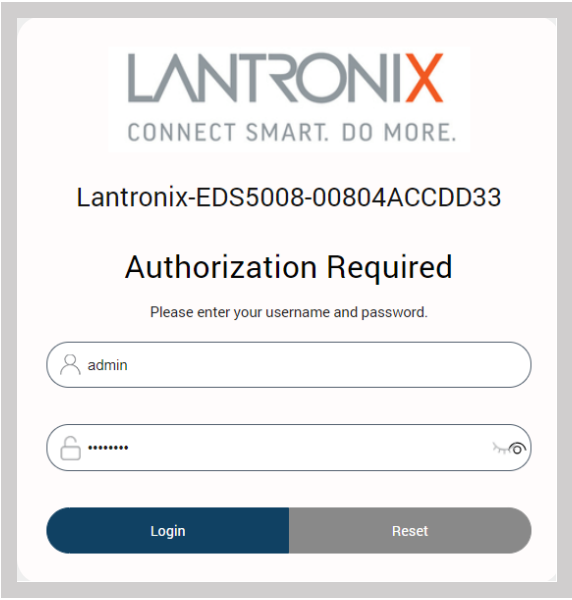
If you are logging in for the first time after installation or after factory reset, login as root using the default credentials and change the default passwords for both admin and root user.

The default username and password credentials are:

Default username	Default password
admin	admin
root	L@ntr0n1x

To access EDS5000 Web Admin interface, perform the following steps:

1. Connect RJ 45 terminated Ethernet cable to WAN network. Make sure computer and EDS5000 device are on the same network.
2. Open a standard web browser. Lantronix supports the latest version of most current web browsers.
3. Enter the EDS5000 IP address 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. For instructions on using the LPM application see the Lantronix Provisioning Manager online help. The Login page displays.



Login Page

4. Enter the Username. The factory default is **admin** (case-sensitive).

5. Enter the Password. The factory default is **admin** (case-sensitive). The password field has icons you can click to alternately hide and show the password characters as you enter them.
6. Click the Login button to log in to the Web Admin interface. If this is first login, the change password screen is displayed. Otherwise, the Quick Setup or the Status page are displayed.

You will be required to change the root and admin user passwords after the first login. After changing the initial passwords, log in again to configure the network settings.

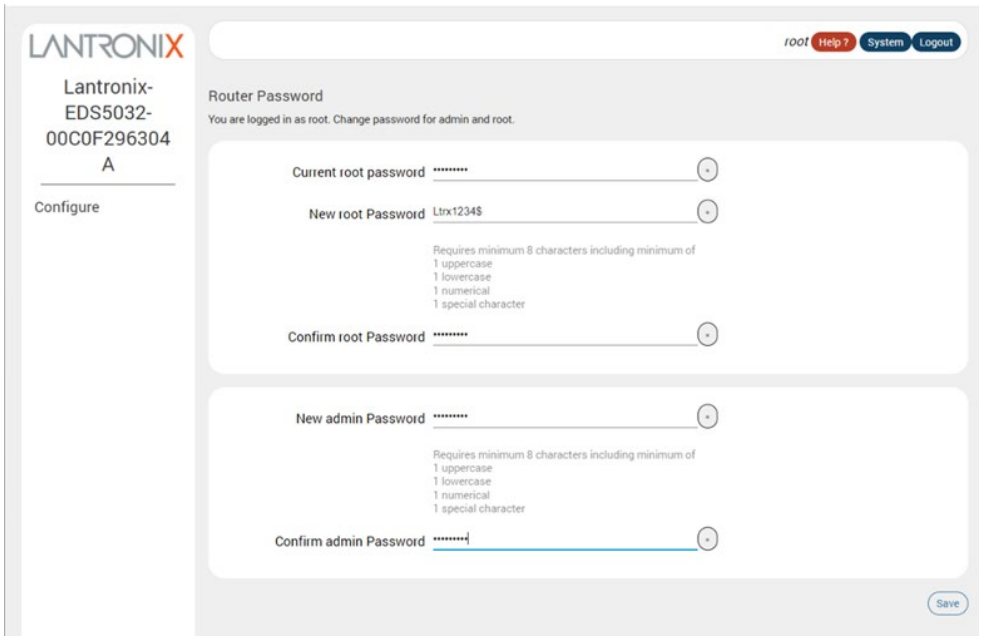
Change Passwords After Initial Login

After first login with a new device or after resetting the device to factory defaults, you should change the factory default passwords for both the admin user and root user before any other EDS5000 configuration is done. The password requirements are as follows:

- Password must consist of at least 8 characters and include a minimum of the following:
- 1 uppercase character
- 1 lowercase character
- 1 numerical character (0-9)
- 1 special character

Note: Log in as root user to change both admin and root password at the same time.

1. Log into the web admin interface as root user. This will allow you to change the passwords for both the root user and the admin user.



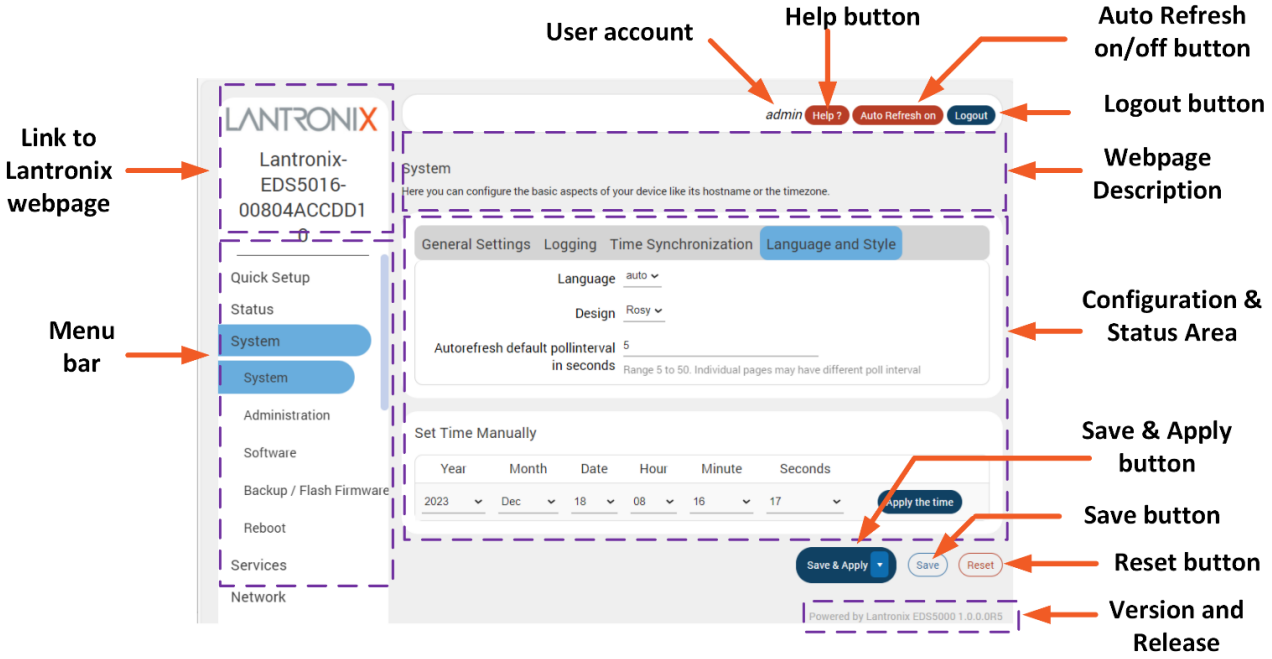
The default username and password credentials are:

Default username	Default password
admin	admin
root	L@ntr0n1x

2. For the root user, enter the new password and then re-enter it to confirm it.
3. For the admin user, enter the new password and then re-enter it to confirm it.
4. Click the Save button. This will log you out and return to the login page automatically.

Web Admin interface Page Components

The layout of a typical Web Admin interface webpage is shown and described below.

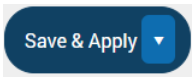
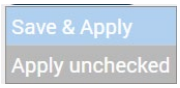
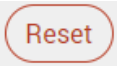


Web Admin interface Page Components

Web Admin Interface Page Controls

The icons and buttons below are common to many webpages; other webpage controls are related to specific webpages and are documented in the related sections of this manual.

Setting	Description
User account e.g., *admin*	Displays the current user's assigned account access level. ♦ The *root* user is the Linux superuser. *root* is the username of the administrative user in OpenWrt. Since this is an extremely powerful account, provide a strong password that you'll remember. ♦ An *admin* user has full administrator rights.
Help ?	**Help**: **P**rovides a link to the Lantronix website.
Unsaved Changes: 7	**Unsaved Changes: *x***; click to show Configuration / Changes (Sections added & removed, Options changed & removed). Shows the number of unsaved changes and lets you Dismiss the changes, or Save & apply the changes to the EDS5000 configuration or revert the changes back to the saved configuration.
Logout	Logout; logs you out of the webpage and displays the Login page.
Auto Refresh on	**Auto Refresh on**: Click to alternate between Auto Refresh on and off.

Setting	Description
	**Auto Refresh off:** Click to alternate between Auto Refresh off and on.
	**Save & Apply**: Click to save and apply webpage changes, or click the down arrow to Apply changes unchecked. Applies and saves the changes on the web page to the EDS5000 (in NVRAM) so that the settings will persist when the EDS5000 is rebooted. After clicking this button, wait for the configuration to be applied before closing the browser, otherwise the old configuration will be restored.
	**Apply unchecked**; click to Apply unsaved webpage changes unchecked. Click the arrow on the Save & Apply button to reveal this option. Applies and saves the changes on the web page to the EDS5000 (in NVRAM), but will not disrupt the active network interface. Use this if you are changing the interface parameters on which the session is active.
	**Save**: Click to save webpage changes but not apply them. Saves the changes on the web page (to RAM) without committing the changes. All saved configuration will be lost when the EDS5000 is rebooted if they are not saved and applied**.**
	**Reset**: Click to refresh the webpage and not save changes. Discards the unsaved changes on the page**.**

Logging Out

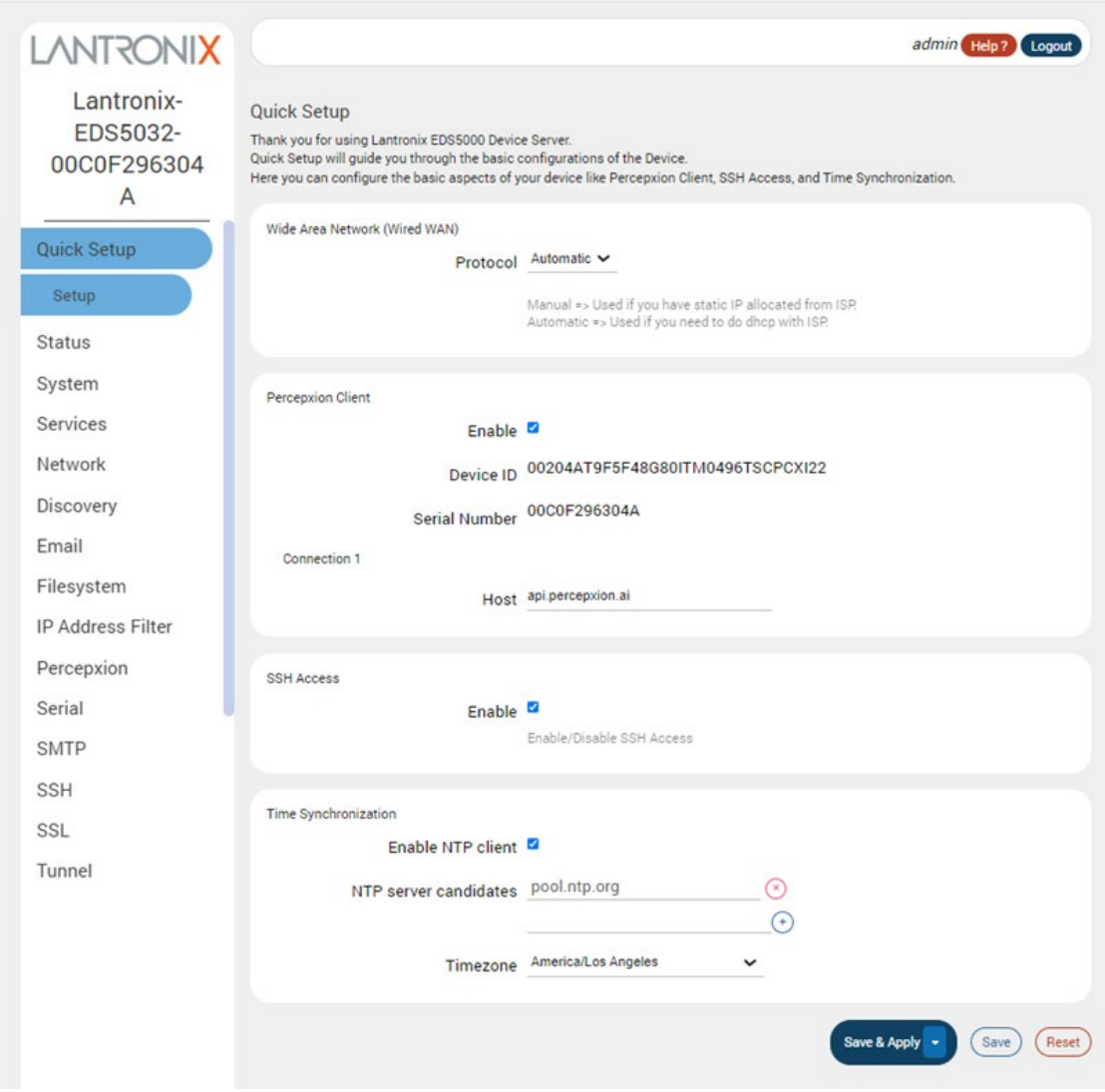
To log off the Web Admin Interface:

1. Click the **Logout** button located in the upper right part of the web admin interface page. When logout is complete, the login screen is displayed so you can log back in.

6. Quick Setup

Setup

Quick Setup will guide you through the basic configurations of the device. Here you can configure the basic device aspects like the WAN protocol, Percepxion Client, SSH Access, and Time Synchronization.



Quick Setup Settings

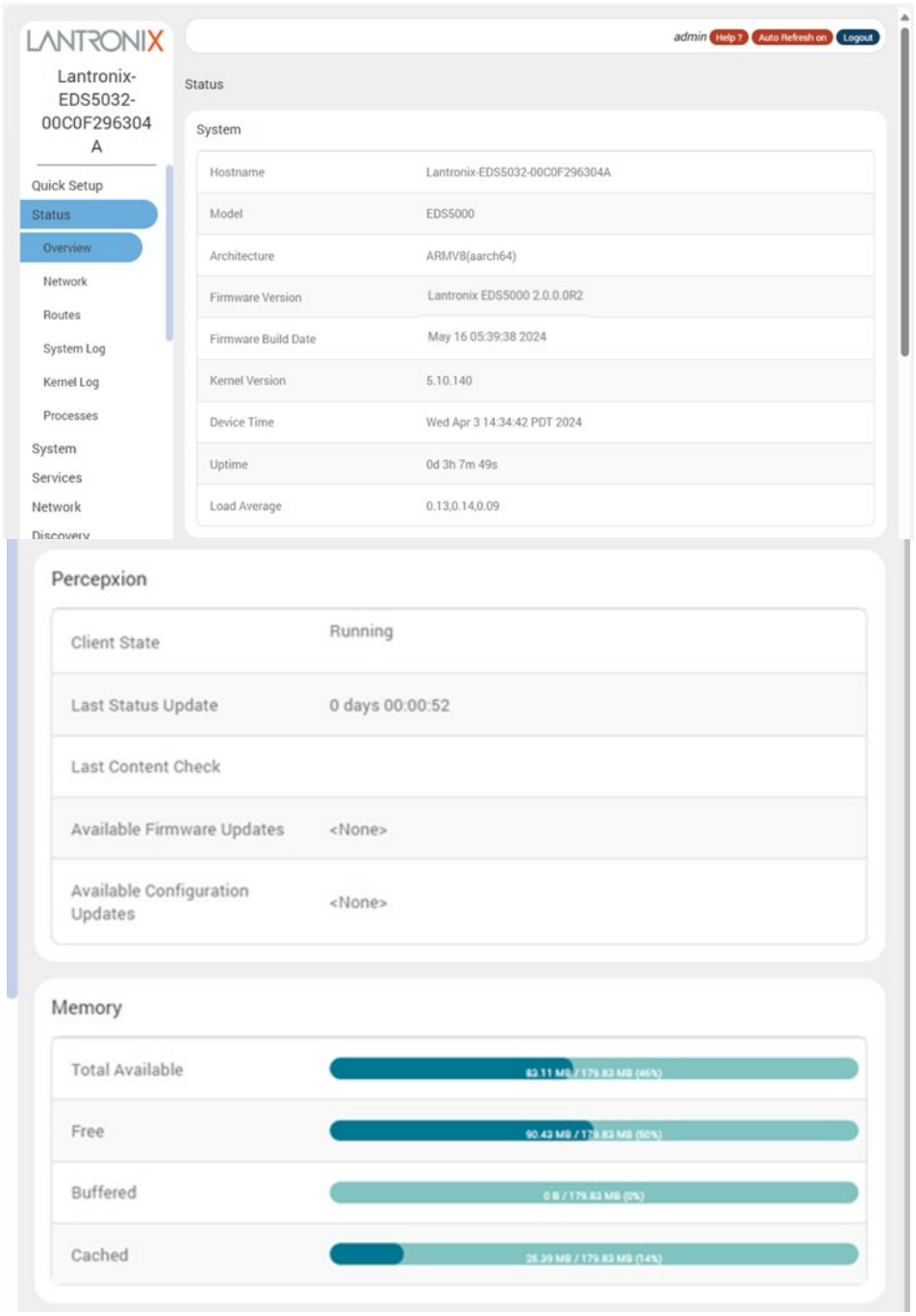
Setting	Description
Wide Area Network (Wired WAN)	At the Protocol dropdown select Manual or Automatic. ♦ **Manual** = Used if you have static IP allocated (e.g., from an ISP). The following settings are required if you select 'Manual': ○ IPv4 Address: enter a valid IP address or network. ○ IPv4 Netmask: enter a valid IP address or network. ○ IPv4 Gateway: enter a valid IP address or network. ○ DNS Server: enter a valid Domain Name Server address. ♦ **Automatic** = Used if you want DHCP to assign an IP address (default).
Percepxion Client	Configure settings for the Percepxion client at Connection 1: **Enable**: Select to enable the Percepxion client. The default is Enabled. **Device ID**: Displays the Percepxion 32-digit Device ID. **Serial Number**: Displays the Percepxion 12-digit serial number. **Host**: Displays the Percepxion server's host location.
SSH Access	Check the box to enable Secure Shell (SSH) access globally or uncheck the box to disable SSH access globally. The default is SSH Enabled globally. See the SSH main menu section below for SSH server and client settings.
Time Synchronization	**Enable NTP client**: Check the box to enable the built-in Network Time Protocol client. The default is NTP client Enabled. **Note**: The EDS5000 will retain the set time for a brief period in the event of a power loss if using local timing mode and not Network Time Protocol (NTP).
	NTP server candidates: Enter a valid hostname or IP address. By default "pool.ntp.org" is enabled.
	Timezone: At the dropdown select your local time zone. By default "America/Los Angeles" is enabled.

7. Status

The Status main menu provides access to settings for Overview, Network, Routes, System Log, Kernel Log, and Processes.

Overview

The Status > Overview page lets you configure and view System, Percepxion, and Memory.



Status > Overview Settings

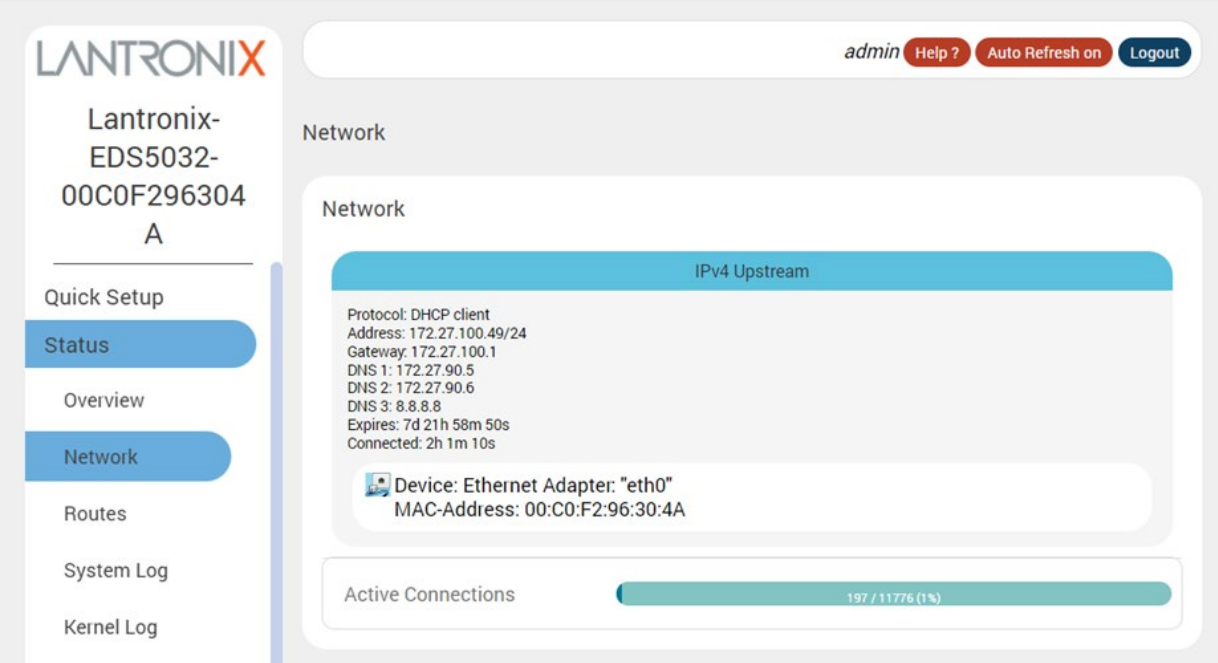
Setting	Description
System	**Hostname**: Displays the factory-assigned hostname for the device (*Lantronix-EDS5016-00804ACCDD10*).
	Model: Displays the assigned model number for the device (EDS5000).
	Architecture: Displays the device's system architecture *(ARMV8(aarch64)*.
	Firmware Version: Displays the current (running) version of firmware on the device (e.g., *Lantronix EDS5000 2.0.0.0R2*).
	Firmware Build Date: Displays the date and time of the device's firmware build (e.g., *May 27 04:17:53 2024*).
	Kernel Version: Displays the current (running) version of kernel (core of the OS) (e.g., *5.10.140*).
	Device Time: Shows the current configured day, date and time (e.g., *Fri May 28 06:53:01 PST 2024*.
	Uptime: Shows how long the device has been running in days, hours and minutes (e.g., *4d 1h 7m 59s*).
	Load Average: CPU load is the number of processes being executed by the CPU or waiting to be executed by the CPU. CPU load average is the average number of processes being or waiting to be executed over the past 1, 5, and 15 minutes. The format is *0.00,0.03,0.01*.
Percepxion	**Client State**: Displays the current state of the Percepxion client. Displays a message if the device credentials are not configured. Message examples: *Running:* *Device credentials are not configured* *WARNING: Device Key is not configured.* *The requested URL returned error: 400 Bad Request*
	Last Status Update: Displays the elapsed time since the Percepxion client sent its status to the server.
	Last Content Check: Displays the elapsed time since the Percepxion client requested a content check from the server.
	Available Firmware Updates: Lists any available firmware updates or *<None>*.
	Available Configuration Updates: Lists any available configuration updates or *<None>*.

Setting	Description
Memory	**Total Available**: Total available RAM memory. Total Memory is sum of used memory, free memory, buffered memory and cached memory.
	Free: Free RAM memory. The bar graph shows the amount of free memory as a percentage of the total memory.
	Buffered: Size of buffered memory. The bar graph shows the amount of buffered memory as a percentage of the total memory.
	Cached: Size of cached memory. The bar graph shows the amount of cached memory as a percentage of the total memory.

Network

The Status > Network page lets you view WAN interface status and Active Connections information.

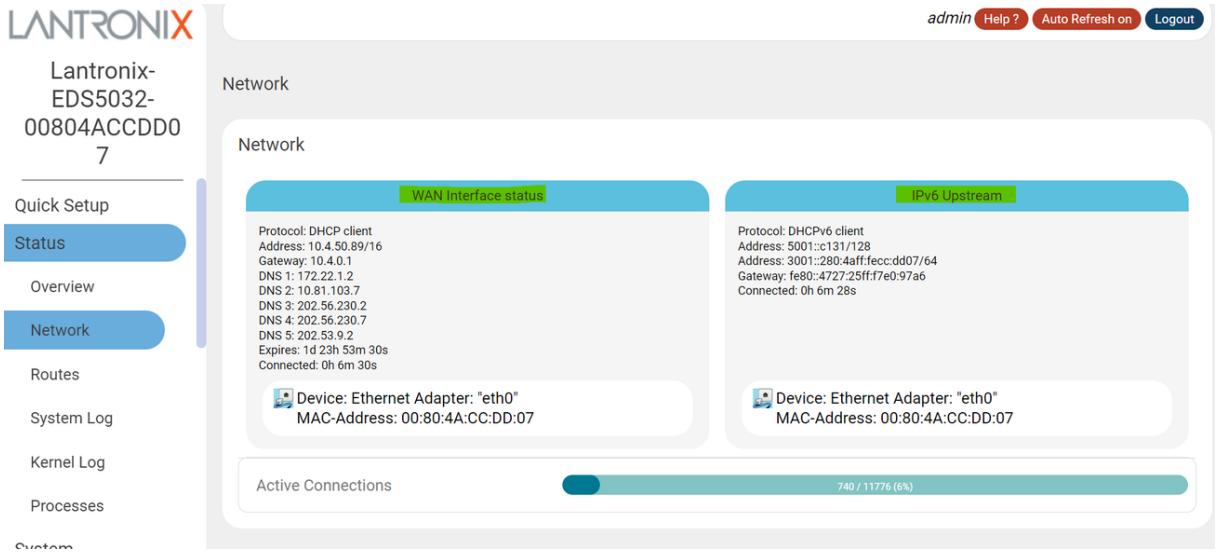
If your network does not support IPv6, then the page will display only IPv4 Upstream status (no IPv6 Upstream status will display).



Network Interface Status

Setting	Description
IPv4 Upstream	Displays the status of IPv4 WAN connections with the following details: *Protocol: DHCP client* *Address: 172.27.100.65/24* *Gateway: 172.27.100.1* *DNS 1: 172.27.90.5* *DNS 2: 172.27.90.6* *Expires: 4d 0h 30m 14s* *Connected: 3d 23h 29m 46s*
Device	Displays the interface name and MAC address; for example: *Device: Ethernet Adapter: "eth0"* *MAC-Address: 00:80:4A:CC:DD:10*
Active Connections	Displays how many active connections exist compared to the total available connections, and a percentage of active to available connections. For example: *319/11776 (2%)*.

If your network supports IPv6, then the Status > Network page will also display IPv6 Upstream status.

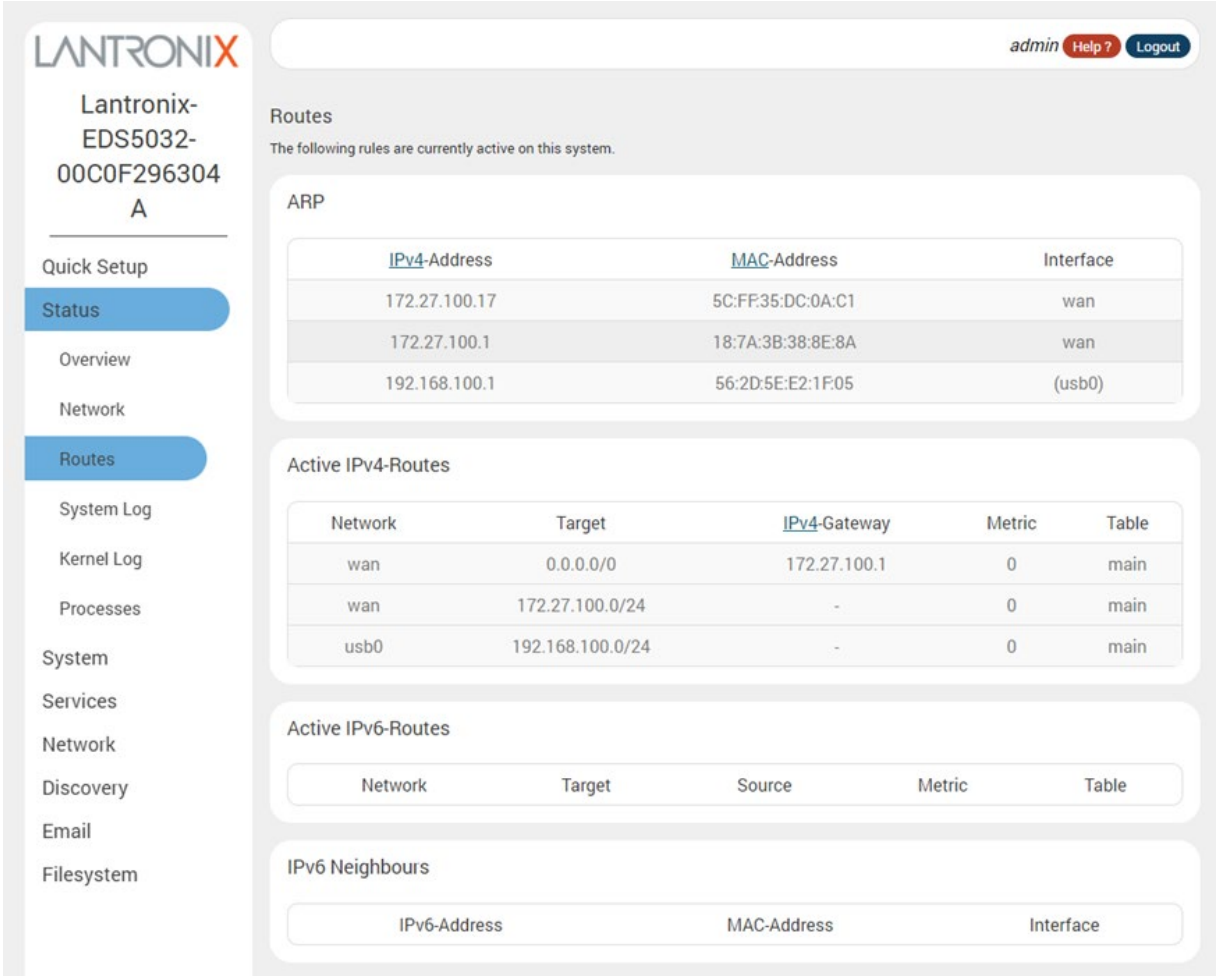


IPv6 Upstream Status

Setting	Description
IPv6 Upstream	Displays status of IPv6 WAN connections with following details: *Protocol: DHCPv6 client* *Address: 5001::c131/128* *Address: 3001::280:4aff:fecc:dd07/64+* *Gateway: fe80::4727:25ff:f7e0:97a6* *Connected: 0h 6m 28s*
Device	Displays the interface name and MAC address; for example: *Device: Ethernet Adapter: "eth0"* *MAC-Address: 00:80:4A:CC:DD:10*
Active Connections	Displays how many active connections exist compared to the total available connections, and a percentage of active to available connections. For example: *740/11776 (6%)*.

Routes

The Status > Routes page displays ARP and Active IPv4 Routes and Active IPv6 Routes and Neighbors.



Routes Settings

Setting	Description
ARP	**IPv4-Address**: Displays the Internet Protocol version 4 address.
	MAC-Address: Displays the related Media Access Control (MAC) address of the peripheral device.
	Interface: Displays the interface name connected to the peripheral device (e.g., *wan*).
Active IPv4-Routes	**Network**: Displays the network type used by the active IPv4 routes (e.g., *wan* or *usb0*).
	Target: Displays the destination IPv4 address and mask.
	IPv4-Gateway: Displays the IPv4 address gateway used for traffic routing.
	Metric: Displays the cost of the IPv4 route in hops. Displays the routing metric assigned to the interface.
	Table: Displays the IPv4 routing table (e.g., *main*).
Active IPv6-Routes	**Network**: Displays the network type used by the active IPv4 routes.
	Target: Displays the destination IPv6 address.
	Source: Displays the IPv6 address gateway used for traffic routing.
	Metric: Displays the cost of the IPv6 route in hops. Displays the routing metric assigned to interface.
	Table: Displays the IPv6 routing table.
IPv6 Neighbors	**IPv6-Address**: Displays the discovered Internet Protocol version 6 addresses.
	MAC-Address: Displays the related Media Access Control (MAC) addresses.
	Interface: Displays the related IPv6 Interfaces.

System Log

The System Log displays detailed system, traffic, and network activity log information. Syslog format is shown in the following example:

```
 Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: Network device
'eth0' link is up
```

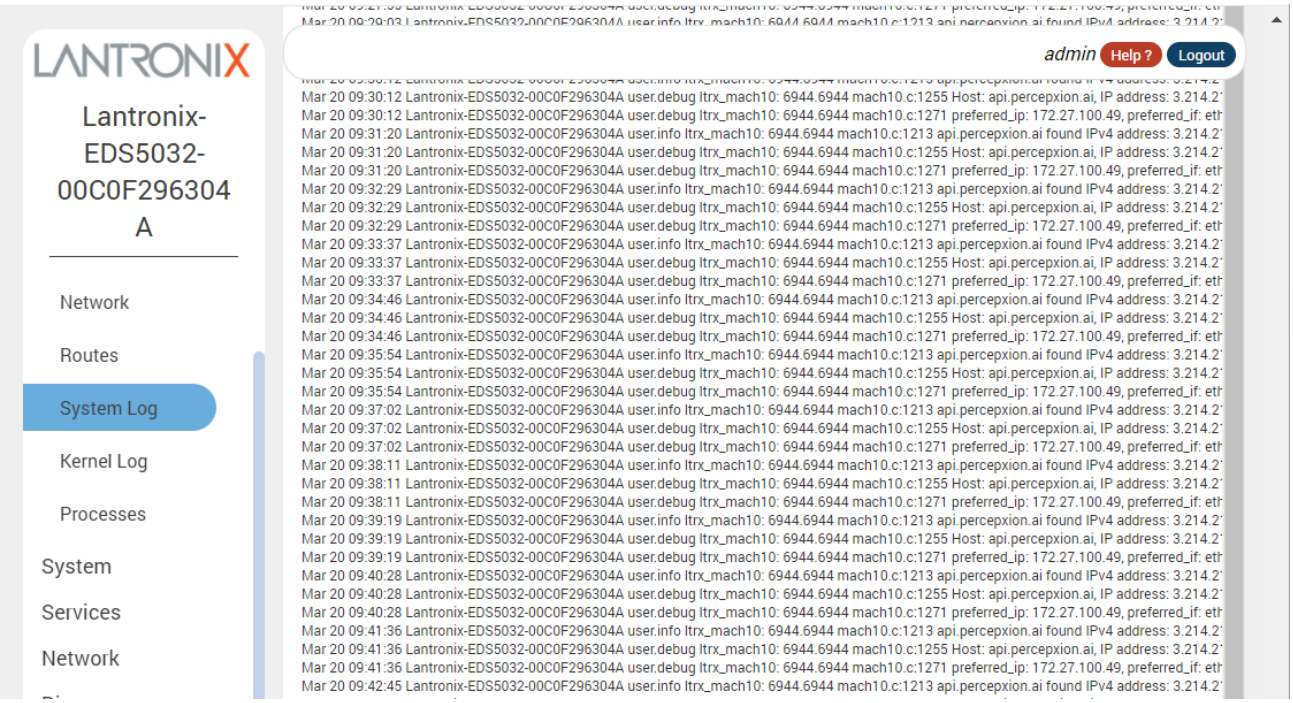
where:

date = `Tue Sep 15 22.33.38 2020`

severity = `user.info`

event details = `Eventsms: BAND: All supported bands`

To configure the system logs, see System > System > Logging.



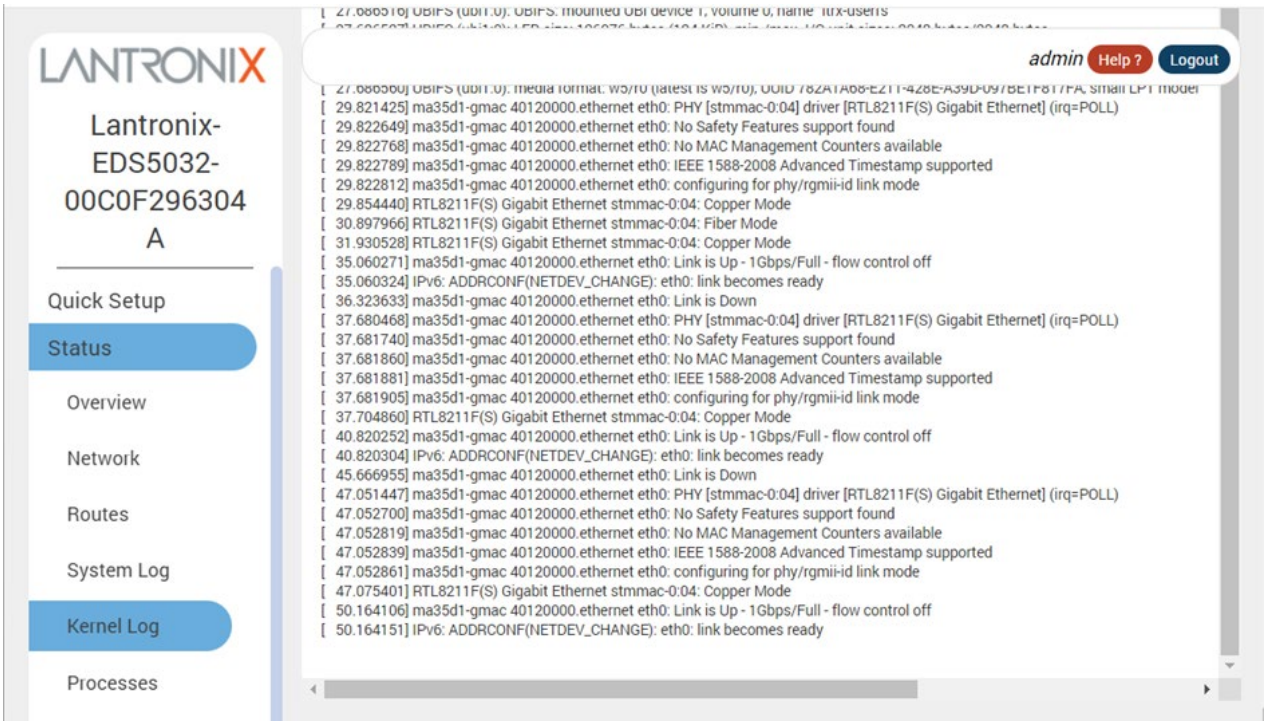
System Log Example:

```
Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: Network device 'eth0' link is up

Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: Interface 'wan' has link connectivity

Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: Interface 'wan' is setting up now

Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: Interface 'wan6' has link connectivity

Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: Interface 'wan6' is setting up now

Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: wan (20850): udhcpc: started, v1.35.0

Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: wan (20850): udhcpc: broadcasting discover

Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: wan (20850): udhcpc: broadcasting select for
172.27.100.90, server 172.27.90.5

Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: wan (20850): udhcpc: lease of 172.27.100.90
obtained from 172.27.90.5, lease time 691200

Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 user.debug ltrx_as: 5409.5513 as_event.c:165 address event:
172.27.100.90 added for eth0(0)
```

```
!
Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 daemon.notice netifd: Interface 'wan' is now up
Mar  8 08:03:26 Lantronix-EDS5032-00804ACCDD10 user.notice firewall: Reloading firewall due to ifup of wan (eth0)
Mar  8 08:03:27 Lantronix-EDS5032-00804ACCDD10 user.info services: SERVICES wan ifup
Mar  8 08:03:27 Lantronix-EDS5032-00804ACCDD10 user.info services: SERVICES
Mar  8 08:05:00 Lantronix-EDS5032-00804ACCDD10 daemon.err uhttpd[2491]: luci: accepted login on / for admin from
172.27.100.17
```

Kernel Log

The Kernel log displays the Linux kernel log events. It shows information about hardware drivers, kernel information and status during boot up and more. It gets reset on every boot.



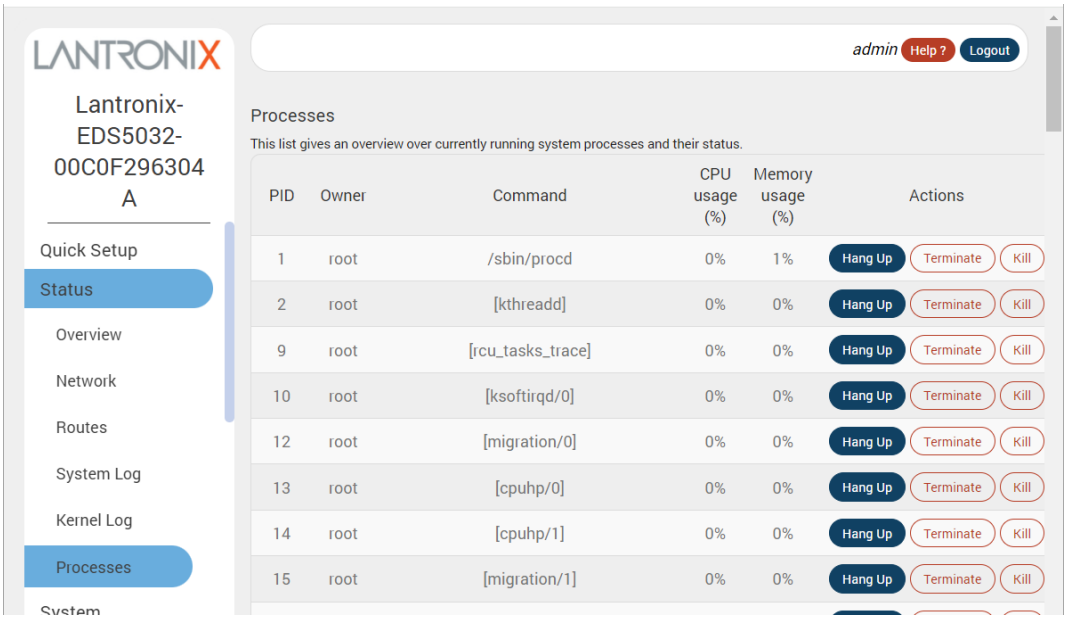
Kernel Log Example:

```
[   38.507490] ma35d1-gmac 40120000.ethernet eth0: PHY [stmmac-0:04] driver [RTL8211F(S) Gigabit
Ethernet] (irq=POLL)
[   38.523623] ma35d1-gmac 40120000.ethernet eth0: No Safety Features support found
[   38.531110] ma35d1-gmac 40120000.ethernet eth0: No MAC Management Counters available
[   38.538921] ma35d1-gmac 40120000.ethernet eth0: IEEE 1588-2008 Advanced Timestamp supported
[   38.547244] ma35d1-gmac 40120000.ethernet eth0: configuring for phy/rgmii-id link mode
[   38.586858] RTL8211F(S) Gigabit Ethernet stmmac-0:04: Copper Mode
[   41.716373] ma35d1-gmac 40120000.ethernet eth0: Link is Up - 1Gbps/Full - flow control off
[   41.724709] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[   46.510322] ma35d1-gmac 40120000.ethernet eth0: Link is Down
[   47.958438] ma35d1-gmac 40120000.ethernet eth0: PHY [stmmac-0:04] driver [RTL8211F(S) Gigabit
Ethernet] (irq=POLL)
```

```
[   47.981635] ma35d1-gmac 40120000.ethernet eth0: No Safety Features support found
[   47.989087] ma35d1-gmac 40120000.ethernet eth0: No MAC Management Counters available
[   47.996779] ma35d1-gmac 40120000.ethernet eth0: IEEE 1588-2008 Advanced Timestamp supported
[   48.005111] ma35d1-gmac 40120000.ethernet eth0: configuring for phy/rgmii-id link mode
[   48.088297] RTL8211F(S) Gigabit Ethernet stmmac-0:04: Copper Mode
[   50.164221] ma35d1-gmac 40120000.ethernet eth0: Link is Up - 1Gbps/Full - flow control off
[   50.172461] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
```

Processes

The Status > Processes page gives an overview of currently running system processes and their status. You can also perform various actions on one or more running processes.



Processes List

Setting	Description
PID	Displays the Process identifier (PID) number associated with the process.
Owner	Shows the task owner (e.g., *root*).
Command	Shows the command name (e.g., */sbin/procd*).
CPU usage (%)	Shows the CPU usage of the process, displayed as a percentage of the total available CPU resources.
Memory usage (%)	Shows the amount of the system's working physical memory that the process is currently using, displayed as a percentage of the total available memory.
Actions	**Hang Up**: Make a process stop executing for some time. When the process is hung, it doesn't run, but it's still present in memory, waiting to be resumed (woken up).
	Terminate: Cause a process to die (like a kill but also include another method such as sending the process a command that tells it to exit).
	Kill: Force a selected process to quit (e.g., if a process is unresponsive, misbehaving, or is consuming too many resources). Sends a kill signal to immediately terminate the process. The process will not perform any cleanup operations.

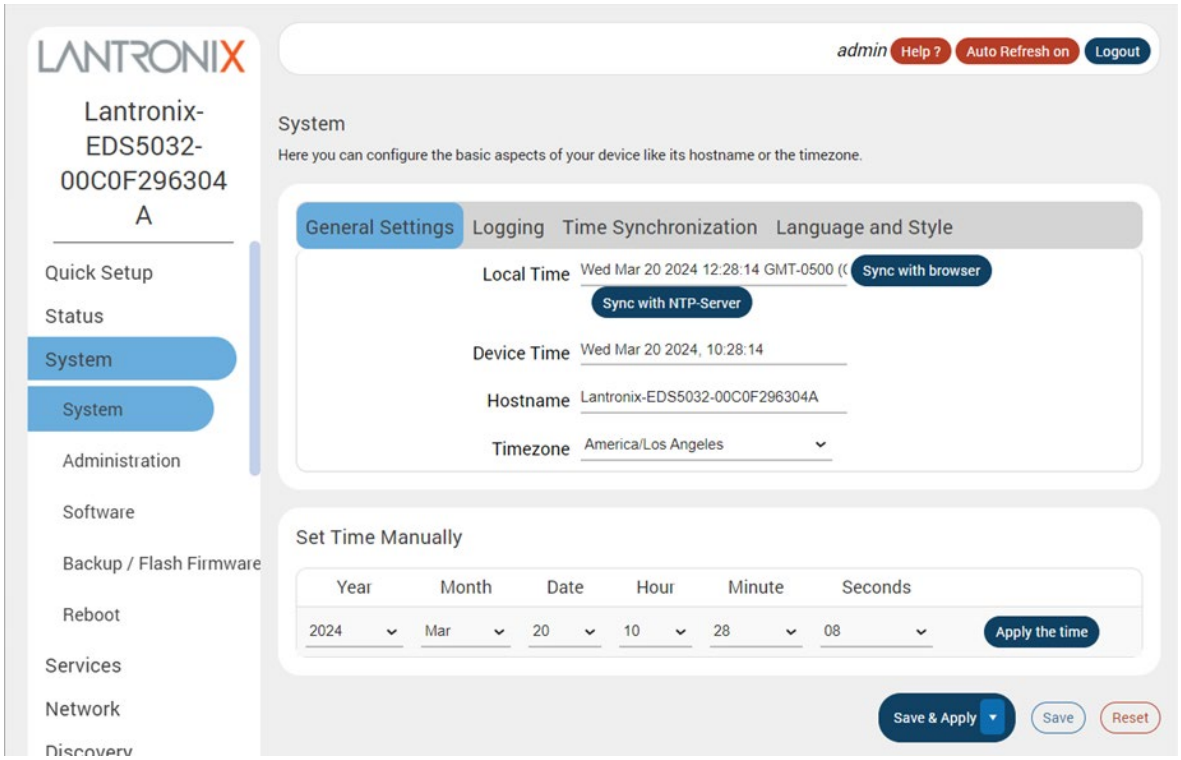
8. System

The System main menu provides submenus to perform system, admin, software, backup & flash firmware, and reboot functions.

System

General Settings

Navigate to System > System and select the General Settings tab to configure time, hostname, timezone and sync functions.



System General Settings

Setting	Description
Local Time	Use the currently selected local time, or click the Sync with browser button, or click the Sync with NTP Server button. The Local Time format is "*Fri Mar 08 2024 10:29:47 GMT-0600 (Central Standard Time)*". Displays the local time of the user's computer. Sync the local time with the browser or with an NTP server: Click **Sync with browser** button to synchronize the EDS5000 clock with the local computer browser. Click **Sync with NTP-Server** to synchronize the EDS5000 clock with an NTP server. **Note**: The displayed time is dependent on the configuration of your local computer that is being used as an NTP server.

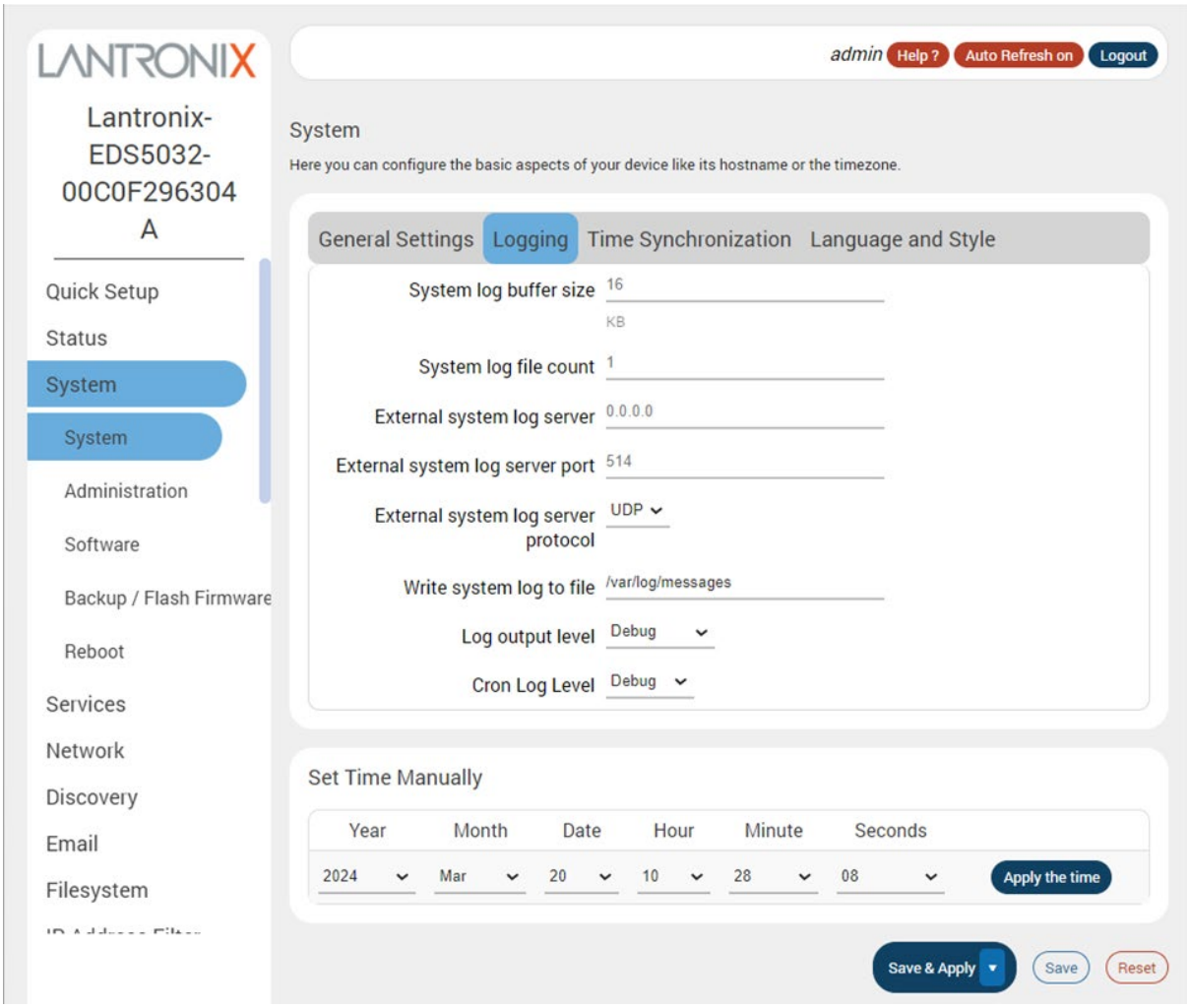
Setting	Description
Device Time	Displays the currently selected device time (e.g., *Fri Mar 08 2024, 08:30:12*).
Hostname	Displays the configured host name (e.g., *Lantronix-EDS5016-00804ACCDD10*).
Timezone	At the dropdown select the desired time zone (e.g., *UTC* or *Europe/Helsinki*)
Set Time Manually	At the dropdown select the Year, Month, Date, Hour, Minute and Seconds settings. Click the **Apply the time** button when done.

Logging

At System > System select the Logging tab to configure and view system logging settings. The System Log displays detailed system, traffic, and network activity log information.

The system logs capture traffic, system, and network activity. The logs are stored in RAM and are reset when the EDS5000 is rebooted.

The system logs can be stored locally or sent to an external UDP or TCP syslog server for storage and archival purposes.



System Logging Settings

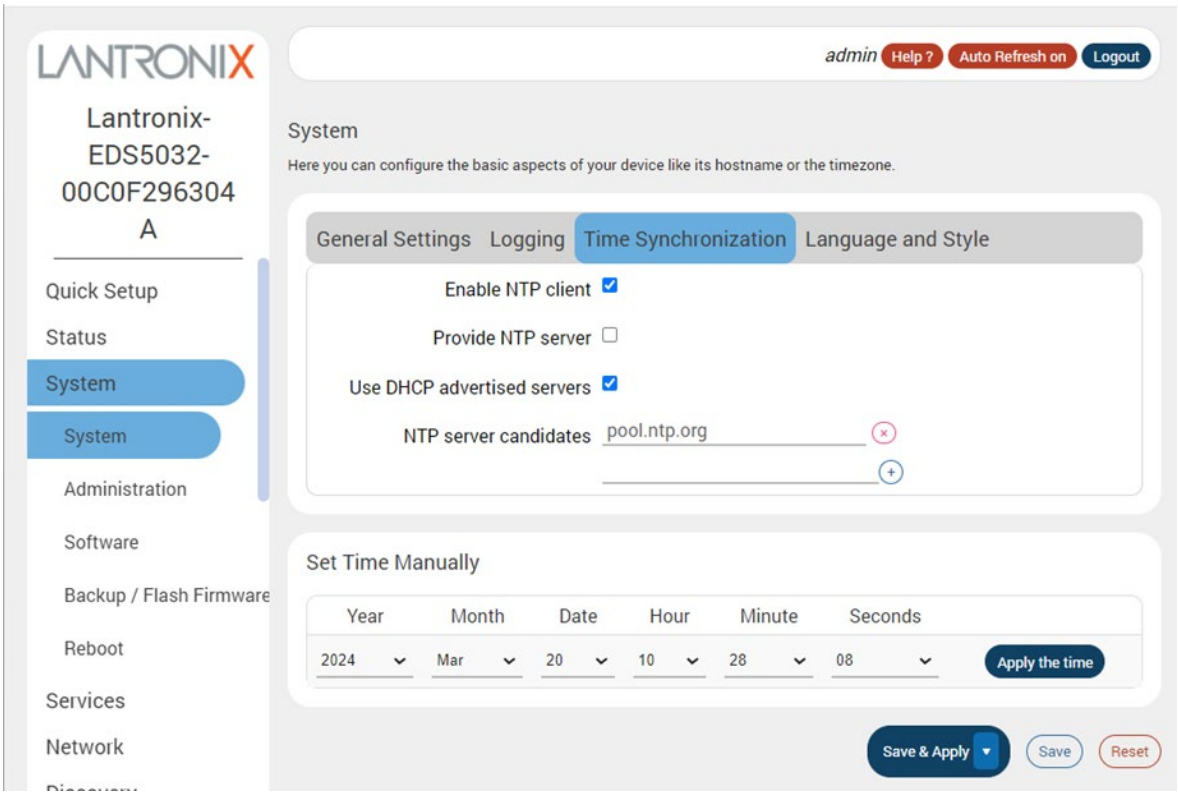
Setting	Description
System log buffer size	The current size of the System log buffer (e.g., *16 KB*). Enter the size of the buffer in Kilobytes (KB) to save logs and status information details. The default system log buffer size is 64 KB. When the buffer is full, records will be overwritten on a first in, first out (FIFO) basis.
System log file count	Shows the number of syslog files that currently exist.
External system log server	Shows the IP address of the configured syslog server if one is configured, otherwise shows *0.0.0.0*. Enter the IP address of an external syslog server to be used to save the real time logs. By default the logs are written to the local system.
External system log server port	Shows the port number of the configured syslog server's commonly-used port number. The default is port *514*. Enter the UDP port number of the external syslog server.
External system log server protocol	Protocol of the external syslog server. The protocol is UDP.
Write system log to file	The location to write syslog files; the default is */var/log/messages*. File path and file name to write the log messages to. If an external filesystem (SD card or USB flash drive) is mounted, add the mount path and file name here. The logs display application (see Services > Logs Information) will download the files written to this file path. Example: /mnt/usbdevice/log.txt.

System Logging Settings

Setting	Description
Log output level	At the dropdown select the desired level of syslog output. The level of severity progresses from Info to Emergency. Lower severity levels are more verbose and will include messages from all higher severity levels. Log levels are listed in order of increasing severity: ♦ Debug – Provides debug messages used by the software developer for debugging the application. These logs are typically not useful during operations. The default is *Debug*. ♦ Info – Provides normal operational information messages that are used for general purposes like reporting. ♦ Notice – Provides alerts for peculiar events that are not an error. These logs help to identify potential issues. Since these logs do not indicate errors, immediate action may/may not be necessary. ♦ Warning – Displays warning messages for a potential issue, indicating to take an action. An error may occur if no action is taken against the warning issued. ♦ Error – Displays the messages indicating an error condition. ♦ Critical – Indicates failure in secondary system and must be corrected immediately. ♦ Alert – Problems which should be corrected immediately. ♦ Emergency – System is unusable.
Cron Log Level	At the dropdown select the desired level of cron command-line utility used for job scheduling. The options are *Debug*, *Normal*, or *Warning*). The default is *Debug*. ♦ Debug – Helps to debug cron process which has failed during runtime. ♦ Normal – Displays informational messages. ♦ Warning – Indicates some issues can happen or error could be generated in cron process
Set Time Manually	At the dropdown select the Year, Month, Date, Hour, Minute and Second settings. Click the Apply the time button when done.

Time Synchronization

At System > System select the Time Synchronization tab to configure and view Network Time Protocol (NTP) and related settings.



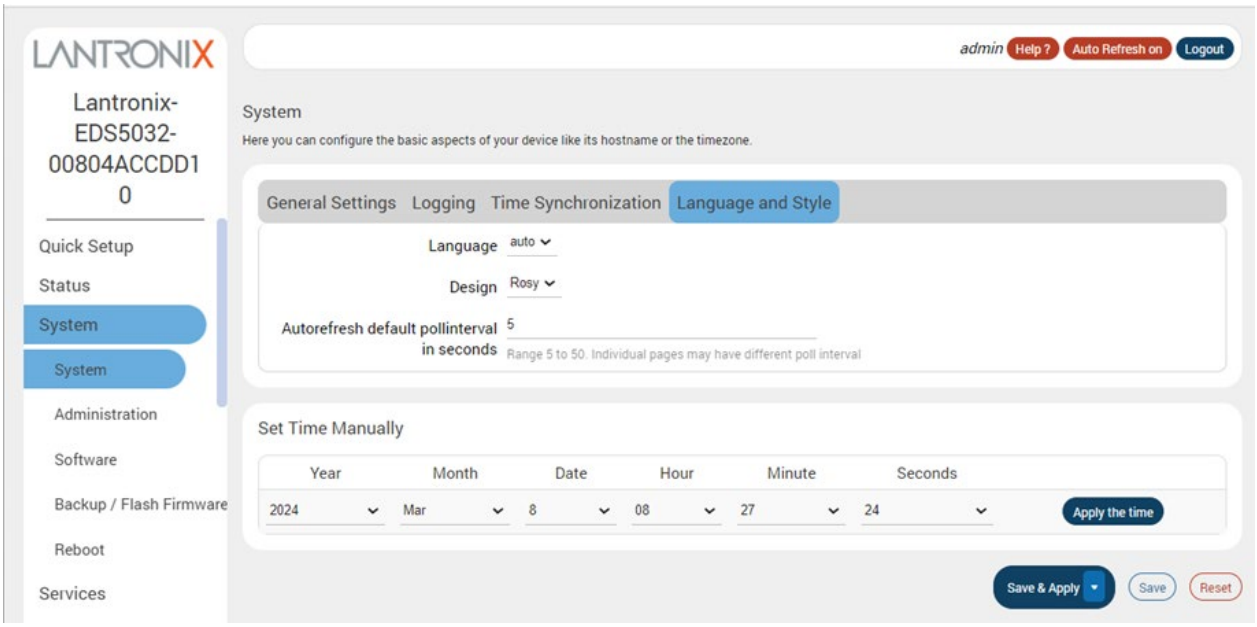
Time Synchronization Settings

Setting	Description
Enable NTP client	Check the box to enable the built-in Network Time Protocol client. The default is NTP client Enabled.
Provide NTP server	Check the box to let you provide an external NTP server "candidate". The default is Disabled.
Use DHCP advertised servers	Check the box to use one or more "advertised" DHCP servers. The default is Enabled.
NTP server candidates	Enter a valid hostname or IP address. By default "pool.ntp.org" is enabled. Click the ⊗ icon to delete the default (or other) NTP Server candidate. Click the ⊕ icon to enter a different or additional NTP Server candidate.
Set Time Manually	At the dropdown select the Year, Month, Date, Hour, Minute and Second settings. Click the Apply the time button when done.

Note: The EDS5000 will retain the set time for a brief period in the event of a power loss if using local time mode and not Network Time Protocol (NTP).

Language and Style

At System > System select the Language and Style tab to view and change device language, design, default polling interval, and manual time settings.



Language and Style Settings

Setting	Description
Language	At the dropdown select the desired Language. The default is *auto*.
Design	At the dropdown select the desired Design. The default is *Rosy*.
Autorefresh default pollinterval in seconds	Enter the amount of time for the device to automatically refresh the default polling interval. The valid range is 5 to 50 seconds. The default is 5 seconds. Note that individual pages may have different poll intervals.
Set Time Manually	At the dropdown select the Year, Month, Date, Hour, Minute and Second settings. Click the “Apply the time” button when done.

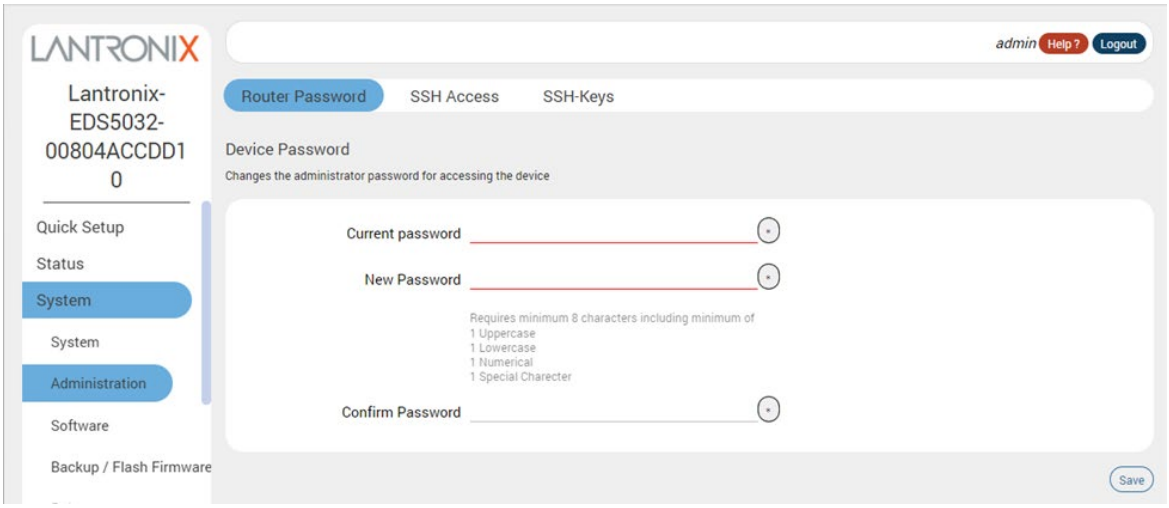
Click the Save & Apply button when done.

Administration

Navigate to System > Administration to access the EDS5000 password, SSH access, and SSH Keys function tabs.

Router Password

At System > Administration select the Router Password tab where you can change the administrator password for accessing the device.



Router Password Settings

Setting	Description
Current Password	Enter the current password.
New Password	Enter the new password. The new password requires at least 8 characters, including 1 uppercase, 1 lowercase, 1 numerical, and 1 special character.
Confirm Password	Enter the new password again; it must match the previous Password entry.
Reveal/hide password	Click the icon to alternately show and hide the password as you type it.

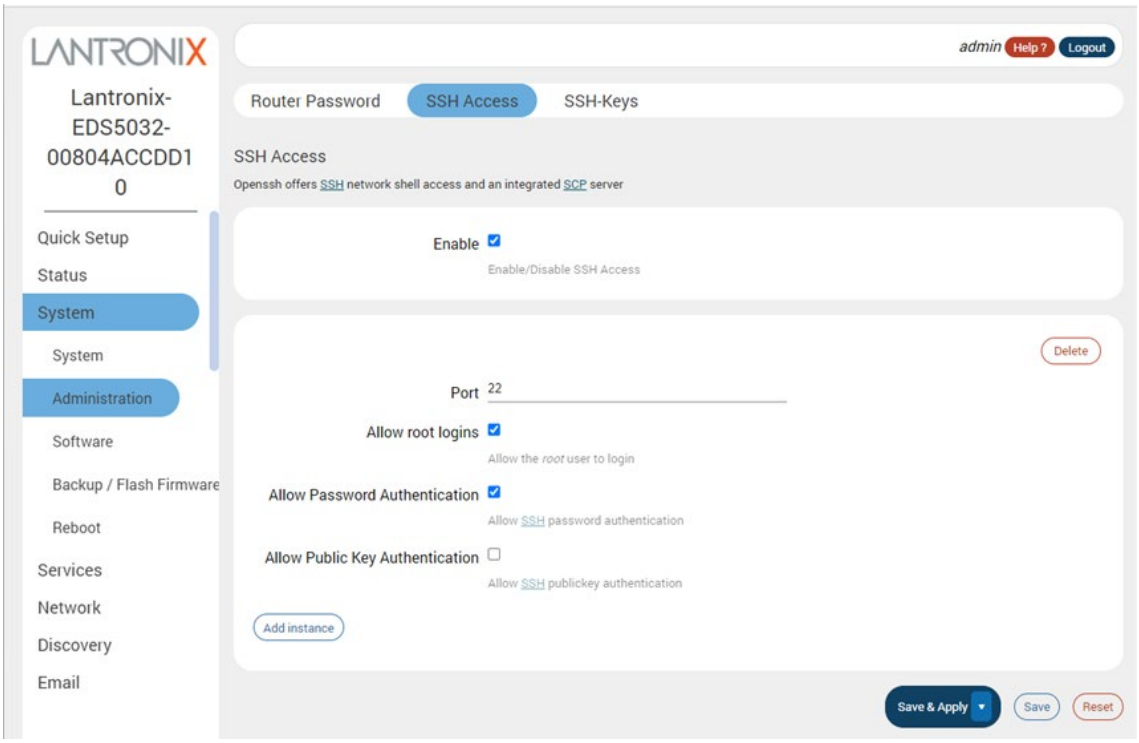
Click the Save button when done.

SSH Access

At System > Administration select the SSH Access tab where you can configure and view SSH access. OpenSSH offers SSH (Secure Shell) network shell access and an integrated SCP (Secure Copy) server.

Secure Shell (SSH) lets you securely and remotely access the EDS5000 over the network from a terminal emulator to view and configure it. SSH provides strong password authentication and public key authentication, as well as encrypted data communication between your computer and the EDS5000. The EDS5000 listens for SSH connections on TCP port 22 (default).

By default password authentication is enabled. If you want to use public-key authentication, you must enable Allow Public Key Authentication and upload public key authentication via the SSH-Keys tab.



SSH Access Settings

Setting	Description
Enable	Check or uncheck the box to Enable/Disable SSH Access. The default is Enabled.
Port	Enter the desired port for SSH access (the listening port of the instance). The default is Port 22.
Allow root logins	Check the box to allow the root user to login via SSH. The default is Enabled.
Allow Password Authentication	Check the box to enable SSH password authentication. The default is Enabled.
Allow Public Key Authentication	Check the box to allow SSH authentication via public key. The default is Disabled.

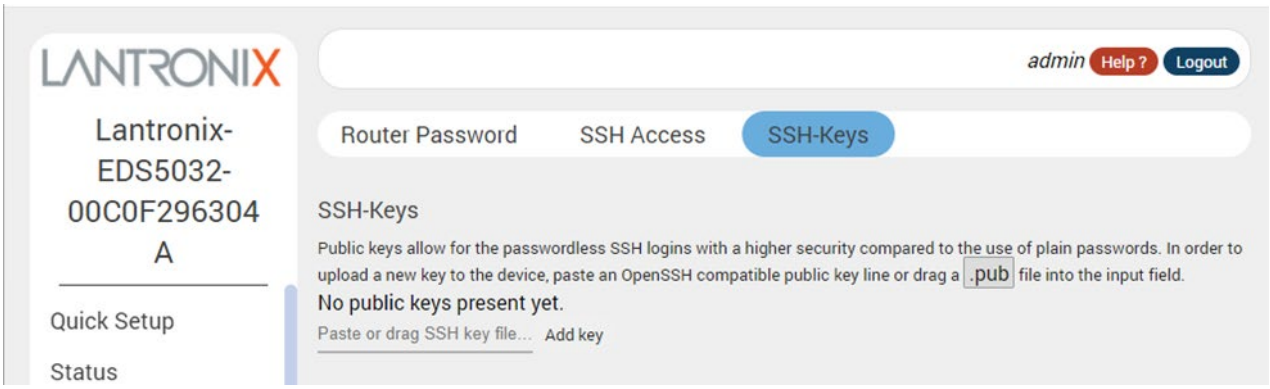
Setting	Description
Add instance	Click the button to add a new SSH Access instance.
Delete	Click the button to remove an added SSH Access instance.

SSH-Keys

At System > Administration select the SSH-Keys tab to add an SSH public key. Public keys allow for passwordless SSH logins with higher security compared to using plain passwords.

To add a new public SSH key:

1. Go to System > Administration > SSH-Keys.
2. Copy the public key from the host system and paste it in the input field. Alternatively, drag and drop the SSH key file (.pub) into the input field.
3. Click Add key.



SSH Keys Settings

Setting	Description
Paste or drag SSH key file…	To upload a new key to the device, paste an OpenSSH compatible public key line or drag a .pub file into the input field.
Add key	Click the button to add the new SSH key

Software

Navigate to System > Software to access the Available, Installed, and Updates function tabs.

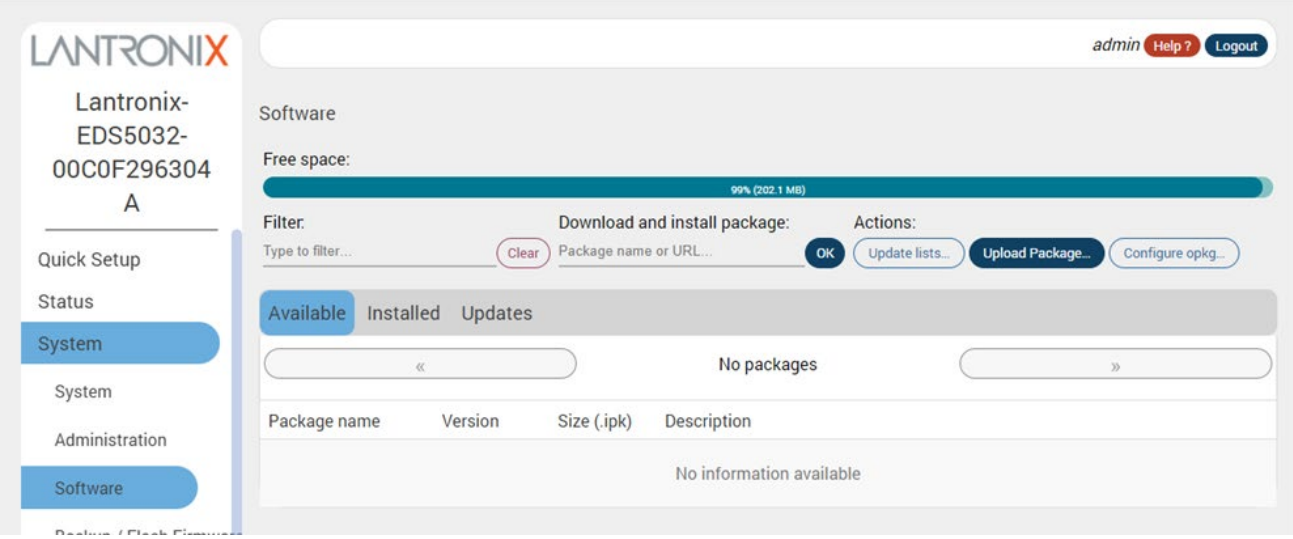
The software package manager lets you upgrade the system by installing, upgrading, or removing additional software packages from package repositories that are local or on the Internet. The package manager (opkg utility) attempts to resolve dependencies with packages in the repositories. If it fails, it reports an error and aborts the installation of the package.

The software package manager is not used to upgrade system firmware (sysupgrade). For firmware upgrade, see Backup / Flash Firmware.

The Software page displays the list of all packages or the packages that match the Filter criteria according to the following categories (tabs).

- **Available** - when selected, the table lists all packages that are available in the configured repository. You can see if the package is installed, or if you have the option to install or upgrade it.
- **Installed** - when selected, the table lists the packages that are currently installed on the device. You can see the option to remove these packages.
- **Updates** - when selected, lists the packages where an updated version is available, as long as you use a supported version of OpenWRT. If none are found, displays "*No packages*".

The Software page Available tab parameters are described below.



Software Page - Available tab

Setting	Description
Free space	Displays the amount of free space available as a percentage and in megabytes.
Filter	Type the desired filter data; click the Clear button to delete the displayed filter data. The message *No packages matching "xxxx".* displays if no matching filter data is found. Click the linked text (Reset) to clear the message.
Download and install package	Enter the package name or a URL and click the OK button to make the entry. The message *Manually install package The package 1.2.3.4 is not available in any configured repository*. displays if the package cannot be found. Click the Cancel button to clear the selection field.

Setting	Description
Actions	**Update lists**: Displays the message *Executing package manager Waiting for the opkg update command to complete…* **Update Package**: Click to select a file to upload. At the message *Uploading file…* *Please select the file to upload.* click the Browse button to and select the desired package file, then click the Upload button. **Configure opkg**: Configure the opkg (Open Package Management) software - a lightweight package management system intended for use on embedded Linux devices and is used in this capacity in OpenWrt projects. The OPKG Configuration page displays with a listing of the various configuration files used by opkg. Use `opkg.conf` for global settings and `customfeeds.conf` for custom repository entries. The configuration in the other files may be changed but is usually not preserved by `sysupgrade`. Click Cancel or Save.
Package name	Displays the selected package name.
Version	Displays the version of the package.
Size (.ipk)	Displays the size of the package. The .ipk packages are the installation packages used by opkg (Open Package Management) software.
Description	Displays a description of the package.

List the Packages

To view all packages in the configured repository:

1. Go to System > Software.
2. Click the Available tab. The packages are displayed. (Click the Installed tab to view the installed packages only.)
3. Click the page back and page forward arrows (<< and >>) to view the entire packages list if it spans more than one page.

To filter the package list by package name:

1. Go to System > Software.
2. Next to Filter, type part or all of the package name.
3. Click the Available, Installed or Updates tab. The packages that match the filter are displayed.
4. Click the page back and page forward arrows (<< and >>) to view the list of packages.

Update the List of Packages

The update command retrieves the list of packages. The package manager needs this information to install or upgrade packages or print information about them. You should run the `update` command before you install a new package. To update the list of available packages:

1. Go to System > Software.
2. Click Update lists. The package manager updates the list of available packages.
3. Click Dismiss.
4. View the available packages.

Install a Package

To install a package:

1. Go to System > Software.
2. Click Update lists to refresh the list of available packages.
3. Do one of the following:
   - Click the Available tab, select the package (or filter the list and select the package) and click Install.
   - Under Download and install package, enter the package name for a package on the download server, or enter the URL for a package on a custom feed, and click OK.
   - Click Upload Package, to select the package from the local machine, and click Upload.
4. The package manager displays the package details including the following:
   - version of the package
   - size of installed package
   - list of dependent packages, with installation status and size if not installed
   - package description
   - space required and the number of packages to install
   - A warning message displays if the installed packages are incompatible with the required packages.
   - The option to Overwrite files from other package(s). By default, it is not selected.
5. Review the package details. Ensure the device has adequate space available to install the required packages. If desired, select Overwrite files from other package(s).
6. Click Install.
7. The package manager displays the installation progress and error messages, if applicable. Click Dismiss when finished.
8. Refresh the web page and view that the package is listed as “Installed” in the list of Available packages. You may need to restart the device, depending on the package and its use.

Upgrade a Package

To upgrade a package:

1. Go to System > Software.
2. Click Update lists to refresh the list of packages.
3. Do one of the following:
   - Click the Available tab, select the package (or filter the list and select the package) and click Upgrade.
   - Under Download and install package, enter the package name for a package on the download server, or enter the URL for a package on a custom feed, and click OK.
   - Click Upload Package and browse to select the package from the local machine.
4. The package manager lists the package details including the following:
   - version of the package
   - size of installed package
   - package description
   - space required and the number of packages to install
   - A warning message is displayed if the installed packages are incompatible with the required packages.
5. Review the package details. If desired, select Overwrite files from other package(s).
6. Click Install.
7. The package manager displays the installation progress and error messages, if applicable. Click Dismiss when finished.
8. To verify, refresh the web page and view that the package is listed as “Installed” in the list of Available packages. You may need to restart the device, depending on the package and its use.

Remove a Package

To remove a package:

1. Go to System > Software.
2. Click the Installed tab, select the package (or filter the list and select the package) and click Remove.
3. Review the package details, including the following:
   - version of the package
   - size of installed package
   - description of the package
   - The option to Automatically remove unused dependencies box (checked by default). To keep all dependent packages, clear this box.
4. To continue, click Remove.
5. The package manager displays the progress and error messages, if applicable. Click Dismiss to close the dialog.

Configure OPKG

The OPKG configuration files define the configuration and feed locations used by the OPKG package manager. It includes the following configuration files:

- opkg.conf – This configuration file sets the default folders.
- opkg/customfeeds.conf – This file is used to add your custom package feeds (repositories).
- opkg/distfeeds.conf – This file is used to set the feeds. By default, it provides the path to the Lantronix package server.

To modify the OPKG configuration:

1. Go to System > Software.
2. Click the Configure opkg button.
3. Modify the configuration (see table below).
4. Click Save.

OPKG Package Manager Configuration

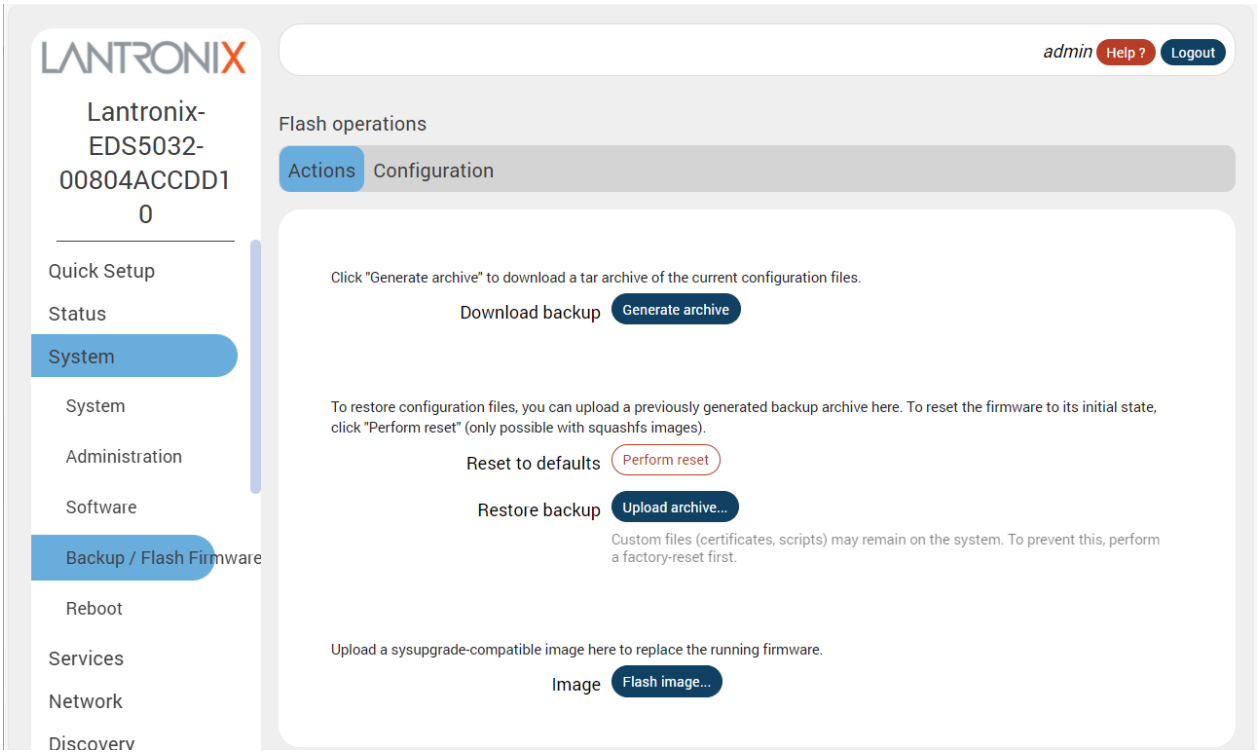
Setting	Description
opkg.conf	The default configuration is shown: ♦ dest root / ♦ dest ram /tmp ♦ lists_dir ext /var/opkg-lists ♦ option overlay_root /overlay ♦ option check_signature The options can be left at the default value.
customfeeds.conf	Enter each custom package feed on its own line. The feed can be on a remote server, in a version control system, on the local file system, or in any location addressable by a single name (path/URL) over a protocol with a supported feed method. An example format is provided: `# src/gz example_feed_name http://www.example.com/path/to/files` Remove the “#” (hash symbol) at the start of the line.
distfeeds.conf	Displays the Lantronix package feeds repository. The feed can be on a remote server, in a version control system, on the local file system, or in any location addressable by a single name (path/URL) over a protocol with a supported feed method.

Backup / Flash Firmware

Navigate to System > Backup / Flash Firmware to access Flash Operations functions at the Actions and Configuration tabs.

Actions

The Actions tab allows you to download, reset, and restore config files, and upload a running config file.



Setting	Description
Download backup	Click **Generate archive** to download a tar archive of the current configuration files. At the “Confirm user password” prompt enter the current password and click the Proceed button. Authentication - ♦ Confirm user password - enter password of logged in user and click Proceed. ♦ Set Password - enter a password to protect the backup archive.
Reset to defaults	To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images). Click the **Perform Reset** button to reset the device to its initial configuration after flashing the firmware. This removes settings and user-installed software packages, which are stored on the overlayfs configuration partition. It works with any install with a squashfs / overlayfs setup. Authentication - Confirm user password: enter the password of the logged in user

Setting	Description
Restore backup	Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first, then click the **Upload archive** button. Click the **Upload archive** button to upload a previously generated backup archive. Authentication - **Enter backup archive password** - Enter the password that was created to download the backup archive. The validity of the backup archive is checked and the files in the backup archive are listed. Review the list of files before you continue or cancel the restore operation.
Image	Click the **Flash image** button to upload a sysupgrade compatible image for replacing the running firmware. **Warning**: *Do not power off the device during the update*. When the image file is uploaded, a file integrity check is done through the use of md5 algorithm. Verify the md5 value with the one given along with the firmware file. **Keep software packages, settings, and current configuration** - This is selected by default. See the Firmware Upgrade Procedure section below. **Warning**: *Software packages are only restored from configured repositories. The device will automatically reboot when packages are restored*. Authentication - **Confirm user password and continue** - Enter the password of the logged in user.

Backup and Restore

Download backups to keep the working configuration data. The backup consists of all policies and all other user-related information.

Restore backups to restore configuration on the EDS5000 or to configure a new EDS5000 with the same settings.

To generate a backup archive:

1. Go to System > Backup/Flash Firmware > Actions.
2. Click the Generate archive to download a backup file.
3. At Confirm user password, enter the password of the logged in user. Click Proceed.
4. At Set Password, enter a password to protect the backup file. Click Download.
5. The backup archive is generated and downloaded to the local download folder.

To restore a backup archive:

1. Go to System > Backup/Flash Firmware > Actions.
2. Click Upload archive to restore a backup archive.
3. At Enter backup archive password, enter the password that was created to secure the backup archive. Click Proceed.
4. Select the backup archive file to upload. Click Upload.
5. The validity of the backup archive is checked and the files in the backup archive are listed. Review the list of files. Click Continue to proceed.

The configuration is applied and the device reboots. If the restored configuration changes the current LAN IP address, you may need to reconnect manually.

Reset to Defaults

A factory reset erases all user-installed packages and settings and returns the device to its initial state after installing the firmware. The EDS5000 uses a squashfs file system, as required for this feature.

To reset the firmware:

1. Go to System > Backup/Flash Firmware > Actions.
2. Click Perform reset.
3. At the Authentication prompt, enter the password of the logged in user. Click Proceed. The system erases the configuration partition and then reboots.
4. Access the device using the default configuration.

Firmware Upgrade Procedure

This section lets you upload a sysupgrade-compatible image to replace the running firmware.

Flash firmware (system upgrade) optionally saves specified configuration files, wipes the entire file system, installs the new version, and then restores the saved configuration files. Any parts of the file system that are not specifically saved will be lost.

For more details, see Restoring IPKs after Firmware Upgrade on the Device.

To do a firmware upgrade:

1. Go to System > Backup/Flash Firmware > Actions.
2. Click the **Flash image…** button.
3. Browse to and select the file (e.g., *EDS5000_210.0.0R1.rom*) to upload and click the **Upload** button. The system confirms the upload and displays the flash image size and checksum. Verify the firmware image checksum.
4. **Keep software packages, settings, and current configuration** - This is selected by default. Leave it selected so that the device will **not** retain installed software packages (IPKs), settings, and current configuration. If you deselect it, the device configuration will be reset to factory settings and user-installed software packages will be removed after updating the firmware.
5. At the Authentication prompt, enter the user password.
6. Click **Continue** to proceed with flashing the image.
7. Do not power off the device while the upgrade is in progress. This may take a couple minutes. After the upgrade completes, the device will reboot. You may need to renew the IP address in your browser to reach the device again.

Messages:

Flash image?

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.

Click "Proceed" below to start the flash procedure.

Size: 23.50 MB

MD5: e0d5c63236decab1aa2d9000b1f21260

SHA256: e02cc77479dcfc5817844d18256b551935eb18a2bd9a8a278bb1d19480625e3e

WARNING: Software packages are only restored from configured repositories.

Device will automatically reboot when packages are restored.

Confirm user password and continue:

Click Cancel or click Continue.

Flashing...

The system is flashing now.

DO NOT POWER OFF THE DEVICE!

Wait a few minutes before you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.

Restoring IPKs after Firmware Upgrade on the Device

To ensure that previously installed software packages and their configurations are retained when upgrading the firmware, follow the flash firmware procedure and make sure that “Keep software packages, settings, and current configuration” is selected.

The device will automatically reboot after packages are restored. To verify that the packages have been restored, go to System > Software > Installed to view the installed packages.

Note: Software packages are only restored from configured repositories. Repositories can be configured from System > Software > Configuration. See Configure OPKG on page 62.

Configuration

Navigate to System > Backup / Flash Firmware > Configuration tab to display the Flash operations page.

The Configuration tab has a list of shell glob patterns for matching files and directories to include during sysupgrade.

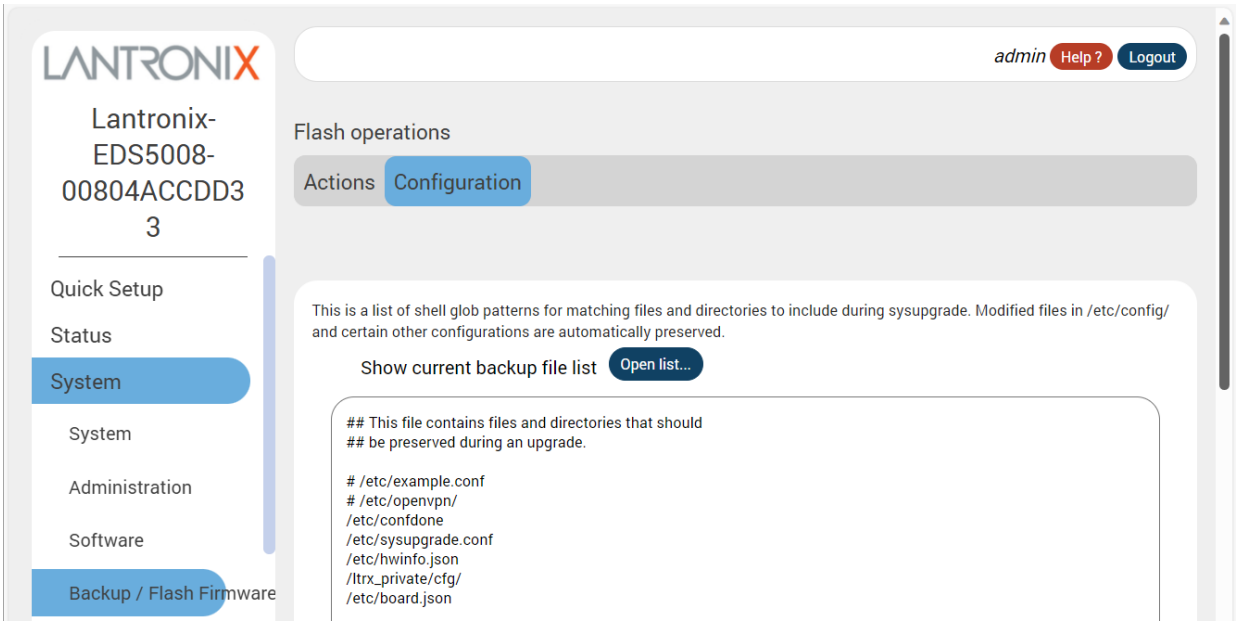
Add files and directories that should be preserved during a system upgrade to the backup file list.

Modified files in /etc/config/ directory and certain other configurations are automatically preserved.

To show the current backup file list, click the **Open list...** button.

To modify the backup file list:

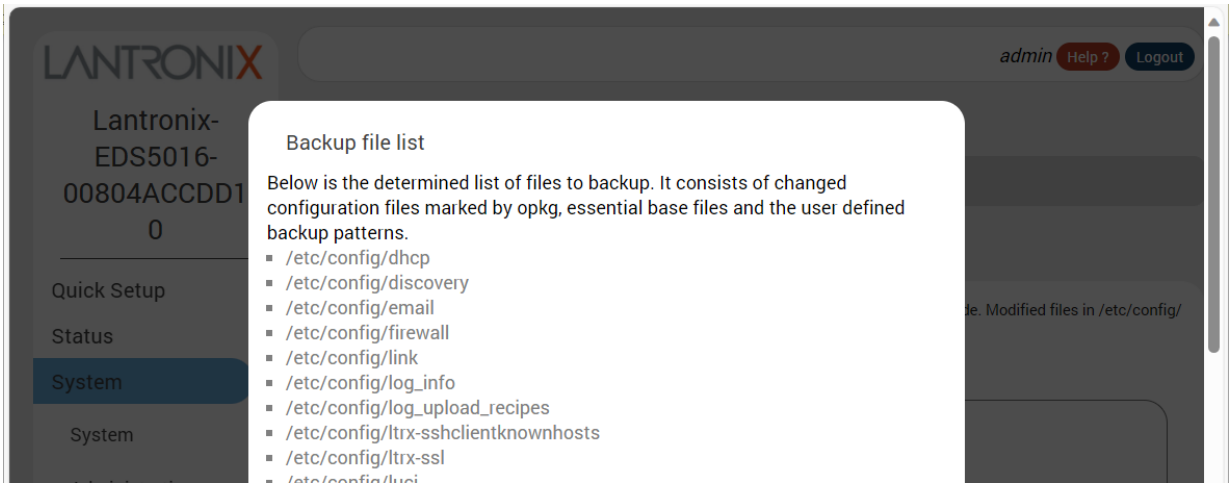
1. Go to System > Backup/Flash Firmware > Configuration.
2. In the editor, place the cursor below the last line.
3. Enter file path for each file or directory on a new line. The file path is relative to the top level directory.
4. Click **Save**.



Flash operations > Configuration

Setting	Description
Show current backup file list	Click the **Open list…** button to display the “Backup file list” which contains “the determined list of files to backup. It consists of changed configuration files marked by opkg, essential base files and the user defined backup patterns.”. Click the **Dismiss** button to clear the list. This file contains files and directories that should be preserved during an upgrade.

To show the current backup file list, click **Open list...**



Reboot

Navigate to the System > Reboot menu path to be able to perform a Reboot or a Scheduled Reboot of the operating system of your EDS5000 device server.

Reboot

At the Reboot tab you can Reboot the operating system of your device. This may take several minutes to complete. Any unsaved configuration will be lost when the device is rebooted. **To reboot the EDS5000**:

1. Go to System > Reboot.
2. Click Perform Reboot.

The device restarts and reloads the configuration. After the device boots, the login page is displayed.

Schedule Reboot

At the Schedule Reboot tab you can set up a scheduled Reboot of your device's operating system. Schedule times when the EDS5000 will reboot itself. You can set the frequency by time of day (hour and minute), day of week, and day of month.

To configure the reboot schedule:

1. Go to System > Reboot > Schedule Reboot.
2. Click Add.
3. Enter the schedule reboot details (see below).
4. Click Save.
5. Click Save & Apply. You can then Add, Edit, or Delete scheduled reboot entries.

Schedule Reboot

Setting	Description
Add	Click the Add button to display the Schedule Reboot parameter selections.
Enable	Check the "Enable" checkbox to enable a scheduled system reboot of your device.
Day of the week	At the dropdown select Any or Sunday - Saturday as the day of the week for the scheduled system reboot to occur.
Month	At the dropdown select Any or January - December as the month for the scheduled system reboot to occur.
Date	At the dropdown select Any or 1 - 31 as the date for the scheduled system reboot to occur.
Hour	At the dropdown select Any or 0 - 23 as the hour of the day for the scheduled system reboot to occur. 0 = midnight.
Minute	At the dropdown select Any or 0 - 59 as the minute of the hour for the scheduled system reboot to occur.

9. Services

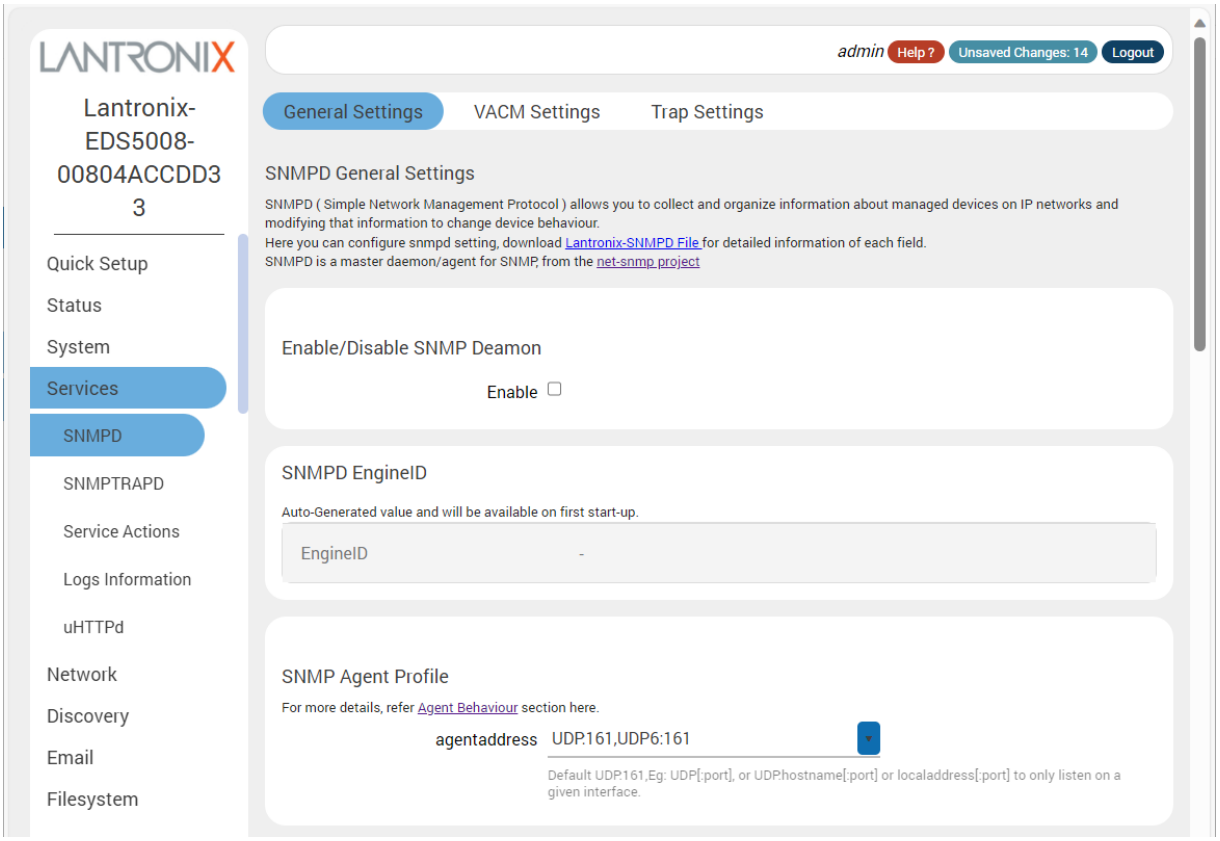
The Services main menu lets you select and configure SNMP and HTTP services for the EDS5000.

SNMPd

This page provides the General Settings, VACM Settings, and Trap Settings tabs for SNMPd configuration. SNMPd is a daemon that supports SNMP, a standard Internet protocol for network device management and monitoring. SNMPd (Simple Network Management Protocol) allows you to collect and organize information about managed devices on IP networks and modifying that information to change device behavior. SNMPd is a master daemon/agent for SNMP, from the net-snmp project.

General Settings

Here you can configure SNMPd settings. You can download the Lantronix-SNMPD File for detailed information of each SNMPd field.



System Information

For more details, refer System Information section here.

sysName	Lantronix-EDS5008-00804ACCDD33
sysContact	-
sysLocation	-
sysDesr	Linux Lantronix-EDS5008-00804ACCDD33 5.10.140 #0 SMP Sat Sep 3 02:55:34 2022 aarch64

Process Monitoring (prTable)

For more details, refer Process Monitoring section here.
Monitors the number of processes running on the local system and registers a command that can be run to fix errors (cmd will not invoked automatically).

Process Name	Max Process	Min Process	Enable Fix Action	Program Name(Procfix action)	Arguments	
Prcs-1	4	1	Yes	PFix-111	aaa	Edit Delete

Add

Disk Usage Monitoring (dskTable)

For more details, refer Disk Usage Monitoring section here.
Monitors the disk mounted at Partition for available disk space, can either be specified in kB (MINSPACE) or as a percentage of the total disk (MINPERCENT% with a '%' character)

Partition	Minimum Space	
/tmp	20	Edit Delete
/overlay	4	Edit Delete

Add

Configures monitoring of all disks found on the system, using the specified (percentage) threshold.
The threshold for individual disks can be adjusted using suitable disk directives configured above.

Include All disks ☐

System Load Monitoring (laTable)

For more details, refer System Load Monitoring section here.
Monitors the load average of the local system.Walking the laTable will succeed even if this directives is not configured.

Enable Load Monitoring ☑

1 - Minute Max. Load

5 - Minute Max. Load

15 - Minute Max. Load

Swap Space Threshold (in KB)

Monitors the amount of swap space available on the local system. Default threshold is 16 MB even if not configured.

SNMPd General Settings

Setting	Description
Enable/Disable SNMP Deamon	Check the box to Enable the SNMP Daemon (SNMPd). The default is Disabled.
SNMPD EngineID	Auto-Generated value and will be available on first start-up.
SNMP Agent Profile	**agentaddress**: At the dropdown select the desired SNMP agent profile: ♦ unspecified: ♦ UDP:161,UDP6:161 (default) ♦ 161 ♦ localhost:161 ♦ localhost:161 ♦ udp:161,tcp:161,udp6:161,tcp6:161 ♦ custom Default UDP:161. For example: UDP[:port], or UDP:hostname[:port] or localaddress[:port] to only listen on a given interface.
System Information	**sysName** : The assigned System Name (e.g., *Lantronix-EDS5016-00804ACCDD10*). **sysContact** : The configured System Contact (if any) or - if none configured. **sysLocation** : The configured System Location (if any) or - if none configured. **sysDesr** : The assigned System Name (e.g., *Linux Lantronix-EDS5016-00804ACCDD10 5.10.140 #0 SMP Sat Sep 3 02:55:34 2023 aarch64*). For more details, refer to the System Information section.

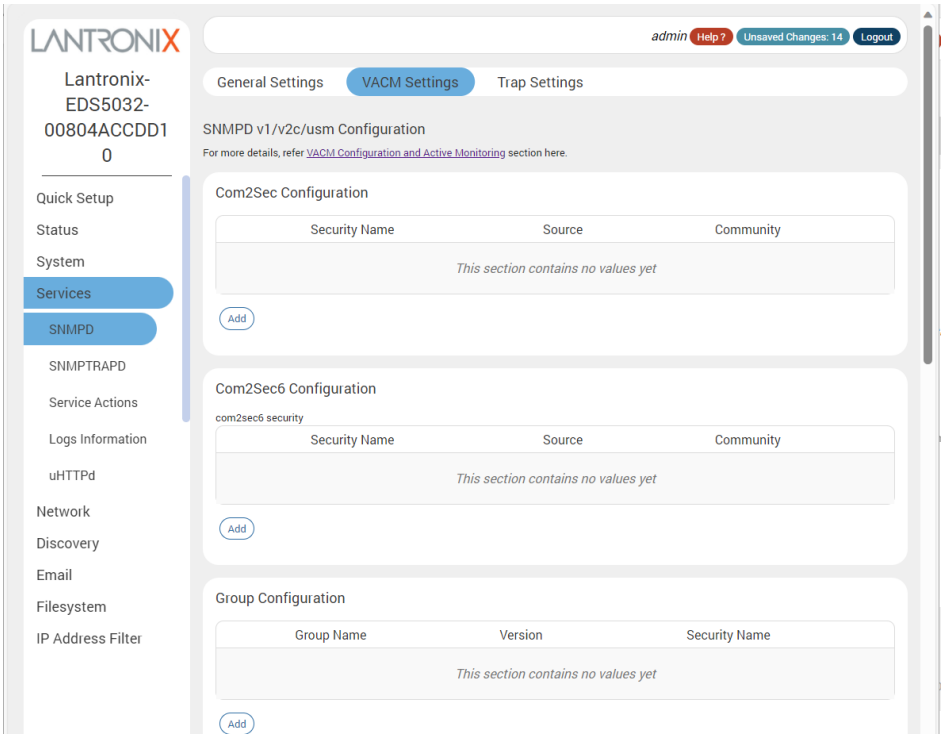
Setting	Description
Process Monitoring (prTable)	Monitors the number of processes running on the local system and registers a command that can be run to fix errors (command not invoked automatically). ♦ Process Name ♦ Max Process ♦ Min Process ♦ Enable Fix Action ♦ Program Name(Procfix action) ♦ Arguments Click the Add button to display the “SNMPD General Settings” screen, enter the required parameters, then click the Save button. For more details, refer to the Process Monitoring section.
Disk Usage Monitoring (dskTable)	Monitors the disk mounted at Partition for available disk space, can either be specified in kB (MINSPACE) or as a percentage of the total disk (MINPERCENT% with a '%' character). Click the Add button to display the SNMPD General Settings: **Partition**: At the dropdown select the (/rom, /tmp, /overlay, or custom). **Minimum Space**: enter in kB (MINSPACE) or as a percentage of the total disk (MINPERCENT% with a '%' character). Click the Save button when done. You can then edit or delete existing entries or add more new entries. For more details, refer to the Disk Usage Monitoring section. **Include All disks**: Check the box to configure monitoring of all disks found on the system, using the specified (percentage) threshold. The threshold for individual disks can be adjusted using suitable disk directives configured above.
System Load Monitoring (laTable)	Monitors the load average of the local system. Walking the laTable will succeed even if this directives is not configured. **Enable Load Monitoring**: Check the box to enable monitoring of the system load. The default is Disabled. When enabled, enter the following parameters: 1 - Minute Max. Load 5 - Minute Max. Load 15 - Minute Max. Load **Swap Space Threshold (in KB)**: Monitors the amount of swap space available on the local system. Default threshold is 16 MB even if not configured. For more details, refer to the System Load Monitoring section.
Log File Monitoring (fileTable)	Click the Add button to display the SNMPD General Settings screen, enter the required parameters, then click the Save button when done. You can then edit or delete existing entries or add more new entries. **Note**: A maximum of 20 files can be monitored. **File Path**: Enter the desired file path for log file monitoring. **Maximum Size (In KB)**: Enter the max file size in Kb. For more details, refer to the Log File Monitoring section.

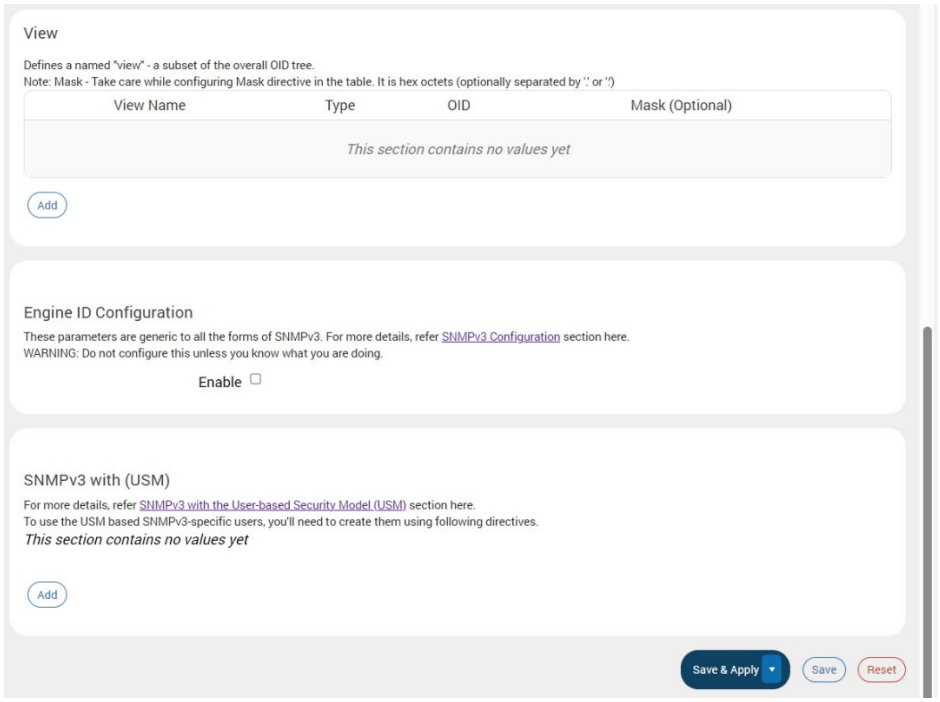
VACM Settings

This page provides the VACM Settings for SNMPD v1/v2c/usm configuration.

The VACM (View-based Access Control) SNMPv3 mechanism that regulates access to MIB objects by providing a fine-grained access control mechanism associating users with MIB views, ensuring a completely secure agent.

For more details, refer to the VACM Configuration and Active Monitoring section.





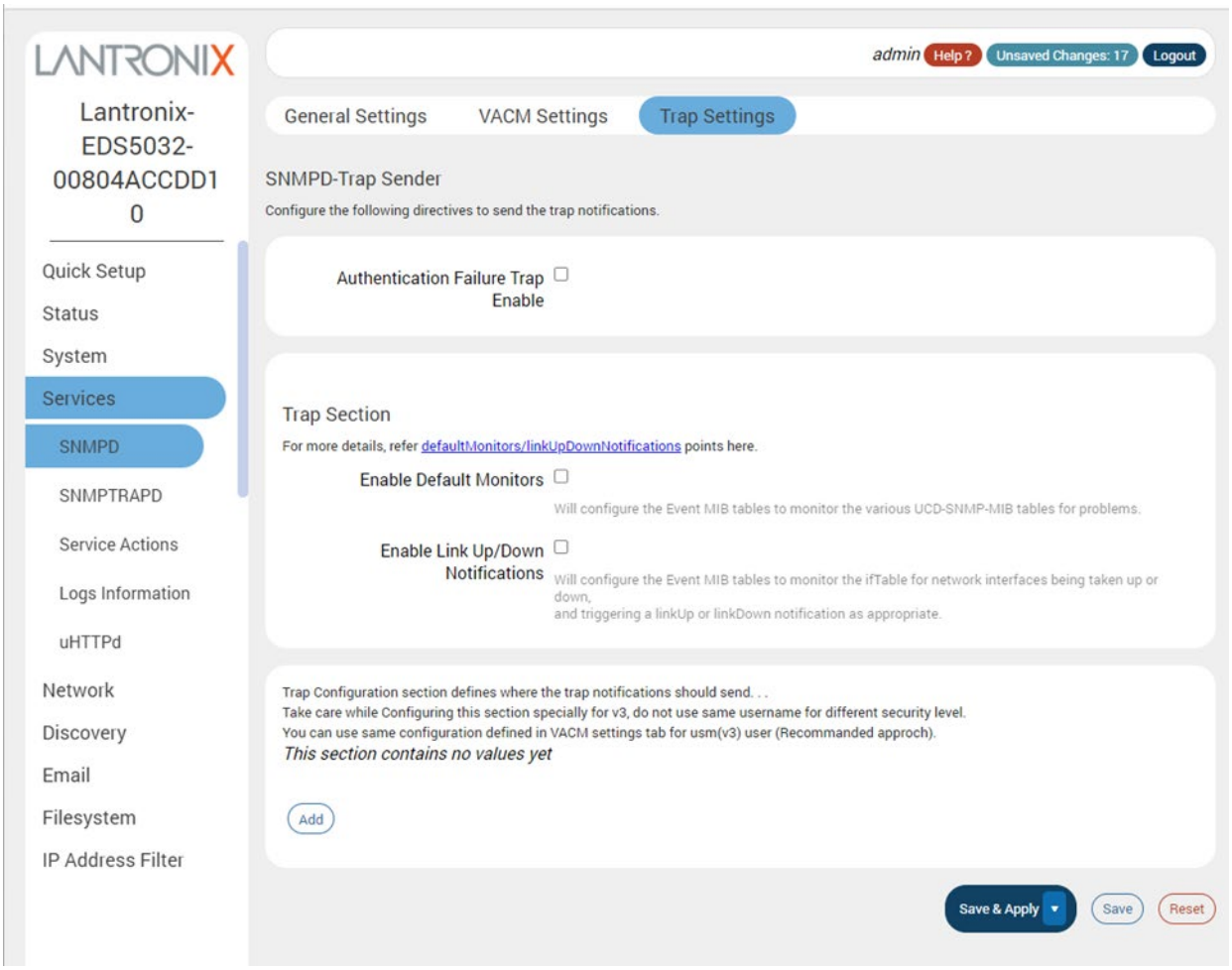
VACM Settings

Setting	Description
Com2Sec Configuration	Click the Add button to display the “SNMPD Com2Sec” parameters screen: **Security Name**: an arbitrary word that is used by the group label. **Source**: Enter a host or network (*unspecified*, *default*, *localhost*, or *custom*). **Community**: Enter the community name to be used. Click the Save button. You can then edit or delete existing entries or add more new entries.
Com2Sec6 Configuration	Click the Add button to display the “SNMPD Com2Sec6” parameters screen: **Security Name**: an arbitrary word that is used by the group label. **Source**: Enter a host or network (unspecified, default, localhost, or custom). **Community**: Enter the community name to be used. Click the Save button. You can then edit or delete existing entries or add more new entries.
Group Configuration	Click the Add button to display the “SNMPD Group Configuration” parameters screen: **Group Name**: Enter an SNMP Group Name. **Version**: At the dropdown select *v1*, *v2c*, or *usm* as the SNMP version to be used. **Security Name**: Enter the SNMP Security Name to be used. Click the Save button. You can then edit or delete existing entries or add more new entries.
Access Configuration	Click the Add button to display the “SNMPD Access Configuration” parameters screen: **Group Name**: Enter the SNMP Group Name to be used. **Context**: At the dropdown select none. **Version**: At the dropdown select *any*, *v1*, *v2c*, or *usm* as the SNMP version to be used. **Level**: At the dropdown select *noauth* (no authentication), *auth* (authentication), or *priv* (privacy) as the access level to be used. **Match**: At the dropdown select *exact* or *match* as the marching criteria to be used. **Read**: At the dropdown select *unspecified*, *none* or *custom* as the Read access method. **Write**: At the dropdown select *unspecified*, *none* or *custom* as the Write access method. **Notify**: At the dropdown select *unspecified*, *none* or *custom* as the Notify access method. Click the Save button when done. You can then edit or delete existing entries or add more new entries.
View Configuration	Defines a named "view" - a subset of the overall OID tree. Click the Add button to display the “SNMPD View Configuration” parameters screen: **View Name**: Enter the SNMP View Name to be used. **Type**: At the dropdown select *included* or *excluded* as the View Type to be used. **OID**: At the dropdown select *.1* or *custom* as the "Object Identifier" (an address used to uniquely identify managed devices and their statuses). **Mask (Optional)**: A mask may be used to modify a View inclusion, designating certain octets of an OID string as wild-card (don't care) values. **Note**: Mask - Take care while configuring Mask directive in the table. It is hex octets (optionally separated by '.' or ':'). Click the Save button when done. You can then edit or delete existing entries or add more new entries.

Setting	Description
Engine ID Configuration	These parameters are generic to all the forms of SNMPv3. For more details, refer to the SNMPv3 Configuration section. **WARNING**: Do not configure this unless you know what you are doing. **Enable**: Check the box to enable SNMP Engine ID globally and to display more parameters to configure. The default is Disabled. * **engineID**: Specify the engineID to be built from the given text STRING (default = *Lantronix*). * **engineIDType**: At the dropdown select either *1 - IPv4 Address*, or *2 - IPv6 Address*, or *3 - MAC Address* (default). * **engineIDNic**: Only applied if engineIDType 3 is specified. Defines which interface to use when determining the MAC address. The default is *eth0*.
SNMPv3 with (USM)	For more details, refer to the SNMPv3 with the User-based Security Model (USM) section. Click the Add button. To use the USM based SNMPv3-specific users, you'll need to create them using following directives: * **User Name**: Username should be same as security name, defined in group directives of the vacm table if version is defined as usm. **Security Level**: At the dropdown select NoAuth,NoPriv, or AuthNoPriv, or Auth,Priv. Map same level defined in access configuration of vacm table for respective user. (*noAuthNoPriv*, *authNoPriv* and *authPriv* are same as *noauth*, *auth* and *priv* respectively.) The default is *NoAuthNoPriv*. **Auth Protocol**: At the dropdown select *MD5* or *SHA* as the Authentication protocol to be used. The default is *MD5*. * **Auth Password**: Enter an authentication password. The minimum pass phrase length is 8 characters. **Priv Protocol**: At the dropdown select DES or AES as the Privacy protocol to be used. * **Priv Password**: Enter a Privacy password. The minimum pass phrase length is 8 characters.

Trap Settings

Navigate to Services > SNMPD and select the Trap Settings tab. Here you can set and view SNMPD-Trap Sender directives to send trap notifications.



Configure the following directives to send trap notifications.

Setting	Description
Authentication Failure Trap Enable	Check the box to Enable sending authentication failure traps. The default is Disabled.
Trap Section	**Enable Default Monitors**: Check the box to configure the Event MIB tables to monitor the various UCD-SNMP-MIB tables for problems. **Enable Link Up/Down Notifications**: Check the box to configure the Event MIB tables to monitor the ifTable for network interfaces being taken up or down, and to trigger a linkUp or linkDown notification as appropriate. Click the Add button to display additional configurable parameters:

Setting	Description
Trap Configuration Section	The Trap Configuration section defines where the trap notifications should be sent. Take care while configuring this section specially for v3, do not use same username for different security levels. You can use the same configuration defined in the VACM settings tab for a usm (v3) user (recommended approach). For more details, refer to the defaultMonitors/linkUpDownNotifications section for more information. **Add**: Click the Add button to add a Trap instance. **Version**: At the dropdown select *v1*, *v2c*, or *usm* as the SNMP version to be used. The default is *v1*. **Community**: Enter the SNMP trap Community Name to be used. *** Host**: At the dropdown specify where to send the trap (e.g., *localhost: 162*). **Type**: At the dropdown select *trap* or *inform*. Refer to the TRAPs vs INFORMs for SNMPv3 section for more information. The default is *trap*. *** User Name**: Enter a User Name for SNMP v3 operation. **Security Level**: At the dropdown select the level of security to use (*NoAuth,NoPriv*, or *AuthNoPriv*, or *AuthPriv*). ♦ NoAuth,NoPriv – no authentication or privacy protocol (default) ♦ Auth,NoPriv – has authentication (MD5|SHA), no privacy protocol ♦ Auth,Priv – has authentication (MD5|SHA), and has privacy protocol (DES|AES). **Auth Protocol**: At the dropdown select *MD5* or *SHA* as the Authentication protocol to be used. The default is *MD5*. *** Auth Password**: Enter an authentication password. The minimum pass phrase length is 8 characters. **Priv Protocol**: At the dropdown select *DES* or *AES* as the Privacy protocol to be used. *** Priv Password**: Enter a Privacy password. The passphrase must be at least 8 characters.

Click the **Save** button when done. You can then edit or delete existing entries or add more new entries.

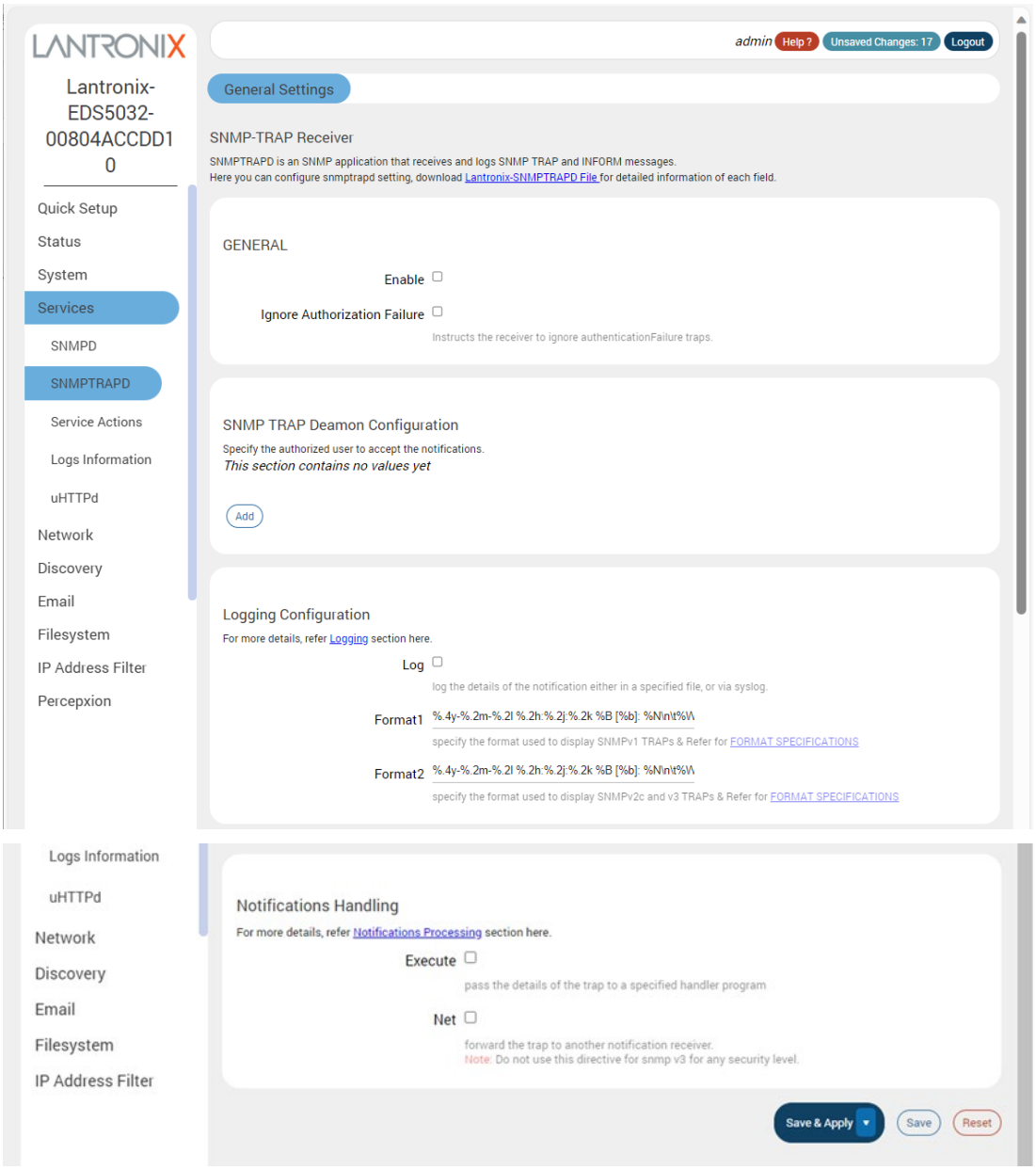
SNMPTRAPD

This page lets you set SNMP-TRAP Receiver parameters. SNMPTRAPD is an SNMP application that receives and logs SNMP TRAP and INFORM messages.

The SNMP-TRAP application listens for incoming SNMP notifications. When it receives a notification, it can log the notification, pass the details to a handler program, or forward the trap to another notification receiver.

General Settings

Here you can configure snmptrapd settings and download the Lantronix-SNMPTRAPD File for detailed information of each field.



Services > SNMPTRAPD > General Settings

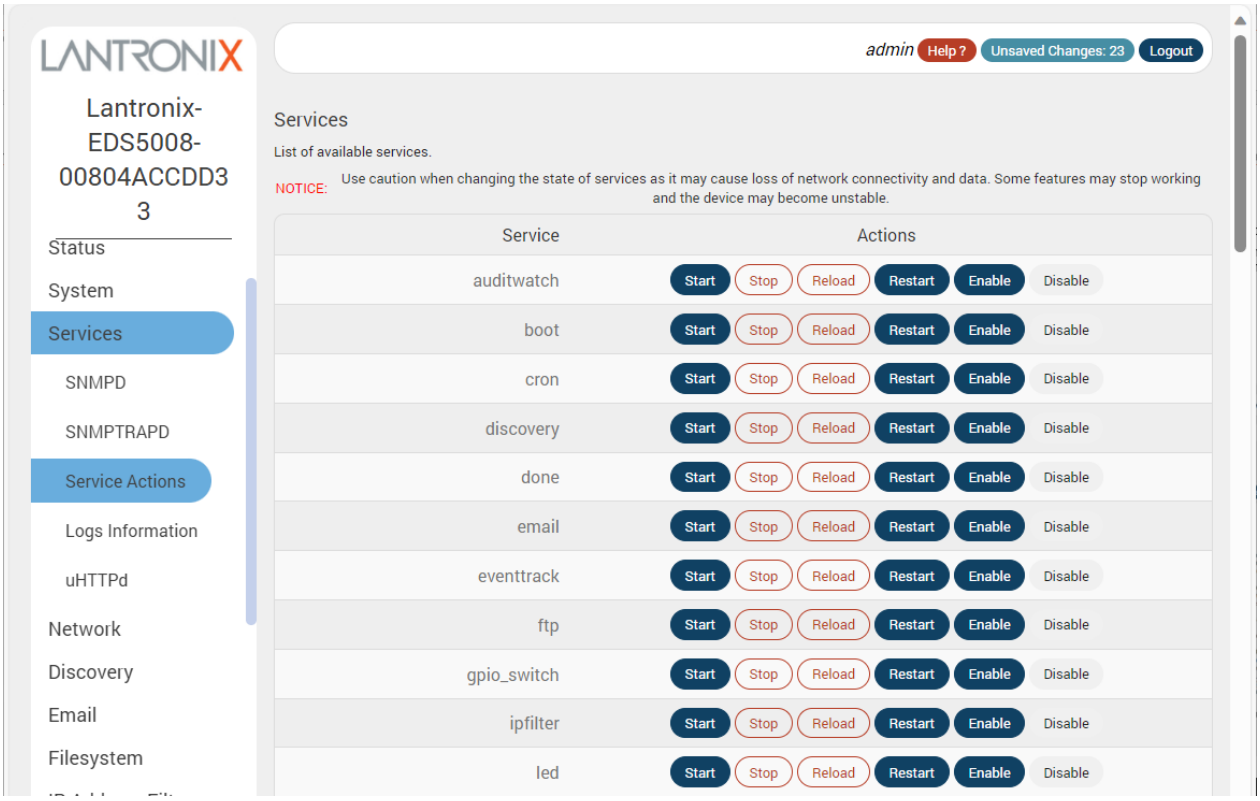
Services > SNMPTRAPD > General Settings

Setting	Description
GENERAL	**Enable**: Check the box to enable the SNMP-TRAP Receiver globally. **Ignore Authorization Failure**: Tells the receiver to ignore authenticationFailure traps.
SNMP TRAP Deamon Configuration	Specify the authorized user to accept the notifications. Click the Add button to display the configurable parameters: **Version**: At the dropdown select *v1*, or *v2c* or *v3*. *** Community**: Enter a name for the SNMPd trap daemon. **Source**: Specify notifications received from particular sources. At the dropdown select *localhost*. **OID**: At the dropdown select *unspecified* or *.1*. *** User Name**: Enter a user name for SNMP v3 operation. **Type**: At the dropdown select *trap* or *inform*. Refer to the TRAPs vs INFORMs for SNMPv3 section for more information. *** EngineID**: Enter the Engine ID. **Security Level**: At the dropdown select *NoAuth,NoPriv* or *Auth,NoPriv* or *Auth, Priv*. **Auth Protocol**: At the dropdown select *MD5* or *SHA* as the Authentication protocol to be used. The default is *MD5*. *** Auth Password**: Enter an authentication password. The minimum pass phrase length is 8 characters. **Priv Protocol**: At the dropdown select *DES* or *AES* as the Privacy protocol to be used. *** Priv Password**: Enter a Privacy password. The minimum pass phrase length is 8 characters.
Logging Configuration	**Log**: Check the box to log the details of the notification either in a specified file, or via syslog. For more details, refer to the Logging section. **Format1**: specify the format used to display SNMPv1 Traps. Refer to the FORMAT SPECIFICATIONS for more information. **Format2**: specify the format used to display SNMPv2c and v3 Traps. Refer to the FORMAT SPECIFICATIONS for more information. **Logging Location**: At the dropdown select *syslog* or *Specific File*. *** File Path**: Enter the File location with a file name.
Notifications Handling	For more details, refer to the Notifications Processing section. **Execute**: Check the box to pass the details of the trap to a specified handler program. *** OID**: At the dropdown select unspecified or default as the specified program (with the given arguments) to use when a notification is received that matches the OID token. *** Program Name**: Program name with path specified followed by space separated arguments if any. For example: */usr/bin/xyz 1 2 3*. **Net**: Check the box to forward the trap to another notification receiver. **Note**: Do not use this directive for SNMP v3 for any security level. *** OID**: At the dropdown select unspecified or default as the specified program (with the given arguments) to use when a notification is received that matches the OID token. *** Destination**: forwards notifications that match the specified OID to another receiver listening on Destination.

Service Actions

This page displays a list of the available services and allows you to manage the system resources. You can start, stop, reload, or restart the service; and enable or disable automatic startup of the service when the device is rebooted.

Note: Use caution when changing the state of services as it may cause loss of network connectivity and data. Some features may stop working and the device may become unstable.



Setting	Description
Service	List all of the available services (e.g., boot, cron, discovery, done, etc.).
Actions	**Start**: Click to begin the service for the row. **Stop**: Click to stop the service for the row. **Reload**: Click to reload the service for the row. **Restart**: Click to restart the service for the row. **Enable**: Click to enable the service for the row. **Disable**: Click to disable the service for the row.

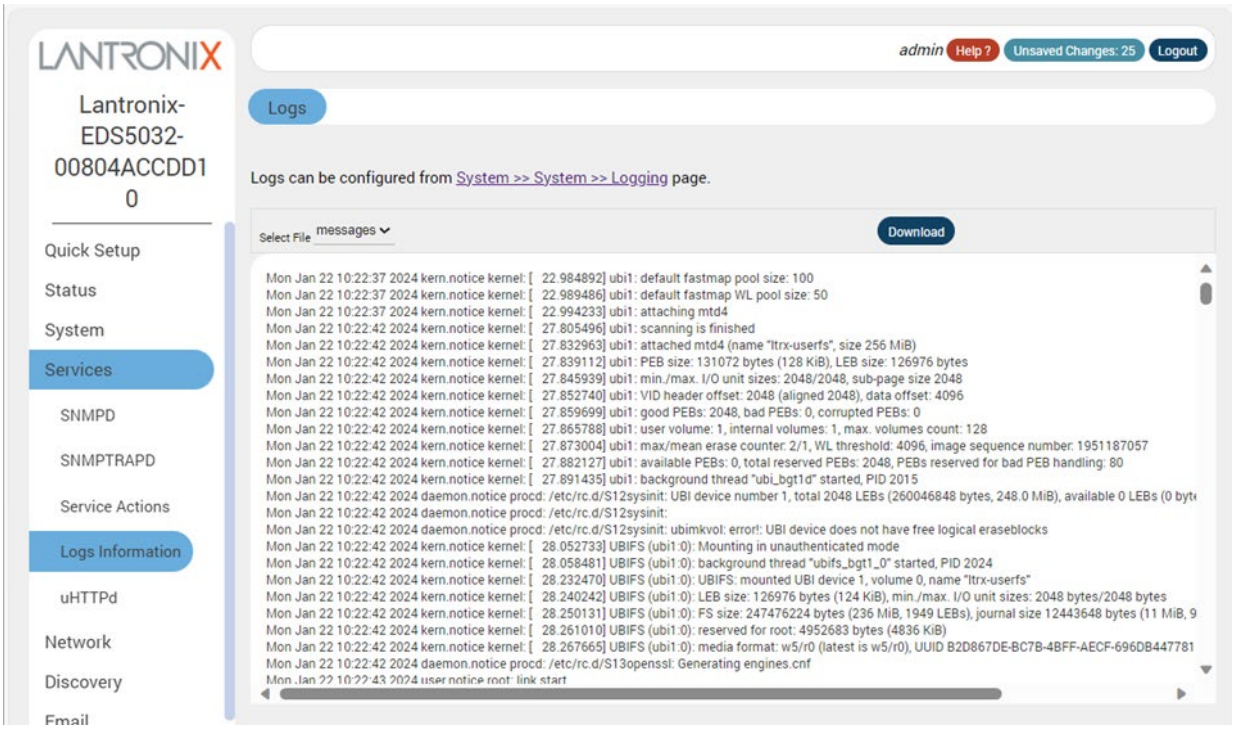
Logs Information

The Logs Information page lets you view the system log file and download them to the local computer.

The current log file and up to 3 historical log files may be saved. The logs configuration is read from the system logging. In order to display and download the log file, the system logging must be configured to write system log to file (see Services > Logging).

To display or download logs:

1. Go to Services > Logs Information. The Logs page appears.
2. At the Select File dropdown select the desired log file. The file is displayed on the page.
3. Click Download. The log file is downloaded to the local computer.



Setting	Description
Select File	At the dropdown select messages.
Download	Click the button to download the displayed message information to your download location in the selected format (e.g., Word, Notepad, etc.).

uHTTPd

This page lets you configure uHTTPd, a lightweight single-threaded HTTP(S) server.

uHTTPd is the web server that runs the web interface. It supports multiple instances such as multiple listening ports each with its own document root directory, TLS (SSL), and other web server features.

uHTTPd requires an X.509 certificate and private key. This has been configured for the Main instance. You only need to configure this section if you choose to upload a new certificate and private key.

This section has three tabs: General Settings, Full Web Server Settings, and Advanced Settings.

Web Server Configuration

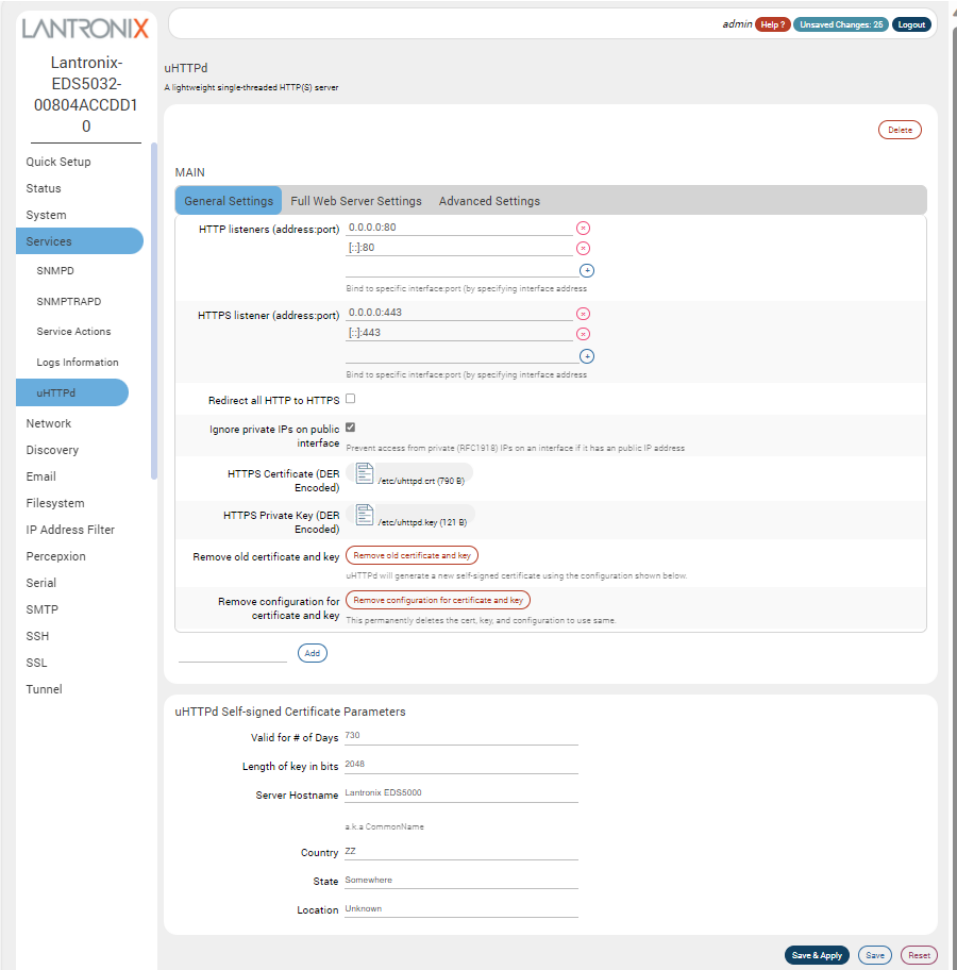
The web server configuration has two sections, one for server settings and the other for default values for SSL certificates. The uHTTPd Main instance is provided by default and is used for configuring the EDS5000.

To configure the HTTP/S server:

1. Go to Services > uHTTPd.
2. Edit the configuration settings for the EDS5000.
3. If you upload a new X.509 certificate and private key in the General Settings tab, you must configure the uHTTPd Self-signed Certificate Parameters section as described below.
4. Click Save & Apply.

Note: If you want to create a new server instance, go to the bottom of the Main instance (on the General Settings tab), enter a name and click Add. For configuration details, see below.

General Settings



Services > uHTTPd > General Settings

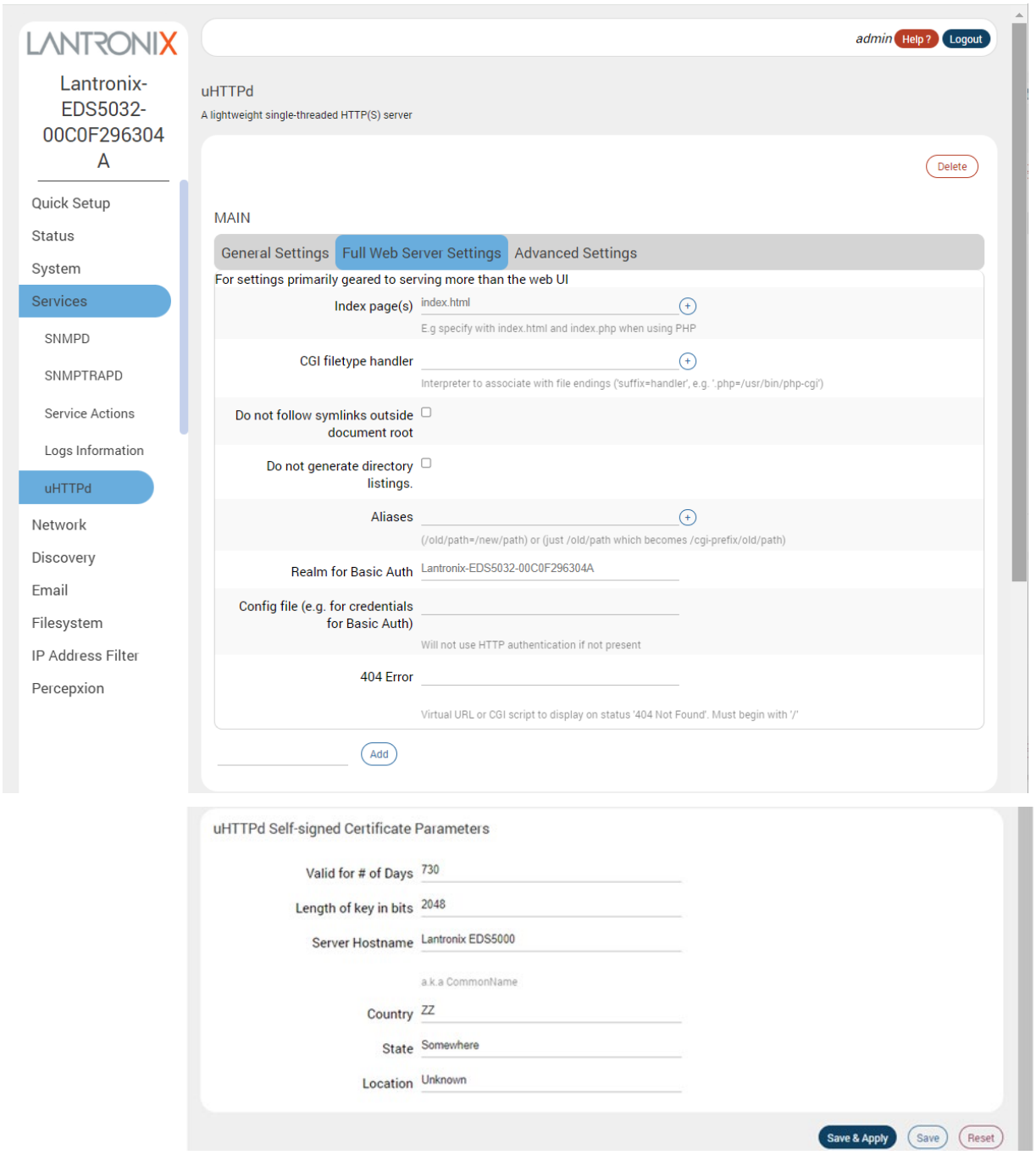
Setting	Description
HTTP listeners (address:port)	Bind to a specific interface:port by specifying an interface address. For example: *0.0.0.0:80* and *[::]:80*. Click the ⊗ icon to delete an existing entry. Click the ⊕ icon to add an entry.
HTTPS listener (address:port)	Bind to a specific interface:port by specifying an interface address. For example: *0.0.0.0:443* and *[::]:443*. Click the ⊗ icon to delete an existing entry. Click the ⊕ icon to add an entry.
Redirect all HTTP to HTTPS	Check the box to Redirect all HTTP to HTTPS.
Ignore private IPs on public interface	Check the box to Prevent access from private (RFC1918) IPs on an interface if it has a public IP address.

Setting	Description
HTTPS Certificate (DER Encoded)	Displays the existing HTTPS Certificate files. **Delete**: Click to delete an entry. **Upload File**: Click to upload the file. **Cancel**: Click to cancel the operation. DER (Distinguished Encoding Rules) is a restricted variant of BER for producing unequivocal transfer syntax for data structures described by ASN.1.
HTTPS Private Key (DER Encoded)	Displays the HTTPS Private Key files. **Delete**: Click to delete an entry. **Upload File**: Click to upload the file. **Cancel**: Click to cancel the operation. DER (Distinguished Encoding Rules) is a restricted variant of BER for producing unequivocal transfer syntax for ASN.1 data structures.
Remove old certificate and key	Click to remove the old cert and key. uHTTPd will generate a new self-signed certificate using the configuration shown below.
Remove configuration for certificate and key	Click to remove the configuration for the certificate and key. This permanently deletes the cert, key, and configuration to use same.
Add	Click the Add button to add a uHTTPd Self-signed Certificate and configure it: **Valid for # of Days**: enter the length of time the cert shall be valid (e.g., 730 days). **Length of key in bits**: enter the cert key length in bits (e.g., 2048 bits). **Server Hostname**: enter a name for the server (a.k.a. CommonName). **Country**: enter the country. **State**: enter the state. **Location**: enter the location (e.g., an address). Click the Save & Apply button when done.
uHTTPd Self-signed Certificate Parameters	**Valid for # of Days**: The default is 730 days. **Length of key in bits**: The default is 2048 bits. **Server Hostname**: The name of the host server (a.k.a. CommonName). The default is Lantronix EDS5000. **Country**: The country location (e.g., ZZ). **State**: The state location (e.g., MN). **Location**: A more exact location (e.g., Irvine or Unknown).

Full Web Server Settings

uHTTPd is the web server that runs the web interface. It supports multiple instances such as multiple listening ports each with its own document root directory, TLS (SSL), and other web server features.

Services > uHTTPd > Full Web Server Settings:

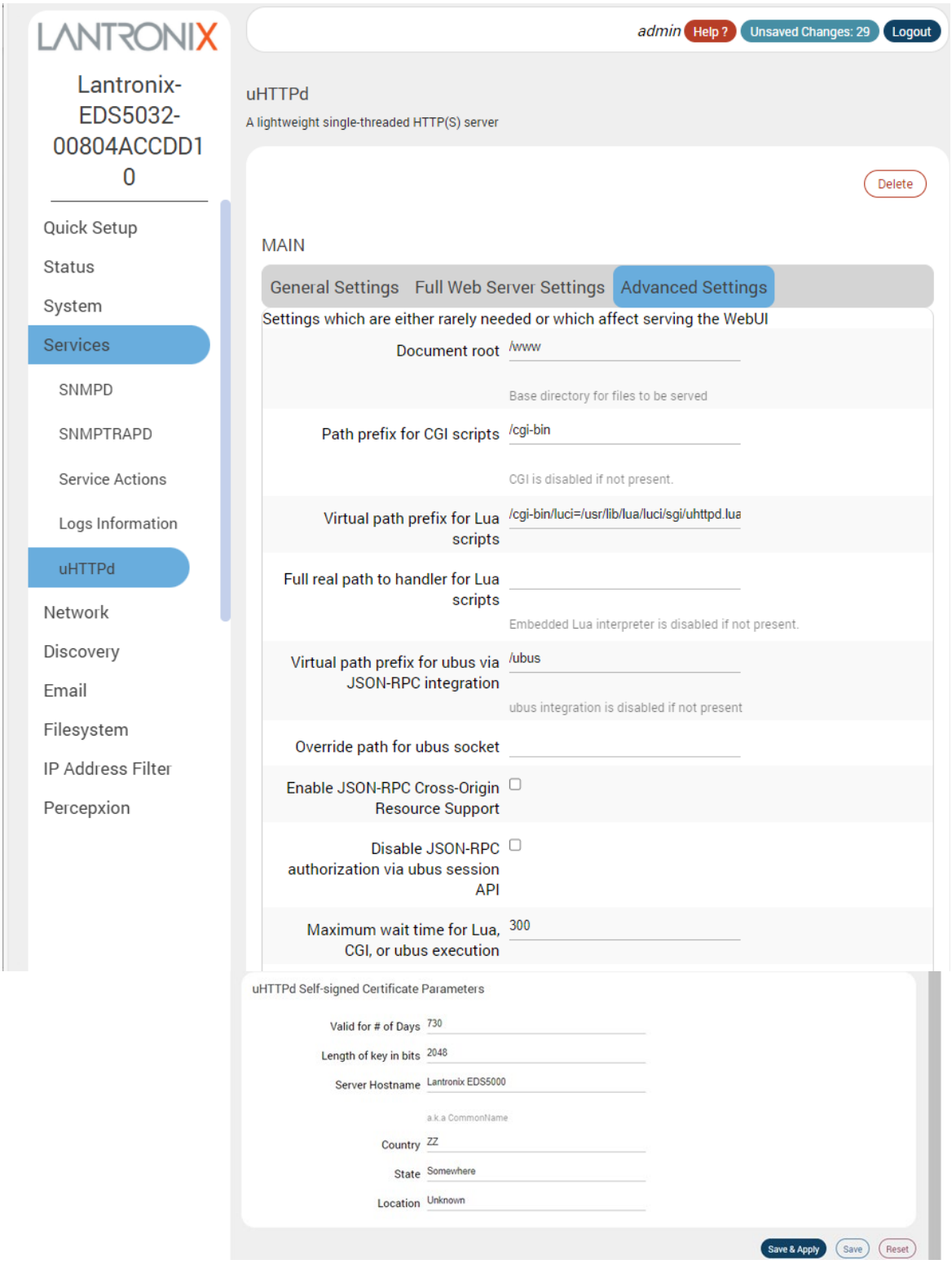


Services > uHTTPd > Full Web Server Settings:

Setting	Description
For settings primarily geared to serving more than the web UI	**Index page(s)**: Enter the index file to use for directories. Usually index.html or index.php. **CGI filetype handler:** Enter the interpreter to associate with file endings in the cgi scripts directory ('suffix=handler', e.g. '.php=/usr/bin/php-cgi'). **Do not follow symlinks outside document root**: If selected, the HTTP/HTTPS server will not follow symbolic links outside the document root. **Do not generate directory listings**: If selected, the HTTP/HTTPS server will not generate directory listings. **Aliases**: Maps URL to filesystem locations outside the document root. The format should be /old/path=/new/path **Realm for Basic Auth**: Enter the realm for basic authentication when prompting the client for credentials. The default is "Lantronix-EDS50xx-xxxxxxxx", which is the local hostname. **Config file (e.g. for credentials for Basic Auth)**: Enter the path of the configuration file for credentials for basic authentication and additional settings. The server will not use HTTP authentication if this field is blank. **404 Error**: Enter the virtual URL of file or CGI script to handle 404 (file not found) request. It must begin with a forward slash '/'.
uHTTPd Self-signed Certificate Parameters	**Valid for # of Days**: Enter the validity time (number of days) of the generated certificate. Default: 730 days **Length of key in bits**: Enter the length of the generated RSA key in bits. Default: 2048 **Server hostname**: Enter the server hostname covered by the certificate. Default: Lantronix EDS5000. **Country**: The Country of the certificate issuer. **State**: The State of the certificate issuer. **Location**: The Location or city of the certificate issuer.

Advanced Settings

This page allows for settings which are either rarely needed or which affect serving the Web UI.



Services > uHTTPd > Advanced Settings:

Setting	Description
Services > uHTTPd > Advanced Settings	**Document root**: Enter the directory path to the server document root. By default the document root is /www. **Path prefix for CGI scripts**: Enter the prefix for CGI scripts, relative to the document root. Leave it blank to disable CGI support. **Virtual path prefix for Lua scripts**: Enter the prefix for sending requests to the embedded Lua interpreter, relative to document root. Leave blank to disable Lua. **Full real path to handler for Lua scripts**: Enter the full path to the Lua handler script to initialize Lua runtime on server start. This field is required if Lua prefix is given, otherwise it's optional. **Virtual path prefix for ubus via JSON-RPC integration**: Enter URL prefix for ubus via JSON-RPC handler, relative to document root. Leave blank to disable UBUS. **Override path for ubus socket**: Enter the override ubus socket path **Enable JSON-RPC Cross-Origin Resource Support**: Select to enable CORS HTTP headers on JSON-RPC API. By default, this setting is disabled. **Disable JSON-RPC authorization via ubus session API**: If selected, do not authenticate JSON-RPC requests against the UBUS session API. By default the requests are authenticated. **Maximum wait time for Lua, CGI, or ubus execution**: Enter the maximum wait time for CGI, Lua or ubus requests in seconds. If no output is generated within the timeout period, the requested executables are terminated. Default is 60 seconds. **Maximum wait time for network activity**: Enter the maximum wait time for network activity. If no network activity occurs within the timeout period, the requested executables are terminated and the connection is shut down. Default is 30 seconds. **Connection reuse**: Sets the time limit for connection reuse. **TCP Keepalive**: Number of unanswered keep alive requests allowed. Default: 1. **Maximum number of connections**: Enter the maximum number of concurrent connections allowed. If the limit is reached, further TCP connection attempts are queued until the number of connections is below the limit. Default: 100. **Maximum number of script requests**: Enter the maximum number of concurrent requests. If the limit is reached, further requests are queued until the number of requests drops below the limit. Default: 6. **Maximum wait time for rpc timeout in seconds per requests**: Enter the maximum wait time for RPC timeout in seconds. Default: 55.
uHTTPd Self-signed Certificate Parameters	**Valid for # of Days**: Enter the validity time (number of days) of the generated certificate. Default: 730 days. **Length of key in bits**: Enter the length of the generated RSA key in bits. Default: 2048. **Server hostname**: Enter the server hostname (aka, CommonName) covered by the certificate. Default: Lantronix. **Country**: The Country of the certificate issuer. **State**: The State of the certificate issuer. **Location**: The Location or city of the certificate issuer.

10. Network

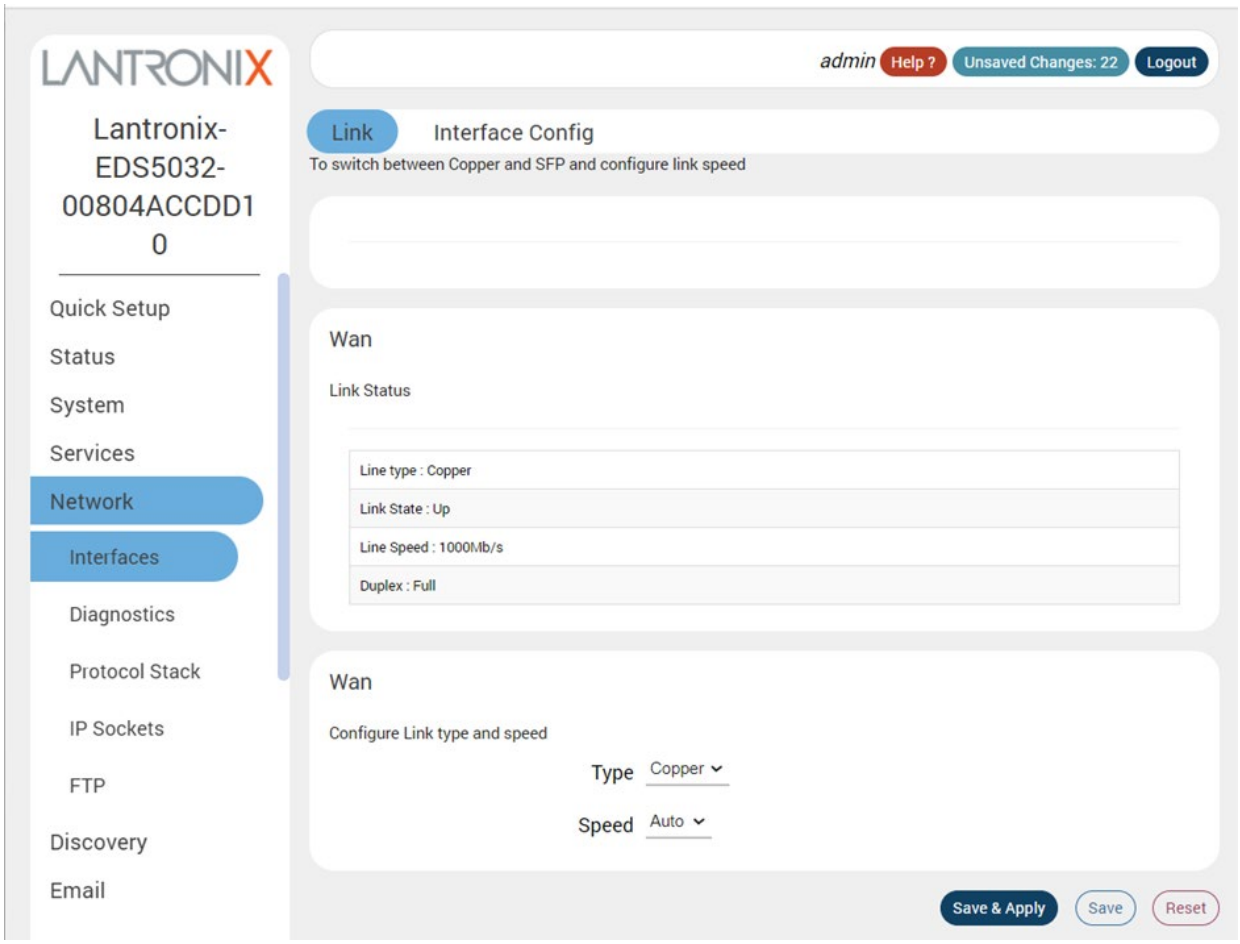
This chapter describes the network configuration settings. It contains the following sections:

- Interfaces
- Diagnostics
- Protocol Stack
- IP Sockets
- FTP

Interfaces

Link

The Link tab shows WAN Link Status, lets you view current WAN Link Status, switch between Copper and SFP operation, and set Link speed.



Network Interfaces Link

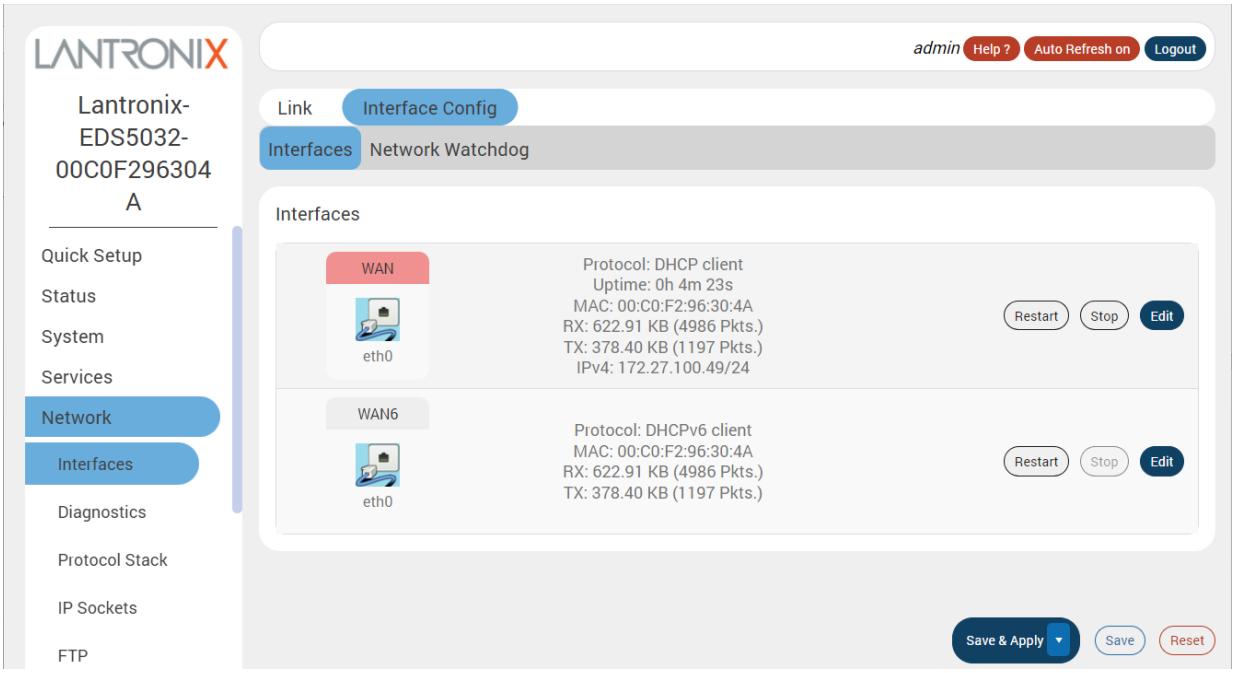
Setting	Description
WAN Link Status	**Line Type**: Displays the current type of link (Copper or SFP). The default is copper. **Link State**: Displays the current link state (Up or Down). **Line Speed**: Displays the current line speed (100 or 1000Mb/s). The default is 1000Mbps. **Duplex**: Displays the current WAN link duplex mode (Full duplex or Half duplex).
WAN Link Type and Speed	**Type**: At the dropdown select the link type (Copper or SFP) to be used. **Speed**: At the dropdown select the desired link speed. ♦ For 'Copper' select Auto, 1000, 100, or 10 Mbps. ♦ For 'SFP' select 1000 or 100 Mbps. **Note**: If wrong SFP is connected or gave an unsupported speed after switching devices, then the device may not reachable. A reset to factory defaults is needed to get the device back to copper mode. **Note**: If 1000 Mb/s is configured but the link only supports 100 Mb/s it will show 100 not 1000 Mb/s.

Network Interface Config

Here you can select the Interfaces tab or the Network Watchdog tab.

Network > Interfaces > Interface Config

This page lets you view and set interfaces parameters.



Parameters	Description
WAN	Displays the current WAN interface (eth0). You can hover the cursor over the icon to display its interface parameters: Type: Ethernet Adapter Ethernet Adapter: "eth0" Device: eth0 Connected: yes MAC: 00:80:4A:CC:DD:10 RX: 11.85 MB (130600 Pkts.) TX: 14.43 MB (15553 Pkts.)
WAN6	Displays the current WAN6 interface (eth0). You can hover the cursor over the icon to display its interface parameters: Protocol: DHCPv6 client MAC: 00:80:4A:CC:DD:10 RX: 5.19 MB (45695 Pkts.) TX: 1.17 MB (2536 Pkts.)
Interface description	Displays a description of the WAN interface (eth0). For example: Protocol: DHCP client Uptime: 0h 60m 45s MAC: 00:80:4A:CC:DD:10 RX: 11.58 MB (127484 Pkts.) TX: 14.39 MB (15392 Pkts.) IPv4: 172.27.100.65/24

Parameters	Description
Restart	Click the button to restart the interface.
Stop	Click the button to stop the interface.
Edit	Click the button to edit the interface parameters.
Protocol	Protocol assigned to the interface.
Uptime	Amount of time that the interface has been active since the last reconnection.
MAC Address	MAC address of the physical interface. **Note**: MAC address is displayed for LAN and WAN interfaces.
RX	Number of received bytes over the interface for the current session.
TX	Number of transmitted bytes over the interface for the current session.
IPv4	IPv4 address.
IPv6	IPv6 address.

Interface Protocols

The protocol assigned to each interface defines rules for exchanging information on the interface. The table below shows the available protocol options for each of the interfaces. When configuring an interface, please make sure that the protocol selection is appropriate for the interface.

Legend: √ = protocol can be assigned. **X** = protocol should not be assigned

Network Interface Protocols

Interface Protocols	WAN
DHCP client	√
DHCPv6 client	√
Static address	√
Unmanaged	√

The interface configuration involves selection or configuration of other settings such as default gateway, gateway metric, DHCP server, and firewall zone to name a few. These settings may or may not be used by the interface; the interface configuration depends on both the protocol selected as well as the network requirements. For descriptions of the protocols used with the LAN and WAN interfaces, see the next section, Protocol Descriptions.

The interfaces can be set to Unmanaged, if no protocol is desired. This setting may be used to enumerate an interface for firewall purposes.

Protocol Descriptions

Static Address

The table below describes the Static Address protocol settings.

Parameters	Description
General Settings	
Protocol	Static Address – Static configuration with fixed address and netmask
Bring up on boot	When enabled (checked) allows the interface to be live after every reboot. Bring up on boot is checked by default.
IPv4 Address	Enter the IPv4 Address. This IP Address must be used to access the gateway. The default LAN IP Address is 198.162.1.1.
IPv4 Netmask	Select the IPv4 Netmask.
IPv4 Gateway	Enter the IPv4 address for gateway.
IPv4 broadcast	Enter the IPv4 address for broadcast.
Use Custom DNS servers	Enter the IP address of the custom DNS server. Click the + button to add more DNS servers.
IPv6 assignment length	Select the IPv6 assignment length. Available options: ♦ 64 or 60 – Assign a part of the given length of public IPv6-prefix to this interface. ♦ disabled – do not assign part of the prefix to this interface. ♦ --custom-- – Assign a part of the given length of public IPv6-prefix to this interface. IPv6 assignment length is disabled by default. If assignment length is disabled, enter the following: ♦ IPv6 address – Enter the IPv6 Address. ♦ IPv6 gateway – Enter the IPv6 Address for Gateway. ♦ IPv6 routed prefix – Enter the public prefix to direct the client distribution to the gateway. If assignment length is 60, 64, or custom, enter the following: ♦ IPv6 assignment hint –Enter hexacimal subprefix ID for this instance to assign prefix parts. ♦ IPv6 suffix – Enter the IPv6 suffix
Advanced Settings	
Use builtin IPv6 - management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.

Setting	Description
Override MAC address	Click to override the default MAC Address for the WAN Interface. On factory reset, it will be set to default MAC address.
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value represents auto MTU Size.
Use gateway metric	Enter the gateway metric. It ensures a separate routing entry for the respective interface in the main routing table. The default metric is 5.
DHCP > General Setup DHCP Server - DHCP Server is used only for LAN interfaces	
Ignore Interface	Check to disable the DHCP interface. ***Note**: If DHCP server is disabled for the interface, all the LAN devices connected to the gateway should have a static LAN IP configured.*
Start	Lowest leased address as offset from the network address. ***Note**: If your LAN IP address is 192.168.1.1 and the parameter Start is configured as 100, then the starting IP Address of the leased IP Address range is 192.168.1.100.*
Limit	Maximum number of leased addresses that can be configured. Example: ♦ If your LAN IP Address is 192.168.1.1, the parameter Start is configured as 100, and parameter Limit is configured as 150, then a total of 150 devices are configured. Thus the leased IP Address range is 192.168.1.100 to 192.168.1.249.
Lease time	Remaining time until the device can use the DHCP server leased IP Address. ***Note**: IP address allocated by the gateway will disappear from the WiFi / Overview / Associated stations list only after individual lease time for each IP expires.*
DHCP > Advanced Settings	
Dynamic DHCP	Check to allocate DHCP IP addresses dynamically to the clients. When unchecked, service will be provided only to the clients having the static IP Address.
Force	Check to override the current configured Server and use DHCP server.
IPv4-Netmask	Enter the IPv4 netmask. This netmask will override the netmask used by the clients. In normal scenario netmask is calculated from the subnet.
DHCP-Options	Define additional DHCP options. Example: ♦ “6,192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients.

Setting	Description
DHCP > IPv6 Settings	
Router Advertisement-Service	Select the Router Advertisement-Service mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Service	Select the DHCPv6-Service mode; disabled, server mode, relay mode, hybrid mode.
NDP-Proxy	Select the NDP mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Mode	Select the DHCPv6-Service mode: ♦ Stateless ♦ Stateful ♦ Stateless + Stateful ♦ Stateful only
Always announce default router	Select to Announce as default router even if no public prefix is available.
Announced DNS servers	Add the DNS servers.
Announced DNS domains	Add the DNS domains

DHCP Client

The table below describes the DHCP Client protocol settings.

DHCP Client Protocol Settings

Parameters	Description
General Settings	
Protocol	Static Address – Static configuration with fixed address and netmask
Bring up on boot	When enabled (checked) allows the interface to be live after every reboot. Bring up on boot is checked by default.
Hostname to send when requesting DHCP	Hostname of the gateway.
Advanced Settings	
Use builtin IPv6 - management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.

Setting	Description
Use broadcast flag	Check to use the broadcast flag. This flag is generally used by the ISPs.
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for WAN interface is checked by default. If unchecked, the advertised DNS server addresses are ignored.
Client ID to send when requesting DHCP	Enter the Client ID that shall be sent when requesting DHCP.
Vendor Class to send when requesting DHCP	To allocate DHCP IP Addresses based on Vendor Class.
Override MAC address	Click to override the default MAC Address for the WAN Interface. On factory reset, it will be set to default MAC address
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value represents auto MTU size

DHCPv6 Client

The table below describes the DHCPv6 Client protocol settings.

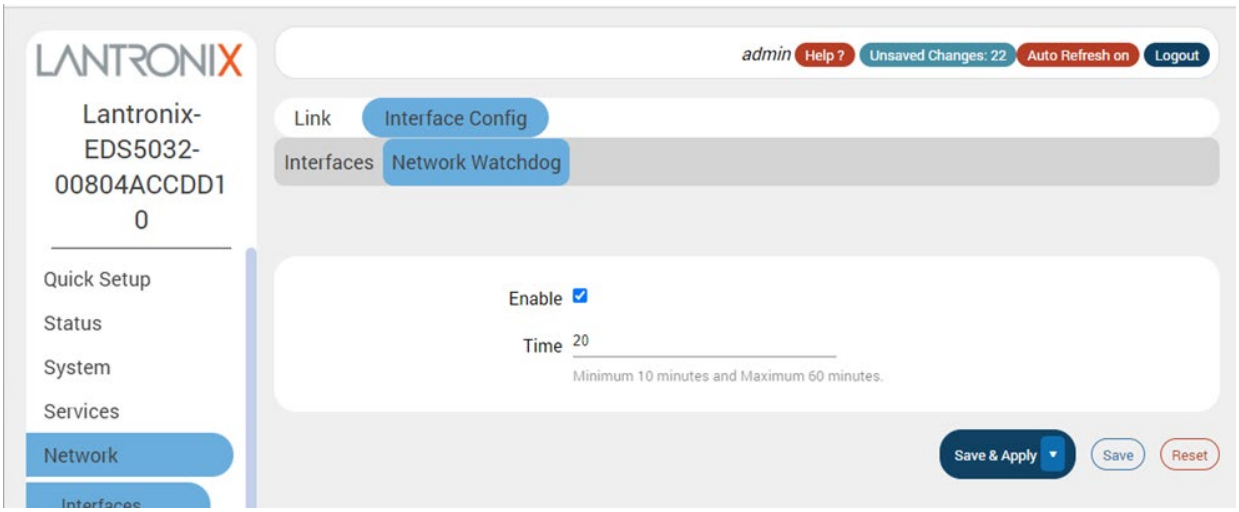
DHCPv6 Client Protocol Settings

Parameters	Description
General Settings	
Protocol	Static Address – Static configuration with fixed address and netmask
Bring up on boot	When enabled (checked) allows the interface to be live after every reboot. Bring up on boot is checked by default.
Request IPv6-address	Enter the behavior for requesting addresses. Options are try (default), force, and disabled.
Request IPv6-prefix of length	Enter the IPv6 address prefix length in bits. Options are: ♦ Unspecified ♦ Automatic (default) ♦ disabled – use if you want single IPv6 address for the AP without a subnet for routing ♦ 48, 52, 56, 60, 64 –hinted prefix length ♦ custom – enter custom prefix length
Advanced Settings	
Use builtin IPv6 - management	Allows to use the built in IPv6 management configuration.

Setting	Description
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Custom delegated IPv6 prefix	Enter the custom IPv6 prefix to be used.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for WAN interface is checked by default. If unchecked, the advertised DNS server addresses are ignored.
Client ID to send when requesting DHCP	Enter the Client ID that shall be sent when requesting DHCP.
Override MAC address	Click to override the default MAC Address for the WAN Interface. On factory reset, it will be set to default MAC address.
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value means auto MTU size.

Network Watchdog

This page lets you enable and configure network watchdog parameters.



Setting	Description
Enable	Select to enable and configure network watchdog parameters.
Time	Select the watchdog time. Minimum 10 minutes and maximum 60 minutes. The default is 20 minutes.
Reset	Click the button to reset the watchdog timer.

Click Save & Apply when done.

Diagnostics

Network Utilities

The diagnostics feature allows you to run network utilities from the web interface. The table describes each of the network utilities..

Setting	Description
Select Tool	At the dropdown select the desired tool to run (Ping, Traceroute, or NSLookup). **Ping**: IP Address or fully qualified domain name to be pinged. Ping determines network connection between EDS5000 and host on the network. The output shows if the response was received, packets transmitted and received, and packet loss if any. At the Network Type dropdown select ipv4 or ipv6. The default is ipv4. **Traceroute**: IP Address or fully qualified domain name. Traceroute displays all the routers present between the destination IP address and the EDS5000. The output shows all the gateways through which data packets pass on way to the destination system from the source system, maximum hops and total time taken by the packet to return measured in milliseconds. At the Network Type dropdown select ipv4 or ipv6. The default is ipv4. At the Protocol dropdown select the desired protocol (TCP, ICMP, or UDP). The default is TCP. **Nslookup**: Enter an IP Address or fully qualified domain name that needs to be resolved. Name lookup is used to query the Domain Name Service for information about domain names and IP addresses. It sends a domain name query packet to a configured domain name system (DNS) server. Enter a valid Host name, a valid IPv4 address, or a valid IPv6 address. If you enter a domain name, you get back the IP address to which it corresponds. If you enter an IP address, you get back the domain name to which it corresponds. A message stating “Unknown Host” indicates that the Internet Name does not exist.
ipv4 / ipv6	At the dropdown select the either ipv4 or ipv6 as the version of the Internet Protocol to run the selected tool. The default is ipv4.
Protocol	For Traceroute, select UDP, TCP, or ICMP as the desired Traceroute protocol.

When done click the Run button to run the selected tool. The output is displayed below the selected utility details that you entered.

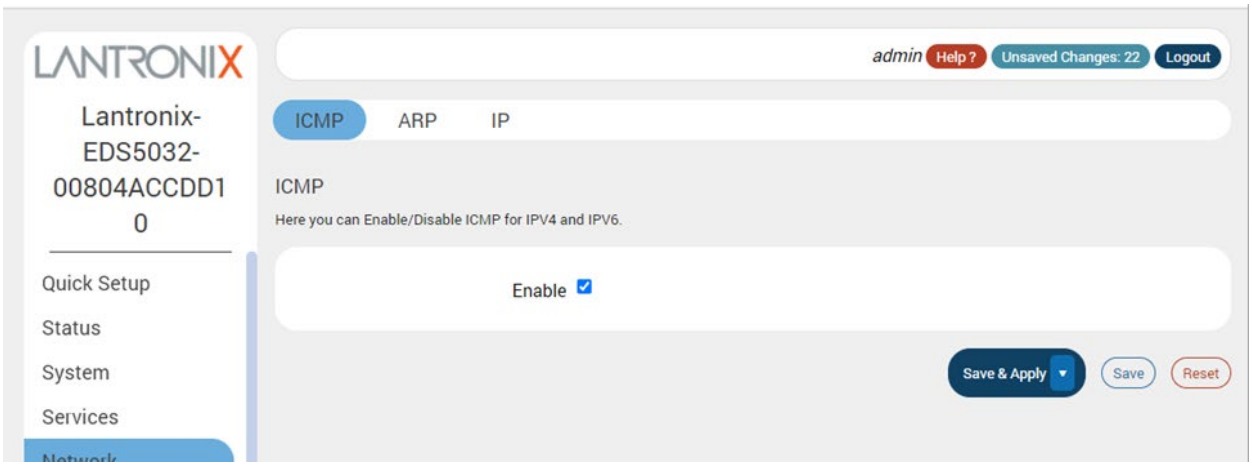
Protocol Stack

This section allows you to configure ICMP, ARP, and IP TTL (Time To Live) settings. These are various low level network stack specific items that are available for configurations described in the sections below.

ICMP

Here you can Enable/Disable ICMP settings for IPV4 and IPV6.

The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices to send error messages and operational information.



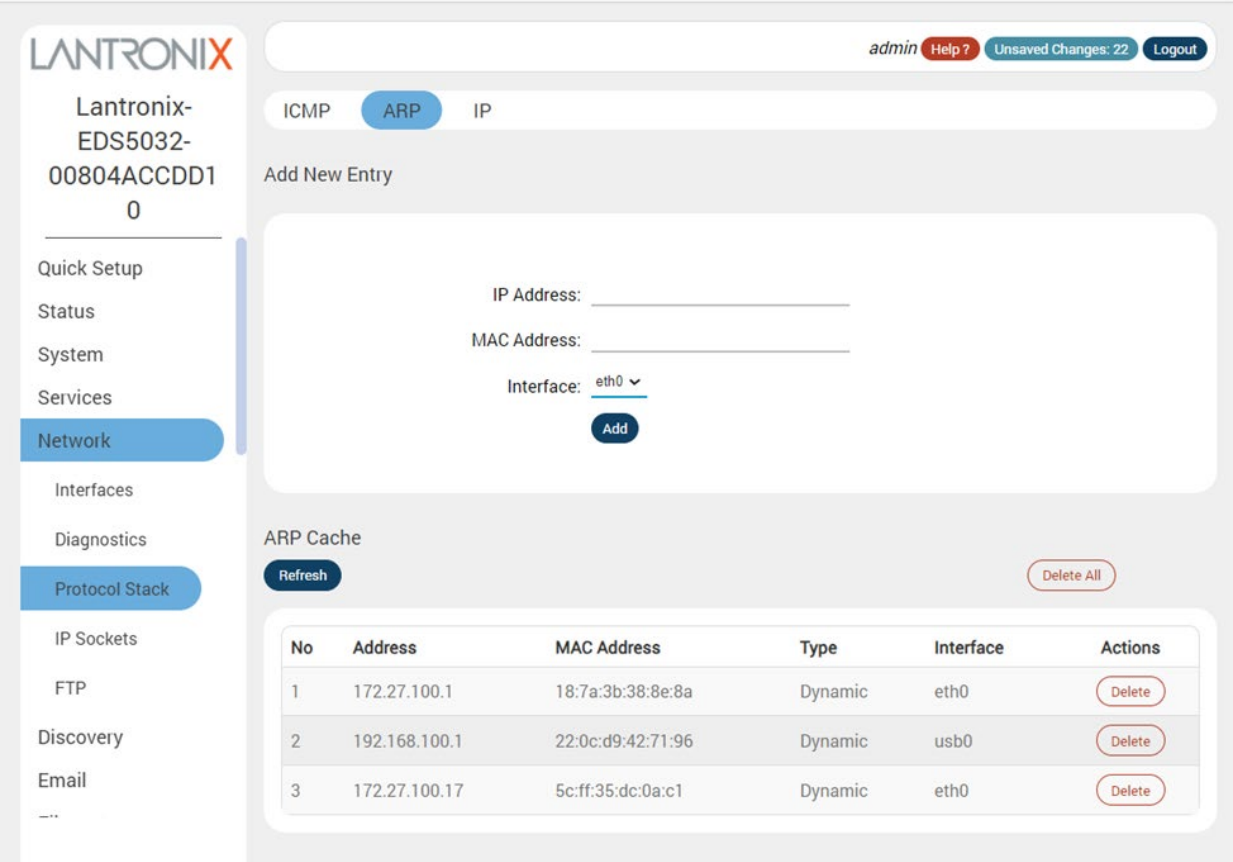
Setting	Description
Enable	Check the box to enable the ICMP protocol.
Reset	Click to reset the page settings.

When done click the Apply & Save button.

ARP

This page lets you create new and view existing ARP entries.

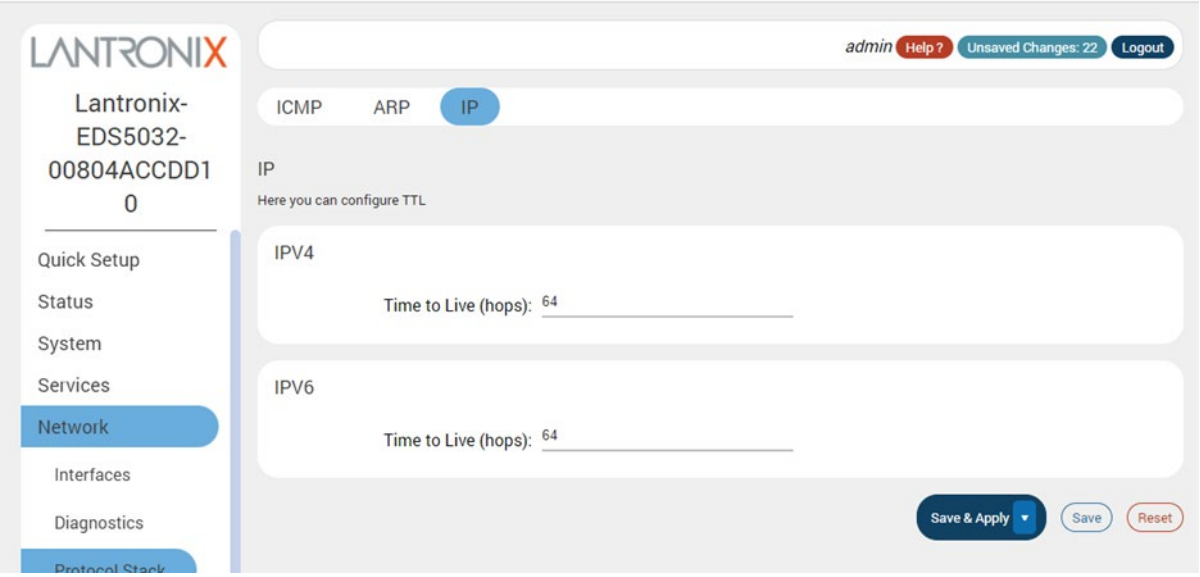
The Address Resolution Protocol (ARP) uses a simple message format containing one address resolution request or response.



Setting	Description
Add New Entry	**IP Address**: Enter an IP address for the new ARP entry. **MAC Address**: Enter an MAC address for the new ARP entry. **Interface**: At the dropdown select the interface (e.g., *eth0*). Click the **Add** button when done.
ARP Cache	**No**: The instance number for the row. **Address**: Displays the IP address for the ARP entry. **MAC Address**: Displays the MAC address for the ARP entry. **Type**: Displays the type of ARP entry (e.g., *Dynamic*). **Interface**: Displays the interface (e.g., *eth0*). **Actions**: Buttons to perform various action on an ARP entry (e.g., *Refresh* the ARP Cache table, *Delete* and entry, *Delete All entries in the table*).

IP

This page lets you set IPv4 and IPv6 TTL (Time To Live). 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.

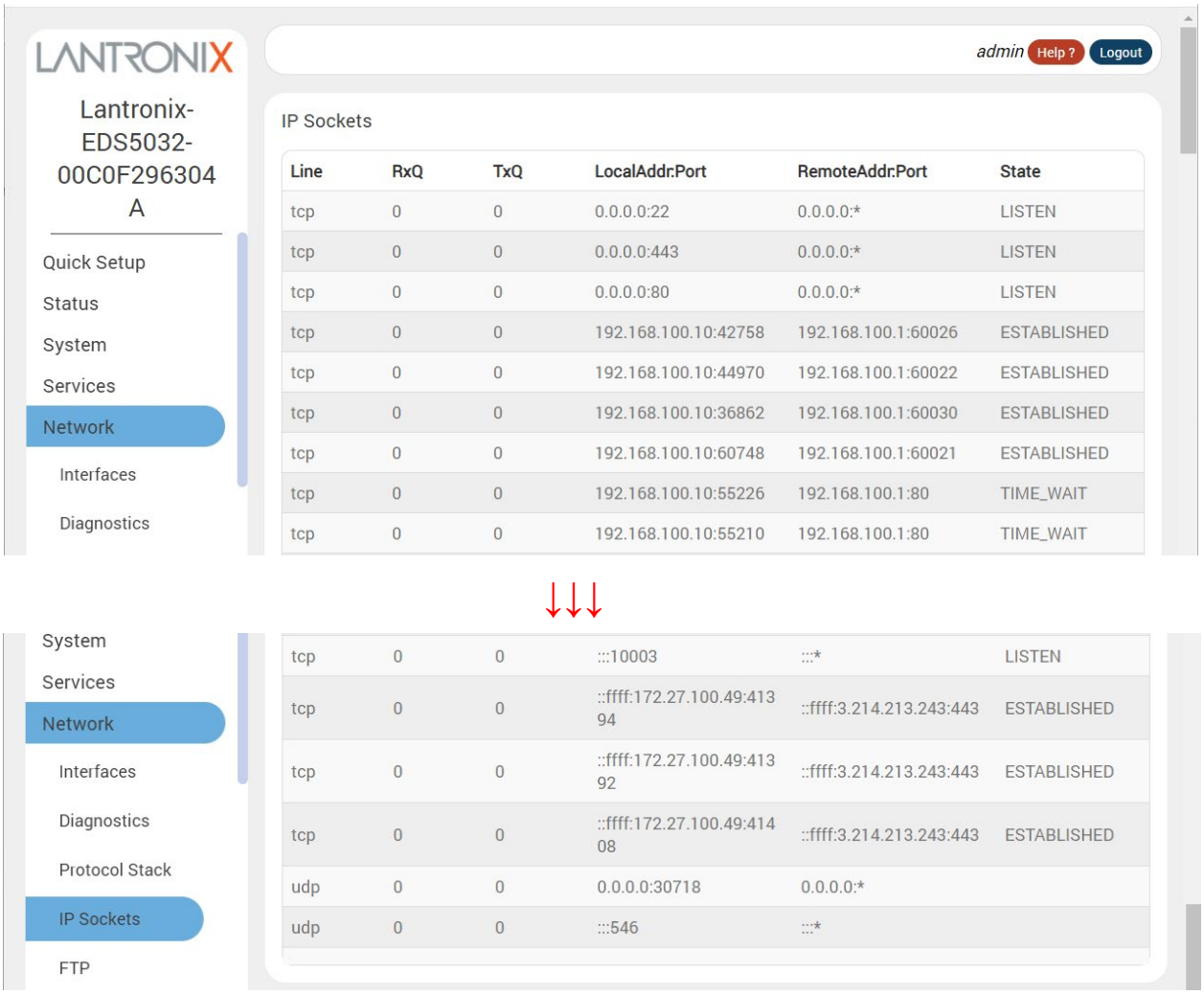


Setting	Description
IPV4 Time to Live (hops)	Enter the desired time to live in hops for IPv4. The valid range is 1-255 hops. The default is 64 hops.
IPV6 Time to Live (hops)	Enter the desired time to live in hops for IPv6. The valid range is 1-255 hops. The default is 64 hops.
Reset	Click to reset the page settings.

Click the Save & Apply button when done.

IP Sockets

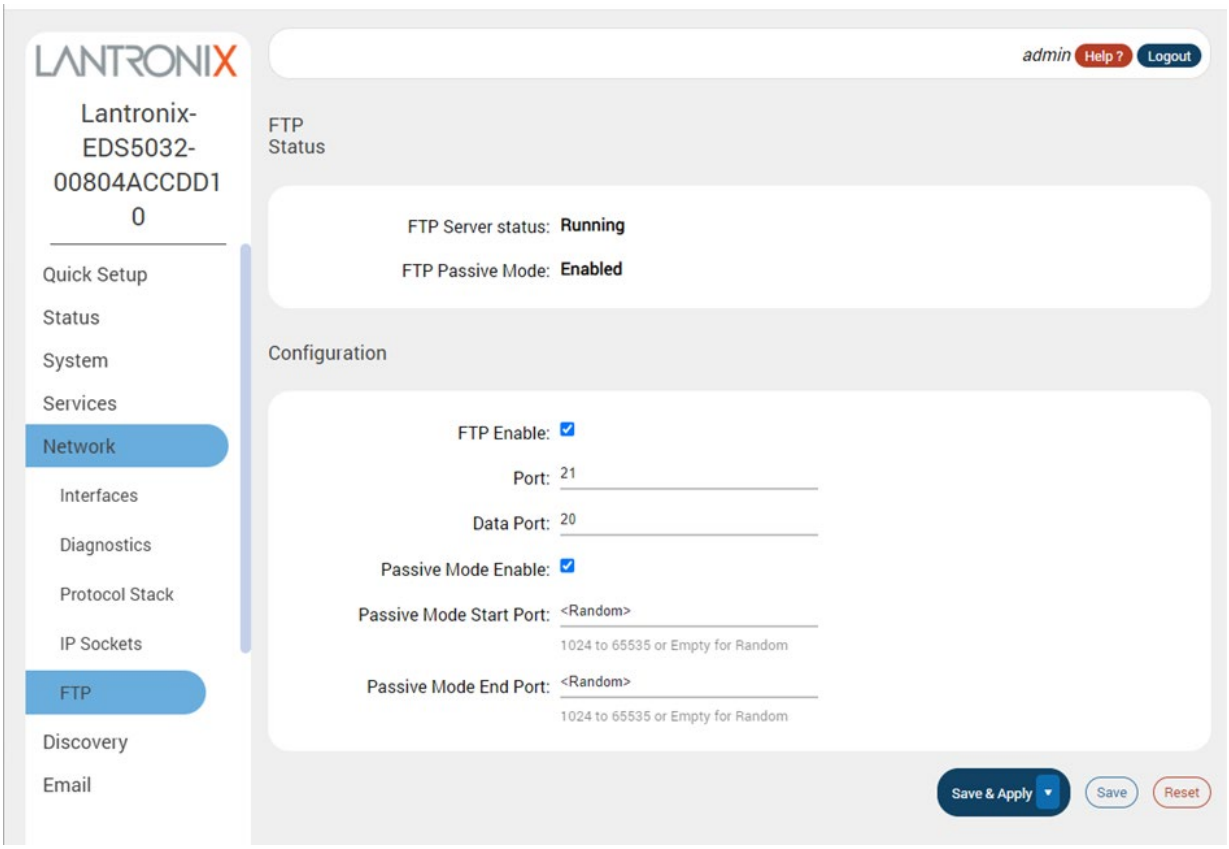
Here you can view the list of listening sockets and connected IP sockets. **Note**: For a TCP socket in LISTEN state the LocalAddr and RemoteAddr will be 0.0.0.0 to indicate that the application is listening on all local interfaces. A UDP socket will not have a state.



Setting	Description
Line	Displays the protocol for the line (e.g., tcp or udp).
RxQ	Displays the receive queue count.
TxQ	Displays the transmit queue count.
LocalAddr:Port	Displays the local IP address and port number.
RemoteAddr:Port	Displays the remote IP address and port number.
State	Displays the current state of the IP socket (e.g., LISTEN, ESTABLISHED, TIME_WAIT, etc.).

FTP

This page lets you view and set File Transfer Protocol parameters.



Setting	Description
FTP Status	**FTP Server status**: Displays the current FTP server status (Running or Disabled). **FTP Passive Mode**: Displays the current FTP server mode (Enabled or Disabled). Note: FTP is disabled by default.
FTP Configuration	**FTP Enable**: Check the box to enable FTP mode. The default is Disabled. **Port**: Enter the desired FTP Port number. The default is port 21. **Data Port**: Enter the desired FTP Data Port number. The default is port 20. **Passive Mode Enable**: Check the box to enable FTP Passive mode. The default is Disabled. With FTP Passive mode enabled, the FTP client initiates both connections to the server. **Passive Mode Start Port**: Enter the starting port number for Passive Mode FTP. The valid range is 1024 to 65535 or Empty for Random. The default is Random port. **Passive Mode End Port**: Enter the ending port number for Passive Mode FTP. The valid range is 1024 to 65535 or Empty for Random. The default is Random port.

11. Discovery

Query Port

The Query port service running on the EDS5000 allows network discovery of devices using Lantronix Provisioning Manager. If enabled, the device responds to auto-discovery messages on port 0x77FE.

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

Setting	Description
Statistics	Displays the current running Query Port statistics: **Query Port Status**: e.g., On (running) or Off (not running) **Valid Queries**: e.g., 347 **Unknown Queries**: e.g., 4 **Erroneous Packets**: e.g., 0 **Query Replies**: e.g., 347 **Errors**: e.g., 0 **Last Connection**: e.g., 172.27.100.80: 50064 or 0.0.0.0: 0.
Configuration	Select to enable or disable the query port server from responding to auto-discovery messages on port 0x77FE. (Port 30718; Lantronix Discovery Protocol for Lantronix serial-to-ethernet devices.) The default is Enabled.

12. Email

The Email main menu provides sub-menus to let you view email statistics and configure and send emails.

Statistics

Here you can view email statistics and show and clear email logs.

Setting	Description
Email-Statistics	**Name**: Shows a name for each email instance (e.g., Email1, Email2, etc.). **Sent Successfully**: The number of emails that were sent successfully. **Retries**: The number of emails that were retried. **Not Sent Due To Excessive Errors**: The number of emails that had too many errors to be able to be sent successfully. **In Transmission Queue**: The number of emails that in the queue yet to be sent. **Clear Log**: Click the button to clear the related email log. **Show Log**: Click the button to display the related email log.
Email Logs	Displays a log of sent emails.

Email > Email

Here you can configure email settings and send emails. View and configure email alerts relating to events occurring within the system.

Setting	Description
Name	Shows a name for each email instance (e.g., *Email1*, *Email2*, etc.).
To	Enter a name for the email recipient.
CC	Enter a name for the email to be copied to.
Reply To	Enter a name for the email recipient to respond to.
Subject	Enter a subject of the email.
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.
Priority	The level of importance of the email: ***Urgent***: The highest priority. ***High***: The second highest priority. ***Normal***: Regular priority (default setting). ***Low***: The second lowest priority. ***Very Low***: The lowest priority.
Send Mail	Click to send the mail instance.

13. Filesystem

Filesystem is the internal filesystem of the EDS5000. It is not part of the /. It will be mounted on /ltrx_user_fs. When any file stored on the filesystem even if we do factory reset the files inside this location won't delete and need to delete using format present in the web manager. This landing point is used for FTP and users that want to save any files inside the device use it.

Statistics

Here you can view available and free filesystem space and perform formatting.

Setting	Description
Total Available	Displays the amount of available filesystem space in Mb and as a percentage.
Free	Displays the amount of free filesystem space in Mb and as a percentage.
Action	Click the **Format** button to reformat the filesystem. At the prompt "*Are you sure do you want to format ?*" click OK. At the "Formatted Successfully" message click OK.

Filesystem

Here you can create, view, and manage Filesystem directories.

1. Click the Create Directory button to create a new filesystem directory.
2. Enter a valid Directory Name and click the Save button.
3. You can now Add new or Delete, Rename, Copy, Cut, or Download existing filesystem directories.

Filesystem Parameters:

Setting	Description
 **or** 	Toggles between current path and Home.
Upload File	Click the button to browse to and select a file to upload.
Create Directory	Click the button to create and save a directory name.
Name	Displays the file name. Click to display its filesystem page.
Size	Displays the size of the file in Mb.
Modified	Displays the date and time the file was created/modified.
Actions 	**Delete**: Click to delete the instance from the table. **Rename**: Click to change the name of the file. **Copy**: Click to copy the file and display a screen to Paste to. **Cut**: Click to cut the file and display a screen to Paste to.. **Download**: Click to download the file in .zip file format.

14. IP Address Filter

This main menu item lets you enable/disable IP Address filters and set Default IP Address Filter Policies.

Statistics

This pagelets you view IP address state and filters.

Setting	Description
Configuration	**IP Address filter State**: Displays the current state (Enabled or Disabled). **Default IP Address Filter Policy**: Displays the current policy setting (ACCEPT or DROP).
IP Address filters	Click the Add button to display a Configuration page (see below). Set the: **IP Address**: Enter a valid IP address. **Action**: At the dropdown select the action to be taken: ACCEPT(default) or DROP. Click Save when done.

Configuration

Here you can enable IP address filtering and set the default IP address filter policy.

Setting	Description
Configuration	**IP Address filter Enable**: Select the desired state (Enabled or Disabled).The default is disabled. **Default IP Address Filter Policy**: At the dropdown select the desired policy setting (Accept or Drop).
IP Address filters	Click the Add button to display a Configuration page (see below). Set the: **IP Address**: Enter a valid IP address. **Action**: At the dropdown select the action to be taken: Accept (default) or Drop. Click Save when done.

When new instances have been added you can then edit and delete the existing entries.

15. Percepxion

The EDS5000 series device servers come integrated with Percepxion platform to allow for the remote management of devices.

Lantronix Percepxion is a cloud or on-premise portal application for secure out-of-band access and centralized management of Lantronix devices.

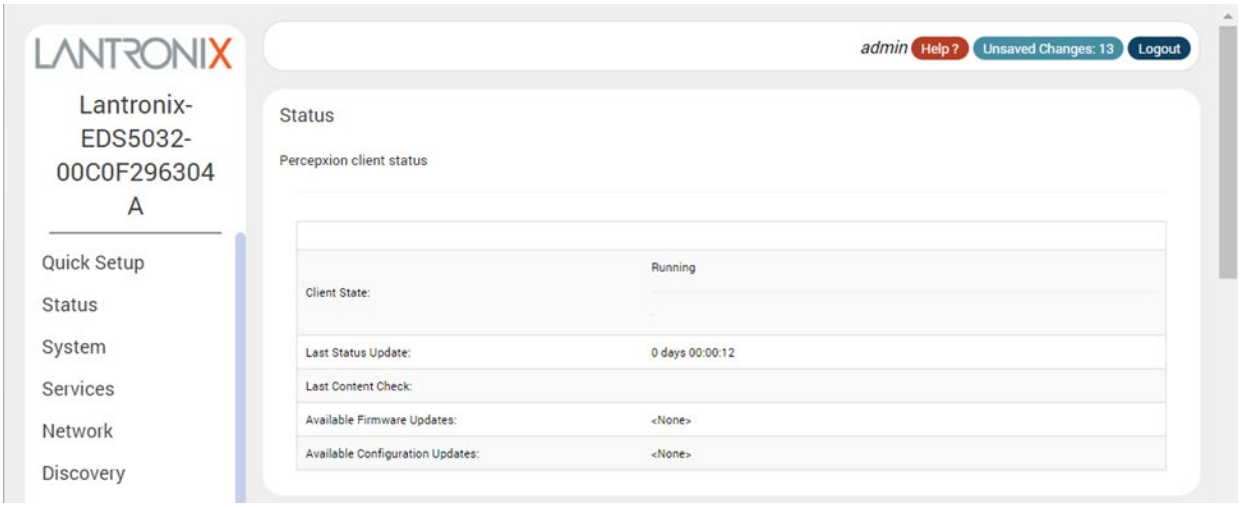
To set up the Percepxion client, you must configure these settings:

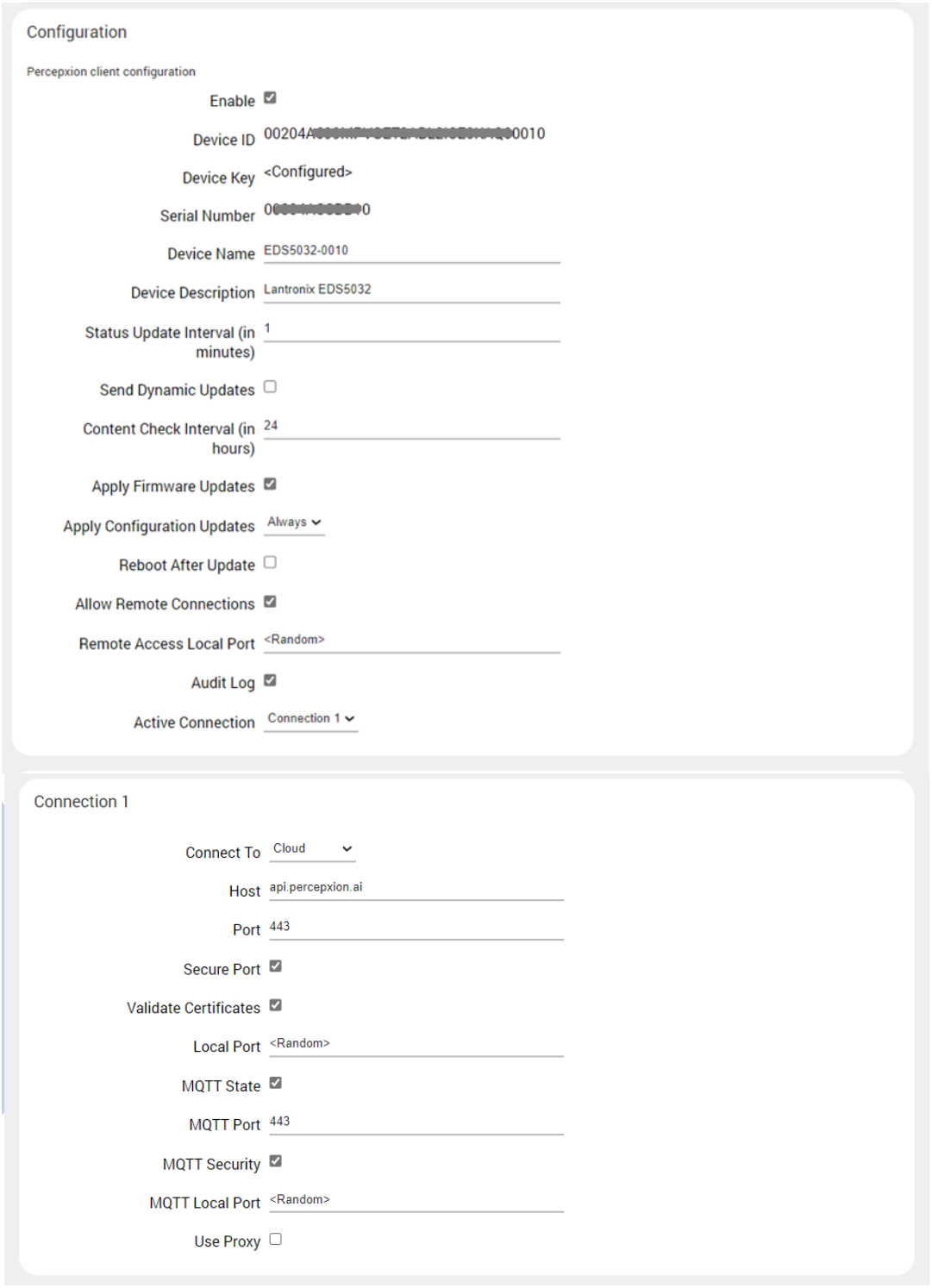
- Percepxion Client – to connect the EDS5000 to the Percepxion platform.
- Line 1 to Line x – to enable remote management and data access to your application or device attached on the serial line where x is 8, 16, or 32.

Client

To configure the Percepxion client:

1. Go to Percepxion > Client to display the configuration and status for the Percepxion client.
2. Enter the client and connection configuration information.
3. Click Save & Apply.





Percepxion Client Configuration

Setting	Description
Status	
Client State	Displays the current Percepxion client's operational state (e.g., Exited, Active, Inactive, Running, or Not Registered). Otherwise displays a message such as Device credentials are not configured.
Last Status Update	Displays the amount of time between status updates (e.g., 12 days 10:20:00 or <Not Available>).
Last Content Check	Displays the amount of time between content checks (e.g., e.g., 9 days 06:11:00 or <Not Available>).
Available Firmware Updates	Displays a list of firmware that is available on the server. Select the firmware from this list and click Update now to upgrade or downgrade the firmware. Displays <None> if no Firmware updates are currently available.
Available Configuration Updates	Displays a list of configuration that is available on the server. Select the configuration from this list and click Update now to upgrade or downgrade the firmware. Displays <None> if no configuration updates are currently available.
Configuration	
Enable	Select to enable or clear to disable the Percepxion client.
Device ID	Read only. Displays the EDS5000 Device ID. The Device ID may be provisioned via Lantronix Provisioning Manager (LPM). Device ID can only be provisioned once. It will persist across resets.
Device Key	Displays the 32 character Percepxion key for this device or displays <Configured>. Read only. Note: Device Key may be configured via the Lantronix Provision Manager (LPM).
Serial Number	Displays the serial number of the device. Read only.
Device Name	Enter the Percepxion Device Name.
Device Description	Enter the Percepxion Device Description.
Status Update Interval (in minutes)	Enter the frequency that the EDS5000 updates the device status to Percepxion. The valid range is between 1 minute and 1440 minutes (1 day).
Send Dynamic Updates	If selected, device agent will send updates for RSSI and Temperature. The fields will be updated dynamically on Percepxion. This field is disabled by default.
Content Check Interval (in hours)	Enter the frequency that the EDS5000 checks Percepxion for updates to configuration or firmware. The valid range is between 1 hour and 2160 hours (90 days).
Apply Firmware Updates	Select to allow firmware updates to be applied via Percepxion. Enabled by default.

Setting	Description
Apply Configuration Updates	Select the option to indicate when to apply configuration updates. ♦ Always: always apply configuration updates. ♦ Never: never apply configuration updates.
Reboot After Update	Automatically reboot device after configuration update.
Allow Remote Connections	Select to allow remote connections or clear to disable. Enabled by default.
Audit Log	If checked, client will send audit events such as user login, firmware update, configuration update, and CLI access to Percepxion server.
Remote Access Local Port	Local port for remote access connection (e.g., <Random>).
Active Connection	Select the connection instance to use when connecting to Percepxion. You can configure two connections. The configuration options for Connection 1 and Connection 2 are listed below.
Connection 1 / Connection 2	
Connect to	Select Cloud or On-Premise connection.
Host	Enter the host name or IP address of the Percepxion server, used to register the device.
Port	Enter the Percepxion port number. Default: 443
Secure Port	Select to enable or clear to disable the Percepxion client secure port 443.
Validate Certificates	Select to enable or clear to disable the validation of the Percepxion server certificates. To validate certificates, both MQTT Security and Secure Port must be enabled.
Local Port	Local port for Percepxion MQTT client. When configured, a total of 32 consecutive ports will be reserved.
MQTT State	Select to enable or clear to disable MQTT. MQTT (originally MQ Telemetry Transport) is a lightweight, publish-subscribe network protocol for message queue/message queuing service. It was designed for connections with remote locations that have devices with resource constraints or limited network bandwidth.
MQTT Port	Enter the port number of the Percepxion MQTT server. When configured, a total of 32 consecutive ports will be reserved.
MQTT Security	Select to enable SSL for MQTT.
MQTT Local Port	Local port for Percepxion MQTT client. When configured, a total of 32 consecutive ports will be reserved.
Use Proxy	Select to enable the use of a proxy for this connection. If enabled, complete the proxy fields displayed under the Use Proxy field. Disabled by default.

Setting	Description
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.
User Name	Username for the proxy server.
Password	Password for the proxy server. The field displays an icon to alternately Reveal and Hide the password as you enter it.

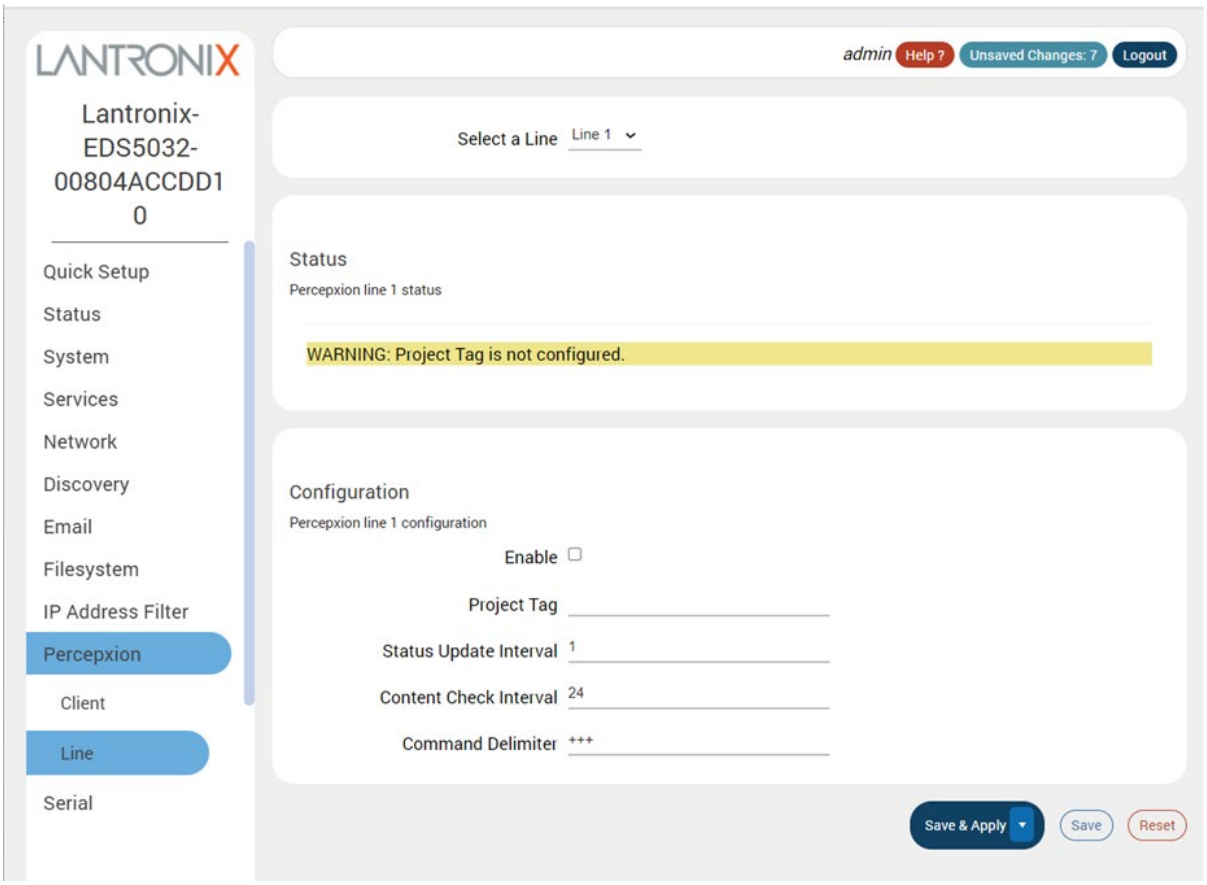
Percepxion Line

Configure Percepxion Line settings to enable remote management and data access to your application or device attached on the serial lines. The EDS5000 offers 8, 16, or 32 serial lines for configuration.

To configure Percepxion Line settings:

1. Go to Percepxion > Line to display the configuration and status for Percepxion Lines.
2. At the dropdown Select a Line.
3. View the current Status information.
4. Enter the Configuration section information. See the Percepxion Line table below.
5. Click Save & Apply.

Note: The Serial line mode should be configured as None or Tunnel.



Percepxion Line

Setting	Description
Status	Displays Percepxion line status for the selected line. If the field displays a message such as *WARNING: Project Tag is not configured* contact the Percepxion project administrator.
Enable	Select to enable or clear to disable the Percepxion line client.
Project Tag	Enter the Percepxion project tag string, as provided by the Percepxion project administrator.

Setting	Description
Status Update Interval	Enter the frequency in minutes that the EDS5000 updates the device status to Percepxion. The valid range is 1 to 1440 minutes (1 day).
Content Check Interval	Enter the frequency in hours that the EDS5000 checks Percepxion for updates to configuration or firmware. The valid range is between 1 hour and 2160 hours (90 days). The default is 24 hours.
Command Delimiter	Enter the command delimiter for attached serial devices. The default is +++. Send the delimiter before the command and after a response is received.

16. Serial

The EDS5000 device server series offers 8, 16, or 32 serial ports. Here you can view serial line statistics and set serial line parameters. All serial settings such as baud rate, parity, data bits, stop bits, and flow control apply to these lines. Note: Only ports 1-4 support RS-485.

The default serial settings:

- Baud rate: 115200
- Parity: None
- Data bits: 8
- Stop bits: 1
- Flow control: None

Statistics

Serial line statistics contain information on transmitted and received bytes, queued bytes, breaks, flow control, parity, framing, and overrun errors, no Rx buffer errors, CTS input, RTS output, and DSR input.

Configuration

To configure Serial line settings:

1. Go to Serial > Serial and select a Serial Line.
2. Scroll to the Configuration section.
3. Enter the line configuration settings. See the Serial Line Configuration table below.
4. Click Save & Apply.

Serial Line Configuration

Setting	Description
Name	Enter a descriptive name.
Enabled	Select to enable the line on the serial port.
Interface	The Serial Port interface type: ♦ RS232 (default) ♦ RS485 Full-Duplex ♦ RS485 Half-Duplex
Termination	Termination of the RS485 bus, if available. At the dropdown select from: ♦ Disabled (default) ♦ Termination on TX ♦ Termination on RX ♦ Termination on TX and RX Note: RS-485 is available only on port1 to port4.

Setting	Description
Is baudrate custom	If using a custom baud rate, select the box and add a value between 2400 bps and 921600 bps.
Baud Rate	Select the desired baud rate from the drop-down list. Baud rate options: 2400, 4800, 9600, 19200, 38400, 57600, 115200 (default), 230400, 460800, and 921600.
Parity	Select parity from the drop-down list: ♦ None (default) ♦ Even ♦ Odd
Data Bits	Select data bits from the drop-down list: ♦ 8 (default) ♦ 7
Stop Bits	Select the stop bits from the drop-down list: ♦ 1 (default) ♦ 2
Flow Control	Select the flow control from the drop-down list: ♦ None (default) ♦ Hardware ♦ Software
Xon character **Xoff character**	If Software Flow Control is selected, enter the Xon and Xoff character to use: ♦ Xon Char (default is <*control*>*Q*) ♦ Xoff Char (default is <*control*>*S*)
Gap Timer	Set the number of milliseconds to delay 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 (default value is 4000 msec).
Threshold	Set the number of threshold bytes which need to be received in order for the driver to forward received characters. Default value is 56 bytes.
Mode	Select the mode of serial communication as determined by the protocols available on the EDS5000 model. ♦ None – can be used if Percepxion line is configured. ♦ Tunnel – (see chapter 20. Tunnel on page 148). ♦ Tunnel/Modbus RTU to Modbus TCP – (see Tunnel Modbus RTU to Modbus TCP). ♦ Managed Device.

17. SMTP

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

SMTP Settings

Setting	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, enter 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's commonly used port number; the default setting is port *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. The default setting is *<Random>*.

18. 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 EDS5000 devices or automatically generated on the EDS5000.

Configuration is required when the EDS5000 devices are either 1) the SSH server or 2) an SSH client.

1. The SSH server is used by the CLI (Command Mode) and for tunneling in Accept Mode.
2. The SSH client is used for tunneling in Connect Mode.

To configure the EDS5000 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 EDS5000 device's SSH server.

The SSH main menu provides tabs for SSH Server and SSH Client settings.

SSH Server

This main menu lets you view current settings and upload or create host keys.

SSH Server: Upload Host Keys tab

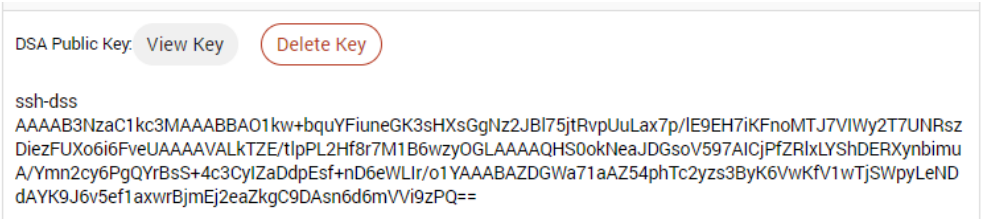
The SSH Server Host Keys are used by all applications that play the role of an SSH Server during Tunneling in Accept Mode. These keys can be created elsewhere and uploaded to the EDS5000 device or automatically generated on the device. If uploading existing keys, take care to ensure the Private Key will 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.

Setting	Description
Current Configuration	
RSA Public Key	Displays the currently configured RSA public key if one is currently configured. ♦ View Key: Click to display the currently configured RSA public key. ♦ Delete Key: Click to remove the currently configured RSA public key.
DSA Public Key	Displays the currently configured DSA public key or displays *(Not Configured)* if none is currently configured.
SSH Server: HostKeys	
Upload Keys	**Private Key**: Click the Select File button to navigate to the existing private key you want to upload, then click the Upload file button. 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 Select File button to navigate to the existing public key you want to upload, then click the Upload file button. **Key Type**: Select a key type to use for the new key: ♦ RSA (default) ♦ DSA

Setting	Description
Create New Keys	**Key Type**: Select a key type to use for the new key: ♦ RSA (default) ♦ DSA **Bit Size**: Select a bit length for the new key: ♦ 512 (DSA only) (default) ♦ 768 (DSA or RSA) ♦ 1024 (DSA or RSA) (1024 RSA is the default) ♦ 2048 (RSA only) ♦ 4096 (RSA only)

View Key Example:



SSH Server: User Configuration tab

This tab displays the current set of Authorized Users and lets you create and configure new SSH server authorized users.

Setting	Description
Current Configuration	
RSA Public Key	Displays the current set of Authorized Users or if none are currently configured displays *No Authorized Users are currently configured for SSH Server*.
SSH Server: Authorized Users	
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 Select 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 Select 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

This main menu lets you view Hosts configured for the SSH Client and upload Known Hosts Keys.

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 then another layer of security is offered which helps prevent Man-in-the-Middle (MITM) attacks. **Note**: These settings are not required for communication. They protect against MITM attacks.

SSH Client: Known Hosts

Setting	Description
Current Configuration	
Known Hosts	Displays the current set of Known Hosts or if none are currently configured displays *No Known Hosts are currently configured for SSH Client*.
SSH Client: Known Hosts	
New Host	Allows you to define a new host in terms of Server and Host Keys.
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 Select 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 Select 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.

SSH Client: Users

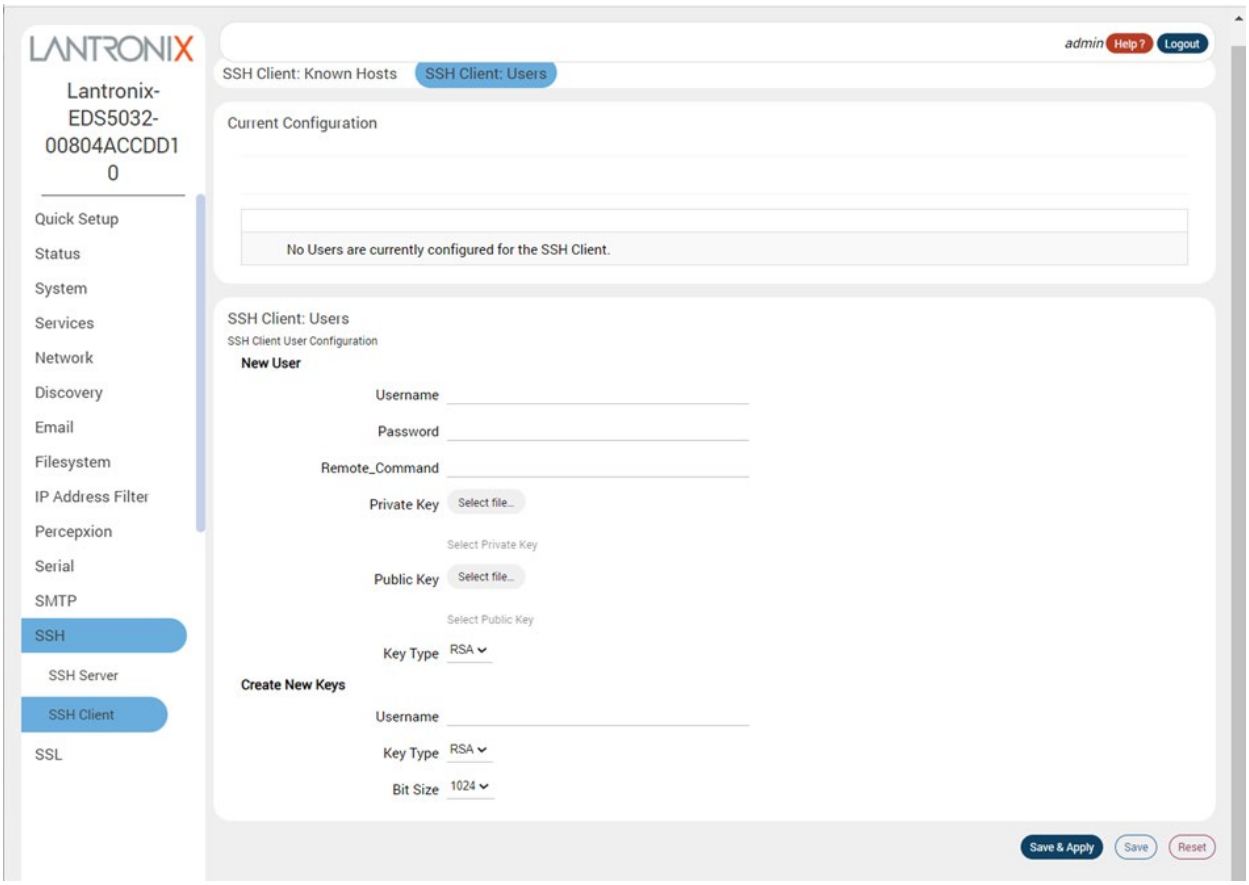
The SSH Client Users are used by all applications that play the role of an SSH Client during Tunneling in Connect Mode. To configure the EDS5000 devices as an SSH client, an SSH client user must be both configured and also exist on the remote SSH server.

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 EDS5000 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.



SSH Client Users

Setting	Description
Current Configuration	
SSH Client Users	Displays the current set of Known Hosts or if none are currently configured displays *No Users are currently configured for the SSH Client*.
SSH Client: Users - Create New User	
Username	Enter the name that the EDS5000 devices uses to connect to an SSH server.

Setting	Description
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.
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.
SSH Client: Users - Create New Keys	
Username	Enter the Username for the new key.
Key Type	Select a key type: ♦ RSA ♦ DSA
Bit Size	Select a bit length for the new key: ♦ DSA: 512 (default), 768, or 1024 ♦ RSA: 1024 (default), 2048, or 4096

19. SSL

This main menu lets you create new SSL credentials, upload a Certificate, and create a new Self-signed certificate. The SSL main menu provides two sub-menus: Credentials and Trusted Authorities.

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 Tunnel application. SSL certificates identify the EDS5000 devices to peers and are used with some methods of wireless authentication. Provide a name at upload time to identify certificates on the EDS5000 devices.

You can upload Certificate and Private key combinations, obtained from an external Certificate Authority (CA) to the EDS5000 devices. The EDS5000 devices can also generate self-signed certificates with associated private keys.

Credentials

The EDS5000 device servers can generate self-signed certificates and their associated keys for RSA and DSA certificate formats. When you generate certificates, assign them a credential name to help identify them on the EDS5000. After you create your credentials, then configure them with the desired certificates.

To configure a new credential:

1. Go to SSL > Credentials.
2. Type the name for your credential in the Credential Name field.
3. Enter the fields under Upload Certificate or Create New Self-Signed Certificate (see tables below).
4. Click Save & Apply. The process to create a self-signed certificate may take up to 30 seconds, depending on the length of the key. The newly created credential is displayed at the top of the SSL Credentials page.

To view a credential:

1. Go to SSL > Credentials.
2. Under Current Credentials, click the name of the credential to view its details.

To delete a credential:

1. Go to SSL > Credentials.
2. Under Current Credentials, click the Delete button next to the name of the credential.

SSL Credentials

Setting	Description
Current Credentials	Displays the current SSL credentials if any exist.
Create New Credential	
Credential Name	Enter a name for the SSL certificate to be uploaded.
SSL Certificate	Click the **Select file** button, select the desired file, click the Upload file button.
Certificate Type	At the dropdown select PEM, PKCS7, or PKCS12. The default is PEM. For PKCS certificates, enter a password. Ensure that the certificate is formatted properly with a valid open and close tag.

Setting	Description
SSL Private Key	Click the Select file... button to browse to and select the SSL private key to be uploaded. The key must belong to the entered certificate. Ensure that the private key associated to the selected certificate and that it is formatted properly with a valid open and close tag. Click the Upload file button
Key Type	At the dropdown select PEM, Encrypted PEM, or PKCS12. The default is PEM. For encrypted PEM or PKCS12 key types, enter a password.
Password	If Key Type Encrypted PEM or PKCS12 was selected, enter a password for the new credential.
Create New Self-Signed Certificate	
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). See the ISO - ISO 3166 — Country Codes.
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 EDS5000 belongs.
Organization Unit	Enter the organization unit which specifies the department or organization to which the EDS5000 belongs.
Common Name	Enter a network name for the EDS5000 when installed in the user’s network (usually the FQDN). It is identical to the name that is used to access the EDS5000 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 EDS5000 is accessed using HTTPS.
Expires	Type the date that the self-signed certificate expires in mm/dd/yyyy format.
Type	At the dropdown select the type of new certificate to use: ♦ **RSA**: the Rivest–Shamir–Adleman public-key cryptosystem is one of the oldest that is widely used for secure data transmission. ♦ **DSA**: use the Digital Signature Algorithm, a public-key cryptosystem and Federal Information Processing Standard for digital signatures. ♦ **ECDSA**: use the Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of the DSA which uses elliptic-curve cryptography.
ECDSA Curve	If Type ECDSA was selected, 256, 384, or 521 bits.
Key Length	At the dropdown select the length of the SSL key: ♦ **RSA**: select 512, 768, 1024, 2048, or 4096 bit key length ♦ **DSA**: select 512, 768, or 1024 bit key length ♦ **ECDSA**: select 256, 384, or 521 bit key length
Clear (button)	Click to clear the fields.

To Configure an SSL Credential to Use an Uploaded Certificate

1. In the Web Admin interface, 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 Admin interface 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 Admin interface, 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.
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

Here you can view current Certificate Authorities and upload SSL certificates. One or more authority certificates are used to verify the identity of a peer. Authority certificates are used with tunnel application. These certificates do not require a private key.

Setting	Description
Current Certificate Authorities	Displays the set of current CAs, if any exist. 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.
SSL Certificate	Click the Select file… button, select a listed SSL Certificate, then click the Upload file button.
Certificate Type	At the dropdown select the desired cert type: ♦ **PEM**: Governed by IETF RFCs, used preferentially by open-source software because it is text-based and therefore less prone to translation errors or transmission errors. It can have a variety of extensions (.pem, .key, .cer, .cert). This is the default. ♦ **PKCS7**: An open standard used by Java and supported by Windows. It does not contain private key material. ♦ **PKCS12**: A Microsoft private standard that was later defined in an IETF RFC that provides enhanced security versus the plain-text PEM format. This can contain private key and certificate chain material. It is used preferentially by Windows systems, and can be freely converted to PEM format using openssl.
Password	If you selected PKCS12 as the Certificate Type, then enter a Password.
Clear (button)	Click to clear the fields.

20. Tunnel

Tunneling allows serial devices to communicate over a network without being aware of the devices that establish the network connection between them. The Tunnel settings let you configure how the serial network tunneling operates. Tunneling is available on 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. Aggregate and individual connection statistics are displayed.

At the dropdown select a Tunnel to view its statistics. The page displays the Aggregate Counters section and the Accept Counters section.

Aggregate Counters: Completed Accepts, Completed Connects, Disconnects, Dropped Accepts, Dropped Connects, Octets forwarded from Line, Octets forwarded from Network, Accept connection times, Connect DNS Address Changes, and Connect DNS Address Invalids.

Accept Counters: Connect 1 Counters - Connect 16 Counters for active connections.

Tunnel Accept

This section controls how data send behaves when a connection attempt originates from the network. In Tunnel Accept mode, the EDS5000 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 ports are 10001 for serial line 1, 10002 for serial line 2, etc. Serial data can still be received while waiting for a network connection, keeping in mind serial data buffer limitations.

To configure Tunnel Accept mode:

1. Go to Tunnel > Tunnel 1.
2. Under Accept, enter the Accept Mode settings. See the table below.
3. Click Save & Apply.

Tunnel Accept Mode Configuration

Setting	Description
Accept Mode	Select the method used to start the tunnel in Accept mode. Choices are: ♦ **Disable** - do not accept an incoming connection. ♦ **Always** - accept an incoming connection (default). ♦ **Any Character** - start waiting for an incoming connection when any character is read on the serial line. ♦ **Start Character** - start waiting for an incoming connection when the start character for the 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.

Setting	Description
Local Port	Set the port number for use as the network local port. The default local port number correlates with the tunnel instance: ♦ Tunnel 1: 10001 ♦ Tunnel 2: 10002 Note: There is no Tunnel SFP. Based on 8,16,32 port will use tunnel 1 to tunnel 32 and 10001 to 10032.
Protocol	Select the desired security protocol: ♦ SSL ♦ SSH ♦ TCP (default protocol) ♦ TCP AES ♦ Telnet Configure the protocol fields as determined by the protocol selection.
TCP Keep Alive	The TCP keep alive time is the time in which probes are periodically sent to the other end of the connection to ensure the other side is still connected. Enter the TCP Keep Alive time in milliseconds. Valid values are 0 - 28800000 milliseconds. The default is 45000 milliseconds. 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. Valid values are 0 - 28800000 milliseconds. Blank the field to restore the default (1 millisecond).
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 1 - 16 milliseconds. The default is 8 milliseconds. Blank the field to restore the default.
Initial Send	The Initial Send data will be sent out the network upon connection establishment before any data from the Line. It may contain one or more Directives of the form %. 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 %% %

Setting	Description
Initial Send Type	The format of the initial send data. ♦ Text (default) ♦ Binary
Flush Serial	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)
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ♦ 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 to the network. Any buffered characters are sent first.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: ♦ 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 to the serial line. Any buffered characters are sent first.
Password	The password can be up to 31 characters in length. Valid characters are alphanumeric characters and punctuation. When set, clients must send the correct password string to the device within 30 seconds from opening network connection in order to enable data transmission. The password sent to the device 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 selected and a password is configured, the user will be prompted for the password upon connection.
Email on Connect	At the dropdown select the serial line on which to send an email on a successful connection. The selections are <None> or Email1 - Email8.
Email on Disconnect	At the dropdown select the serial line on which to send an email on a successful disconnection. The selections are <None> or Email1 - Email8.

Tunnel Connect

This section controls how data send behaves when a connection attempt originates from the device. At least one Host is required to enable Connect Mode. A maximum of 8 hosts can be configured in Tunnel Connect mode.

In Connect mode, the EDS5000 continues to attempt an outgoing connection on the network until established. If the connection attempt fails or the connection drops, then it retries after a timeout. The remote node on the network must listen for the Connect mode's connection.

For Connect mode to function, it must be enabled, have a remote station (node) configured, and a remote port configured (TCP or UDP). When established, Connect mode is always on. Enter the remote station as an IPv4 or IPv6 address or DNS name. The EDS5000 will not make a connection unless it can resolve the address. For Connect mode using UDP, the EDS5000 accepts packets from any device on the network. It will send packets to the last device that sent it packets.

***Note 1**: The port in Connect mode is not the same port as the one 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.*

***Note 2**: If Host is configured as UDP or UDP AES then only one host can be configured.*

***Note 3**: TCP Keep Alive is not applicable to UDP and UDP AES.*

Configuration Procedure

1. To configure Connect Mode for a specific tunnel, click Tunnel > Connect and then select a tunnel number from the Select a Tunnel drop-down list at the top of the webpage.

Tunnel Connect mode

Setting	Description
Select a Tunnel	At the dropdown select the desired tunnel to configure. The default is Tunnel 1.
Connect 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 EDS5000 retries 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.

Setting	Description
Host Mode	If more than one host is configured, set the method to be used to access multiple hosts. ♦ **Sequential** – A tunnel will connect to hosts in sequential order. Host 1 will be attempted first. If that fails, it will proceed in order to Host 2, 3, and then 4. When a connection drops, the cycle starts again with Host 1 and proceeds in order. (default setting) ♦ **Simultaneous** – A tunnel will connect to all hosts accepting a connection. Simultaneous connections occur at the same time to all listed hosts. The EDS5000 supports a maximum of 8 host connections.
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.
Reconnect Timer	Set the value of the reconnect timeout (in milliseconds) for outgoing connections established by the EDS5000. The valid range is 1 to 65535 milliseconds. Default is 15000 ms.
Flush Serial	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)
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	Where to send an email notifying of a connection. At the dropdown select None or Email 1 - Email 8. The default is <None>.
Email on Disconnect	Where to send an email notifying of a disconnection. At the dropdown select None or Email 1 - Email 8. The default is <None>.

Hosts

Connect mode supports up to 16 hosts. Hosts may be accessed sequentially or simultaneously. Notes:

- Configure the keep alive timeout to be larger than the user timeout.
- 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. The user timeout will not be an exact limit; in practice, it will always take somewhat longer for the connection to be closed.
- 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. 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.
- The user timeout expiration during retransmission returns an error to the application; it does not automatically reset the connection as happens with the keep alive timeout. It is up to the application (e.g., tunneling) to close the connection (this happens almost immediately with tunneling).

Setting	Description
Address	Enter the destination IP address or DNS address for the connection.
Port	Enter the TCP or UDP port number on the target host for the connection.
Protocol	Select the desired security protocol. ♦ SSL ♦ TCP ♦ TCP AES ♦ Telnet ♦ UDP ♦ UDP AES Configure the remaining protocol fields as determined by the protocol selection. **Note**: If Host configured as UDP or UDP AES then only one host can be configured. TCP Keep Alive is not applicable to UDP and UDP AES.
Secure Protocols	When using SSL, select the secure protocols and the SSL credential. Protocol options are: ♦ SSL3 ♦ TLS1.0 ♦ TLS1.1 (default = selected) ♦ TLS1.2 (default = selected) ♦ TLS1.3 (default = selected)

Setting	Description
TCP Keep Alive	Enter the time, in milliseconds, the EDS5000 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. **Note**: If Host configured as UDP or UDP AES then only one host can be configured. TCP Keep Alive is not applicable to UDP and UDP AES.
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 1 - 16 probes. 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.
AES Encrypt Key	Enter the AES Encrypt Key. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
AES Encrypt Key Type	Select *Text* or *Hexadecimal* to indicate the encryption format.
AES Decrypt Key	Enter the AES Decrypt Key. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
AES Decrypt Key Type	Select *Text* or *Hexadecimal* to indicate format.
Initial Send	Enter the Initial Send character 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>. This configuration field becomes available when the TCP, UDP, or UDP AES protocol is selected.
Initial Send Type	Select *Text* or *Hexadecimal* to indicate format.
Credentials	If SSL is the selected protocol, select an existing credential from the drop-down list. Go to SSL > Credentials to create, view, or edit SSL credentials.
Validate Certificate	Select to enable validation of the SSL certificate on the server. This configuration field becomes available when the SSL protocol is selected.

Connecting Multiple Hosts

Connect mode supports up to 8 hosts. Hosts may be accessed sequentially or simultaneously.

- Sequential – A tunnel will connect to hosts in sequential order. The host specified as Host 1 will be attempted first. If that fails, it will proceed to Host 2, 3, and 4. When a connection drops, the cycle starts again with Host 1 and proceeds in order. 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 EDS5000 can support a maximum of 8 connections.

When hosts have been added you can then use the icons to reorder, Edit, or Delete instances.

Disconnect

These settings relate to disconnecting a Tunnel. Disconnect specifies the optional conditions for disconnecting any tunnel connection that may be established. If any of these conditions are selected but do not occur and the network disconnects the tunnel, a Connect mode connection will attempt to reconnect. However, if none of these conditions are selected, a closure from the network is taken as a disconnected host.

Tunnel Disconnect mode

Setting	Description
Select a Tunnel	At the dropdown select the desired tunnel to configure. The default is Tunnel 1.
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 these forms: ♦ *<control>J* ♦ *0xA (hexadecimal)* ♦ *\10 (decimal)*. To disable the Stop Character, blank the field, which sets it to *<None>*.
Flush Stop Character	Set whether to flush the stop character when the tunnel is disconnected, either: ♦ Enabled ♦ Disabled (default)
Timeout	Enter the number of milliseconds a tunnel may be idle before disconnection. The valid range is 0 - 28800000. To disable the timeout, set the field to zero (0).
Flush Serial Data	Set whether to flush the serial line when the tunnel is disconnected. Choices are: ♦ Enabled ♦ Disabled (default)

Tunnel Packing Mode

When Tunneling, instead of sending data on the network immediately after being read on the Serial Line, the data can be Packed (queued) and sent in larger chunks.

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.

Tunnel Packing Mode

Setting	Description
Packing Mode	At the dropdown, select Disable (default), Timeout, or Send Character mode: **Disable** - Data not packed. The default is Disabled. **Timeout** - Data sent after timeout occurs. **Send Character** - Enter the Initial Send character to be sent out the network upon connection establishment before any data from the line.
Threshold	Set the threshold (byte count). If the received serial data reaches this threshold, then the data will be sent on the network. The valid range is 100 to 1450 bytes. The default is 512 bytes. **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. The valid range is 1 to 30000 milliseconds. The default is 1000 milliseconds. **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.
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.

Serial DTR Options

Navigate to Tunnel > Serial to display the Serial Data Terminal Ready config page.

The serial DTR options select the conditions in which the Data Terminal Ready control signal on the Serial Line is asserted.

Serial DTR Options

Setting	Description
Select a Tunnel	At the dropdown select the tunnel to be configured.
Data Terminal Ready	Select the conditions in which the Data Terminal Ready (DTR) control signal on the serial line are asserted. Choices are: ♦ **Asserted while connected** - The DTR is asserted whenever either a connect or an accept mode tunnel connection is active (default). ♦ **Continuously asserted** - DTR is always asserted. ♦ **Unasserted** - DTR is not asserted. ♦ **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.

Modem Emulation Mode

Tunnel connections can be initiated and accepted using Modem 'AT' commands incoming from the Serial Line.

In Modem Emulation mode, the EDS5000 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.

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 EDS5000 devices mimic the modem's behavior.

Modem Emulation Mode Parameters

Setting	Description
Select a Tunnel	At the dropdown select the desired tunnel. The default is Tunnel 1.
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)

Modbus RTU to Modbus TCP

This section controls how data send behaves when Modbus is selected.

When Enabled, the selections are Protocol (TCP), Mode (Server), and Port (0-65535).

The EDS5000 acts as a converter between a Modbus RTU and a Modbus TCP device. Modbus RTU polls the data from the Modbus slave and sends it to the Modbus master using Modbus TCP.

To use this feature, configure the serial interface and TCP interface.

Tunnel for Modbus RTU to Modbus TCP

Setting	Description
Select a Tunnel	At the dropdown select the desired Tunnel. The default is Tunnel 1.
Enable	Select to enable and configure the Modbus RTU to Modbus TCP settings.
Protocol	TCP option is selected.
Mode	Server - the EDS5000 acts as a server and listens for the TCP connection from external Modbus master. A TCP Port is required.
Port	Modbus TCP port number that the server is listening on (port 0-65535).

Appendix A. Troubleshooting

Basic Troubleshooting

1. Ensure that devices at both ends are set to the same communication settings, including baud rate, parity, number of data bits, and number of stop bits.
2. Make sure you are using the correct Serial Cable, that it is working, and that it is correctly connected.
3. Verify the Power connection (AC or DC).
4. Verify the COM Port selection and that the COM port you want to use is available and not in use.
5. Verify that the operation you are attempting is supported by the EDS5000.
6. Check the EDS5000 System Log and Kernel Log for issues.
7. Try Rebooting the EDS5000 operating system. See System > Backup / Flash Firmware > Reboot.
8. Try running the Network Utilities at Network > Diagnostics (Ping, Traceroute, NSLookup).
9. Refresh the web browser.
10. Check the Release Notes for possible known issues or work-arounds.
11. Check the Lantronix website for possible new firmware and update EDS5000 software if possible. See System > Backup / Flash Firmware > Actions.
12. Make sure the DHCP server's Lease time has not expired (if DHCP is used).
13. Contact Lantronix Technical Support.

RS232 Troubleshooting

These are very general procedures that can be used to troubleshoot a serial connection to a Lantronix product. For details of 3rd party serial devices please consult the documentation for the product or contact the manufacturer. When troubleshooting a serial connection only make one change at a time, and document each change when you make it. That way it's easy to get back to where you started, if needed.

1. Make sure that the Lantronix product and the serial device are both set to the same speed, character size, parity, stop bits and flow control method.
2. Try a different serial cable. If the new cable works, discard the old one.
3. Disable flow control on both the Lantronix product and the serial device. If you get communication without flow control, but no communication with flow control, make sure that both ends of the connection are using the same kind of flow control, or just don't use flow control.
4. Check that the Data Output pin of the Lantronix product is connected to the Data Input pin of your serial device, and that the Data Input pin of the Lantronix product is connected to the Data Output pin of your serial device. There must also be a connection from the Signal Ground pin(s) on the Lantronix product to the Signal Ground pin of the serial device.
5. Some RS232 serial ports are DCE (Data Computing Equipment) ports. DCEs are usually labeled "backwards", i.e. TX is an input and RX is an output. Make sure you understand which pin(s) are outputs and which are inputs on both sides of the connection when designing the connecting cable.
6. Make sure your serial cables are not excessively long, especially in electrically noisy environments. In general a serial cable should not be longer than 50' for communication at 9600bps. Faster speeds require shorter cables, slower speeds allow longer cables. In general, the shorter the cable and the slower the serial speed the more reliable the connection will be.

7. Try a different serial device of the same make and model. If the new one works, replace the original..
8. Try a different Lantronix product of the same model. If the new one works, replace the original.
9. Many 3rd party products come with a cable so they can be connected to a PC's serial Com port. If your product has such a cable, connect it to a PC and check to see if it works. If not the serial port on the 3rd party device may be defective.

Troubleshooting Link Type and Speed Issues

The Network > Interfaces > Link page lets you shift between Copper and SFP operating modes and set Link type and speed.

Uplink 1000 Mbps		
Device Speed	**SFP = 100 Mbps**	**SFP = 1000 Mbps**
100	The shift succeeds or fails depending on SFP module. Warning messages display, and to get proper status you must reboot the device.	The shift succeeds or fails depending on SFP module. Warning messages display, and to get proper status you must reboot the device.
1000	The shift succeeds or fails depending on SFP module. Warning messages display, and to get proper status you must reboot the device.	Both LEDs blink.
Uplink 100 Mbps		
Device Speed	**SFP = 100 Mbps**	**SFP = 1000 Mbps**
100	Only one LED blinks.	The shift succeeds or fails depending on SFP module. Warning messages display, and to get proper status you must reboot the device.
1000	The shift succeeds or fails depending on SFP module. Warning messages display, and to get proper status you must reboot the device.	The shift succeeds or fails depending on SFP module. Warning messages display, and to get proper status you must reboot the device.

Appendix B. Compliance

Compliance Information

(According to ISO/IEC Guide and EN 45014)

Manufacturer's Name & Address:

Lantronix, Inc. 48 Discovery, Suite 250, Irvine, CA 92618 USA

Product Family:

EDS5000 Series

Conforms to the following standards or other normative documents:

Regional Certifications

Country	Specification
USA	♦ FCC CFR Title 47 Part 15 Subpart B:2021, Class A ♦ Conducted Emission: FCC CFR Title 47 Part 15 Subpart B:2021, Class A. CISPR 22:2008, ANSI C63.4-2014. ANSI C63.4a-2017. ♦ Radiated Emission: FCC CFR Title 47 Part 15 Subpart B:2021, Class A. CISPR 22:2008, ANSI C63.4-2014. ANSI C63.4a-2017. ♦ EN 55032:2015:A1:2020, Class A. EN 55035:2017/A11:2020. EN IEC 61000-3-2:2019/A1:2021. ♦ EN 61000-3-3:2013/A2:2021 ♦ TAA compliant. ♦ NDAA compliant ♦ EN IEC 62368-1:2020+A11:2020
United Kingdom	♦ UK Declaration of Conformity - see below ♦ BS EN IEC 62368-1:2020+A11:2020
Canada	CSA/UL 62368-1:2019
Saudi Arabia	SASO-IEC 62368-1:2020
Japan	J62368-1(2023)
Australia	AS/NZS 62368.1:2022
New Zealand	AS/NZS 62368.1:2022
Singapore	Special National Conditions for Singapore
European Union	EU Declaration of Conformity - see below

Additional application considerations:

- The equipment is intended to be supplied by approved external power source (UL listed / IEC 60950-1 / IEC 62368-1) which output is complied with SELV/ES1, output rating 24-48Vdc, 1A min., ambient temperature 60 Deg. C minimum (for DC input).
- The following circuit locations (with circuit/schematic designation) were investigated as a limited power source (LPS) or PS2: all output ports except optical transceiver port.
- The Class of laser product is: for Fiber Optical transceiver (Class 1).

FCC Statement

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations are restricted to indoor usage only.

UK Declaration of Conformity

UK Declaration of Conformity

LANTRONIX®

UK CA

UK DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 USA
Model Number: EDS5008, EDS5016, EDS5032

Manufacturer's Quality System:

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

Electrical Equipment Regulations 2016

- EN IEC 62368-1:2020+A11:2020

Electromagnetic Compatibility Regulations 2016

- EN 55032:2015/A1:2020, Class A
- EN 50035:2017/A11:2020
- EN IEC61000-3-2:2019/A1:2021
- EN IEC61000-3-3:2013/A2:2021

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: Eric Bass Date: 7 March 2024

Name: Eric Bass Title: VP of Engineering

EU Declaration of Conformity

EU Declaration of Conformity

LANTRONIX®

CE

EU DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 USA
Model Number: EDS5008, EDS5016, EDS5032

Manufacturer's Quality System:

TÜVRheinland

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

is in conformity with the essential requirements of the Directive 2014/53/EU,2014/30/EU and of the Directive 2015/863/EU (RoHS). The product has been tested against the following standards or technical specifications:

1. Directive 2014/53/EU:
   - EN IEC 62368-1:2020+A11:2020
2. Directive 2014/30/EU:
   - EN 55032:2015/A1:2020, Class A
   - EN 50035:2017/A11:2020
   - EN IEC61000-3-2:2019/A1:2021
   - EN IEC61000-3-3:2013/A2:2021
3. Requirements in the Article 4 of Directive 2015/863/EU (RoHS III), towards the maximum tolerated concentrations of the substances listed in Annex II:
   - EN IEC 63000:2018

Signature: Eric Bass Date: 7 March 2024

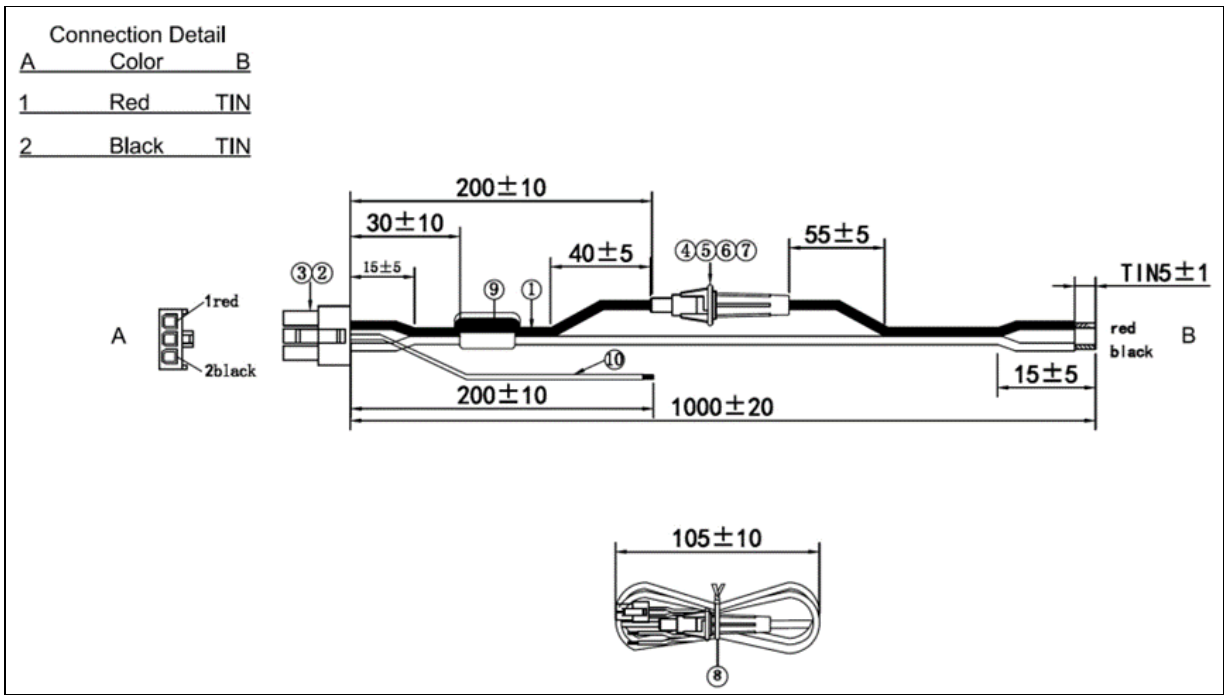
Name: Eric Bass Title: VP of Engineering

CERT-PNT-SG3FS rev B

Appendix C. Cables

3-pin Power Cable

Power Cable Schematic - 3-pin power cable schematic



Console port cable: ACC-500-103-R

Appendix D. Glossary

Acronym	Description
AES	Advanced Encryption Standard is the encryption key protocol applied in the IEEE 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.
ARP	Address Resolution Protocol; a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given Internet layer address, typically an IPv4 address.
CGI	A Common Gateway Interface script that is used by a web server to run an external program to process user requests.
Command delimiter	Command delimiter characters are special characters or spaces that identify the beginning or end of a group of characters in a command.
comsec com2sec com2Sec6	Communications Security; a component of CS that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Includes cryptographic, transmission, emissions, and physical security.
CPU	Central Processing Unit
cron	The cron command-line utility is a job scheduler on Unix-like operating systems. Users who set up and maintain software environments use cron to schedule jobs (commands or shell scripts) to run periodically at fixed times, dates, or intervals.
CTS	Clear to send
DER	Distinguished Encoding Rules is a restricted variant of BER for producing unequivocal transfer syntax for data structures described by ASN.1.
DES	DES (Data Encryption Standard) provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.
DHCP	Dynamic Host Configuration Protocol is a standardized networking protocol used by hosts to dynamically discover and lease an IP address, and learn the correct subnet mask, default EDS5000, and DNS server IP address.
DNS	Domain Name System is an application layer protocol used throughout the Internet for translating hostnames into their associated IP addresses.
DSR	Data Set Ready

DTR	Data Terminal Ready
filesystem (file system or fs)	An index or database containing the physical location of every piece of data on the device. The data is usually organized in folders called directories, which can contain other folders and files.
glob	glob (global) patterns specify sets of filenames with wildcard characters. For example, the Unix Bash shell command `mv *.txt textfiles/` moves all files with names ending in .txt from the current directory to the directory `textfiles`. Here, `*` is a wildcard and `*.txt` is a glob pattern. The wildcard `*` stands for "any string of any length including empty, but excluding the path separator characters (`/` in unix and `\` in windows)".
HTTP	Hyper Text Transfer Protocol
HTTPs	Secure Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol (ICMP) is a TCP/IP network layer protocol that reports errors and provides other information relevant to IP packet processing.
IGMP	Internet Group Management Protocol is a communications protocol used by hosts and adjacent gateways on IP networks to establish multicast group memberships
JSON	JSON (JavaScript Object Notation) is a lightweight data-interchange format that is easy for humans to read and write
JSON-RPC	JSON-RPC is a stateless, light-weight remote procedure call (RPC) protocol.
LAN	Local Area Network
LED	Light emitting diode
Lua	Lua is a powerful, efficient, lightweight, embeddable scripting language.
MAC address	Media Access Control address is a unique identifier (6 bytes) assigned to a network interface for use as a network address.
MD5	MD5 (Message-Digest algorithm 5) is a message digest algorithm used as a checksum to verify data integrity. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.
Modbus	Modbus is a data communication protocol used for connecting industrial electronic devices.
Modbus RTU	Modbus RTU (Remote Terminal Unit), is the most common implementation available for Modbus; it uses a compact binary representation of the data for protocol communication.
Modbus TCP	Modbus TCP/IP is a Modbus variant used for communications over TCP/IP networks, connecting over port 502.[29] It does not require a checksum calculation, as lower layers already provide checksum protection.

MTU	Maximum Transmission Unit of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards
NMS	Network Management System. Component in SNMP architecture that includes SNMP manager.
NTP	Network Time Protocol is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
OID	Object Identifier in SNMP
overlayfs	A union mount filesystem implementation for Linux. An overlay filesystem tries to present a filesystem which is the result of over overlaying one filesystem on top of another.
Passive FTP	An FTP mode that can be requested by a client to alleviate issues caused by client-side firewalls. Both the server and the client must support passive FTP for it to work. With passive FTP, the client initiates the connection to the server.
PEM PKCS7 PKCS12	**PEM** is governed by RFCs and is preferred by open -source software because it is text-based and thus less prone to translation or transmission errors. It can have a variety of extensions (.pem, .key, .cer, .cert, etc.). **PKCS7** is an open standard used by Java and supported by Windows. PKCS7 does not contain private key material. **PKCS12** is a Microsoft private standard later defined in IETF RFC 7292 to provide enhanced security versus the plain-text PEM format. This can contain private key and certificate chain material. It's used by Windows systems, and can be freely converted to PEM format using openssl.
.pub file	A public key used in public-key cryptography. It contains encrypted text used to encrypt and decrypt data, alongside a corresponding private key. The .pub file is used to authenticate a user's credentials when that user logs in to a server.
RSA	RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission
RTS	Ready To Send
RTU	Remote terminal unit
Rx	Reception or Receive
SCP	Secure Copy Protocol
SHA1 SHA2	Secure Hash Algorithm is an encryption cipher type. SHA was designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length. SHA2 is more secure than SHA 1.
SMTP	Simple Mail Transfer Protocol used for Email
SNMP	Simple Network Management Protocol

SNMPd	Simple Network Management Protocol daemon
Squashfs	Squashfs is a compressed read-only file system for Linux.
SSH	Secure Shell
SSL	Secure Sockets Layer encryption-based security protocol designed to provide data security for Internet communications.
symlink	A symbolic link (soft link) is a file whose purpose is to point to a file or directory (called the "target") by specifying a path thereto.
TCP	Transmission Control Protocol
Tx	Transmission or transmit
UDP	User Datagram Protocol
uHTTPd	A small multi-threaded HTTP server.
USM	User-based Security Model for SNMP v3.
VACM	View-based Access Control Model for SNMPv3.
WAN	Wide Area network

Appendix E. Commands

Commands can be run on the EDS5000 series device servers using the following methods:

- **SSH (login as root using SSH)**: The user has full control and can run commands as described.
- **System/Custom commands**: The user can run commands as described. It is not recommended to run a command or series of commands (in a series, commands are separated by semicolon) which take more than 60s to complete or require additional user interaction. For example: `vi`.
- **Percepxion/CLI commands**: The user can run commands as described. It is not recommended to run a command or series of commands (commands separated by semicolon) which take more than 60s to complete or require additional user interaction. For example: `vi`.

Types of Commands

The following types of commands are available:

- Bash commands
- opkg commands
- UCI commands

Bash Commands

Bash shell is distributed with BusyBox which provides a stripped down implementation of common Linux commands.

Usage

BusyBox is a multi-call binary. A multi-call binary is an executable program that performs the same job as more than one utility program. That means there is just a single BusyBox binary, but that single binary acts like a large number of utilities. This allows BusyBox to be smaller since all the built-in utility programs can share code for many common operations. Please refer to https://www.busybox.net/downloads/BusyBox.html for usage of these commands.

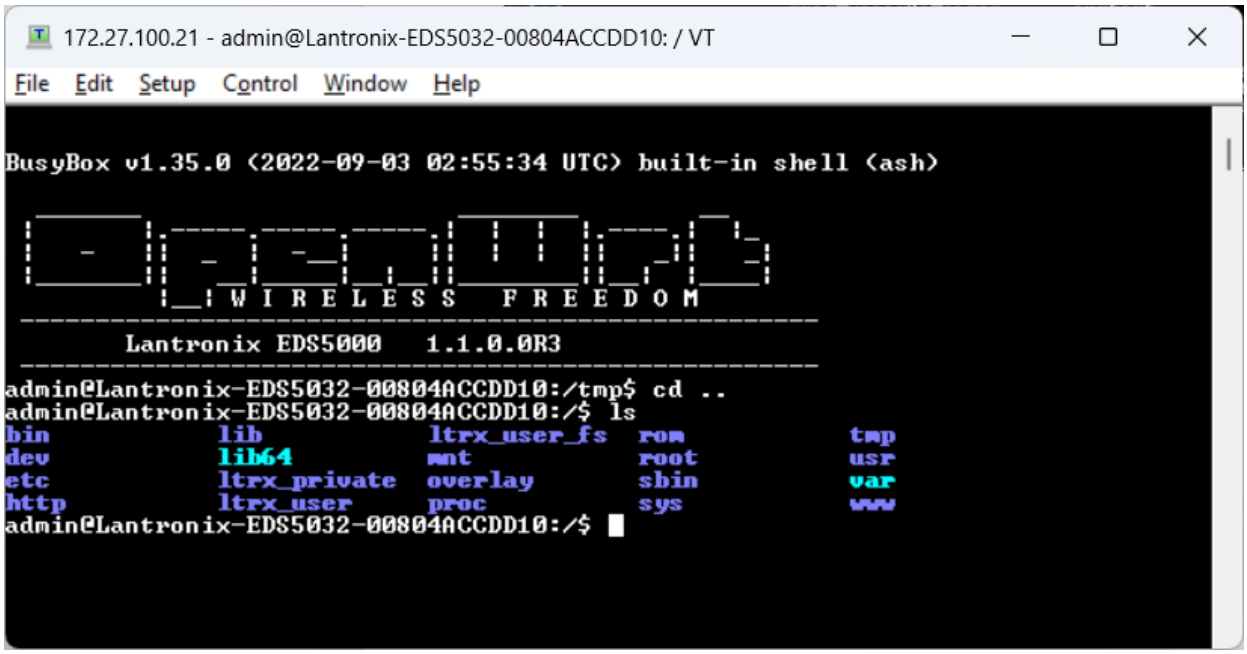
Note: Some configuration and commands may not be available on the EDS5000.

Bash Command Examples

ls

List directory contents

Examples




```
Lantronix EDS5000     1.1.0.0R7
admin@lantronix-EDS5032-00804ACCDD10:/tmp$ cd ..
admin@lantronix-EDS5032-00804ACCDD10:/$ ls
bin             lib               ltrx_user_fs      rom         tmp
dev             lib64             mnt               root        usr
etc             ltrx_private      overlay           sbin        var
http            ltrx_user         proc              sys         www
admin@lantronix-EDS5032-00804ACCDD10:/$
```

ifconfig

Configure a network interface

Example

To show information for eth1 interface:

```
admin@Lantronix-EDS5032-00804ACCDD10:/tmp$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:80:4A:CC:DD:10
          inet addr:172.27.100.27  Bcast:172.27.100.255  Mask:255.255.255.0
          inet6 addr: fe80::280:4aff:fecc:dd10/64 Scope:Link
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:1580763 errors:68 dropped:120112 overruns:0 frame:0
          TX packets:2095 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:140226881 (133.7 MiB)  TX bytes:402681 (393.2 KiB)
          Interrupt:43

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

usb0      Link encap:Ethernet  HWaddr E2:24:16:B0:42:33
          inet addr:192.168.100.10  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::e024:16ff:feb0:4233/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2085 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2691 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:710488 (693.8 KiB)  TX bytes:248719 (242.8 KiB)

admin@Lantronix-EDS5032-00804ACCDD10:/tmp$
```

ip

Replaces the older and now deprecated ifconfig command. The ip command can display and administer the network configuration of a system. It is used to view, add, and delete network interfaces, routing table entries, and IP addresses.

Example

To show current routing table:

```
admin@Lantronix-EDS5032-00804ACCDD10:/tmp$ ip route
default via 172.27.100.1 dev eth0  src 172.27.100.27
172.27.100.0/24 dev eth0 scope link  src 172.27.100.27
admin@Lantronix-EDS5032-00804ACCDD10:/tmp$
admin@Lantronix-EDS5016-00804ACCDD10:/tmp$ ip
BusyBox v1.35.0 (2022-09-03 02:55:34 UTC) multi-call binary.

Usage: ip [OPTIONS] address|route|link|neigh|rule [ARGS]

OPTIONS := -f[amily] inet|inet6|link | -o[neline]

ip addr add|del IFADDR dev IFACE | show|flush [dev IFACE] [to PREFIX]
ip route list|flush|add|del|change|append|replace|test ROUTE
ip link set IFACE [up|down] [arp on|off] [multicast on|off]
        [promisc on|off] [mtu NUM] [name NAME] [qlen NUM] [address MAC]
        [master IFACE | nomaster] [netns PID]
ip neigh show|flush [to PREFIX] [dev DEV] [nud STATE]
ip rule [list] | add|del SELECTOR ACTION
admin@Lantronix-EDS5016-00804ACCDD10:/tmp$
```

cat

Displays the contents of a file

Example

To show contents of a file:

```
# cat /etc/sysupgrade.conf
## This file contains files and directories that should
## be preserved during an upgrade.

# /etc/example.conf
# /etc/openvpn/
/etc/confdone
/etc/sysupgrade.conf
/etc/hwinfo.json
/ltrx_private/cfg/
/etc/board.json
```

logread

Displays logs for diagnostics and troubleshooting

Example

To show syslogd diagnostic logs

```
# logread
Mar 11 09:56:32 Lantronix-EDS5032-00804ACCDD10 user.err ltrx_mach10:
5595.5595 mach10.c:468 message: [Device credentials are not
configured]
Mar 11 09:57:12 Lantronix-EDS5032-00804ACCDD10 user.debug root:
mhcfgupdate tunnel2:wait
Mar 11 09:57:17 Lantronix-EDS5032-00804ACCDD10 user.debug root:
mhcfgupdate tunnel2:wait
Mar 11 09:57:18 Lantronix-EDS5032-00804ACCDD10 user.info
ltrx_mhcfgupdate: 3119.3119 mhcfgupdate.c:3209 The changes have been
written to Flash.
Mar 11 09:57:18 Lantronix-EDS5032-00804ACCDD10 user.notice Changed
Echo Commands to 'Disabled'. Changed Verbose Response to 'Disabled'.
Changed Response Type to 'Numeric'. Changed Error Unknown Commands to
'Enabled'. Changed Incoming Connection to 'Automatic'. Changed Connect
String to 'aaaa'. Changed Display Remote IP to 'Enabled'. WARNING:
Tunnel Connect Mode is not 'Modem Emulation'.
Mar 11 10:01:32 Lantronix-EDS5032-00804ACCDD10 user.warn ltrx_mach10:
5595.5595 mach10.c:7307 waiting for valid credentials
[00204A699MPVGET2ABL2ICE0KAQ00010]
Mar 11 10:16:32 Lantronix-EDS5032-00804ACCDD10 user.err ltrx_mach10:
5595.5595 mach10.c:468 message: [Device credentials are not
configured]
root@Lantronix-EDS5032-00804ACCDD10:/#
```

opkg Commands

The functionality of the system can be upgraded by downloading and installing pre-made packages from package repositories. The packages may be built using the SDK or hosted on the Lantronix package server (at updates.d2sphere.com).

opkg update

Update the packages list

opkg install

Install software package

opkg remove

Remove software package

Example

To update the packages list, install, and remove zerotier package:

```
# opkg update

# opkg install zerotier
Installing zerotier (1.4.6-1) to root...
Downloading
http://updates.d2sphere.com/G526RP/ipks/main/zerotier_1.4.6-
1_arm_arm926ej-s.ipk
Installing libminiupnpc (2.1.20190408-2) to root...
Downloading
http://updates.d2sphere.com/G526RP/ipks/main/libminiupnpc_2.1.20190408
-2_arm_arm926ej-s.ipk
Installing libnatpmp (20150609-1) to root...
Downloading
http://updates.d2sphere.com/G526RP/ipks/main/libnatpmp_20150609-
1_arm_arm926ej-s.ipk
Configuring libminiupnpc.
Configuring libnatpmp.
Configuring zerotier.
disabled in config

# opkg remove zerotier
Removing package zerotier from root...
```

Refer to https://openwrt.org/docs/guide-user/additional-software/opkg for opkg command usage.

The System > Software menu on the Web GUI of the EDS5000 provides methods to configure repositories and install software packages. See *Software* on *page 59*.

UCI Commands

Unified Configuration Interface (UCI) is a small utility written in C (a shell script-wrapper is available as well) and is intended to centralize the entire device configuration. UCI is the main configuration user interface for the most important system settings including the main network interface configuration, logging functionality, and remote access configuration.

Example

To change Percepxion client status update interval:

```
# uci get percepxion.Basic.Status_Update_Interval
1
# uci set percepxion.Basic.Status_Update_Interval=5
# uci commit percepxion
# /etc/init.d/percepxion reload
Changed Status Update Interval to '5 minutes'.
```

Please refer to: https://openwrt.org/docs/guide-user/base-system/uci for usage of the UCI commands.

Some configuration and commands may not be available on the device server.

```
admin@Lantronix-EDS5008-00804ACCDD33:/tmp$ uci get
percepxion.Basisc.Status.Update.Interval
uci: Parse error
admin@Lantronix-EDS5008-00804ACCDD33:/tmp$

admin@Lantronix-EDS5008-00804ACCDD33:/tmp$ uci get
Usage: uci [<options>] <command> [<arguments>]

Commands:
        batch
        export      [<config>]
        import      [<config>]
        changes     [<config>]
        commit      [<config>]
        add         <config> <section-type>
        add_list    <config>.<section>.<option>=<string>
        del_list    <config>.<section>.<option>=<string>
        show        [<config>[.<section>[.<option>]]]
        get         <config>.<section>[.<option>]
        set         <config>.<section>[.<option>]=<value>
        delete      <config>[.<section>[[.<option>][=<id>]]]
        rename      <config>.<section>[.<option>]=<name>
        revert      <config>[.<section>[.<option>]]
        reorder     <config>.<section>=<position>

admin@Lantronix-EDS5008-00804ACCDD33:/tmp$
```

Appendix F. Technical Support

Lantronix offers many resources to support our customers and products at http://www.lantronix.com/support.

For example, you can browse the knowledge base, open a support issue, find firmware downloads, view tutorials, and more. At this site you can also find FAQs, product bulletins, warranty information, extended support services, and product documentation.

To submit a support request, please use the Lantronix Technical Support portal at https://ltrxdev.atlassion.net/wiki/spaces/LTRXTS/overview (registration required).

To contact Lantronix Sales, look up your local office at https://www.lantronix.com/about-us/contact.