



# EDS-MD

## Wired IoT Gateway for Medical Devices

### User Guide

- ◆ EDS-MD 4
- ◆ EDS-MD 8
- ◆ EDS-MD 16

Part Number 900-591  
Revision N January 2020

---

## Intellectual Property

© 2020 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

*Lantronix*, *EDS-MD*, *MACH10*, and *TruPort* are registered trademarks of Lantronix, Inc. in the United States and other countries. *Lantronix Provisioning Manager* is a trademark of Lantronix, Inc.

Patented: [patents.lantronix.com](http://patents.lantronix.com); additional patents pending

*Windows* and *Internet Explorer* are registered trademarks of Microsoft Corporation. *Mozilla* and *Firefox* are registered trademarks of the Mozilla Foundation. *Chrome* is a trademark of Google Inc. *Safari* is a registered trademark of Apple Inc. All other trademarks and trade names are the property of their respective holders.

## Warranty

For details on the Lantronix warranty policy, please go to our web site at [www.lantronix.com/support/warranty](http://www.lantronix.com/support/warranty).

## Contacts

### Lantronix, Inc.

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

Toll Free: 800-526-8766  
Phone: 949-453-3990  
Fax: 949-453-3995

### Technical Support

Online: [www.lantronix.com/support](http://www.lantronix.com/support)

### Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at [www.lantronix.com/about/contact](http://www.lantronix.com/about/contact).

## Disclaimer

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.**

The EDS-MD wired IoT device gateway is not a medical device as such term is defined in the U.S. Food, Drug and Cosmetic Act, as amended, and is not subject to regulation by the U.S. Food and Drug Administration (FDA).

---

## Revision History

Date	Rev.	Comments
September 2011	A	Initial Document for firmware release 7.2.0.0.
October 2011	B	Updated power cord part number information.
November 2011	C	Updated ethernet port information and cover product image.
November 2011	D	Added Suppliers Declaration of Conformity document.
March 2013	E	Updated pinout diagrams and part number information.
March 2013	F	Updated revision and trademark information.
January 2014	G	Added RJ45 serial port image.
June 2014	H	Updated power rating information.
April 2015	I	Updated to firmware release 7.2.0.3 which includes the addition of Ethernet 2 and 3 functionality.
April 2017	J	Added wall mount information. Updated temperature and new certification information.
January 2019	K	Updated Compliance standards and Declaration of Conformity documents.
May 2019	L	Updated to firmware release 8.1.0.3 which includes the addition of the following: <ul style="list-style-type: none"><li>◆ Gateway port forwarding, static routes, and DHCP server</li><li>◆ Support for NTP in clock</li><li>◆ Support for Action settings</li><li>◆ Ethernet ports work separately</li><li>◆ MACH10 client</li></ul>
October 2019	M	Updated to firmware release 8.1.0.4, including Ethernet switch functionality. Updated product label and compliance information.
January 2020	N	Updated to include new default password.

# Table of Contents

Intellectual Property _____	2
Warranty _____	2
Contacts _____	2
Disclaimer _____	2
Revision History _____	3
<b>Table of Contents</b>	<b>4</b>
List of Figures _____	11
List of Tables _____	12
<b>1: Using This Guide</b>	<b>14</b>
Purpose and Audience _____	14
Summary of Chapters _____	14
Safety Information _____	15
Cover _____	15
Power Plug _____	15
Input Supply _____	16
Grounding _____	16
Fuses _____	16
Battery _____	16
Wall Mounting _____	16
Port Connections _____	16
WARNINGS OF NETWORK CONNECTIONS _____	17
Equipment Classifications _____	17
Environmental Conditions for Transportation and Storage _____	17
Cleaning Instructions _____	17
Electromagnetic Interference _____	18
Additional Documentation _____	18
<b>2: Introduction</b>	<b>19</b>
Key Features _____	19
Applications _____	19
Protocol Support _____	19
Troubleshooting Capabilities _____	20
Configuration Methods _____	20
Addresses and Port Numbers _____	20
Hardware Address _____	20
IP Address _____	21
Port Numbers _____	21
Product Information Label _____	21

---

<b>3: Installation of EDS-MD Gateways</b>	<b>22</b>
Package Contents _____	22
User-Supplied Items _____	22
Identifying Hardware Components _____	22
Serial Ports _____	23
Ethernet Port _____	23
LEDs _____	25
Reset to Default Button _____	26
Technical Specification _____	26
Installing the EDS-MD _____	27
Finding a Suitable Location _____	27
Connect the EDS-MD to one or more serial devices _____	27
Wall Mounting Instructions _____	28
For Installations to Walls Requiring Anchors _____	28
For Installations to Walls Not Requiring Anchors _____	29
<b>4: Using Lantronix Provisioning Manager</b>	<b>31</b>
Installing Lantronix Provisioning Manager _____	31
Accessing the EDS-MD Using Lantronix Provisioning Manager _____	31
<b>5: Configuration Using Web Manager</b>	<b>32</b>
Accessing Web Manager _____	32
Device Status Page _____	32
Web Manager Components _____	34
Navigating Web Manager _____	35
<b>6: Network Settings</b>	<b>37</b>
Network 1 (eth0) Status _____	37
Network 1 (eth0) Interface Settings _____	37
To Configure Network 1 (eth0) Interface Settings _____	38
Network 1 (eth0) Link Settings _____	39
To Configure Network 1 (eth0) Link Settings _____	39
Network 2 (eth1) and Network 3 (eth2) Status _____	40
Network 2 (eth1) and Network 3 (eth2) Interface Settings _____	40
To Configure Network 2 (eth1) and Network 3 (eth2) Interface Settings _____	40
Network 2 (eth1) and Network 3 (eth2) Link Settings _____	41
To Configure Network 2 (eth1) and Network 3 (eth2) Link Settings _____	41
Gateway _____	41
Status _____	41
WAN _____	42
To Configure Gateway WAN Settings _____	42
Port Forwarding _____	43

---

To Configure Gateway Port Forwarding Settings _____	44
Static Routes _____	44
To Configure Gateway Static Route Settings _____	45
DHCP Server _____	45
To Configure Gateway DHCP Server Settings _____	45
Static Lease Listing _____	46
<b>7: Action Settings</b>	<b>47</b>
Alarms and Reports _____	47
Actions _____	47
To Configure Action Settings _____	48
<b>8: Line and Tunnel Settings</b>	<b>49</b>
Line Statistics _____	49
Line Settings _____	49
To Configure Line Settings _____	49
To Configure Line Command Mode _____	51
Tunnel Statistics _____	52
To View Tunnel Statistics _____	52
Tunnel Settings _____	52
Serial Settings _____	52
To Configure Tunnel Serial Settings _____	53
Packing Mode _____	53
To Configure Tunnel Packing Mode Settings _____	54
Accept Mode _____	54
To Configure Tunnel Accept Mode Settings _____	56
Connect Mode _____	56
Connecting Multiple Hosts _____	59
Host List Promotion _____	60
Disconnect Mode _____	60
To Configure Tunnel Disconnect Mode Settings _____	60
Modem Emulation _____	61
To Configure Tunnel Modem Emulation Settings _____	61
<b>9: Terminal and Host Settings</b>	<b>62</b>
Terminal Settings _____	62
To Configure the Terminal Network Connection _____	63
To Configure the Terminal Line Connection _____	63
Host Configuration _____	63
To Configure Host Settings _____	64
<b>10: Network Services</b>	<b>65</b>

---

DNS Settings _____	65
To View or Configure DNS Settings: _____	65
FTP Settings _____	65
To Configure FTP Settings _____	66
Syslog Settings _____	66
To View or Configure Syslog Settings _____	67
HTTP Settings _____	67
To Configure HTTP Settings _____	68
To Configure HTTP Authentication _____	69
RSS Settings _____	69
To Configure RSS Settings _____	70
Discovery _____	70
To Configure Discovery _____	70
SMTP Settings _____	71
To Configure SMTP Settings _____	71
Email Settings _____	71
To View, Configure, and Send Email _____	72

## **11: Security Settings 73**

Public Key Infrastructure _____	73
TLS (SSL) _____	73
Digital Certificates _____	74
Trusted Authorities _____	74
Obtaining Certificates _____	74
Self-Signed Certificates _____	74
Certificate Formats _____	74
OpenSSL _____	75
Steel Belted RADIUS _____	75
Free RADIUS _____	75
SSH Settings _____	76
SSH Server Host Keys _____	76
SSH Client Known Hosts _____	77
SSH Server Authorized Users _____	77
SSH Client Users _____	78
To Configure SSH Settings _____	79
SSL Settings _____	79
Create a New Credential _____	79
To Create a New Credential _____	80
Upload Certificate _____	80
Certificate and Key Generation _____	81
To Configure an Existing SSL Credential _____	81
Trusted Authorities _____	82

---

## 12: Maintenance and Diagnostics Settings 84

Filesystem Settings _____	84
Statistics _____	84
To View Statistics _____	84
File Display _____	84
To Display Files _____	85
File Modification _____	85
File Transfer _____	85
To Transfer or Modify Filesystem Files _____	86
Protocol Stack Settings _____	86
IP Settings _____	87
To Configure IP Protocol Stack Settings _____	87
ICMP Settings _____	87
To Configure ICMP Protocol Stack Settings _____	87
To View ICMP Protocol Stack Settings _____	88
ARP Settings _____	88
To Configure ARP Network Stack Settings _____	88
SMTP Settings _____	89
To Configure SMTP Protocol Stack Settings _____	89
Diagnostics _____	89
Hardware _____	89
To View Hardware Information _____	89
IP Sockets _____	89
To View the List of IP Sockets _____	90
Ping _____	90
To Ping a Remote Host _____	90
Traceroute _____	90
To Perform a Traceroute _____	91
Log _____	91
To Configure the Diagnostic Log Output _____	91
Memory _____	92
To View Memory Usage _____	92
Processes _____	92
To View Process Information _____	92
Threads _____	92
To View Thread Information _____	93
Clock _____	93
To Specify Clock Setting Method _____	93
System Settings _____	93
To Reboot or Restore Factory Defaults _____	94

## 13: Management Interface Settings 95

---

Command Line Interface Settings _____	95
Basic CLI Settings _____	95
To View and Configure Basic CLI Settings _____	95
Telnet Settings _____	95
To Configure Telnet CLI Settings _____	96
SSH CLI Settings _____	96
To Configure SSH Settings _____	96
XML Settings _____	97
XML: Export Configuration _____	97
To Export Configuration in XML Format _____	98
XML: Export Status _____	98
To Export in XML Format _____	98
XML: Import Configuration _____	99
To Import Configuration in XML Format _____	99
<b>14: MACH10 Client Settings _____</b>	<b>100</b>
MACH10 Client _____	100
To Configure MACH10 Client _____	100
Line Configuration _____	101
To Configure MACH10 Line _____	101
To Configure MACH10 _____	102
<b>15: Updating Firmware _____</b>	<b>103</b>
Obtaining Firmware _____	103
Loading New Firmware through Web Manager _____	103
Loading New Firmware through FTP _____	104
<b>16: Branding the EDS-MD Gateway _____</b>	<b>105</b>
Web Manager Customization _____	105
Short and Long Name Customization _____	105
To Customize Short or Long Names _____	106
<b>Appendix A: Lantronix Technical Support _____</b>	<b>107</b>
<b>Appendix B: Binary to Hexadecimal Conversions _____</b>	<b>108</b>
Converting Binary to Hexadecimal _____	108
Conversion Table _____	108
Scientific Calculator _____	108
<b>Appendix C: Compliance _____</b>	<b>110</b>

---

<b>Appendix D: Lantronix Power Cords, Cables, Adapters and Serial Port Pinouts</b>	<b>114</b>
Cables and Adapters _____	114
Adapters and Serial Port Pinouts _____	115

## List of Figures

Figure 2-1 EDS-MD Unit Product Label	21
Figure 3-1 Front View of the EDS-MD 16	23
Figure 3-2 Back View of the EDS-MD 4, EDS-MD 8 and EDS-MD 16	23
Figure 3-3 RJ45 Serial Port	23
Figure 3-4 EDS-MD Ethernet Switch in a Sample Hospital Record System	24
Figure 3-8 EDS-MD Dimensions	28
Figure 3-9 Mounting Screws Included with the EDS-MD in Inches	29
Figure 3-10 Mounting the EDS-MD	30
Figure 5-1 Device Status Page	33
Figure 5-2 Components of the Web Manager Page	34
Figure 15-1 Uploading New Firmware	103
Figure B-2 Windows Scientific Calculator	109
Figure B-3 Hexadecimal Values in the Scientific Calculator	109
Figure C-3 Suppliers Declaration of Conformity	111
Figure C-4 EU Declaration of Conformity	112
Figure D-2 RJ45 Pinout Diagram	115
Figure D-3 RJ45 Receptacle to DB25M DTE Adapter (PN 200.2066A)	115
Figure D-4 RJ45 Receptacle to DB25M DCE Adapter (PN 200.2073)	116
Figure D-5 RJ45 Receptacle to DB25F DTE Adapter (PN 200.2067A )	116
Figure D-6 RJ45 Receptacle to DB25F DCE Adapter (PN 200.2074)	117
Figure D-7 RJ45 Receptacle to DB9M DTE Adapter (PN 200.2069A)	117
Figure D-8 RJ45 Receptacle to DB9M DCE Adapter (PN 200.2071)	118
Figure D-9 RJ45 Receptacle to DB9F DTE Adapter (PN 200.2070A)	118
Figure D-10 RJ45 Receptacle to DB9F DCE Adapter (PN 200.2072)	119

## List of Tables

Table 3-5 System LEDs on the Top of EDS-MD	25
Table 3-6 Serial Indicator LEDs on the Top of EDS-MD	25
Table 3-7 RJ45 LEDs on the Back Panel (Ethernet Indicators).	25
Table 5-3 Web Manager Pages	35
Table 6-1 Network 1 (eth0) Interface Settings	37
Table 6-2 Network 1 (eth0) Link Settings	39
Table 6-3 Network 2 (eth1) and Network 3 (eth2) Interface Settings	40
Table 6-4 Network 2 (eth1) and Network 3 (eth2) Link Settings	41
Table 6-5 WAN Configuration	42
Table 6-6 Port Forwarding Rules List	43
Table 6-7 Adding a New Port Forwarding Rule	43
Table 6-8 Static Route Setting Routes	44
Table 6-9 Adding a New Static Route	44
Table 6-10 DHCP Settings	45
Table 6-11 Static Lease Listing	46
Table 6-12 Add a Static Lease	46
Table 7-1 Action Settings	47
Table 8-1 Line Configuration Settings	50
Table 8-2 Line Command Mode Settings	51
Table 8-3 Tunnel Serial Settings	52
Table 8-4 Tunnel Packing Mode Settings	53
Table 8-5 Tunnel Accept Mode Settings	55
Table 8-6 Tunnel Connect Mode Settings	57
Table 8-7 Tunnel Disconnect Mode Settings	60
Table 8-8 Tunnel Modem Emulation Settings	61
Table 9-1 Terminal on Network and Line Settings	62
Table 9-2 Host Configuration	63
Table 10-1 DNS Settings	65
Table 10-2 FTP Settings	66
Table 10-3 Syslog Settings	66
Table 10-4 HTTP Settings	67
Table 10-5 HTTP Authentication Settings	68
Table 10-6 RSS Settings	69
Table 10-7 Discovery Settings	70
Table 10-8 SMTP Settings	71
Table 10-9 Email Configuration	71

---

Table 11-1 SSH Server Host Keys	76
Table 11-2 SSH Client Known Hosts	77
Table 11-3 SSH Server Authorized Users	77
Table 11-4 SSH Client Users	78
Table 11-5 Create New Keys	78
Table 11-6 Create a New Credentials	80
Table 11-7 Upload Certificate Settings	80
Table 11-8 Certificate and Key Generation Settings	81
Table 12-1 File Statistics	84
Table 12-2 File Display Settings	84
Table 12-3 File Modification Settings	85
Table 12-4 File Transfer Settings	85
Table 12-5 IP Protocol Stack Settings	87
Table 12-6 ICMP Protocol Stack Settings	87
Table 12-7 ARP Protocol Stack Settings	88
Table 12-8 SMTP Protocol Stack Settings	89
Table 12-9 Ping Settings	90
Table 12-10 Traceroute Settings	91
Table 12-11 Log Settings	91
Table 12-12 Clock Settings	93
Table 12-13 System Settings	94
Table 13-1 CLI Configuration Settings	95
Table 13-2 Telnet Settings	96
Table 13-3 SSH Settings	96
Table 13-4 XML Exporting Configuration	97
Table 13-5 Exporting Status	98
Table 13-6 Import Configuration from Filesystem Settings	99
Table 14-1 MACH10 Client Status	100
Table 14-1 MACH10 Client Configuration	100
Table 14-2 MACH10 Connection 1 Configuration	101
Table 14-2 MACH10 Line Configuration	101
Table 16-1 Short and Long Name Settings	106
Table B-1 Binary to Hexadecimal Conversion	108
Table C-1 Applicable Medical Standards	110
Table C-2 Applicable ITE Standards	110
Table D-1 Lantronix Cables and Adapters	114

# 1: Using This Guide

## Purpose and Audience

This guide provides the information needed to configure, use, and update the Lantronix® EDS-MD® wired IoT device gateways for medical devices. It offers the following models: EDS-MD 4, EDS-MD 8 and EDS-MD 16. It is intended for system integrators who are installing this product into their designs.

**Note:** EDS-MD wired IoT device gateways for medical devices are commonly referred to as either EDS-MD 4/8/16 or as EDS-MD when mentioned within a description equally applicable to any of the three models.

## Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
<a href="#">2: Introduction</a>	Main features of the product and the protocols it supports. Includes technical specifications.
<a href="#">3: Installation of EDS-MD Gateways</a>	Instructions for installing the EDS-MD.
<a href="#">4: Using Lantronix Provisioning Manager</a>	Instructions for using Lantronix Provisioning Manager to detect the device and perform configuration.
<a href="#">5: Configuration Using Web Manager</a>	Instructions for accessing Web Manager and using it to configure settings for the device.
<a href="#">6: Network Settings</a>	Instructions for configuring network settings.
<a href="#">7: Action Settings</a>	Instructions for configuring alarms
<a href="#">8: Line and Tunnel Settings</a>	Instructions for configuring line and tunnel settings.
<a href="#">9: Terminal and Host Settings</a>	Instructions for configuring terminal and host settings.
<a href="#">10: Network Services</a>	Instructions for configuring DNS, FTP, HTTP and Syslog settings.
<a href="#">11: Security Settings</a>	Instructions for configuring SSL security settings.
<a href="#">12: Maintenance and Diagnostics Settings</a>	Instructions EDS-MD to view statistics, files, and diagnose problems.
<a href="#">13: Management Interface Settings</a>	Instructions for configuring CLI and XML settings.
<a href="#">14: MACH10 Client Settings</a>	Instructions for configuring MACH10 client and line settings
<a href="#">15: Updating Firmware</a>	Instructions for obtaining and updating the latest firmware for the EDS-MD device.
<a href="#">16: Branding the EDS-MD Gateway</a>	Instructions on how to brand your device.
<a href="#">Appendix A: Lantronix Technical Support</a>	Instructions for contacting Lantronix Technical Support.
<a href="#">Appendix B: Binary to Hexadecimal Conversions</a>	Instructions for converting binary values to hexadecimals.
<a href="#">Appendix C: Compliance</a>	Lantronix compliance information.

Chapter (continued)	Description
<a href="#">Appendix D: Lantronix Power Cords, Cables, Adapters and Serial Port Pinouts</a>	Information about the device driver for Windows host.

## Safety Information

This section describes the safety precautions that should be followed when installing and operating the EDS-MD.

### Warning:

- ◆ ***This equipment is not suitable for use in the presence of a flammable anesthetic mixture including air, oxygen or nitrous oxide. To avoid the risk of electric shock, this equipment must only be connected to a supply mains with protective earth.***
- ◆ ***The EDS-MD is not to be used in life support or as a life sustaining product.***
- ◆ ***No modification of this equipment is allowed.***

### Cover



**Warning:** *Do not remove the cover of the EDS-MD wired IoT device gateway. There are no user-serviceable parts inside. Opening or removing the cover may expose you to dangerous voltage that could cause fire or electric shock. Do not operate the EDS-MD if the housing is broken.*

**Note:** *Refer all servicing to Lantronix.*

### Power Plug

- ◆ When disconnecting the power cord from the socket, pull on the plug, not the cord.
- ◆ Always connect the power cord to a properly wired and grounded power source. Do not use adapter plugs or remove the grounding prong from the cord.
- ◆ Only use a power cord with a voltage and current rating greater than the voltage and current rating marked on the unit.
- ◆ The appliance inlet serves as the main supply disconnect. Do not position the EDS-MD in such a way that it is difficult to the disconnect EDS-MD.

### Note:

- ◆ Install the unit near an AC outlet that is easily accessible.
- ◆ Always connect any equipment used with the product to properly wired and grounded power sources.
- ◆ To help protect the product from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- ◆ Do not connect or disconnect this product during an electrical storm.

## Input Supply

- ◆ Check nameplate ratings to assure there is no overloading of supply circuits that could affect over current protection and supply wiring.

## Grounding

- ◆ Maintain reliable grounding of this product.
- ◆ Pay particular attention to supply connections when connecting to power strips, rather than directly to the branch circuit.

## Fuses

There are fuses on the internal power supply serviceable only by Lantronix.

## Battery

A Lithium battery cell inside the unit maintains the unit's date and time when the device is powered off. **Do not attempt to replace it.** The battery is serviceable only by Lantronix.

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

### Attention

***IL Y A DANGER D'EXPLOSION S'IL Y A REMPLACEMENT INCORRECT DE LA BATTERIE, REMPLACER UNIQUEMENT AVEC UNE BATTERIE DU MÊME TYPE OU D'UN TYPE ÉQUIVALENT RECOMMANDÉ PAR LE CONSTRUCTEUR. METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÉMENT AUX INSTRUCTIONS DU FABRICANT.***

## Wall Mounting

If wall-mounted units are installed, the following items must be considered:

- ◆ Do not install the unit in such a way that a hazardous stability condition results because of uneven loading. A drop or fall could cause injury.
- ◆ Make sure to install the EDS-MD unit in an environment with an ambient temperature less than the maximum operating temperature of the EDS-MD device. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T<sub>ma</sub>) specified by the manufacturer.
- ◆ Maintain reliable earthing of wall-mounted equipment. Give particular attention to supply connections other than direct connections to the branch circuit (e.g. use of power strips) because of the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

**Note:** *Before operating the EDS-MD device, make sure the device mounting is secured.*

## Port Connections

- ◆ Only connect the network port to an Ethernet network that supports 10 Base-T/100 Base-TX/1000 Base-T.

- ◆ Only connect device ports to equipment with serial ports that support EIA-232 (formerly RS-232C). Unless specified otherwise, only connect USB ports to USB thumb drives.

**Warning:** *To avoid overloading and overheating, do not use a USB port as a charger port or a power port for other devices such as a cellular phone, PDA device, disk drive, etc.*

## WARNINGS OF NETWORK CONNECTIONS

The integration of the EDS-MD wired IoT device gateway into an IT network may constitute a Medical Electrical (ME) System. It is recommended that the system leakage current be measured to verify that the basic requirement for the safety of the ME System, after installation or subsequent modification of the system, does not result in an unacceptable risk.

The integration of the EDS-MD into a IT network may result in unforeseen risks associated with the interconnection of the EDS-MD Programmable Electronic Subsystem (PESS)/Programmable Electrical Medical Systems (PEMS) to IT Networks. Connection of equipment containing PEMS to an IT NETWORK/DATA COUPLING that includes other equipment could result in previously unidentified risks to patients, operators or third parties. The entity accountable for the use and maintenance of an ME EQUIPMENT or an ME SYSTEM should identify, analyze, evaluate and control these RISKS. Subsequent changes to the IT NETWORK/DATA COUPLING could introduce new RISKS and require additional analysis. Changes to the IT NETWORK/DATA COUPLING include:

- ◆ Changes in NETWORK/DATA COUPLING configuration
- ◆ Connection of additional items to the IT NETWORK/DATA COUPLING
- ◆ Disconnecting items from the IT NETWORK/DATA COUPLING
- ◆ Update of equipment connected to the IT NETWORK/DATA COUPLING
- ◆ Upgrade of equipment connected to the IT NETWORK/DATA COUPLING

## Equipment Classifications

- ◆ Classification according to the type of protection against electric shock: Class I Equipment
- ◆ Classification according to the degree of protection against electric shock: No Applied Parts
- ◆ Classification according to the degree of protection against ingress of water: IP20
- ◆ Classification according to the mode of operation: Continuous Operation

## Environmental Conditions for Transportation and Storage

- ◆ An ambient temperature range of -30°C to +80°C
- ◆ A relative humidity range of 0% to 95%, noncondensing
- ◆ An atmospheric pressure range of 50 kPa to 106 kPa

## Cleaning Instructions

1. Disconnect all cables and unplug AC power cord from the device.
2. Prepare a disinfectant solution using 1 part bleach mixed with 9 parts water.
3. Lightly moisten a tissue with the mild detergent and wipe down only the outside of the device.
4. Allow the device to air-dry or wipe dry with a clean dry tissue before use.

**Caution:** *To avoid electric shock and for the device to work properly, do not allow cleaning solution to get inside the device, specifically the interface port connectors or the power inlet. Do not immerse the device in any liquid.*

## Electromagnetic Interference

This equipment has been tested and found to comply with the EMC limits for the Medical Device Directive 93/42/EEC (EN 55022 Class A and EN 60601-1-2). These limits are designed to provide reasonable protection against harmful interference in a typical medical installation. The equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to other devices in the vicinity. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference with other devices, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ◆ Reorient or relocate the receiving device
- ◆ Increase the separation between the equipment
- ◆ Connect the equipment into an outlet on a circuit different from that to which the other device(s) is connected
- ◆ Consult the manufacturer or field service technician for help

## Additional Documentation

Visit the Lantronix Web site at [www.lantronix.com/products/eds-md/](http://www.lantronix.com/products/eds-md/) for the latest documentation and the following additional documentation.

Document	Description
<b>EDS-MD Wired IoT Device Gateway Command Reference</b>	Instructions for accessing Command Mode (the command line interface) using a Telnet connection, SSH connection or through the serial port. Detailed information about the commands. Also provides details for XML configuration and status.
<b>EDS-MD Wired IoT Device Gateway Quick Start</b>	Instructions for getting the EDS-MD device up and running.
<b>Com Port Redirector Quick Start and Online Help</b>	Instructions for using the Windows operating system-based utility to create virtual com ports.
<b>Lantronix Provisioning Manager User Guide</b>	Instructions for using Lantronix Provisioning Manager to discover, configure, upgrade, and manage an EDS-MD 4/8/16 wired IoT device gateway.
<b>Secure Com Port Redirector User Guide</b>	Instructions for using the Windows operating system-based utility to create secure virtual com ports.

## 2: Introduction

The EDS-MD wired IoT device gateway is a complete network-enabling solution. This gateway allows system integrators and administrators to go to market quickly and easily with Ethernet networking and web server capabilities. EDS-MD models are available in 4, 8 and 16 port configurations.

### Key Features

- ◆ **Power Supply:** Direct plug-in to wall AC with universal 100-240 VAC input.
- ◆ **Controller:** 32-bit ARM11 microprocessor running at 600 megahertz
- ◆ **Memory:** 64 megabit Flash, 2 gigabit DDR2 DRAM, and a 4 gigabyte SDHC card (internal only-not user replaceable).
- ◆ **Ethernet:** Gigabit Ethernet support (10/100/1000Base-T) speed auto-sensing, automatic MDI/MDIX (straight and cross-over cables are OK to use)
- ◆ **Serial Ports:** 4 to 16 ports depending on model (EDS-MD 4, EDS-MD 8 or EDS-MD 16), electrically isolated from one another and other circuits. Hardware/Software handshaking capability. Custom/standard baud rates up to 921600 bits per second (bps).
- ◆ **USB Ports:** 2 ports of fixed full-speed 2.0 USB Host, electrically isolated from one another and other circuits, capable of providing 0.5A each.
- ◆ **Temperature Range:** 0°C to +50°C (32° to 122°F).

### Applications

The EDS-MD 4, EDS-MD 8 and EDS-MD 16 wired IoT device gateways are suitable for these application scenarios:

- ◆ Patient Monitoring Devices
- ◆ Glucose Analyzers
- ◆ Infusion Pumps

### Protocol Support

The EDS-MD wired IoT device gateways contain a full-featured IP networking stack:

- ◆ ARP, UDP, TCP, ICMP, DHCP, Auto IP, Telnet, SMTP, DNS, FTP, TFTP, SSH, SSL, and Syslog for network communications and management.
- ◆ TCP, UDP and tunneling to the serial port.
- ◆ TFTP for uploading/downloading files.
- ◆ FTP, SFTP, HTTPS and HTTP for firmware upgrades and uploading/downloading files.

---

## Troubleshooting Capabilities

The EDS-MD wired IoT device gateways offer a comprehensive diagnostic toolset that lets you troubleshoot problems quickly and easily. Available from the CLI or Web Manager, the diagnostic tools let you:

- ◆ View critical hardware, memory, buffer pool, IP socket information and routing table
- ◆ Perform ping and traceroute operations
- ◆ Conduct forward or reverse DNS lookup operations
- ◆ View all processes currently running on the EDS-MD 4, EDS-MD 8 and EDS-MD 16 wired IoT device gateway including CPU utilization
- ◆ View system log messages

## Configuration Methods

After installation, the EDS-MD unit requires configuration. For the unit to operate correctly on a network, it must have a unique IP address on the network. There are four basic methods for logging into the EDS-MD 4/8/16 wired IoT device gateway and assigning IP addresses and other configurable settings:

- ◆ **Web Manager:** View and configure all settings easily through a web browser using the Lantronix Web Manager. (See [Configuration Using Web Manager on page 32.](#))
- ◆ **Lantronix Provisioning Manager:** Upgrade firmware and update configuration on the EDS-MD 4/8/16 wired IoT device gateway using a Graphical User Interface (GUI) on a PC attached to a network. You will need the latest version of the Lantronix Provisioning Manager utility. (See [Using Lantronix Provisioning Manager on page 31.](#))
- ◆ **Command Mode:** There are a few methods for accessing Command Mode (CLI): making a Telnet connection, or connecting a PC or other host running a terminal emulation program to the unit's port. (See the *EDS-MD Wired IoT Device Gateway Command Reference* for instructions and available commands.)
- ◆ **XML:** The EDS-MD 4/8/16 wired IoT device gateway supports XML-based configuration and setup records that make device configuration transparent to users and administrators. XML is easily editable with a standard text or XML editor. (See the *EDS-MD Wired IoT Device Gateway Command Reference* for instructions and commands).

## Addresses and Port Numbers

### Hardware Address

The hardware address is also referred to as the Ethernet address, physical address, or MAC address. The first three bytes of the Ethernet address are fixed and identify the unit as a Lantronix product. The fourth, fifth, and sixth bytes are unique numbers assigned to each unit. Sample hardware address:

- ◆ 00-80-4A-14-1B-18
- ◆ 00:80:4A:14:1B:18

## IP Address

Every device connected to an IP network must have a unique IP address. This address references the specific unit.

## Port Numbers

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

The following is a list of the default server port numbers running on the EDS-MD 4/8/16 wired IoT device gateway:

- ◆ TCP Port 23: Telnet Server (Command Mode configuration)
- ◆ TCP Port 80: HTTP (Web Manager Configuration)
- ◆ TCP Port 21: FTP
- ◆ UDP Port 30718: LDP (Lantronix Discovery Protocol) port
- ◆ TCP/UDP Port 10001: Tunnel 1 (see note below)

**Note:** Additional TCP/UDP ports and tunnels will be available, depending on the product type. The default numbering of each additional TCP/UDP port and corresponding tunnel will increase sequentially (i.e., TCP/UDP Port 1000X: Tunnel X).

## Product Information Label

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

- ◆ Part Number
- ◆ Serial Number (MAC Address)
- ◆ Country of Origin
- ◆ Product Revision
- ◆ Manufacturing Date Code
- ◆ MACH10 Device ID

**Note:** The hardware address on the label is also the product serial number. The hardware address on the label is the address for the Ethernet (eth0) interface.



## 3: Installation of EDS-MD Gateways

This chapter describes how to install the EDS-MD 4, EDS-MD 8 and EDS-MD 16 wired IoT device gateways.

### Package Contents

Your EDS-MD package includes the following items:

- ◆ One EDS-MD wired IoT device gateway (an EDS-MD 4, EDS-MD 8 or EDS-MD 16)
- ◆ One RJ45 CAT 5E cable (part number 500-207-R) for network connection
- ◆ One RJ45 cable loopback adapter (part number 500-153)
- ◆ *EDS-MD Wired IoT Device Gateway Quick Start Guide*

**Note:** Power cords designed for the EDS-MD are sold separately. Refer to [Table D-1](#) for a list of power cords.

### User-Supplied Items

To complete installation of your EDS-MD wired IoT device gateway, you need the following items:

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

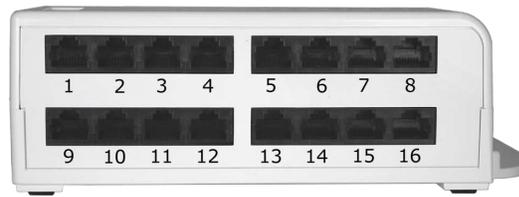
**Note:** To connect the serial port of an EDS-MD wired IoT device gateway to a DTE device, you need a DTE cable, such as the one supplied with your EDS-MD package, or an RJ45 patch cable and DTE adapter. To connect the serial port of the EDS-MD wired IoT device gateway to a DCE device, you need a DCE (modem) cable, or an RJ45 patch cable and DCE adapter. For a list of the Lantronix cables and adapters you can use with the EDS-MD, see the [Appendix D: Lantronix Power Cords, Cables, Adapters and Serial Port Pinouts](#) on page 114.

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

### Identifying Hardware Components

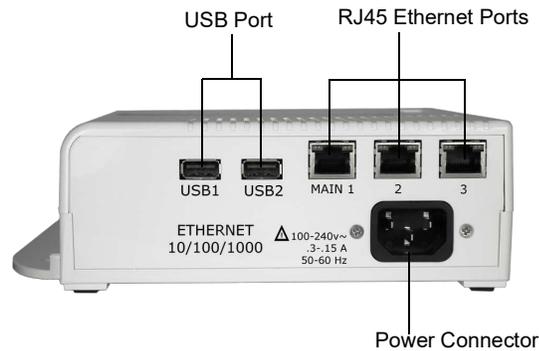
[Figure 3-1](#) shows the front of the EDS-MD 16. [Figure 3-2](#) shows the back of the EDS-MD 4, EDS-MD 8 or EDS-MD 16.

Figure 3-1 Front View of the EDS-MD 16



**Note:** EDS-MD 4 has 4 RJ45 Serial Ports and EDS-MD 8 has 8 RJ45 Serial Ports.

Figure 3-2 Back View of the EDS-MD 4, EDS-MD 8 and EDS-MD 16



### Serial Ports

In the front of the device, the EDS-MD 4 has 4 serial ports, the EDS-MD 8 has 8 serial ports, and the EDS-MD 16 has 16 serial ports. All are configured as DTE and support up to 921600 baud.

### Ethernet Port

The back panel of the EDS-MD 4/8/16 provides a network interface via the “Main 1” RJ45 port. This port can connect to an Ethernet network at 10/100/1000Base-T. The Speed LED on the back of the EDS-MD shows the connection of the attached Ethernet network. The EDS-MD 4/8/16 can be configured to operate at a fixed Ethernet speed and duplex mode (half- or full-duplex). Otherwise by default, the EDS-MD auto-negotiates the connection to the Ethernet network.

**Note:** Additional Ethernet interfaces can be enabled through the Ethernet switching function. The EDS-MD switch includes one Ethernet uplink connection and two downlink connections. See [Figure 3-4](#) for an example demonstrating a sample network topology and constraints.

Figure 3-3 RJ45 Serial Port

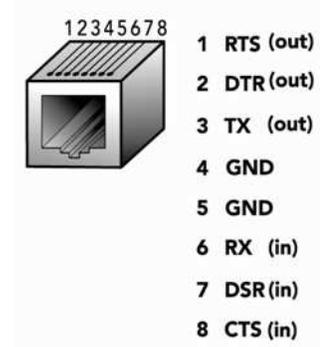
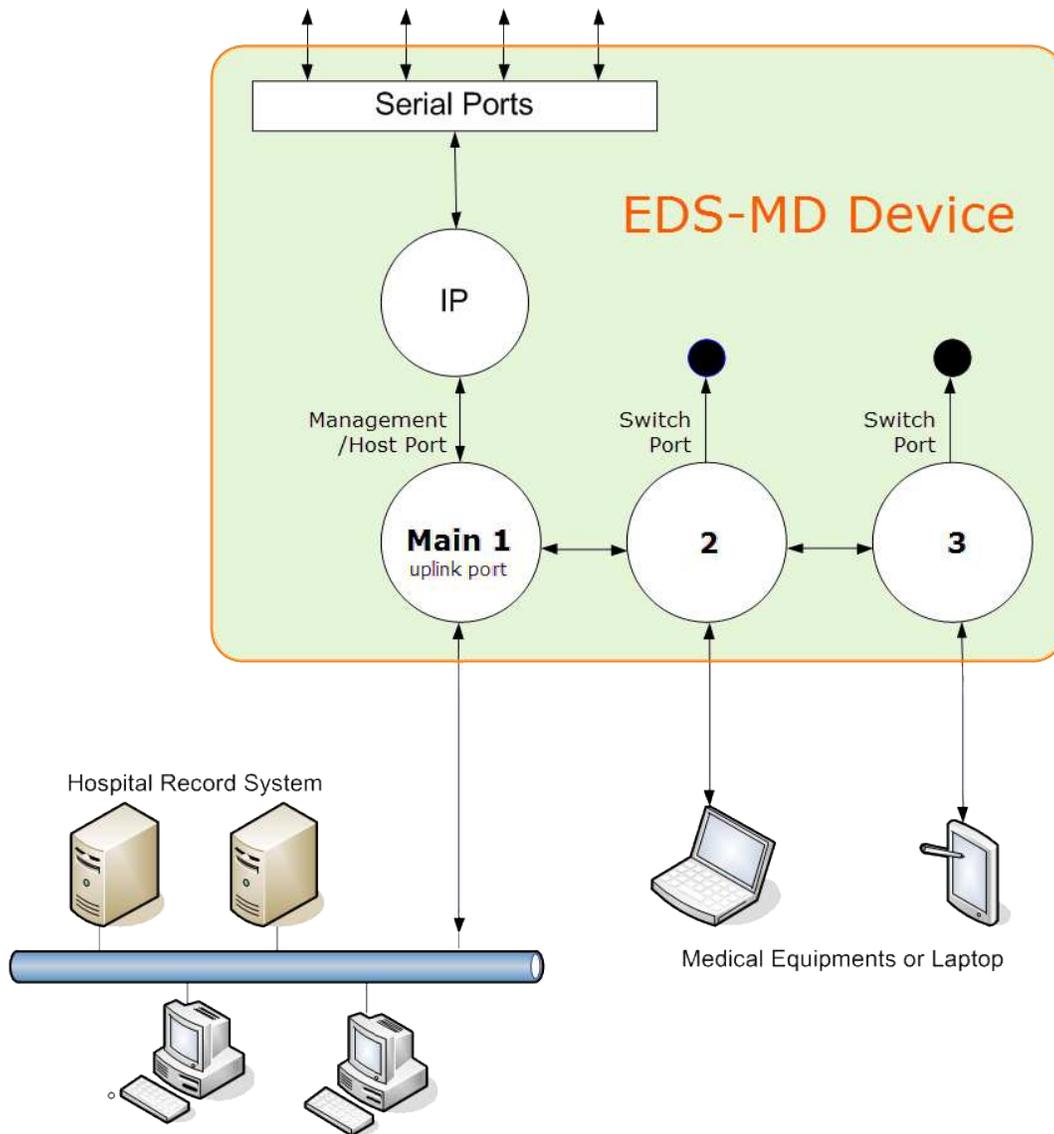


Figure 3-4 EDS-MD Ethernet Switch in a Sample Hospital Record System



- (1) Single IP only
- (2) The EDS-MD device server can only be managed through the management port (**Main 1**)
- (3) Devices attached to **switch port 2** or **3** can communicate with the hospital record system
- (4) Devices attached to **switch port 2** and **3** cannot access EDS-MD device applications

## LEDs

Light-emitting diodes (LEDs) on the EDS-MD show status information.

- ◆ Each serial port has a corresponding status LED.
- ◆ The Ethernet port LEDs indicate Speed, Activity, Power, and Status.

The tables below describe the LEDs on the EDS-MD 4, EDS-MD 8 or EDS-MD 16.

**Table 3-5 System LEDs on the Top of EDS-MD**

LED	Description
Steady Green	Unit operational.
Off	Unit powered down or not operational.

**Table 3-6 Serial Indicator LEDs on the Top of EDS-MD**

LED	Description
Green	Indicates there is a tunnel connection to or from the EDS-MD.
Red	Not supported.
Off	There is no tunnel connection on the serial line.

**Note:** Number of Serial LEDs correspond with the EDS-MD model number. For instance, EDS-MD 4 has 4 LEDs, EDS-MD 8 has 8 LEDs, and EDS-MD 16 has 16 LEDs.

**Table 3-7 RJ45 LEDs on the Back Panel (Ethernet Indicators).**

LED	Description
Left LED Green	Connected at 1000 Mbps.
Left LED Amber	Connected at 100 Mbps.
Left LED Off	Connected at 10 Mbps or no link.
Right LED Green (Solid)	Full duplex with no activity
Right LED Green (Blinking)	Full duplex with activity
Right LED Amber (Solid)	Half duplex with no activity.
Right LED Amber (Blinking)	Half duplex with activity.
Right LED Off	No connection.

## Reset to Default Button

The EDS-MD device can be restored to factory defaults which includes clearing all networking settings. The IP address, gateway and netmask are set to all zeros. The reset-to-default button is located on the side of the housing, accessible with a paper clip or other similar object, through a pin hole.

### To restore factory default settings:

1. Power cycle the unit.
2. *During the bootup*, hold down the reset-to-default button for a minimum of 25 seconds.
3. Release the button. The firmware restores factory default settings to the configuration.

## Technical Specification

Category	Description
<b>NETWORK INTERFACE</b>	
<b>Ethernet Ports</b>	3 RJ45 10Base-T/100Base-TX/1000Base-T Ethernet ports Auto sensing Automatic MDI/MDI-X crossover Full duplex IEEE 802.3x flow control Half-duplex back pressure flow control
<b>Left LED Indicator</b>	See <a href="#">Table 3-7</a> .
<b>Right LED Indicator</b>	See <a href="#">Table 3-7</a> .
<b>Isolation from internal circuit</b>	1.5 KVAC
<b>Isolation from adjacent port</b>	1.5 KVAC
<b>USB INTERFACE</b>	
<b>USB Ports</b>	2 of USB-A Host, USB 2.0, Full Speed only
<b>Output Capability</b>	0.5 A
<b>Isolation from internal circuit</b>	1.5 KVAC
<b>Isolation from adjacent port</b>	1.5 KVAC
<b>SERIAL INTERFACE</b>	
<b>Serial Ports</b>	Options of 4-port, 8-port, 16-port RS232 Serial Ports DTE via RJ45 connectors
<b>Baud rate</b>	Selectable from 300 bps to 921600 bps
<b>Serial Line Formats</b>	Characters: 7 or 8 data bits Stop bits: 1 or 2 Parity: odd, even, none
<b>Modem Control</b>	DTR/DSR
<b>Flow Control</b>	Hardware: CTS/RTS Software: XON/XOFF

Category (continued)	Description
Serial LED Indicators	See <a href="#">Table 3-6</a> .
Protection from ESD	15kV (human body model)
Isolation from internal circuit	1.5 KVAC
Isolation from adjacent port	1.5 KVAC
Reset-to-Default-Parameters Switch	Side panel pin-hole recessed push button switch

Category (continued)	Description
<b>POWER RATING</b>	
Power Input AC Connector	IEC60320 C14 receptacle with no power switch
Power Usage	100-240 VAC, 50/60 Hz, 0.4A, 23W maximum
<b>PHYSICALS</b>	
Dimensions	L x W x H = 8.25 x 7.5 x 2.4 in. (21 x 19 x 6 cm)
Weight	16-port = 2.0 lbs (0.9 Kg) 8-port = 1.8 lbs (0.82 Kg) 4-port = 1.75 lbs (0.8 Kg)
Environmental	Temperature Operating 0° to 50°C (32° to 122°F) Temperature for Transportation and Storage -30° to 80°C Humidity 0% to 95% non-condensing Atmospheric Pressure 50 kPa to 105 kPa
Humidity Operating	20% to 90% relative humidity, non-condensing

## Installing the EDS-MD

### Finding a Suitable Location

- ◆ You can install the EDS-MD wired IoT device gateway either on a shelf, on a desktop or mounted on the wall (see [Wall Mounting Instructions on page 28](#)).
- ◆ If using AC power, do not use outlets controlled by a wall switch.

**Warning:** *To avoid the risk of electric shock, this equipment must only be connected to a supply mains with protective earth.*

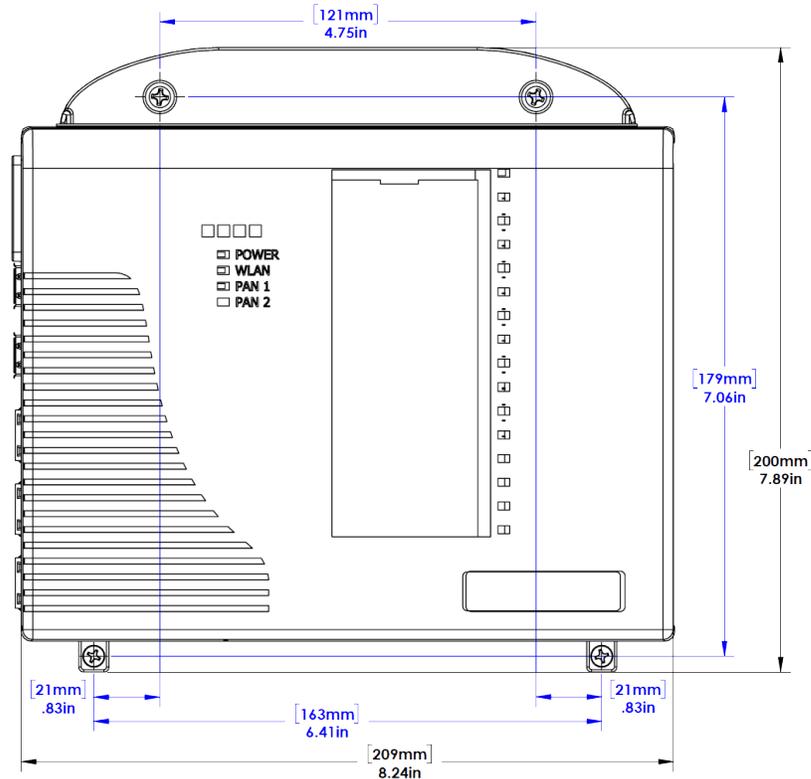
### Connect the EDS-MD to one or more serial devices

All serial ports on the EDS-MD wired IoT device gateway support RS-232 devices.

1. Power off the serial devices.
2. Attach a CAT 5 serial cable between the EDS-MD unit and your serial device.  
See [Appendix D: Lantronix Power Cords, Cables, Adapters and Serial Port Pinouts on page 114](#), for a list of cables and adapters you can use.
3. Connect an Ethernet cable between the Ethernet port of the EDS-MD device and your Ethernet network.

4. Insert the power cord into the power connector located in the back of the EDS-MD wired IoT device gateway. Plug the other end into an AC wall outlet.
5. Power up the serial devices.

Figure 3-8 EDS-MD Dimensions



## Wall Mounting Instructions

### For Installations to Walls Requiring Anchors

These instructions are for mounting the EDS-MD wired IoT device gateway to walls made of solid concrete, block, brick or plasterboard.

1. Locate the place where you want to mount your EDS-MD and mark four holes using your EDS-MD mount as a guide for the screws.
2. Drill four 3/16 inch (4.8 mm) diameter holes at a depth of 1.25 inches (32 mm). See [Figure 3-10](#) for the screws the dimensions of the screws that come with your EDS-MD wired IoT device gateway, and [Figure 3-10](#) for the location of the screw holes.
3. Insert the anchors until they are flush with the surface.
4. Thread four pan head top mount screws through your EDS-MD mount hole and through the anchor, tightening them.

## For Installations to Walls Not Requiring Anchors

These instructions are for mounting the EDS-MD wired IoT device gateway to walls made of solid wood at least 2 inches thick.

1. Locate the place where you want to mount your EDS-MD and mark four holes using your EDS-MD mount as a guide for the screws. See [Figure 3-10](#) for the location of the screw holes.
2. Drill four 1/8 inch (3.2 mm) diameter holes at a hole depth of 1.25 inches (32 mm). See [Figure 3-10](#) for the screws the dimensions of the screws that come with your EDS-MD wired IoT device gateway.
3. Thread four pan head top mount screws through your EDS-MD mount hole, tightening them.

**Figure 3-9 Mounting Screws Included with the EDS-MD in Inches**

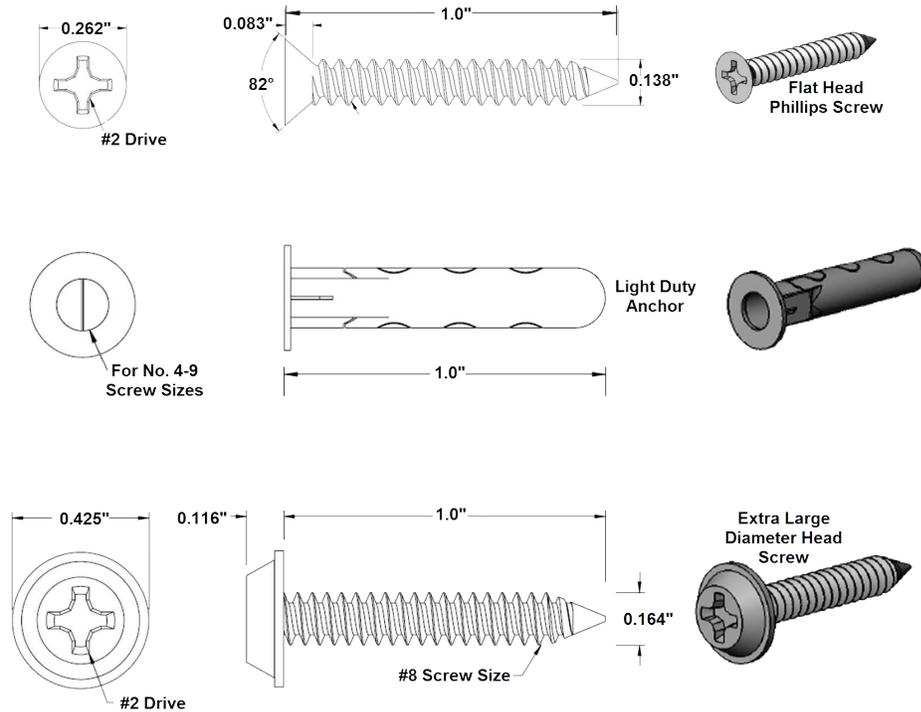
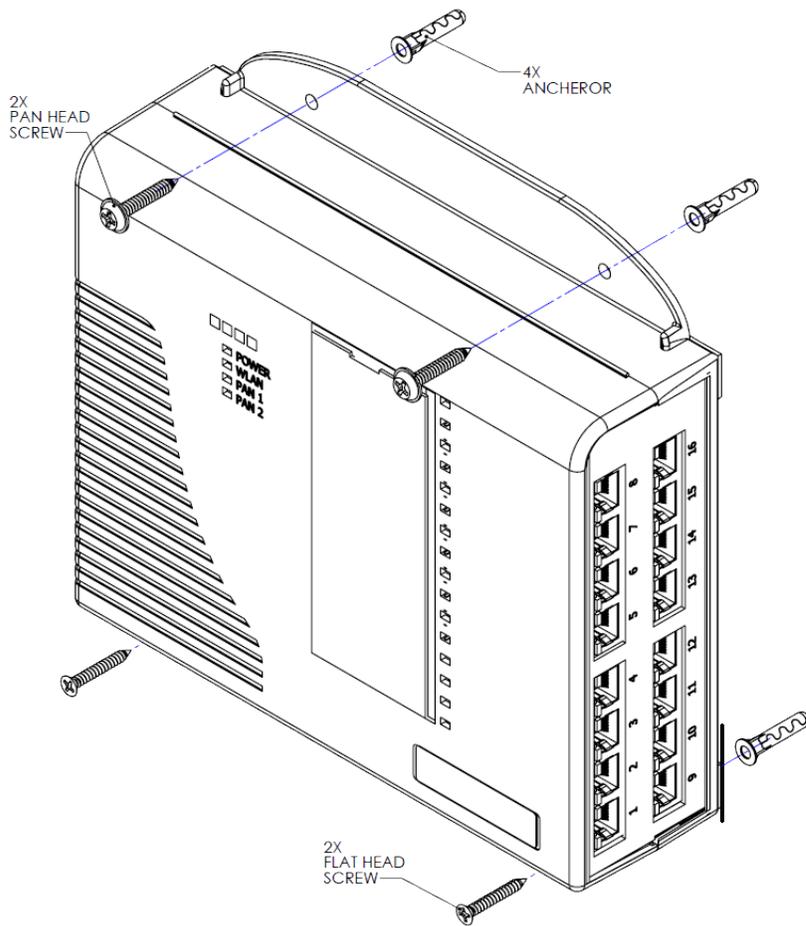


Figure 3-10 Mounting the EDS-MD



**Note:** Figure 3-10 represents the installation of an EDS-MD wired IoT device gateway to a wall, indicating where anchors and screws should be positioned. The actual screw type to be used and whether an anchor is necessary for your installation will depend on the material of the wall to which the EDS-MD will be installed. See Figure 3-9 for the screw types and the anchors that come with the EDS-MD wired IoT device gateway and see the correct installation section depending on your wall type: [For Installations to Walls Requiring Anchors](#) or [For Installations to Walls Not Requiring Anchors](#).

## 4: Using Lantronix Provisioning Manager

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

### Installing Lantronix Provisioning Manager

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

### Accessing the EDS-MD Using Lantronix Provisioning Manager

The device's factory default username is "admin" and factory default password is the last 8 characters of the Device ID (for devices manufactured after January 1, 2020) or "PASS" (for all older devices). For detailed instructions on using Lantronix Provisioning Manager, see the [Lantronix Provisioning Manager online help](#).

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

## 5: Configuration Using Web Manager

This chapter describes how to configure the EDS-MD 4, EDS-MD 8 or EDS-MD 16 wired IoT device gateway using Web Manager, the Lantronix browser-based configuration tool. The unit's configuration is stored in non-volatile memory and is retained without power. All changes take effect immediately, unless otherwise noted. It contains the following sections:

- ◆ [Accessing Web Manager](#)
- ◆ [Device Status Page](#)
- ◆ [Web Manager Components](#)
- ◆ [Navigating Web Manager](#)

### Accessing Web Manager

To access Web Manager, perform the following steps:

1. Open a standard web browser. Lantronix supports the latest versions of Internet Explorer, Mozilla Firefox, Safari or Chrome web browsers.
2. Enter the IP address or hostname of the EDS-MD unit in the address bar. The IP address may have been assigned automatically by DHCP. You may want to use Lantronix Provisioning Manager to determine the IP address (see [Using Lantronix Provisioning Manager on page 31](#)).
3. Enter your username and password. The factory default username is "**admin**" and factory default password is the last 8 characters of the Device ID (for devices manufactured after January 1, 2020) or "**PASS**" (for all older devices). The Device Status web page displays configurations including network settings, line settings, tunneling settings, and product information.

### Device Status Page

The Device Status page (see [Figure 5-1](#)) is the first to appear after you log into Web Manager. The Device Status page also appears when you click **Status** in the menu bar in Web Manager.

Figure 5-1 Device Status Page

EDS-MD
LANTRONIX

Status ⬆

Action

CLI

Clock

Diagnostics

Discovery

DNS

Email

Filesystem

FTP

Gateway

Host

HTTP

Line

MACH10

Network

Protocol Stack

RSS

SMTP

SSH

SSL

Syslog

System

Terminal

Tunnel

XML

## Device Status

[\[Logout\]](#)

Product Information		
Product Type:	Lantronix EDS-MD8 (EDS-MD8)	
Firmware Version:	8.1.0.4R4	
Build Date:	Aug 6 02:08:16 PDT 2019	
Serial Number:	00204A9D01A6	
Device ID:	00204A9D01A6	
Uptime:	0 days 00:03:50	
Current Date/Time:	Fri Sep 13 01:07:03 UTC 2019	
Temperature:	Board Temperature = 33.64C CPU Temperature = 56.128C	
Permanent Config:	Saved	
Network Settings		
Name servers		
Primary DNS:	10.153.90.1	
Secondary DNS:	10.167.90.1	
Interface eth0		
Link:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)	
MAC Address:	00:20:4A:9D:01:A6	
Hostname:	<None>	
MTU:	1500	
IP Address:	172.20.197.125/24 <DHCP>	
Network Mask:	255.255.255.0 <DHCP>	
Default Gateway:	172.20.197.254 <DHCP>	
Domain:	int.lantronix.com <DHCP>	
Interface eth1		
State:	Disabled	
Interface eth2		
Link:	Auto 10/100 Mbps Auto Half/Full (No link)	
MAC Address:	00:00:00:00:00:00	
Hostname:	<None>	
MTU:	1500	
IP Address:		
Network Mask:	0.0.0.0	
Default Gateway:	<None>	
Domain:	int.lantronix.com	
Line Settings		
Line 1:	RS232, 9600, None, 8, 1, None	
Line 2:	RS232, 9600, None, 8, 1, None	
Line 3:	RS232, 9600, None, 8, 1, None	
Line 4:	RS232, 9600, None, 8, 1, None	
Line 5:	RS232, 9600, None, 8, 1, None	
Line 6:	RS232, 9600, None, 8, 1, None	
Line 7:	RS232, 9600, None, 8, 1, None	
Line 8:	RS232, 9600, None, 8, 1, None	
Tunneling		
	Connect Mode	Accept Mode
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Waiting
Tunnel 3:	Disabled	Waiting
Tunnel 4:	Disabled	Waiting
Tunnel 5:	Disabled	Waiting
Tunnel 6:	Disabled	Waiting
Tunnel 7:	Disabled	Waiting
Tunnel 8:	Disabled	Waiting
MACH10		
Status:	Running	

Copyright © Lantronix, Inc. 2007-2019. All rights reserved.

## Web Manager Components

The layout of a typical Web Manager page is below.

Figure 5-2 Components of the Web Manager Page

The screenshot shows the EDS-MD Web Manager interface. The header contains the EDS-MD logo and the LANTRONIX logo. A menu bar on the left lists various system settings such as Status, Action, CLI, Clock, Diagnostics, Discovery, DNS, Email, Filesystem, FTP, Gateway, Host, HTTP, Line, MACH10, Network (highlighted), Protocol Stack, RSS, SMTP, SSH, SSL, Syslog, System, Terminal, Tunnel, and XML. The main content area displays the 'Network 1 (eth0) Interface Status' page, which includes a table of current and after-reboot settings, a statistics table, and a 'Link' button. The right sidebar contains help text and a '[Logout]' button. Annotations with arrows point to various components: 'Items to configure' points to the 'Network 1', 'Network 2', and 'Network 3' buttons; 'Links to subpages' points to the 'Link' button; 'Logout button' points to the '[Logout]' button; 'Configuration and/or Status Area' points to the table of settings; and 'Information and Help Area' points to the help text in the sidebar.

**Header**

**Menu Bar**

**Footer**

**Items to configure**

**Links to subpages**

**Logout button**

**Configuration and/or Status Area**

**Information and Help Area**

### Web Manager pages have these sections:

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

The main area of the page has these additional sections:

- ◆ Links near the top of many pages, such as the one in the example above, enable you to link to additional subpages. On some pages, you must also select the item you are configuring, such as a tunnel.
- ◆ In the middle of many pages, you can select or enter new configuration settings. Some pages show status or statistics in this area rather than allow you to enter settings.

- ◆ At the bottom of most pages, the current configuration is displayed. In some cases, you can reset or clear a setting.
- ◆ When a parameter is changed on the page, a **Submit** button will appear. Click on this button to save the change.
- ◆ The information or help area shows information or instructions associated with the page.
- ◆ A **Logout** link is available at the upper right corner of every page. In Chrome or Safari, it is necessary to close out of the browser to completely logout. If necessary, reopen the browser to log back in.
- ◆ The footer appears at the very bottom of the page. It contains copyright information and a link to the Lantronix home page.

## Navigating Web Manager

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

**Note:** *There may be times when you must reboot the EDS-MD device for the new configuration settings to take effect. The chapters that follow indicate when a change requires a reboot. Anytime you reboot the unit, this operation will take some time to complete. Please wait a minimum of 25-30 seconds after rebooting the unit before attempting to make any subsequent connections.*

**Table 5-3 Web Manager Pages**

Web Manager Page	Description	See Page
<b>Status</b>	Shows product information, network, line, and tunneling settings.	<a href="#">32</a>
<b>Action</b>	Shows the status and configuration of alarms.	<a href="#">47</a>
<b>CLI</b>	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	<a href="#">95</a>
<b>Clock</b>	Shows the current local date and time configured on the device and lets you configure the method to change the date and time.	<a href="#">93</a>
<b>Diagnostics</b>	Shows the hardware information for the device.	<a href="#">89</a>
<b>Discovery</b>	Shows the device discovery statistics and lets you enable or disable the query port server.	<a href="#">70</a>
<b>DNS</b>	Shows the status of the DNS subsystem.	<a href="#">65</a>
<b>Email</b>	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	<a href="#">71</a>
<b>Filesystem</b>	Shows file system statistics and lets you browse the file system to view a file, create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.	<a href="#">84</a>
<b>FTP</b>	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	<a href="#">65</a>
<b>Gateway</b>	Shows the statistics for the gateway and lets you configure gateway WAN settings.	<a href="#">41</a>

<b>Web Manager Page (continued)</b>	<b>Description</b>	<b>See Page</b>
<b>Host</b>	Lets you view and change settings for a host on the network.	<a href="#">63</a>
<b>HTTP</b>	Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	<a href="#">67</a>
<b>Line</b>	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	<a href="#">49</a>
<b>MACH10</b>	Lets you view and configure the MACH10 client on the device.	<a href="#">100</a>
<b>Network</b>	Shows status and lets you configure the network interface.	<a href="#">37</a>
<b>Protocol Stack</b>	Lets you perform lower level network stack-specific activities.	<a href="#">86</a>
<b>RSS</b>	Lets you change current Really Simple Syndication (RSS) settings.	<a href="#">69</a>
<b>SMTP</b>	Lets you configure SMTP settings for outgoing mail.	<a href="#">71</a>
<b>SSH</b>	Lets you view and configure SSH server and SSH client settings.	<a href="#">76</a>
<b>SSL</b>	Lets you view and configure SSL credentials on the device.	<a href="#">79</a>
<b>Syslog</b>	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	<a href="#">66</a>
<b>System</b>	Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.	<a href="#">93</a>
<b>Terminal</b>	Lets you change current settings for a terminal.	<a href="#">62</a>
<b>Tunnel</b>	Lets you change the current configuration settings for an incoming tunnel connection.	<a href="#">52</a>
<b>XML</b>	Lets you export XML configuration and status records, and import XML configuration records.	<a href="#">97</a>

## 6: Network Settings

The Network Settings show the status of the EDS-MD device interface/link and let you configure the settings on the device. Interface settings are related to the configuration of the IP and related protocols. Link settings are related to the physical link connection, which carries the IP traffic.

The EDS-MD wired IoT device gateway contains three interfaces:

- ◆ Network 1 Interface (eth0) or Link (eth0)
- ◆ Network 2 Interface (eth1) or Link (eth1)
- ◆ Network 3 Interface (eth2) or Link (eth2)

### Notes:

- ◆ *Some settings require a reboot to take effect. These settings are noted below.*
- ◆ *Wait a minimum of 10-20 seconds after rebooting the unit before attempting to make any subsequent connections.*
- ◆ *The blue text in the XML command strings of this chapter are to be replaced with a user-specified name.*

### Network 1 (eth0) Status

In the Network 1 status pages, you can view the current interface status and link status.

- ◆ To view Ethernet (eth0) Interface status, click Network on the menu and select Network 1 -> Interface -> Status.
- ◆ To view Ethernet (eth0) Link status, click Network on the menu and select Network 1 -> Link -> Status.

### Network 1 (eth0) Interface Settings

Configure the Ethernet interface on the device.

[Table 6-1](#) shows the network interface settings that can be configured.

**Table 6-1 Network 1 (eth0) Interface Settings**

Network 1 (eth0) Interface Settings	Description
State	Select to enable or disable the interface.
BOOTP Client	Select to turn <b>On</b> or <b>Off</b> . At boot up, after the physical link is up, the EDS-MD device will attempt to obtain IP settings from a BOOTP server.  <i>Note: Overrides the configured IP address/mask, gateway, hostname, and domain. When DHCP is <b>Enabled</b>, the system automatically uses DHCP, regardless of whether BOOTP is <b>Enabled</b>. Changing this value requires you to reboot the device.</i>

Network 1 (eth0) Interface Settings	Description
<b>DHCP Client</b>	Select to turn <b>On</b> or <b>Off</b> . At boot up, after the physical link is up, the EDS-MD 4/8/16 unit will attempt to obtain IP settings from a DHCP server and will periodically renew these settings with the server.  <i>Note: Overrides BOOTP, the configured IP address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the device.</i> <i>Note: Within Web Manager, click <b>Renew</b> to renew the DHCP lease.</i>
<b>Priority</b>	Each interface can be assigned a priority from 0-10. Lower priority means higher preference.
<b>IP Address</b>	Enter the static IP address to use for the interface. You may enter it alone or in CIDR format.  <i>Note: This setting will be used if Static IP is active (both DHCP and BOOTP are Disabled). Changing this value requires you to reboot the device. When DHCP or BOOTP is enabled, the EDS-MD 4/8/16 device tries to obtain an IP address from a DHCP or BOOTP server. If it cannot, the EDS-MD 4/8/16 unit generates and uses an Auto IP address in the range of 169.254.xxx.xxx, with a network mask of 255.255.0.0.</i>
<b>Default Gateway</b>	Enter the IP address of the router for this network.  <i>Note: This setting will be used if Static IP is active (both DHCP and BOOTP are Disabled).</i>
<b>Hostname</b>	Enter the hostname for the interface. It must begin with a letter or number, continue with a sequence of letters, numbers, or hyphens, and end with a letter or number. This setting will take effect immediately, but will not register the hostname with a DNS server until the next reboot.
<b>Domain</b>	Enter the domain name suffix for the interface.  <i>Note: This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no Domain Suffix was acquired from the server.</i>
<b>DHCP Client ID</b>	Enter the ID if the DHCP server requires a DHCP Client ID option. The DHCP server's lease table shows IP addresses and MAC addresses for devices. The lease table shows the Client ID, in hexadecimal notation, instead of the EDS-MD 4/8/16 wired IoT device gateway MAC address.
<b>Primary DNS</b>	Enter the IP address of the primary Domain Name Server.  <i>Note: This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server.</i>
<b>Secondary DNS</b>	Enter the IP address of the secondary Domain Name Server.  <i>Note: This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server.</i>
<b>MTU</b>	When DHCP is enabled, the MTU size is (usually) provided with the IP address. When not provided by the DHCP server, or using a static configuration, this value is used. The MTU size can be from 576 to 1500 bytes, the default being 1500 bytes.

## To Configure Network 1 (eth0) Interface Settings

### Using Web Manager

- ◆ To modify Ethernet (eth0) settings, click **Network** on the menu and select **Network 1 -> Interface -> Configuration**.

### Using the CLI

- ◆ To enter the eth0 command level: `enable -> config -> if 1`

### Using XML

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

## Network 1 (eth0) Link Settings

Configure the physical link parameters for an Ethernet Link (see [Table 6-2](#)).

**Table 6-2 Network 1 (eth0) Link Settings**

Network 1 Ethernet (eth0) Link Settings	Description
<b>Speed</b>	Select the Ethernet link speed. (Default is Auto) <ul style="list-style-type: none"> <li>◆ <b>Auto</b> = Auto-negotiation of Link Speed</li> <li>◆ <b>10 Mbps</b> = Force 10 Mbps</li> <li>◆ <b>100 Mbps</b> = Force 100 Mbps</li> <li>◆ <b>1000 Mbps</b> = Force 1000 Mbps</li> </ul>
<b>Duplex</b>	Select the Ethernet link duplex mode. (Default is Auto) <ul style="list-style-type: none"> <li>◆ <b>Auto</b> = Auto-negotiation of Link Duplex</li> <li>◆ <b>Half</b> = Force Half Duplex</li> <li>◆ <b>Full</b> = Force Full Duplex</li> </ul>

### Notes:

- ◆ When speed is **Auto**, duplex must be **Auto** or **Half**.
- ◆ When speed is not **Auto**, duplex must be **Half** or **Full**.
- ◆ Fixed speed Full duplex will produce errors connected to Auto, due to duplex mismatch.

## To Configure Network 1 (eth0) Link Settings

### Using Web Manager

- ◆ To configure Ethernet (eth0) Link settings, click **Network** on the menu and select **Network 1 -> Link -> Configuration**.

### Using the CLI

- ◆ To enter the eth0 command level: `enable -> config -> if 1`

### Using XML

- ◆ Include in your file: `<configgroup name="link" instance="eth0">`

## Network 2 (eth1) and Network 3 (eth2) Status

In the Network 2 and Network 3 status pages, you can view the current interface status and link status of Network 2 (eth1) and Network 3 (eth2).

**Note:** The following section describes the steps to view Network 2 (eth1) status pages; these steps also apply to the Network 3 (eth2) status pages.

- ◆ To view Ethernet (eth1) Interface status, click **Network** on the menu and select **Network 2 -> Interface -> Status**.
- ◆ To view Ethernet (eth2) Interface status, click **Network** on the menu and select **Network 3 -> Interface -> Status**.
- ◆ To view Ethernet (eth1) Link status, click **Network** on the menu and select **Network 2 -> Link -> Status**.
- ◆ To view Ethernet (eth2) Link status, click **Network** on the menu and select **Network 3 -> Interface -> Status**.

## Network 2 (eth1) and Network 3 (eth2) Interface Settings

Table 6-3 shows the Network 2 (eth1) and Network 3 (eth2) interface settings that can be configured.

**Table 6-3 Network 2 (eth1) and Network 3 (eth2) Interface Settings**

Interface Settings	Description
State	Select to enable or disable. Click the <b>Submit</b> button to enter your choice.

### To Configure Network 2 (eth1) and Network 3 (eth2) Interface Settings

#### Using Web Manager

- ◆ To modify Network 2 (eth1) interface settings, click **Network** on the menu and select **Network 2 -> Interface -> Configuration**.
- ◆ To modify Network 3 (eth2) interface settings, click **Network** on the menu and select **Network 3 -> Interface -> Configuration**.

#### Using the CLI

- ◆ To enter the eth1 command level: `enable -> config -> if 2`
- ◆ To enter the eth2 command level: `enable -> config -> if 3`

#### Using XML

- ◆ To configure Network 2, include in your file: `<configgroup name="interface" instance="eth1">`
- ◆ To configure Network 3, include in your file: `<configgroup name="interface" instance="eth2">`

## Network 2 (eth1) and Network 3 (eth2) Link Settings

Table 6-4 shows the Network 2 (eth1) and Network 3 (eth2) link settings that can be configured.

**Table 6-4 Network 2 (eth1) and Network 3 (eth2) Link Settings**

Link Settings	Description
<b>Speed</b>	Select the wlan0 link speed. (Default is Auto) ◆ <b>Auto</b> = Auto-negotiation of Link Speed ◆ <b>10 Mbps</b> = Force 10 Mbps ◆ <b>100 Mbps</b> = Force 100 Mbps ◆ <b>1000 Mbps</b> = Force 1000 Mbps
<b>Duplex</b>	Select the wlan0 link duplex mode. (Default is Auto) ◆ <b>Auto</b> = Auto-negotiation of Link Duplex ◆ <b>Half</b> = Force Half Duplex ◆ <b>Full</b> = Force Full Duplex

### To Configure Network 2 (eth1) and Network 3 (eth2) Link Settings

#### Using Web Manager

- ◆ To modify Network 2 (eth1) link settings, click **Network** on the menu and select **Network 2 -> Link -> Configuration**.
- ◆ To modify Network 3 (eth2) link settings, click **Network** on the menu and select **Network 3 -> Interface -> Configuration**.

#### Using the CLI

- ◆ To enter the eth1 command level: `enable -> config -> if 2`
- ◆ To enter the eth2 command level: `enable -> config -> if 3`

#### Using XML

- ◆ To configure Network 2, include in your file: `<configgroup name="link" instance="eth1">`
- ◆ To configure Network 3, include in your file: `<configgroup name="link" instance="eth2">`

## Gateway

The EDS-MD wired IoT device gateway can be configured as a wired router with DHCP server functionality.

### Status

This page displays the current configuration and statistics information for the gateway.

- ◆ To view gateway status: click **Gateway** on the menu and select **Status**.

## WAN

**Table 6-5 WAN Configuration**

Gateway Settings	Description
<b>Operating Mode</b>	Select the type of operating mode: <ul style="list-style-type: none"> <li>◆ <b>Disabled:</b> prevents the device to be used as a gateway; use the device normally. The eth1 and eth2 ports will act as switch ports.</li> <li>◆ <b>Gateway:</b> allows the device to be used as a router with NAT. The eth1 and eth2 ports will act as LAN ports.</li> <li>◆ <b>Router:</b> allows the device to be used as a router without NAT. The eth1 and eth2 ports will act as LAN ports.</li> </ul>
<b>Firewall</b>	Select to enable or disable firewall: <ul style="list-style-type: none"> <li>◆ <b>Enabled:</b> enables the device firewall.</li> <li>◆ <b>Disabled:</b> disable the device firewall.</li> </ul>
<b>Interface</b>	Specify the WAN interface.
<b>IP Address</b>	Assign a static IP address to the gateway.
<b>Primary DNS</b>	Enter the IP address of the primary Domain Name Server. This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server. <i>Note: Router Primary and Secondary DNS override the WAN Interface Configuration.</i>
<b>Secondary DNS</b>	Enter the IP address of the secondary Domain Name Server. This setting will be used when either Static IP or Auto IP is active, or if DHCP/BOOTP is active and no DNS server was acquired from the server. <i>Note: Router Primary and Secondary DNS override the WAN Interface Configuration.</i>

## To Configure Gateway WAN Settings

### Using Web Manager

- ◆ To modify gateway WAN information, click **Gateway** on the menu and select **Configuration > WAN**.

### Using the CLI

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

### Using XML

- ◆ Include in your file: `<configgroup name="gateway"> <configitem name="wan">`

## Port Forwarding

Port forwarding allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN). Port Forwarding rules apply to inbound traffic and will not work if the device is not reachable or traffic to certain ports is blocked before it reaches the device.

If traffic is going through firewalls, all referenced ports on the gateway and LAN devices must be accessible.

**Table 6-6 Port Forwarding Rules List**

Port Forwarding Rule	Description
Enabled	Enables the port forwarding rule.
Delete	Deletes the port forwarding rule.
Name	User friendly name for the rule. Click on the [Edit] icon to make changes.
Ingress IP Address: Port Range	Port or Port range for the rule.
Protocol	Protocols for the rule: TCP, UDP, or Both.
IP Address: Target Port	Target for the port forwarding rule.

**Table 6-7 Adding a New Port Forwarding Rule**

Adding New Port Forwarding Rule Settings	Description
Name	Enter a user friendly name for the rule (optional).
Ingress IP Address (Optional)	Enter the destination address of the packets. This option can only be used with single ports and not with port range.
Start Port	Enter the starting port number
End Port	End port number (optional). If start port and end port are same it assumes a single port. If start port and end port are not the same – it is a port range.
Protocol	Select the protocol for the rule: TCP, UDP, or Both
IP Address	Enter the target for the port forwarding rule. If firewall is enabled, use an address of 127.0.0.1 to open the port or port range in the firewall.
Target Port (Optional)	Indicate the target port. This is the port which the packets are to be forwarded. This option can only be used with single ports and not with port range. If this value is not specified, the packets are forwarded to same port or port range.
Add	Click <b>Add</b> to add the rule.

**Note:** If the firewall is enabled, port forwarding from one port to another on the device requires adding rules for both ports. You will need to add a rule to open the port on the device. Both the WAN and LAN ports must be accessible for port forwarding to work.

## To Configure Gateway Port Forwarding Settings

### Using Web Manager

- ◆ To modify gateway port forwarding information, click **Gateway** on the menu and select **Configuration > Port Forwarding**.

### Using the CLI

- ◆ To enter the gateway command level: `enable -> config -> gateway -> port forwarding rule <number>`

### Using XML

- ◆ Include in your file: `<configgroup name="gateway"> <configitem name="port forwarding" instance="<number>">`

## Static Routes

Add routes to the device routing table.

**Table 6-8 Static Route Setting Routes**

Static Route Settings	Description
<b>Enabled</b>	Enables the static route.
<b>Delete</b>	Deletes the static route.
<b>Name</b>	User friendly name for the route. Click on the [Edit] icon to make changes.
<b>Route</b>	Network or Host address for the route.
<b>Applied</b>	Indicates if the route was successfully applied. New or edited routes are applied after a reboot. If a route is not applied, please check all parameters and try again.
<b>Routing Table</b>	The Routing Table shows the current system routing table. Some fields may differ from the static route definitions.

**Table 6-9 Adding a New Static Route**

Adding New Static Route Settings	Description
<b>Name</b>	Enter the user friendly name for the route.
<b>Network</b>	Enter the Network or Host address for the route.
<b>Gateway</b>	Enter the Gateway address for the route.
<b>Interface</b>	Select the Interface for the route. The options are eth0, eth1, or eth2.
<b>Metric</b>	Enter the priority for the route. Lower metric means higher priority.
<b>Add</b>	Click <b>Add</b> to add the static route.

## To Configure Gateway Static Route Settings

### Using Web Manager

- ◆ To modify gateway static route information, click **Gateway** on the menu and select **Configuration > Static Routes**.

### Using the CLI

- ◆ To enter the gateway command level: enable -> config -> gateway -> static route <number>

### Using XML

- ◆ Include in your file: <configgroup name ="gateway"> <configitem name="static routes" instance="<number>"

## DHCP Server

Configure the device as a DHCP server.

**Table 6-10 DHCP Settings**

DHCP Settings	Description
<b>Lease time</b>	Enter the duration for which lease is initially assigned. Clients must renew after this duration.
<b>State</b>	Enable or Disable the DHCP server for the DHCP settings. ◆ <b>Enabled:</b> DHCP server is enabled. ◆ <b>Disabled:</b> DHCP server is disabled.
<b>Start IP Address</b>	View or edit the Start IP Address of address pool. <i>Note: The IP addresses must be in the same network as the Router IP address.</i>
<b>End IP Address</b>	View or edit the End IP Address of address pool. <i>Note: The IP addresses must be in the same network as the Router IP address.</i>

## To Configure Gateway DHCP Server Settings

### Using Web Manager

- ◆ To modify gateway DHCP server information, click **Gateway** on the menu and select **Configuration > DHCP Server**.

### Using the CLI

- ◆ To enter the gateway command level: enable -> config -> gateway -> dhcp server

### Using XML

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

## Static Lease Listing

The device also provides the ability to pre-assign specific IP addresses to connected devices using static leases. This ensures that the connected device (identified by the MAC address) always gets the same IP address even while using DHCP.

**Table 6-11 Static Lease Listing**

Static Lease List Settings	Description
<b>Delete</b>	Click checkbox beside existing static lease MAC Address/IP Address to delete.
<b>MAC Address</b>	MAC Address of existing static leases are listed here.
<b>IP Address</b>	Static IP Address of existing static leases are listed here.

**Table 6-12 Add a Static Lease**

Add a Static Lease Settings	Description
<b>MAC Address</b>	Enter the MAC Address of the static lease to be added.
<b>IP Address</b>	Enter static IP address of the static lease to be added.
<b>Add</b>	Click <b>Add</b> to add the new static lease information.

## 7: Action Settings

Actions can be configured for alarms and reports available in EDS-MD.

### Alarms and Reports

The EDS-MD device updates the action settings page to display and configure the alarms. The following alarm and report actions are available in EDS-MD:

- ◆ eth1 link state change
- ◆ eth2 link state change

One or more types of “action” can be configured and triggered when an event occurs.

### Actions

[Table 7-1](#) contains the configuration options for all the alarms and reports listed above.

**Table 7-1 Action Settings**

Action Settings	Description
<b>Delay</b>	Use Delay to defer alarm processing. Alarm actions will not be executed if the cause is corrected within this time.
<b>Email</b>	Use Email to send an email to configured Email recipients. <ul style="list-style-type: none"><li>◆ If an <b>Alarm Email</b> profile number is selected, that email will be sent when the alarm is turned on. The contents of <b>Alarm Message</b> will be placed into the email body when an alarm email is sent. If the alarm stays on longer than the Reminder Interval, another alarm email is sent.</li><li>◆ If a <b>Normal Email</b> profile number is selected, that email will be sent when the alarm is turned off. The contents of <b>Normal Message</b> will be placed into the email body when a normal email is sent. If the alarm stays off longer than the Reminder Interval, another normal email is sent.</li></ul>
<b>FTP Put</b>	Use FTP Put to put a file on configured FTP server. Filename will be used to upload to remote FTP server. The IP <b>Address</b> or hostname is the FTP server to connect. Port number is port on which FTP server is listening on. Use Protocol to connect to FTP server. FTPS is a SSL encrypted communication channel and SSL Trusted Authorities must be setup with FTP server SSL certificate. Username is used to logon to FTP server. If FTP server does not require authentication, use anonymous. Password is used to logon to FTP server. If FTP server does not require authentication, a common practice is to use user's email address. If the alarm stays on or off longer than the <b>Reminder Interval</b> , another FTP Put is performed. In <b>Sequential</b> mode, connections will be attempted starting with number 1 until a connection is successful. In <b>Simultaneous</b> mode, all possible connections will be made.

Action Settings	Description
<b>HTTP Post</b>	Use HTTP Post to post to configured HTTP server. The URL appears behind the HTTP server IP address or hostname. E.g. http://some_http_server/some_url The IP <b>Address</b> or hostname is the HTTP server to connect to. <b>Port</b> number is the port which HTTP server is listening on. Use <b>Protocol</b> to connect to HTTP server. HTTPS is a SSL encrypted communication channel and SSL Trusted Authorities must be setup with HTTP server SSL certificate. <b>Username</b> used to logon to HTTP server if authentication is required. <b>Password</b> used to logon to HTTP server if authentication is required. If the alarm stays on or off longer than the <b>Reminder Interval</b> , another HTTP Post is performed. In <b>Sequential</b> mode, connections will be attempted starting with number 1 until a connection is successful. In <b>Simultaneous</b> mode, all possible connections will be made.

## To Configure Action Settings

### Using Web Manager

- ◆ To view Action status information, click **Action** on the menu and select **Status**.
- ◆ To modify Action information, click **Action** on the menu, select the Ethernet interface, and then click **Configuration**. [Alarms and Reports \(on page 47\)](#) lists the options.

### Using the CLI

- ◆ To enter the eth1 link state change command level: enable -> config -> action -> eth1 link state change
- ◆ To enter the eth2 link state change command level: enable -> config -> action -> eth2 link state change

### Using XML

- ◆ Include in your file: <configgroup name = "action" instance = "eth1 link state change">
- ◆ Include in your file: <configgroup name = "action" instance = "eth2 link state change">

## 8: Line and Tunnel Settings

The EDS-MD wired IoT device gateways contain four, eight or sixteen serial lines depending on the specific model. All lines use standard RS232 serial ports and can be configured to operate in RS232 mode.

All serial settings such as Baud Rate, Parity, Data Bits, etc, apply to these lines.

### Line Statistics

This page displays the current status and various statistics for the serial line.

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

#### Using Web Manager

- ◆ To view statistics for Line 1, click **Line** in the menu and select **Line 1 -> Statistics**.

#### Using the CLI

- ◆ To view Line statistics: `enable -> line 1, show statistics`

#### Using XML

- ◆ Include in your file: `<statusgroup name="line" instance="1">`

### Line Settings

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

#### To Configure Line Settings

##### Using Web Manager

- ◆ To configure Line 1, click **Line** in the menu and select **Line 1 -> Configuration**.

##### Using the CLI

- ◆ To view Line statistics: `enable -> line 1, show statistics`

##### Using XML

- ◆ Include in your file: `<statusgroup name="line" instance="1">`

The Line Settings allow configuration of the serial lines (ports).

**Table 8-1 Line Configuration Settings**

Line Settings	Description
<b>Name</b>	Enter a name or short description for the line, if desired. By default, there is no name specified. A name that contains white space must be quoted.
<b>State</b>	Select to enable or disable the operational state of the Line. The default is <b>Enabled</b> .
<b>Protocol</b>	Set the operational protocol for the Line. The default is Tunnel. Choices are: <ul style="list-style-type: none"> <li>◆ <b>None</b></li> <li>◆ <b>Tunnel</b> = Serial-Network tunneling protocol.</li> </ul>
<b>Baud Rate</b>	Set the Baud Rate (speed) of the Line. The default is <b>9600</b> . Any set speed between 300 and 921600 may be selected: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600. When selecting a Custom baud rate, you may manually enter any value between 300 and 5000000.  <i>Note: Custom baud rates are not supported when a line is configured for Command Mode.</i>
<b>Parity</b>	Set the Parity of the Line. The default is <b>None</b> .
<b>Data Bits</b>	Set the number of data bits for the Line. The default is <b>8</b> .
<b>Stop Bits</b>	Set the number of stop bits for the Line. The default is <b>1</b> .
<b>Flow Control</b>	Set the flow control for the Line. The default is <b>None</b> .
<b>Xon Char</b>	Set Xon Char to be used when Flow Control is set to Software. Prefix decimal with \ or prefix hexadecimal with 0x or prefix a single control character <control>.  <i>Note: This field becomes available for configuration when Software is selected under Flow Control.</i>
<b>Xoff Char</b>	Set Xoff Char to be used when Flow Control is set to Software. Prefix decimal with \ or prefix hexadecimal with 0x or prefix a single control character <control>.  <i>Note: This field becomes available for configuration when Software is selected under Flow Control.</i>
<b>Gap Timer</b>	Set the Gap Timer delay to Set the number of milliseconds to pass from the last character received before the driver forwards the received serial bytes. By default, the delay is four character periods at the current baud rate (minimum 1 msec).
<b>Threshold</b>	Set the number of threshold bytes which need to be received in order for the driver to forward received characters.

Table 8-2 Line Command Mode Settings

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

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

## To Configure Line Command Mode

### Using Web Manager

- ◆ To configure a specific line, click **Line** in the menu and select **Line 1 -> Configuration** ([Table 8-1](#)).
- ◆ To configure a specific line in Command Mode, click **Line** in the menu and select **Line 1 -> Command Mode** ([Table 8-2](#)).

### Using the CLI

- ◆ To enter Line 1 command level: `enable -> line 1`

### Using XML

- ◆ Include in your file: `<configgroup name="line" instance="1">`
- ◆ Include in your file: `<configgroup name="serial command mode" instance="1">`

## Tunnel Statistics

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

**Note:** The following section describes the steps to view Tunnel 1 statistics; these steps apply to other tunnel instances of the device.

### To View Tunnel Statistics

#### Using Web Manager

- ◆ To view statistics for a specific tunnel, click **Tunnel** in the menu and select the **Tunnel 1 -> Statistics**.

#### Using the CLI

- ◆ To view Tunnel 1 statistics: enable -> tunnel 1, show statistics

#### Using XML

- ◆ Include in your file: `<statusgroup name="tunnel" instance="1">`

## Tunnel Settings

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

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

### Serial Settings

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

**Table 8-3 Tunnel Serial Settings**

Tunnel Serial Settings	Description
Line Settings	Line Settings information here is display only. Go to the section, <a href="#">To Configure Line Command Mode</a> to modify these settings.
Protocol	Protocol information here is display only. Go to the section, <a href="#">To Configure Line Command Mode</a> to modify these settings.

Tunnel Serial Settings (continued)	Description
<b>DTR</b>	<p>Select the conditions under which the Data Terminal Ready (DTR) control signal on the serial line is asserted. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Unasserted</b></li> <li>◆ <b>TruPort</b> = the DTR is asserted whenever either a connect or an accept mode tunnel connection is active with the Telnet Protocol RFC2217 saying that the remote DSR is asserted.</li> <li>◆ <b>Asserted while connected</b> = the DTR is asserted whenever either a connect or an accept mode tunnel connection is active.</li> <li>◆ <b>Continuously asserted</b></li> </ul>

## To Configure Tunnel Serial Settings

### Using Web Manager

- ◆ To configure the Serial Settings for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Serial Settings**.

### Using the CLI

- ◆ To enter Tunnel 1 command level: `enable -> tunnel 1 -> serial`

### Using XML

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

## Packing Mode

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

**Table 8-4 Tunnel Packing Mode Settings**

Tunnel Packing Mode Settings	Description
<b>Mode</b>	<p>Configure the Tunnel Packing Mode. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Disable</b> = Data not packed.</li> <li>◆ <b>Timeout</b> = data sent after timeout occurs.</li> <li>◆ <b>Send Character</b> = data sent when the Send Character is read on the Serial Line.</li> </ul>
<b>Threshold</b>	<p>Set the threshold (byte count). If the received serial data reaches this threshold, then the data will be sent on the network. Valid range is 100 to 1450 bytes. Default is 512.</p>
<b>Timeout</b>	<p>Set the timeout value, in milliseconds, after the first character is received on the serial line, before data is sent on the network. Valid range is 1 to 30000 milliseconds. Default is 1000. This setting becomes available when the Timeout mode is selected.</p>

Tunnel Packing Mode Settings	Description
<b>Send Character</b>	Enter Control Characters in any of the following forms: <ul style="list-style-type: none"> <li>◆ &lt;control&gt;J</li> <li>◆ 0xA (hexadecimal)</li> <li>◆ \10 (decimal)</li> </ul> If used, the Send Character is a single printable character or a control character that, when read on the Serial Line, forces the queued data to be sent on the network immediately.
<b>Trailing Character</b>	Enter Control Characters in any of the following forms: <ul style="list-style-type: none"> <li>◆ &lt;control&gt;J</li> <li>◆ 0xA (hexadecimal)</li> <li>◆ \10 (decimal).</li> </ul> If used, the Trailing Character is a single printable character or a control character that is injected into the outgoing data stream right after the Send Character. Disable the Trailing Character by blanking the field (setting it to <None>).

## To Configure Tunnel Packing Mode Settings

### Using Web Manager

- ◆ To configure the Packing Mode for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Packing Mode**.

### Using the CLI

- ◆ To enter the Tunnel 1 Packing command level: `enable -> tunnel 1 -> packing`

### Using XML

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

## Accept Mode

In Accept Mode, the EDS-MD device listens (waits) for incoming connections from the network. A remote node on the network initiates the connection.

The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. Supported serial lines and associated local port numbers progress sequentially in matching value. For instance, the default local port is 10001 for serial line 1 and the default local port for serial line 2 is 10002, and so on for the number of serial lines supported.

Serial data can still be received while waiting for a network connection, keeping in mind serial data buffer limitations.

Table 8-5 Tunnel Accept Mode Settings

Tunnel Accept Mode Settings	Description
<b>Mode</b>	Set the method used to start a tunnel in Accept mode. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Disable</b> = do not accept an incoming connection.</li> <li>◆ <b>Always</b> = accept an incoming connection (<i>default</i>).</li> <li>◆ <b>Any Character</b> = start waiting for an incoming connection when any character is read on the serial line.</li> <li>◆ <b>Start Character</b> = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line.</li> <li>◆ <b>Modem Control Asserted</b> = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made.</li> <li>◆ <b>Modem Emulation</b> = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.</li> </ul>
<b>Local Port</b>	Set the port number for use as the network local port. The default local port number for each supported serial line number progresses sequentially in equal value so that Tunnel X: 1000X. For example: <ul style="list-style-type: none"> <li>◆ Tunnel 1: 10001</li> <li>◆ Tunnel 2: 10002</li> </ul>
<b>Protocol</b>	Select the protocol type for use with Accept Mode: <ul style="list-style-type: none"> <li>◆ SSH</li> <li>◆ SSL</li> <li>◆ TCP (default protocol)</li> <li>◆ TCP AES</li> </ul> <p><i>Note:</i> Telnet</p>
<b>TCP Keep Alive Idle Time</b>	Enter the time, in milliseconds, the EDS-MD device waits during a silent TCP connection before the first Keep Alive probe is sent to the remote host in order to keep the TCP connection up during idle transfer periods. Set to 0 to disable TCP Keep Alive and blank the field to restore the default.
<b>TCP Keep Alive Interval</b>	Enter the time, in milliseconds, to wait before probing the remote host, after the initial TCP Keep Alive probe, in order to keep the TCP connection up during idle transfer periods. Blank the display field to restore the default.
<b>TCP Keep Alive Probes</b>	Enter the number of TCP Keep Alive probes to send before closing the connection if no response is received. The probes are sent after the initial TCP Keep Alive probe is sent. Valid values are between 1 and 16. Blank the field to restore the default.
<b>Flush Serial</b>	Set whether the serial line data buffer is flushed upon a new network connection. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = serial data buffer is flushed on network connection</li> <li>◆ <b>Disabled</b> = serial data buffer is not flushed on network connection (<i>default</i>)</li> </ul>
<b>Block Serial</b>	Set whether Block Serial is enabled for debugging purposes. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = if Enabled, incoming characters from the serial line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the serial line if hardware or software flow control is configured.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.</li> </ul>

Tunnel Accept Mode Settings (continued)	Description
<b>Block Network</b>	Set whether Block Network is enabled for debugging purposes. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = if Enabled, incoming characters from the network will not be forwarded to the Serial Line. Instead, they will be buffered and will eventually flow off the network side.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.</li> </ul>
<b>Password</b>	Enter a password. This password can be up to 31 characters in length and must contain only alphanumeric characters and punctuation. When set, clients must send the correct password string to the unit within 30 seconds from opening network connection in order to enable data transmission. The password sent to the unit must be terminated with one of the following: <ul style="list-style-type: none"> <li>◆ 0A (Line Feed)</li> <li>◆ 00 (Null)</li> <li>◆ 0D 0A (Carriage Return/Line Feed)</li> <li>◆ 0D 00 (Carriage Return/Null)</li> </ul> If, <b>Prompt for Password</b> is set to <b>Enabled</b> and a password is provided, the user will be prompted for the password upon connection.
<b>Email on Connect</b>	Select an email profile number to which an email notification will be sent upon the establishment of an accept mode tunnel.
<b>Email on Disconnect</b>	Select an email profile number to which an email notification will be sent upon the disconnection of an accept mode tunnel.

## To Configure Tunnel Accept Mode Settings

### Using Web Manager

- ◆ To configure the Accept Mode for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Accept Mode**.

### Using the CLI

- ◆ To enter Tunnel 1 Accept Mode command level: `enable -> tunnel 1 -> accept`

### Using XML

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

## Connect Mode

In Connect Mode, the EDS-MD unit continues to attempt an outgoing connection on the network, until established (based on which connection method is selected in the configuration described in [Table 8-6](#)). 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 IP address or DNS name. The EDS-MD device will not make a connection unless it can resolve the address.

For Connect Mode using UDP, the EDS-MD module accepts packets from any device on the network. It will send packets to the last device that sent it packets.

**Note:** *The port in Connect Mode is not the same port configured in Accept Mode.*

The TCP keepalive time is the time in which probes are periodically sent to the other end of the connection. This ensures the other side is still connected.

**Table 8-6 Tunnel Connect Mode Settings**

Tunnel Connect Mode Settings	Description
<b>Mode</b>	<p>Set the method to be used to attempt a connection to a remote host or device. Choices are:</p> <ul style="list-style-type: none"> <li>◆ <b>Disable</b> = an outgoing connection is never attempted. (<i>default</i>)</li> <li>◆ <b>Always</b> = a connection is attempted until one is made. If the connection gets disconnected, the device retries until it makes a connection.</li> <li>◆ <b>Any Character</b> = a connection is attempted when any character is read on the serial line.</li> <li>◆ <b>Start Character</b> = a connection is attempted when the start character for the selected tunnel is read on the serial line.</li> <li>◆ <b>Modem Control Asserted</b> = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made.</li> <li>◆ <b>Modem Emulation</b> = a connection is attempted when triggered by modem emulation AT commands.</li> </ul>
<b>Local Port</b>	<p>Enter an alternative Local Port. The Local Port is set to &lt;Random&gt; by default but can be overridden. Blank the field to restore the default.</p>
<b>Host (Number)</b>	<p>Click on the displayed information to expand it for editing. If &lt;None&gt; is displayed, clicking it will allow you to configure a new host. At least one Host is required to enable Connect Mode as this information is necessary to connect to that host. Once you start to edit Host 1, a box for Host 2 will show up. Editing Host 2 will cause a Host 3 box to appear. Up to 32 hosts are available. Complete the following fields to configure a host:</p> <ul style="list-style-type: none"> <li>◆ <b>Address:</b> enter the address for the remote host connection. Either a DNS address or an IP address may be provided.</li> <li>◆ <b>Port:</b> designate the TCP or UDP port on the remote host for connection.</li> <li>◆ <b>Protocol:</b> select the desired security protocol. SSH is recommended for circumstances with high security concerns. When using SSH, both the SSH server host keys and the SSH server authorized users must be configured.</li> <li>◆ <b>TCP Initial Keep Alive:</b> specify the amount of time to wait 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 and blank the display field to restore the default.</li> <li>◆ <b>TCP Keep Alive Interval:</b> specify the amount of time to wait before probing the remote host, after the initial probe, in order to keep the TCP connection up during idle transfer periods. Blank the display field to restore the default.</li> <li>◆ <b>TCP Keep Alive Probes:</b> specify the number of TCP Keep Alive probes (after the TCP Initial Keep Alive Probe) to send before closing the connection if no response is received. Valid values are between 1 and 16. Blank the display field to restore the default.</li> </ul>

Tunnel Connect Mode Settings (continued)	Description
Host (Number) (continued)	<ul style="list-style-type: none"> <li>◆ <b>TCP User Timeout:</b> specify the amount of time the TCP segments will be retransmitted before the connection is closed.</li> <li>◆ <b>AES Encrypt Key:</b> enter the AES encrypt key to encrypt outgoing data. Enter the key in the fixed 16, 24, or 32 byte length and either in <b>Text</b> or <b>Hexadecimal</b> form. Keys are stored and exchanged in Hexadecimal form only. To remove a key, delete &lt;Configured&gt; in the display. All keys are shared secret keys which are known by both sides of the connection and kept secret.</li> <li>◆ <b>AES Decrypt Key:</b> enter the AES decrypt key to decrypt outgoing data. Enter the key in the fixed 16, 24, or 32 byte length and either in <b>Text</b> or <b>Hexadecimal</b> form. Keys are stored and exchanged in Hexadecimal form only. To remove a key, delete &lt;Configured&gt; in the display. All keys are shared secret keys which are known by both sides of the connection and kept secret.</li> <li>◆ <b>Initial Send:</b> enter the Initial Send string for data sent out of the network upon connection establishment (before any data from the Line). The string may contain one or more Directives of the form %&lt;char&gt; and can be entered in Text or Binary form.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>◆ <i>If the keep alive idle time (the initial keep alive probe) 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 they are 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 the probe count can be disregarded in these cases: if the keep alive timers are significantly smaller than the user timeout, probes will continue to be sent for an unreachable host until the user timeout expires.</i></li> <li>◆ <i>If there is data in flight when the TCP retransmission timeout kicks in, the user timeout is checked as a limiting condition only when the timer expirations would normally be checked during RTO handling. In other words, the user timeout will not be an exact limit; in practice, it will always take somewhat longer for the connection to be closed. The longer the user timeout is, the more likely it will expire between exponentially slower retransmissions, and the connection will not experience an error until the next retransmission timeout is checked. Also note that the user timeout expiration during retransmission returns an error to the application; it does not automatically reset the connection as happens with keep alive timeout. It is up to the application (e.g., tunneling) to close the connection (this happens almost immediately with tunneling).</i></li> </ul>
Reconnect Timer	Set the value of the reconnect timeout (in milliseconds) for outgoing connections established by the device. Valid range is 1 to 65535 milliseconds. Default is 15000.
Flush Serial Data	Set whether the serial Line data buffer is flushed upon a new network connection. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = serial data buffer is flushed on network connection</li> <li>◆ <b>Disabled</b> = serial data buffer is not flushed on network connection (<i>default</i>)</li> </ul>

Tunnel Connect Mode Settings (continued)	Description
<b>Block Serial</b>	Set whether Block Serial is enabled for debugging purposes. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = If Enabled, incoming characters from the Serial Line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the Serial Line if hardware or software flow control is configured.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.</li> </ul>
<b>Block Network</b>	Set whether Block Network is enabled for debugging purposes. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> = If Enabled, incoming characters from the network will not be forwarded to the Serial Line. Instead, they will be buffered and will eventually flow off the network side.</li> <li>◆ <b>Disabled</b> = this is the default setting; incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.</li> </ul>
<b>Email on Connect</b>	Select an email profile number to which an email notification will be sent upon the establishment of an accept mode tunnel.
<b>Email on Disconnect</b>	Select an email profile number to which an email notification will be sent upon the disconnection of an accept mode tunnel.

### To Configure Tunnel Connect Mode Settings

#### Using Web Manager

- ◆ To configure the Connect Mode for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Connect Mode**.

#### Using the CLI

- ◆ To enter the Tunnel 1 Connect Mode command level: `enable -> tunnel 1 -> connect`

#### Using XML

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

### Connecting Multiple Hosts

If more than one host is configured, a **Host Mode** option appears. Host Mode controls how multiple hosts will be accessed. For the EDS-MD device, the Connect Mode supports up to 32 hosts. Hosts may be accessed sequentially or simultaneously:

- ◆ **Sequential** – Sequential host lists establish a prioritized list of tunnels. The host specified as Host 1 will be attempted first. If that fails, it will proceed to Host 2, 3, etc, in the order they are specified. When a connection drops, the cycle starts again with Host 1 and proceeds in order. Establishing the host order is accomplished with host list promotion (see [Host List Promotion on page 60](#)). 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 device can support a maximum of 64 total aggregate connections.

## Host List Promotion

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

### To promote a specific Host:

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

## Disconnect Mode

Specifies the optional conditions for disconnecting any Accept Mode or Connect Mode connection that may be established. If any of these conditions are selected but do not occur and the network disconnects to the device, 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 disconnect.

**Table 8-7 Tunnel Disconnect Mode Settings**

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

## To Configure Tunnel Disconnect Mode Settings

### Using Web Manager

- ◆ To configure the Disconnect Mode for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Disconnect Mode**.

### Using the CLI

- ◆ To enter the Tunnel 1 Disconnect command level: `enable -> tunnel 1 -> disconnect`

### Using XML

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

## Modem Emulation

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

**Table 8-8 Tunnel Modem Emulation Settings**

Tunnel Modem Emulation Settings	Description
<b>Echo Pluses</b>	Set whether the pluses will be echoed back during a "pause +++ pause" escape sequence on the Serial Line. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b></li> <li>◆ <b>Disabled</b> (default)</li> </ul>
<b>Echo Commands</b>	Set whether characters read on the Serial Line will be echoed, while the Line is in Modem Command Mode. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b></li> <li>◆ <b>Disabled</b> (default)</li> </ul>
<b>Verbose Response</b>	Set whether Modem Response Codes are sent out on the Serial Line. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b></li> <li>◆ <b>Disabled</b> (default)</li> </ul>
<b>Response Type</b>	Select a representation for the Modem Response Codes sent out on the Serial Line: <ul style="list-style-type: none"> <li>◆ <b>Text</b> (ATV1) (default)</li> <li>◆ <b>Numeric</b> (ATV0)</li> </ul>
<b>Error Unknown Commands</b>	Set whether the Error Unknown Commands is enabled (ATU0) and ERROR is returned on the Serial Line for unrecognized AT commands. Otherwise (ATU1) OK is returned for unrecognized AT commands. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b></li> <li>◆ <b>Disabled</b> (default)</li> </ul>
<b>Incoming Connection</b>	Set if and how requests are answered after an incoming RING (ATS0=2): <ul style="list-style-type: none"> <li>◆ <b>Disabled</b> (default)</li> <li>◆ <b>Automatic</b></li> <li>◆ <b>Manual</b></li> </ul>
<b>Connect String</b>	Enter the customized Connect String sent to the Serial Line with the Connect Modem Response Code.
<b>Display Remote IP</b>	Set whether the Display Remote IP is enabled so that the incoming RING sent on the Serial Line is followed by the IP address of the caller. Choices are: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b></li> <li>◆ <b>Disabled</b> (default)</li> </ul>

## To Configure Tunnel Modem Emulation Settings

### Using Web Manager

To configure the Modem Emulation for a specific tunnel, click **Tunnel** in the menu and select **Tunnel 1 -> Modem Emulation**. *Using the CLI*

- ◆ To enter the Tunnel 1 Modem command level: `enable -> tunnel 1 -> modem`

### Using XML

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

## 9: Terminal and Host Settings

Predefined connections are available via Telnet, SSH, or a serial port. A user can choose one of the presented options and the device automatically makes the predefined connection.

Either the Telnet, SSH, or serial port connection can present the CLI or the Login Connect Menu. By default, the CLI is presented when the device is accessed. When configured to present the Login Connect Menu, the hosts configured via the Host selections, and named serial lines are presented.

### Terminal Settings

You can configure whether each serial line or the Telnet/SSH server presents a CLI or a Login Connect menu when a connection is made.

**Table 9-1 Terminal on Network and Line Settings**

Terminal on Network and Line Settings	Description
<b>Terminal Type</b>	Enter text to describe the type of terminal. The text will be sent to a host via IAC. <i>Note:</i> IAC means, "interpret as command." It is a way to send commands over the network such as <b>send break</b> or <b>start echoing</b> . IAC is only supported in Telnet.
<b>Login Connect Menu</b>	Select the interface to display when the user logs in. Choices are: ◆ <b>Enabled</b> = shows the Login Connect Menu. ◆ <b>Disabled</b> = shows the CLI (default)
<b>Exit Connect Menu</b>	Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are: ◆ <b>Enabled</b> = a choice allows the user to exit to the CLI. ◆ <b>Disabled</b> = there is no exit to the CLI (default)
<b>Send Break</b>	Enter a Send Break control character, e.g., <control> Y, or blank to disable. When the Send Break control character is received from the network on its way to the serial line, it is not sent to the line; instead, the line output is forced to be inactive (the break condition). <i>Note:</i> This configuration option is only available for Line Terminals.
<b>Break Duration</b>	Enter how long the break should last in milliseconds, up to 10000. Default is 500. <i>Note:</i> This configuration option is only available for Line Terminals.
<b>Echo</b>	Select whether to enable echo: ◆ <b>Enabled</b> ◆ <b>Disabled</b> <i>Note:</i> Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable <b>Echo</b> if your terminal echoes, in which case you will see double of each character typed. Default is enabled.

## To Configure the Terminal Network Connection

### Using Web Manager

- ◆ To configure the Terminal on Network, click **Terminal** on the menu and select **Network -> Configuration**.

### Using the CLI

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

### Using XML

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

## To Configure the Terminal Line Connection

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

### Using Web Manager

- ◆ To configure a particular Terminal Line, click **Terminal** on the menu and select **Line 1 -> Configuration**.

### Using the CLI

- ◆ To enter the Terminal Line command level: `enable -> config -> terminal 1`

### Using XML

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

## Host Configuration

**Table 9-2 Host Configuration**

Host Settings	Description
<b>Name</b>	Enter a name for the host. This name appears on the Login Connect Menu. To leave a host out of the menu, leave this field blank.
<b>Protocol</b>	Select the protocol to use to connect to the host. Choices are: <ul style="list-style-type: none"> <li>◆ Telnet</li> <li>◆ SSH</li> </ul> <p><b>Note:</b> SSH keys must be loaded or created on the SSH page for the SSH protocol to work.</p>

Host Settings	Description
<b>SSH Username</b>	Appears if you selected SSH as the protocol. Enter a username to select a pre-configured Username/Password/Key (configured on the SSH: Client Users page), or leave it blank to be prompted for a username and password at connect time.  <i>Note: This configuration option is only available when SSH is selected for Protocol.</i>
<b>Remote Address</b>	Enter an IP address for the host to which the device will connect.
<b>Remote Port</b>	Enter the port on the host to which the device will connect.

## To Configure Host Settings

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

### Using Web Manager

- ◆ To configure a particular Host, click **Host** on the menu and select **Host 1 -> Configuration**.

### Using the CLI

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

### Using XML

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

# 10: Network Services

## DNS Settings

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

**Note:** The blue text in the XML command strings of this chapter are to be replaced with a user-specified name.

**Table 10-1 DNS Settings**

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

### To View or Configure DNS Settings:

#### Using Web Manager

- ◆ To view DNS current status, click **DNS** in the menu.
- ◆ To lookup DNS name or IP address, click **DNS** in the menu to access the **Lookup** field.

**Note:** To configure DNS for cases where it is not supplied by a protocol, click **Network** in the menu and select **Interface -> Configuration**.

#### Using the CLI

- ◆ To enter the DNS command level: `enable -> dns`

#### Using XML

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

## FTP Settings

The FTP protocol can be used to upload and download user files, and upgrade the EDS-MD wired IoT device gateway firmware. A configurable option is provided to enable or disable access via this protocol.

Table 10-2 FTP Settings

FTP Settings	Description
State	Select to enable or disable the FTP server: <ul style="list-style-type: none"> <li>◆ Enabled (default)</li> <li>◆ Disabled</li> </ul>

## To Configure FTP Settings

### Using Web Manager

- ◆ To configure FTP and view FTP statistics, click **FTP** in the menu.

### Using the CLI

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

### Using XML

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

## Syslog Settings

The Syslog information shows the current configuration and statistics of the syslog. Here you can configure the syslog host and the severity of the events to log.

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

Table 10-3 Syslog Settings

Syslog Settings	Description
State	Select to enable or disable the syslog: <ul style="list-style-type: none"> <li>◆ Enabled</li> <li>◆ Disabled (default)</li> </ul>
Host	Enter the IP address of the remote server to which system logs are sent for storage.
Remote Port	Enter the number of the port on the remote server that supports logging services. The default is 514.
Severity Log Level	Specify the minimum level of system message the EDS-MD device should log by selecting from the drop-down menu. This setting applies to all syslog facilities. The drop-down list in the Web Manager is in descending order of severity (e.g., Emergency is more severe than Alert.)

## To View or Configure Syslog Settings

### Using Web Manager

- ◆ To configure the Syslog and view current Syslog status, click **Syslog** in the menu.

### Using the CLI

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

### Using XML

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

## HTTP Settings

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

**Table 10-4 HTTP Settings**

HTTP Settings	Description
<b>State</b>	Select to enable or disable the HTTP server: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> (default)</li> <li>◆ <b>Disabled</b></li> </ul>
<b>Port</b>	Enter the port for the HTTP server to use. The default is <b>80</b> .
<b>Secure Port</b>	Enter the port for the HTTPS server to use. The default is <b>443</b> . The HTTP server only listens on the <b>HTTPS Port</b> when an SSL certificate is configured.
<b>Secure Protocols</b>	Select to enable or disable the following protocols: <ul style="list-style-type: none"> <li>◆ <b>SSL3</b> = Secure Sockets Layer version 3</li> <li>◆ <b>TLS1.0</b> = Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF.</li> <li>◆ <b>TLS1.1</b> = Transport Layer Security version 1.1</li> </ul> The protocols are enabled by default. <p><i>Note: A server certificate and associated private key need to be installed in the <b>SSL configuration section</b> to use <b>HTTPS</b>.</i></p>
<b>Secure Credentials</b>	Specify the name of the set of RSA and/or DSA certificates and keys to be used for the secure connection.
<b>Max Timeout</b>	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is <b>10</b> seconds.
<b>Max Bytes</b>	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is <b>40 KB</b> (this prevents DoS attacks). <p><i>Note: You may need to increase this number in some cases where the browser is sending data aggressively within TCP Windows size limit, when file (including firmware upgrade) is uploaded from webpage.</i></p>

HTTP Settings (continued)	Description
<b>Logging State</b>	Select to enable or disable HTTP server logging: <ul style="list-style-type: none"> <li>◆ <b>Enabled</b> (default)</li> <li>◆ <b>Disabled</b></li> </ul>
<b>Max Log Entries</b>	Set the maximum number of HTTP server log entries. Only the last <b>Max Log Entries</b> are cached and viewable.
<b>Log Format</b>	Set the log format string for the HTTP server. Follow these <b>Log Format</b> rules: <ul style="list-style-type: none"> <li>◆ <b>%a</b> - remote IP address (could be a proxy)</li> <li>◆ <b>%b</b> - bytes sent excluding headers</li> <li>◆ <b>%B</b> - bytes sent excluding headers (0 = '-')</li> <li>◆ <b>%h</b> - remote host (same as '%a')</li> <li>◆ <b>%{h}i</b> - header contents from request (h = header string)</li> <li>◆ <b>%m</b> - request method</li> <li>◆ <b>%p</b> - ephemeral local port value used for request</li> <li>◆ <b>%q</b> - query string (prepend with '?' or empty '-')</li> <li>◆ <b>%t</b> - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t')</li> <li>◆ <b>%u</b> - remote user (could be bogus for 401 status)</li> <li>◆ <b>%U</b> - URL path info</li> <li>◆ <b>%r</b> - first line of request (same as '%m %U%q &lt;version&gt;')</li> <li>◆ <b>%s</b> - return status</li> </ul>
<b>Authentication Timeout</b>	The timeout period applies if the selected authentication type is either <b>Digest</b> or <b>SSL/Digest</b> . After this period of inactivity, the client must authenticate again.
<b>Submit (button)</b>	Click the <b>Submit</b> button which appears when any changes are entered in the HTTP Configuration table. Clicking the <b>Submit</b> button submits the changes.

## To Configure HTTP Settings

### Using Web Manager

- ◆ To view HTTP statistics, click **HTTP** in the menu and select **Statistics**.
- ◆ To configure HTTP settings, click **HTTP** in the menu and select **Configuration**.

### Using the CLI

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

### Using XML

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

**Table 10-5 HTTP Authentication Settings**

HTTP Authentication Settings	Description
<b>URI</b>	Enter the Uniform Resource Identifier (URI). <p><i>Note:</i> The URI must begin with '/' to refer to the filesystem.</p>

HTTP Authentication Settings (continued)	Description
<b>Auth Type</b>	Select the authentication type: <ul style="list-style-type: none"> <li>◆ <b>None</b> = no authentication is necessary.</li> <li>◆ <b>Basic</b> = encodes passwords using Base64.</li> <li>◆ <b>Digest</b> = encodes passwords using MD5.</li> <li>◆ <b>SSL</b> = can only be accessed over SSL (no password is required).</li> <li>◆ <b>SSL/Basic</b> = is accessible only over SSL and encodes passwords using Base64.</li> <li>◆ <b>SSL/Digest</b> = is accessible only over SSL and encodes passwords using MD5.</li> </ul> <p><i>Note: When changing the parameters of Digest or SSL Digest authentication, it is often best to close and reopen the browser to ensure it does not attempt to use cached authentication information.</i></p>
<b>Submit (button)</b>	Click the <b>Submit</b> button after entering the HTTP authentication information.
<b>Delete (button)</b>	Click the <b>Delete</b> button to delete the HTTP authentication information.

## To Configure HTTP Authentication

### Using Web Manager

- ◆ To configure HTTP Authentication, click **HTTP** in the menu and select **Authentication**.

### Using the CLI

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

### Using XML

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

## RSS Settings

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

**Table 10-6 RSS Settings**

RSS Settings	Description
<b>RSS Feed</b>	Select <b>On</b> or <b>Off</b> for RSS feeds to an RSS publisher. The default setting is off.
<b>Persistent</b>	Select <b>On</b> or <b>Off</b> for RSS feed to be written to a file ( <code>cfg_log.txt</code> ) and to be available across reboots. The default setting is off.
<b>Max Entries</b>	Set the maximum number of log entries. Only the last <b>Max Entries</b> are cached and viewable.
<b>View</b>	Click the button to view RSS feeds.
<b>Clear</b>	Click the button to clear RSS feed data.

## To Configure RSS Settings

### Using Web Manager

- ◆ To configure RSS and view current RSS statistics, click **RSS** in the menu.

### Using the CLI

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

### Using XML

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

## Discovery

View the statistics and enable or disable the EDS-MD for device discovery. The query port server only responds to auto-discovery messages on port 0x77FE.

**Table 10-7 Discovery Settings**

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

## To Configure Discovery

### Using Web Manager

- ◆ To access the area with options to configure discovery and view current discovery statistics, click **Discovery** in the menu.

### Using the CLI

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

### Using XML

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

## SMTP Settings

**Table 10-8 SMTP Settings**

SMTP Settings	Description
<b>From Address</b>	Enter the From Address here. This is an email address and is required. If you wish to direct outbound email messages through a mail server, put your client email address here.
<b>Server Address</b>	Enter the Server Address to direct outbound email messages through a mail server.
<b>Server Port</b>	Enter the SMTP server port number. The default is 25
<b>Username</b>	Enter a Username to direct outbound email messages through a mail server.
<b>Password</b>	Enter a Password to direct outbound email messages through a mail server.
<b>Overriding Domain</b>	Enter the domain name to forge the sender domain name in the outgoing email message.  This might be necessary 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 that the email message is really from whom it says it's from.

### To Configure SMTP Settings

#### Using Web Manager

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

#### Using the CLI

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

#### Using XML

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

## Email Settings

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

**Table 10-9 Email Configuration**

Email – Configuration Settings	Description
<b>To</b>	Enter the email address to which the email alerts will be sent. Multiple addresses are separated by semicolon (;). Required field if email is to be sent.
<b>CC</b>	Enter the email address to which the email alerts will be copied. Multiple addresses are separated by semicolon (;).
<b>From</b>	Enter the email address from which email alerts will be sent. Multiple addresses are separated by semicolon (;). Required field if email is to be sent.

Email – Configuration Settings (continued)	Description
<b>Reply To</b>	Enter the email address to list in the Reply-To field of the email alert.
<b>Subject</b>	<b>Note:</b> Enter the subject for the email alert.
<b>Message File</b>	Enter the path of the file to send with the email alert. This file appears within the message body of the email, not as an attachment.
<b>Priority</b>	Select the priority level for the email alert: <ul style="list-style-type: none"> <li>◆ Urgent</li> <li>◆ High</li> <li>◆ Normal</li> <li>◆ Low</li> <li>◆ Very Low</li> </ul>

## To View, Configure, and Send Email

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

### Using Web Manager

- ◆ To view Email statistics, click **Email** in the menu and select **Email 1 -> Statistics**.
- ◆ To configure basic Email settings, click **Email** in the menu and select **Email 1 -> Configuration**.
- ◆ To send an email, click **Email** in the menu and select **Email 1 -> Send Email**.

### Using the CLI

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

### Using XML

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

## 11: Security Settings

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

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

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

### Public Key Infrastructure

Public key infrastructure (PKI) is based on an encryption technique that uses two keys: a public key and private key. Public keys can be used to encrypt messages which can only be decrypted using the private key. This technique is referred to as asymmetric encryption, as opposed to symmetric encryption, in which a single secret key is used by both parties.

### TLS (SSL)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), use asymmetric encryption for authentication. In some scenarios, only a server needs to be authenticated, in others both client and server authenticate each other. Once authentication is established, clients and servers use asymmetric encryption to exchange a secret key. Communication then proceeds with symmetric encryption, using this key.

SSH and some authentication methods on the EDS-MD wired IoT device gateways make use of SSL. The EDS-MD 4/8/16 unit supports SSLv3, TLS1.0, and TLA1.1.

TLS/SSL application hosts use separate digital certificates as a basis for authentication in both directions: to prove their own identity to the other party, and to verify the identity of the other party. In proving its own authenticity, the EDS-MD wired IoT device gateways will use its own "personal" certificate. In verifying the authenticity of the other party, the EDS-MD devices will use a "trusted authority" certificate.

In short:

- ◆ When using EAP-TLS, the EDS-MD wired IoT device gateway needs a personal certificate with matching private key to identify itself and sign its messages.
- ◆ When using EAP-TLS, EAP-TTLS or PEAP, the EDS-MD unit needs the authority certificate(s) that can authenticate those it wishes to communicate with.

## Digital Certificates

The goal of a certificate is to authenticate its sender. It is analogous to a paper document that contains personal identification information and is signed by an authority, for example a notary or government agency. With digital certificates, a cryptographic key is used to create a unique digital signature.

## Trusted Authorities

A private key is used by a trusted certificate authority (CA) to create a unique digital signature. Along with this private key is a certificate of authority, containing a matching public key that can be used to verify the authority's signature but not re-create it.

A chain of signed certificates, anchored by a root CA, can be used to establish a sender's authenticity. Each link in the chain is certified by a signed certificate from the previous link, with the exception of the root CA. This way, trust is transferred along the chain, from the root CA through any number of intermediate authorities, ultimately to the agent that needs to prove its authenticity.

## Obtaining Certificates

Signed certificates are typically obtained from well-known CAs, such as VeriSign, Inc. This is done by submitting a certificate request for a CA, typically for a fee. The CA will sign the certificate request, producing a certificate/key combo: the certificate contains the identity of the owner and the public key, and the private key is available separately for use by the owner.

As an alternative to acquiring a signed certificate from a CA, you can act as your own CA and create self-signed certificates. This is often done for testing scenarios, and sometimes for closed environments where the expense of a CA-signed root certificate is not necessary.

## Self-Signed Certificates

A few utilities exist to generate self-signed certificates or sign certificate requests. The EDS-MD wired IoT device gateways also have the ability to generate its own self-signed certificate/key combo. You can use XML to export the certificate in PEM format, but you cannot export the key. Hence, the internal certificate generator can only be used for certificates that are to identify that particular EDS-MD module.

## Certificate Formats

Certificates and private keys can be stored in several file formats. Best known are PKCS12, DER and PEM. Certificate and key can be in the same file or in separate files. Additionally, the key can be either be encrypted with a password or left in the clear. However, EDS-MD wired IoT device gateways currently only accept separate PEM files, with the key unencrypted.

Several utilities exist to convert between the formats.

---

## OpenSSL

OpenSSL is a widely used open source set of SSL related command line utilities. It can act as server or client. It can also generate or sign certificate requests, and can convert from and to several different of formats.

OpenSSL is available in binary form for Linux and Windows.

To generate a self-signed RSA certificate/key combo:

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

See [www.openssl.org](http://www.openssl.org) or [www.madboa.com/geek/openssl](http://www.madboa.com/geek/openssl) for more information.

**Note:** *Signing other certificate requests is also possible with OpenSSL but the details of this process are outside the scope of this document.*

## Steel Belted RADIUS

Steel Belted RADIUS is a commercial RADIUS server from Juniper Networks that provides a GUI administration interface. It also provides a certificate request and self-signed certificate generator.

The self-signed certificate has extension `.sbrpvk` and is in the PKCS12 format. OpenSSL can convert this into a PEM format certificate and key:

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

The `sbr_certkey.pem` file contains both certificate and key. If loading the SBR certificate into an EDS-MD wired IoT device gateway as an authority, you will need to edit it:

1. Open the file in any plain text editor.
2. Delete all info before `"----- BEGIN CERTIFICATE-----"` and after `"----- END CERTIFICATE-----"`, and then save as `sbr_cert.pem`.

SBR accepts trusted-root certificates in the DER format. Again, OpenSSL can convert any format into DER:

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

**Note:** *With SBR, when the identity information includes special characters such as dashes and periods, SBR changes the format it uses to store these strings and becomes incompatible with the current EDS-MD wired IoT device gateway release. Support may be added for this and other formats in future releases.*

## Free RADIUS

**Note:** Free RADIUS is another versatile Linux open-source RADIUS server.

## SSH Settings

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

Configuration is required when the EDS-MD device is either (1) the SSH server or (2) an SSH client. The SSH server is used by the CLI (Command Mode) and for tunneling in Accept Mode. The SSH client is for tunneling in Connect Mode.

To configure the EDS-MD wired IoT device gateway as an SSH server, there are two requirements:

- ◆ **Defined Host Keys:** both private and public keys are required. These keys are used for the Diffie-Hellman key exchange (used for the underlying encryption protocol).
- ◆ **Defined Users:** these users are permitted to connect to the EDS-MD device SSH server.

### SSH Server Host Keys

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

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

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

**Table 11-1 SSH Server Host Keys**

SSH Settings	Description
<b>Private Key</b>	Click <b>Choose File</b> to browse to and select the existing private key you want to upload. In Web Manager, you can also browse to the private key to be uploaded. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
<b>Public Key</b>	Click <b>Choose File</b> to browse to and select the existing public key you want to upload. In Web Manager, you can also browse to the public key to be uploaded.
<b>Key Type</b>	Select a key type to use for the new key: <ul style="list-style-type: none"> <li>◆ RSA</li> <li>◆ DSA</li> </ul>
<b>Bit Size</b>	Select a bit length for the new key: <ul style="list-style-type: none"> <li>◆ 512</li> <li>◆ 768</li> <li>◆ 1024</li> </ul>
<b>Submit (button)</b>	Click the <b>Submit</b> button after setting the information for <b>Upload Keys</b> or <b>Create New Keys</b> .

**Note:** SSH Keys from other programs may be converted to the required EDS-MD 4/8/16 unit format. Use Open SSH to perform the conversion.

## SSH Client Known Hosts

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

**Table 11-2 SSH Client Known Hosts**

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

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

## SSH Server Authorized Users

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

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

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

**Table 11-3 SSH Server Authorized Users**

SSH Settings	Description
<b>Username</b>	Enter a new username or edit an existing one.
<b>Password</b>	Enter a new password or edit an existing one.
<b>Public RSA Key</b>	Click <b>Choose File</b> to browse to and select the existing public RSA key you want to use with this user. In Web Manager, you can also browse to the public RSA key to be uploaded. If authentication is successful with the key, no password is required.
<b>Public DSA Key</b>	Click <b>Choose File</b> to browse to and select the existing public DSA key you want to use with this user. In Web Manager, you can also browse to the public DSA key to be uploaded. If authentication is successful with the key, no password is required.
<b>Add/Edit (key)</b>	Click the <b>Add/Edit</b> button after setting the information for <b>SSH Client: Authorized Users</b> .

## SSH Client Users

The SSH Client Users are used by all applications that play the role of an SSH Client. Specifically Tunneling in Connect Mode. To configure the EDS-MD wired IoT device gateway 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 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.

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

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

**Table 11-4 SSH Client Users**

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

**Table 11-5 Create New Keys**

SSH Settings	Description
<b>Username</b>	Enter the name that the device uses to connect to an SSH server.
<b>Key Type</b>	Select a bit length for the key: <ul style="list-style-type: none"> <li>◆ RSA</li> <li>◆ DSA</li> </ul>

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

## To Configure SSH Settings

### Using Web Manager

- ◆ To configure SSH, click **SSH** in the menu.

### Using the CLI

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

### Using XML

- ◆ Include in your file: `<configitem name="ssh username">`

## SSL Settings

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

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

**Note:** The blue text in the XML command strings of this chapter are to be replaced with a user-specified name.

### Create a New Credential

After creating a new credential, you can either establish your credential through [Certificate and Key Generation](#) or [Upload Certificate](#).

**Table 11-6 Create a New Credentials**

Upload Field	Description
Create new credential	Enter the name of the new credential to be created.
Submit (button)	Click the <b>Submit</b> button after entering the new credential name.

## To Create a New Credential

### Using Web Manager

- ◆ To create a new credential, click **SSL** in the menu and select **Credentials**.

### Using the CLI

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

### Using XML

- ◆ Not applicable.

## Upload Certificate

SSL certificates identify the EDS-MD wired IoT device gateway to peers. Certificate and key pairs can be uploaded to the EDS-MD unit through either the CLI or XML import mechanisms. Certificates can be identified on the EDS-MD wired IoT device gateway by a name provided at upload time.

**Table 11-7 Upload Certificate Settings**

Upload Certificate Settings	Description
New Certificate	Click <b>Choose File</b> to browse to and select the new certificate file to be uploaded. The SSL certificate to be uploaded. RSA or DSA certificates are allowed.  The format of the certificate must be PEM. It must start with “-----BEGIN CERTIFICATE-----” and end with “-----END CERTIFICATE-----”. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
New Private Key	Click <b>Choose File</b> to browse to and select the certificate type being uploaded. The key needs to belong to the certificate entered above.  The format of the file must be PEM. It must start with “-----BEGIN RSA PRIVATE KEY-----” and end with “-----END RSA PRIVATE KEY-----”. Read DSA instead of RSA in case of a DSA key. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
Submit (button)	Click the <b>Submit</b> button after selecting the certificate and private key information for the uploaded certificate.

## Certificate and Key Generation

The EDS-MD wired IoT device gateway can generate self signed certificates and their corresponding keys. This can be done for both the rsa and dsa certificate formats. Certificates can be identified on the EDS-MD unit by a name provided at generation time.

**Table 11-8 Certificate and Key Generation Settings**

Certificate Generation Settings	Description
<b>Country (2 Letter Code)</b>	Enter the 2-letter country code to be assigned to the new self-signed certificate. Examples: US for United States and CA for Canada
<b>State/Province</b>	Enter the state or province to be assigned to the new self-signed certificate.
<b>Locality (City)</b>	Enter the city or locality to be assigned to the new self-signed certificate.
<b>Organization</b>	Enter the organization to be associated with the new self-signed certificate.
<b>Organization Unit</b>	Enter the organizational unit to be associated with the new self-signed certificate.
<b>Common Name</b>	Enter the common name to be associated with the new self signed certificate, preferably matching the host name or the ip address of the device, whichever will be the intended access approach. This is a required field.
<b>Expires</b>	Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate. Example: An expiration date of May 9, 2018 is entered as 05/09/2018.
<b>Type</b>	Select the type of key: <ul style="list-style-type: none"> <li>◆ <b>RSA</b> = Public-Key Cryptography algorithm based on large prime numbers, invented by Rivest Shamir and Adleman. Used for encryption and signing.</li> <li>◆ <b>DSA</b> = Digital Signature Algorithm also based on large prime numbers, but can only be used for signing. Developed by the US government to avoid the patents on RSA.</li> </ul>
<b>Key Length</b>	Select the bit size of the new self-signed certificate. Choices are: <ul style="list-style-type: none"> <li>◆ 512 bit</li> <li>◆ 768 bit</li> <li>◆ 1024 bit</li> <li>◆ 2048 bit</li> <li>◆ 4096 bit</li> </ul> <p>The larger the bit size, the longer it takes to generate the key.</p>
<b>Submit (button)</b>	Click the <b>Submit</b> button after setting the information for new self-signed certificate.

## To Configure an Existing SSL Credential

Follow these steps after a new credential has been established via [Create a New Credential on page 79](#).

### Using Web Manager

- ◆ To configure an existing SSL Credential, click **SSL** in the menu, select **Credentials**, and click on the name of an existing SSL credential.

### Using the CLI

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

### Using XML

- ◆ Include in your file:

```
<configgroup name="ssl">
  and <configitem name="credentials" instance="name">
  and <value name="RSA certificate"/> or <value name="DSA certificate"/>
```

## Trusted Authorities

One or more authority certificates are needed to verify a peer's identity. These certificates do not require a private key.

Trusted Authorities Settings	Description
<b>Authority</b>	Click <b>Choose File</b> to browse to and select the SSL authority certificate.  RSA or DSA certificates are allowed.  The format of the authority certificate can be PEM or PKCS7. PEM files must start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----". Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
<b>Delete</b>	Click the <b>Delete</b> button beside a specific certificate authority to delete it.
<b>Delete All</b>	Click the <b>Delete All</b> button to delete all existing certificate authorities.

### Using Web Manager

- ◆ To upload an Authority Certificate, click **SSL** in the menu and select **Trusted Authorities**.

### Using the CLI

- ◆ To enter the SSL command level: `enable -> ssl`
- ◆ To enter the Trusted Authorities command level: `enable -> ssl -> trusted authorities`

**Using XML**

- ◆ Include in your file:

```
<configgroup name="ssl">
```

```
and <configitem name="trusted authority" instance="1">
```

```
and <configitem name="intermediate authority" instance="1">
```

# 12: Maintenance and Diagnostics Settings

## Filesystem Settings

Use the file system to list, view, create, upload, copy, move, remove, and transfer files. The EDS-MD wired IoT device gateway uses an EXT3 flash file system to store files.

### Statistics

The filesystem statistics page displays statistics and current usage information of the flash filesystem. The filesystem can be formatted here.

**Warning:** *Formatting the filesystem will delete all files on it.*

When the USB drive is connected to one of the two USB ports on the device, it will be automatically mounted and accessed using the filesystem. USB drives can be simultaneously connected to both the USB ports.

**Table 12-1 File Statistics**

Filesystem Commands	Description
Format	Displays a list of files on the EDS-MD 4/8/16 device, and their respective sizes.

### To View Statistics

#### Using Web Manager

- ◆ To view statistics, format the filesystem or configure USB auto mount features, click **Filesystem** in the menu and select **Statistics**.

This is a journaled file system, which means that changes to the file system are recorded before the actual changes themselves are made. In the event of power loss, the use of journaling can usually recover from changes that had been started but not completed.

Some file systems may contain a 'lost+found' directory. In the event of power loss in the midst of file system I/O, file data that cannot be fully recovered will be placed in this directory. It is recommended to always restart the system from the Web Manager application or the CLI.

**Note:** *It is recommended to always use the Web Manager application or the CLI to shutdown/restart the system.*

### File Display

View the list of existing files and their contents in the ASCII or hexadecimal formats.

**Table 12-2 File Display Settings**

File Display Commands	Description
ls	Displays a list of files on the EDS-MD 4/8/16 device, and their respective sizes.

<b>cat</b>	Displays the specified file in ASCII format.
<b>dump</b>	Displays the specified file in a combination of hexadecimal and ASCII formats.
<b>pwd</b>	Print working directory.
<b>cd</b>	Change directories.
<b>show tree</b>	Display file/directory tree.

## To Display Files

### Using Web Manager

- ◆ To view existing files and file contents, click **Filesystem** in the menu and select **Browse**.

### Using the CLI

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

### Using XML

- ◆ Not applicable.

## File Modification

The EDS-MD 4/8/16 wired IoT device gateway allows for the creation and removal of files on the Filesystem.

**Table 12-3 File Modification Settings**

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

## File Transfer

Files can be transferred to and from the EDS-MD 4/8/16 device via the TFTP protocol. This can be useful for saving and restoring XML configuration files. Files can also be uploaded via HTTP.

**Table 12-4 File Transfer Settings**

File Transfer Settings	Description
<b>Create</b>	Type in a <b>File</b> or <b>Directory</b> name and click the <b>Create</b> button. The newly created File or Directory will appear above.

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

## To Transfer or Modify Filesystem Files

### Using Web Manager

- ◆ To create a new file or directory, upload an existing file, copy or move a file, or view existing files, click **Filesystem** in the menu and select **Browse**.

### Using the CLI

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

### Using XML

- ◆ Not applicable.

## Protocol Stack Settings

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

## IP Settings

**Table 12-5 IP Protocol Stack Settings**

Protocol Stack IP Settings	Description
<b>IP Time to Live</b>	This value typically fills the Time To Live in the IP header. SNMP refers to this value as "ipDefaultTTL". Enter the number of hops to be transmitted before the packet is discarded.
<b>Multicast Time to Live</b>	This value fills the Time To Live in any multicast IP header. Normally this value will be one so the packet will be blocked at the first router. It is the number of hops allowed before a Multicast packet is discarded. Enter the value to be greater than one to intentionally propagate multicast packets to additional routers.

### To Configure IP Protocol Stack Settings

#### Using Web Manager

- ◆ To configure IP protocol settings, click **Protocol Stack** in the menu and select **IP**.

#### Using the CLI

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

#### Using XML

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

## ICMP Settings

**Table 12-6 ICMP Protocol Stack Settings**

Protocol Stack ICMP Settings	Description
<b>State</b>	Click to enable or disable the processing of ICMP messages. This includes both incoming and outgoing messages.

### To Configure ICMP Protocol Stack Settings

#### Using Web Manager

- ◆ To configure ICMP protocol settings, click **Protocol Stack** in the menu and select **ICMP**.

#### Using the CLI

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

#### Using XML

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

## To View ICMP Protocol Stack Settings

### Using Web Manager

- ◆ To view ICMPv6 protocol settings, click **Protocol Stack** in the menu and select **ICMPv6**.

### Using the CLI

- ◆ Not applicable.

### Using XML

- ◆ Not applicable.

## ARP Settings

*Table 12-7 ARP Protocol Stack Settings*

Protocol Stack ARP Settings	Description
<b>IP Address</b>	Enter the IP address to add to the ARP cache. After entering the MAC address, click the <b>Add</b> button.
<b>MAC Address</b>	Enter the MAC address to add to the ARP cache. After also entering the IP address, click the <b>Add</b> button.
<b>Add (button)</b>	Click the <b>Add</b> button after entering the ARP Cache information.
<b>Remove</b>	Click the <b>Remove</b> link beside a specific address to remove it.
<b>Remove All</b>	Click the <b>Remove All</b> link underneath all listed addresses to remove all the addresses.

## To Configure ARP Network Stack Settings

### Using Web Manager

- ◆ To configure ARP protocol settings, click **Protocol Stack** in the menu and select **ARP**.

### Using the CLI

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

### Using XML

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

## SMTP Settings

*Table 12-8 SMTP Protocol Stack Settings*

Protocol Stack SMTP Settings	Description
Relay Address	Enter the relay address to be used to direct all outbound email messages through a mail server.
Relay Port	Enter the relay port to be used for all outbound email messages through a mail server.

### To Configure SMTP Protocol Stack Settings

#### Using Web Manager

- ◆ To configure ARP protocol settings, click **Protocol Stack** in the menu and select **SMTP**.

#### Using the CLI

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

#### Using XML

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

## Diagnostics

The EDS-MD wired IoT device gateways have several tools for diagnostics and statistics. Various options allow for the configuration or viewing of IP socket information, ping, traceroute, memory, and processes.

### Hardware

#### To View Hardware Information

##### Using Web Manager

- ◆ To view hardware information, click **Diagnostics** in the menu and select **Hardware**.

##### Using the CLI

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

##### Using XML

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

### IP Sockets

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

## To View the List of IP Sockets

### Using Web Manager

- ◆ To view IP Sockets, click **Diagnostics** in the menu and select **IP Sockets**.

### Using the CLI

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

### Using XML

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

## Ping

The ping command can be used to test connectivity to a remote host.

**Table 12-9 Ping Settings**

Diagnostics: Ping Settings	Description
<b>Host</b>	Enter the IP address or host name for the EDS-MD unit to ping.
<b>Count</b>	Enter the number of ping packets EDS-MD device should attempt to send to the <b>Host</b> . The default is <b>5</b> .
<b>Timeout</b>	Enter the time, in seconds, for the EDS-MD to wait for a response from the host before timing out. The default is <b>5</b> seconds.
<b>Submit (Button)</b>	Click the <b>Submit</b> button after entering ping information.

## To Ping a Remote Host

### Using Web Manager

- ◆ To ping a Remote Host, click **Diagnostics** in the menu and select **Ping**.

### Using the CLI

- ◆ To enter the command level: `enable, ping <host> <count> <timeout>`

### Using XML

- ◆ Not applicable.

## Traceroute

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

Table 12-10 Traceroute Settings

Diagnostics: Traceroute Settings	Description
Host	Enter the IP address or DNS hostname. This address is used to show the path between it and the EDS-MD device when issuing the traceroute command.
Protocol	Select the traceroute protocol from the drop-down menu.
Submit (button)	Click the <b>Submit</b> button after entering traceroute information.

## To Perform a Traceroute

### Using Web Manager

- ◆ To perform a Traceroute, click **Diagnostics** in the menu and select **Traceroute**.

### Using the CLI

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

### Using XML

- ◆ Not applicable.

## Log

Table 12-11 Log Settings

Diagnostics: Log	Description
Output	Select a diagnostic log output type: <ul style="list-style-type: none"> <li>◆ <b>Disable</b> - Turn off the logging feature.</li> <li>◆ <b>Filesystem</b> - Directs logging to /log.txt.</li> <li>◆ <b>Line (1 2 3 or 4)</b> - Directs logging to the selected serial line.</li> </ul>
Max Length	Set the maximum length of the log.txt file in Kbytes. <i>Note: This setting becomes available when Filesystem is selected.</i>

## To Configure the Diagnostic Log Output

### Using Web Manager

- ◆ To configure the Diagnostic Log output, click **Diagnostics** in the menu and select **Log**.

### Using the CLI

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

### Using XML

- ◆ Include in your file:  

```
<configgroup name="diagnostics">  
and  
<configitem name="log">
```

## Memory

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

### To View Memory Usage

#### Using Web Manager

- ◆ To view memory information, click **Diagnostics** in the menu and select **Memory**.

#### Using the CLI

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

#### Using XML

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

## Processes

The EDS-MD 4/8/16 device shows all the processes currently running on the system. It shows the Process ID (PID), Parent Process ID (PPID), user, CPU percentage, percentage of total CPU cycles, and process command line information.

### To View Process Information

#### Using Web Manager

- ◆ To view process information, click **Diagnostics** in the menu and select **Processes**.

#### Using the CLI

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

#### Using XML

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

## Threads

The EDS-MD 4/8/16 unit threads information shows details of threads in the `ltrx_evo` task which can be useful for technical experts in debugging.

## To View Thread Information

### Using Web Manager

- ◆ To view thread information, click **Diagnostics** in the menu and select **Threads**.

### Using the CLI

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

## Clock

The Clock settings page can be updated by manually entering the date and time or synchronizing with the SNTP.

**Table 12-12 Clock Settings**

Clock	Description
<b>Method</b>	Select a clock change method from the drop-down menu: <ul style="list-style-type: none"> <li>◆ <b>Manual:</b> this option allows you to directly set the date and time.</li> <li>◆ <b>SNTP:</b> this option keeps the time synchronized with the NTP Server.</li> </ul>
<b>Date</b>	Use the drop-down menu to select the <b>Year, Month and Day</b> . This option becomes available when the <b>Manual</b> method is selected.
<b>Time (24 hour)</b>	Use the drop-down menu to select the <b>Hour, Min and Sec</b> . This option becomes available when the <b>Manual</b> method is selected.
<b>NTP Server</b>	Set NTP Server to an NTP server's IP address or hostname. This option becomes available when the <b>SNTP</b> method is selected.
<b>Time Zone</b>	Select the geographical time zone from the drop-down list.

## To Specify Clock Setting Method

### Using Web Manager

- ◆ To view clock information, click **Clock** in the menu.

### Using the CLI

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

### Using the XML

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

## System Settings

The EDS-MD wired IoT device gateway system settings allow for rebooting the device, restoring factory defaults, uploading new firmware and updating a system's short and long name.

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

**Table 12-13 System Settings**

System Settings	Description
<b>State</b>	Click to enable or disable the reboot schedule.
<b>Reboot Device</b>	Click the <b>Reboot</b> button to reboot the device.
<b>Restore Factory Defaults</b>	Click <b>Factory Defaults</b> to restore the device to the original factory settings. All configuration will be lost. The EDS-MD unit automatically reboots upon setting back to the defaults.
<b>Upload New Firmware</b>	FTP to the EDS-MD device. Upload new firmware to the EDS-MD unit by clicking <b>Choose File</b> to browse to the new firmware file, and click <b>Upload</b> button to upload the chosen file to the system. The device automatically reboots upon the installation of new firmware.
<b>Short Name</b>	Enter a short name for the system name. A maximum of 32 characters are allowed.
<b>Long Name</b>	Enter a long name for the system name. A maximum of 64 characters are allowed.
<b>Submit (button)</b>	Click <b>Submit</b> after entering the system name.

## To Reboot or Restore Factory Defaults

### Using Web Manager

- ◆ To access the area with options to reboot, restore to factory defaults, upload new firmware, update the system name (long or short names) or to view the current configuration, click **System** in the menu.

### Using the CLI

- ◆ To enter the command level: `enable`

### Using XML

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

# 13: Management Interface Settings

## Command Line Interface Settings

The Command Line Interface settings allow you to control how users connect to and interact with the command line of the EDS-MD wired IoT device gateway. It is possible to configure access via the Telnet and SSH protocols, in addition to general CLI options.

### Basic CLI Settings

The basic CLI settings control general CLI access and usability options.

**Table 13-1 CLI Configuration Settings**

Command Line Interface Configuration Settings	Description
<b>Login Password</b>	Enter the password for the admin account. The factory default password is the last 8 characters of the Device ID (for devices manufactured after January 1, 2020) or "PASS" (for all older devices).
<b>Enable Level Password</b>	Enter the password for access to the Command Mode Enable level. There is no password by default.
<b>Quit Connect Line</b>	Enter the <b>Quit Connect Line</b> string to be used to terminate a Telnet and SSH session and resume the CLI. Type <control> before the key to be pressed while holding down the <b>[Ctrl]</b> key (example: <b>&lt;control&gt;L</b> )
<b>Inactivity Timeout</b>	Set a time period in which the CLI session should disconnect if no data is received. Enter 0 to disable. Blank the display field to restore the default.
<b>Line Authentication</b>	Select to enable or disable authentication for CLI access on the serial lines.

### To View and Configure Basic CLI Settings

#### Using Web Manager

- ◆ To view CLI statistics, click **CLI** in the menu and select **Statistics**.
- ◆ To configure basic CLI settings, click **CLI** in the menu and select **Configuration**.

#### Using the CLI

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

#### Using XML

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

### Telnet Settings

The Telnet settings control CLI access to the EDS-MD 4/8/16 wired IoT device gateway telnet over the Telnet protocol.

**Table 13-2 Telnet Settings**

Telnet Settings	Description
<b>Telnet State</b>	Select to enable or disable CLI access via Telnet
<b>Telnet Port</b>	Enter an alternative Telnet Port to override the default used by the CLI server. Blank the field to restore the default.
<b>Telnet Max Sessions</b>	Specify the maximum number of concurrent Telnet sessions that will be allowed.
<b>Telnet Authentication</b>	Select to enable or disable authentication for Telnet logins.

## To Configure Telnet CLI Settings

### Using Web Manager

- ◆ To configure Telnet settings, click **CLI** in the menu and select **Configuration**.

### Using the CLI

- ◆ To enter the Telnet command level: enable -> config -> cli -> Telnet

### Using XML

- ◆ Include in your file:
 

```
<configgroup name="Telnet">
and
<configitem name="state">
and
<configitem name="authentication">
```

## SSH CLI Settings

The SSH settings control CLI access to the EDS-MD device over the SSH protocol.

**Table 13-3 SSH Settings**

SSH Settings	Description
<b>SSH State</b>	Select to enable or disable CLI access via SSH.
<b>SSH Port</b>	Specify the SSH Port and override the default, as needed. Blank the field to restore the default.
<b>SSH Max Sessions</b>	Specify the maximum number of concurrent SSH sessions that will be allowed.

## To Configure SSH Settings

### Using Web Manager

- ◆ To configure SSH settings, click **CLI** in the menu and select **Configuration**.

### Using the CLI

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

### Using XML

- ◆ Include in your file:

```
<configgroup name="ssh"> and <configitem name="state">
```

## XML Settings

The EDS-MD wired IoT device gateway allows for the configuration of units using an XML configuration record (XCR). Export a current configuration for use on other EDS-MD unit or import a saved configuration file.

### XML: Export Configuration

You can export the current system configuration in XML format. The generated XML file can be imported later to restore a configuration. It can also be modified and imported to update the configuration on this EDS-MD unit or another. The XML data can be dumped to the screen or exported to a file on the file system.

By default, all groups are exported. You may also select a subset of groups to export.

**Table 13-4 XML Exporting Configuration**

XML Export Configuration Settings	Description
<b>Export to browser</b>	Select this option to export the XCR data in the selected fields to the browser. Use the "xcr dump" command to export the data to the browser.
<b>Export to local file</b>	Select this option to export the XCR data to a file on the device. If you select this option, enter a file name for the XML configuration record. Use the "xcr export" command to export the data to a local file.
<b>Export secrets</b>	Select to export secret password and key information. Use only with a secure link, and save only in secure locations. <b>Note:</b> Only use with extreme caution.
<b>Comments</b>	Select this option to include descriptive comments in the XML.
<b>Lines to Export</b>	Select instances to be exported in the line, serial, tunnel and terminal groups. Click <b>Clear All</b> to clear all checkmarks, or <b>Select All</b> to check all checkmarks.
<b>Groups to Export</b>	Check the configuration groups that are to be exported to the XML configuration record. The group list should be comma delimited and encased in double quotes. The list of available groups can be viewed with the "xcr list" command. Click <b>Clear All</b> to clear all checkmarks, or <b>Select All but Networking</b> to check all checkmarks except Networking.
<b>Export (button)</b>	Click <b>Export</b> after selecting the <b>XML: Export Configuration</b> settings.

## To Export Configuration in XML Format

### Using Web Manager

- ◆ To export configuration format, click **XML** in the menu and select **Export Configuration**.

### Using the CLI

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

### Using XML

- ◆ Not applicable.

## XML: Export Status

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

**Table 13-5 Exporting Status**

XML Export Status Settings	Description
<b>Export to browser</b>	Select this option to export the XCR data in the selected fields to the browser. Use the “xcr dump” command to export the data to the browser.
<b>Export to local file</b>	Select this option to export the XCR data to a file on the device. If you select this option, enter a file name for the XML configuration record. Use the “xcr export” command to export the data to a local file.
<b>Lines to Export</b>	Select instances to be exported in the line, serial, tunnel and terminal groups. Click <b>Clear All</b> to clear all checkmarks, or <b>Select All</b> to check all checkmarks.
<b>Groups to Export</b>	Check the configuration groups that are to be exported to the XML configuration record. The group list should be comma delimited and encased in double quotes. The list of available groups can be viewed with the “xcr list” command. Click <b>Clear</b> Click <b>Clear All</b> to clear all checkmarks, or <b>Select All</b> to check all checkmarks.
<b>Export (button)</b>	Click <b>Export</b> after selecting the <b>XML: Export Status</b> settings.

## To Export in XML Format

### Using Web Manager

- ◆ To export configuration format, click **XML** in the menu and select **Export Status**.

### Using the CLI

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

### Using XML

- ◆ Not applicable.

## XML: Import Configuration

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

The XML data can be imported from a file on the file system or pasted into a CLI session. The groups to import can be specified at the command line, the default is all groups.

### Configuration from External File

This import option requires entering the path and file name of the external XCR file you want to import.

### Configuration from Filesystem

This import option picks up settings from a file and your import selections of groups, lines, and instances. The list of files can be viewed from the filesystem level of the CLI.

### Line(s) from single line Settings on the Filesystem

This import option copies line settings from an the input file containing only one Line instance to all of the selected Lines.

**Table 13-6 Import Configuration from Filesystem Settings**

Import Configuration from Filesystem Settings	Description
<b>Filename</b>	Enter the name of the file on the EDS-MD unit (local to its filesystem) that contains XCR data.
<b>Lines to Import</b>	Select filter instances to be imported in the line, serial, tunnel and terminal groups. This affects both Whole Groups to Import and Text List selections. Click <b>Clear All</b> to clear all checkmarks, or <b>Select All</b> to check all checkmarks.
<b>Whole Groups to Import</b>	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group. Click <b>Clear All</b> to clear all checkmarks, or <b>Select All but Networking</b> to check all checkmarks except Networking.
<b>Import (button)</b>	Click <b>Import</b> after selecting the <b>XML: Import Configuration</b> settings.

## To Import Configuration in XML Format

### Using Web Manager

- ◆ To import configuration, click **XML** in the menu and select **Import Configuration**.

### Using the CLI

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

### Using XML

- ◆ Not applicable.

## 14: MACH10 Client Settings

The EDS-MD wired IoT device gateway comes integrated with MACH10® cloud platform to allow for the remote management of devices. To set up the MACH10 client, you need to configure the following settings:

- ◆ **MACH10 Client** - to connect to the MACH10 cloud platform.
- ◆ **Line Configuration** - to enable remote management and data access to your application or device attached on the serial line.

### MACH10 Client

#### To Configure MACH10 Client

This page displays the configuration and status for MACH10 client.

**Table 14-1 MACH10 Client Status**

MACH10 Client	Description
Client	Status of the MACH10 client.
Last Status Update	Time of the last status update.
Last Content Check	Time of the last content check.
Available Updates	Available firmware or configuration updates.

**Table 14-1 MACH10 Client Configuration**

MACH10 Client	Description
State	Click to enable or disable the MACH10 client.
Device ID	Enter the MACH10 Device ID.
Device Key	Enter the MACH10 Device Key.
Device Name	Enter the MACH10 Device Name.
Device Description	Enter the MACH10 Device Description.
Status Update Interval	Enter the <b>Status Update Interval</b> in minutes.
Content Check Interval	Enter the <b>Content Check Interval</b> in hours.
Apply Firmware Updates	Select to enable or disable the automatic setting.
Apply Configuration Updates	Select when to <b>Apply Configuration Updates</b> from the drop-down menu: <ul style="list-style-type: none"><li>◆ <b>Never</b>: signifying no configuration updates will be applied.</li><li>◆ <b>If unchanged</b>: signifying configuration updates will only be applied if no changes have been made locally.</li><li>◆ <b>Always</b>: signifying configuration updates will always apply.</li></ul>
Reboot After Update	Automatically reboot device after firmware or configuration update. <b>Note:</b> Setting causes automatic reboot after a firmware update.

MACH10 Client	Description
Active Connection	Select the connection instance to use when connecting to MACH10.

**Table 14-2 MACH10 Connection 1 Configuration**

**Note:** The following section describes the fields to configure MACH10 Connection 1 settings; these steps also apply to Connection 2.

MACH10 Client	Description
Host	Enter the host name or IP address
Port	Enter the MACH10 port
Secure Port	Click to enable or disable the MACH10 client secure port 443.
Validate Certificates	Click to enable or disable the MACH10 client <b>Validate Certificates</b> .
MQTT State	Enable or Disable MQTT.
MQTT Host	Hostname or IP address of MQTT server.
MQTT Port	Update the port of MACH10 MQTT server. When configured, a total of 32 consecutive ports will be reserved.
MQTT Security	Enable SSL for MQTT.
Use Proxy	Enable or disable using a proxy for this connection.
Proxy Type	Proxy server type. The supported type is: SOCKS5.
Proxy Host	Enter the Hostname or IP address of the proxy server.
Proxy Port	Enter the port number of the proxy server.
Proxy Username	Enter the username of the proxy server.
Proxy Password	Enter the password of the proxy server.
Submit (button)	Click the <b>Submit</b> button to enter the settings. The <b>Submit</b> button appears when new settings are entered.

## Line Configuration

### To Configure MACH10 Line

This page displays the configuration and status for the MACH10 Line client. The number of lines that can be configured depends on the specific model of the EDS-MD wired IoT device gateway. EDS-MD devices contain four, eight, or sixteen serial lines.

**Table 14-2 MACH10 Line Configuration**

MACH10 Line	Description
Select Line:	Select the serial line to configure.
State	Click to enable or disable the MACH10 line client.
Project Tag	Enter the <b>MACH10 Project Tag</b> name.
Status Update Interval	Enter the <b>Status Update Interval</b> in minutes. The status update interval is the frequency in which the gateway will contact the MACH10 server.

MACH10 Line	Description
<b>Content Check Interval</b>	Enter the <b>Content Check Interval</b> in hours. The content check interval is the frequency in which the gateway contacts the server for new content.
<b>Command Delimiter</b>	Enter the Command Delimiter for attached serial devices. <i>Note: Send delimiter before command and after response is received.</i>
<b>Submit (button)</b>	Click the <b>Submit</b> button to enter the settings. The <b>Submit</b> button appears when new settings are entered.

## To Configure MACH10

### Using Web Manager

- ◆ To configure MACH10 Client, click **MACH10 > Client**.
- ◆ To configure MACH10 Line, click **MACH10 > Line Configuration**.

### Using the CLI

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

### Using XML

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

# 15: Updating Firmware

## Obtaining Firmware

Obtain the most up-to-date firmware and release notes for the unit from the Lantronix Web site ([www.lantronix.com/products/eds-md/](http://www.lantronix.com/products/eds-md/)) or by using anonymous FTP (<ftp://ftp.lantronix.com/>).

## Loading New Firmware through Web Manager

Upload the firmware using the web manager System page.

*To upload new firmware:*

1. Select **System** in the menu bar. The System page appears.

Figure 15-1 Uploading New Firmware

The screenshot shows the EDS-MD web manager interface. The top header includes the 'EDS-MD' logo and the 'LANTRONIX' brand name. A left-hand navigation menu lists various system functions, with 'System' highlighted in orange. The main content area is titled 'System' and contains several sections: 'Reboot Device' with a 'Reboot' button; 'Restore Factory Defaults' with a 'Factory Defaults' button; 'Upload New Firmware' with 'Choose File' (showing 'No file chosen') and 'Upload' buttons; and 'Name' configuration with 'Short Name' and 'Long Name' input fields and a 'Submit' button. Below this is a 'Current Configuration' table. On the right side, there is a '[Logout]' link and a 'WARNING' section with detailed instructions about rebooting and configuration restoration.

Current Configuration	
Firmware Version:	8.1.0.4R4
Short Name:	EDS-MD8
Long Name:	Lantronix EDS-MD8

2. Click **Browse** (under the **Upload New Firmware** heading) to browse to the firmware file.

3. Select the file and click **Open**.
4. Click **Upload** to install the firmware on the EDS-MD unit.
5. Click **OK** in the confirmation popup which appears. The firmware will be installed and the device will automatically reboot afterwards.
6. Close and reopen the web manager internet browser to view the device's updated web pages.

**Note:** You may need to increase *HTTP Max Bytes* in some cases where the browser is sending data aggressively within *TCP Windows size limit* when file (including firmware upgrade) is uploaded from webpage. See [HTTP Settings on page 67](#).

## Loading New Firmware through FTP

Firmware may be updated by sending the file to the EDS-MD 4, EDS-MD 8 or EDS-MD 16 wired IoT device gateway over an FTP connection. The destination file name on the EDS-MD unit must have a "firmware.rom" type of format. The device will reboot upon successful completion of the firmware upgrade.

Example FTP session:

```
$ ftp 192.168.10.127
Connected to 192.168.10.127.
220 (vsFTPD 2.0.7)
Name (192.168.10.127:user): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put edsmd_8_1_0_4R4
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 File receive OK.
9308164 bytes sent in 3.05 seconds (3047859 bytes/s)
ftp> quit
221 Goodbye.
```

## 16: Branding the EDS-MD Gateway

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

- ◆ [Web Manager Customization](#)
- ◆ [Short and Long Name Customization](#)

### Web Manager Customization

Customize the Web Manager's appearance by modifying `index.html`, `style.css`, and the product logo. The style (fonts, colors, and spacing) of the Web Manager is controlled with `style.css`. The text and graphics are controlled with `index.html`. The product logo is the image in top-left corner of the page and defaults to a product name image.

**Note:** *The recommended dimensions of the new graphic are 300px width and 50px height.*

The Web Manager files are hidden and are incorporated directly into the firmware image but may be overridden by placing the appropriate file in the appropriate directory on the EDS-MD 4/8/16 unit file system.

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

1. FTP to the EDS-MD 4/8/16 device.
2. Make a directory (`mkdir`) and name it `http/config`.
3. Change to the directory (`cd`) that you created in step 2 (`http/config`).
4. Save the contents of `index.html` and `style.css` by using a web browser and navigating to `http://<EDS-MD hostname>/config/index.html` and `http://<EDS-MD hostname>/config/style.css`.
5. Modify the file as required or create a new one with the same name.
6. To customize the product logo, save the image of your choice as `logo.gif`.
7. Put the file(s) by using `put <filename>`.
8. Type `quit`. The overriding files appear in the file system's `http/config` directory.
9. Restart any open browser to view the changes.
10. If you wish to go back to the default files in the firmware image, simply delete the overriding files from the file system.

### Short and Long Name Customization

You can customize the short and long names in your EDS-MD wired IoT device gateway. The names display in the CLI show command and in the System web page in the Current Configuration table. The short name is used for the show command. Both names display in the CLI Product Type field.

**Note:** See [System Settings \(on page 93\)](#) for additional configuration options available on the Systems page.

**Table 16-1 Short and Long Name Settings**

Name Settings	Description
<b>Short Name</b>	Enter a short name for the system name. A maximum of 32 characters are allowed.
<b>Long Name</b>	Enter a long name for the system name. A maximum of 64 characters are allowed.

## To Customize Short or Long Names

### Using Web Manager

- ◆ To access the area with options to customize the short name and the long name of the product, or to view the current configuration, click **System** in the menu.

### Using the CLI

- ◆ To enter the command level: `enable`

### Using XML

- ◆ Include in your file:
 

```
<configitem name="short name">
and
<configitem name="long name">
```

## Appendix A: Lantronix Technical Support

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

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

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

## Appendix B: Binary to Hexadecimal Conversions

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

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

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

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

### Converting Binary to Hexadecimal

Following are two simple ways to convert binary numbers to hexadecimal notation.

#### Conversion Table

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

#### Scientific Calculator

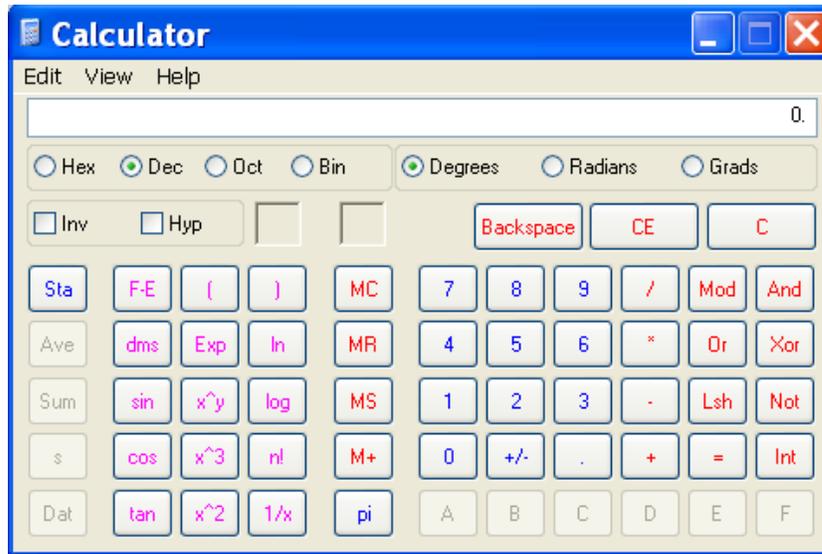
Another simple way to convert binary to hexadecimal is to use a scientific calculator, such as the one available on the Windows operating systems. For example:

1. On the Windows Start menu, click **Programs -> Accessories -> Calculator**.
2. On the View menu, select **Scientific**. The scientific calculator appears.
3. Click **Bin** (Binary), and type the number you want to convert.

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

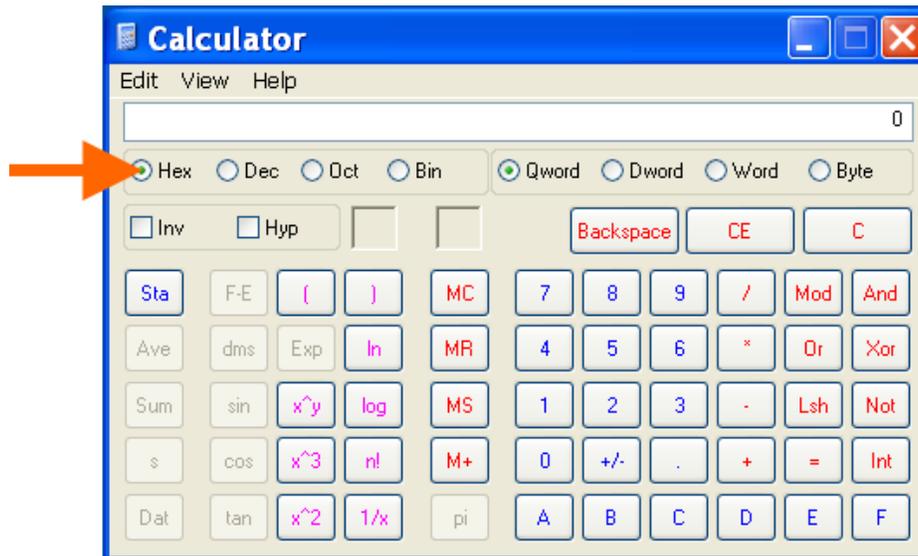
Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Figure B-2 Windows Scientific Calculator



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

Figure B-3 Hexadecimal Values in the Scientific Calculator



## Appendix C: Compliance

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

Manufacturer's Name & Address:

Lantronix, Inc.  
7535 Irvine Center Drive  
Suite 100  
Irvine, CA 92618, USA

Product Name Model: Lantronix® EDS-MD® 4, EDS-MD 8 and EDS-MD 16 Port Device Servers

Conform to the following standards or other normative documents:

**Table C-1 Applicable Medical Standards**

Emissions	Immunity
EN 60601-1-2: 2015	EN 60601-1-2: 2015
CISPR 11:2015 + A1: 2016	IEC/EN 61000-4-2: 2009
EN 61000-3-2: 2014	IEC/EN 61000-4-3: 2006 + A1: 2008 + A2: 2010
EN 61000-3-3: 2013	IEC/EN 61000-4-4: 2012
	IEC/EN 61000-4-5: 2014
	IEC/EN 61000-4-6: 2013
	IEC/EN 61000-4-8: 2009, 2010
	IEC/EN 61000-4-11: 2004

**Table C-2 Applicable ITE Standards**

Emissions	Immunity
FCC Part 15 Subpart B, Class A	EN 55024: 2010
ICES-003 Issue 6, Class A	EN 61000-4-2: 2009
CISPR 32: 2012, Class A	EN 61000-4-3: 2006 + A1: 2008 + A2: 2010
VCCI V-3/2010-04, Class A Emissions	EN 61000-4-4: 2012
EN 61000-3-2: 2014	EN 61000-4-5: 2014
EN 61000-3-3: 2013	EN 61000-4-6: 2013
	EN 61000-4-8: 2009, 2010
	EN 61000-4-11: 2004

**Note:** In the event of an ESD surge to the unit, a full power cycle may be needed on the unit for it to regain its full functionality.

Figure C-3 Suppliers Declaration of Conformity



### SUPPLIERS DECLARATION OF CONFORMITY

We, Lantronix, hereby declare that the product listed below, to which this Declaration of Conformity relates, is in conformity with the Standards and other Normative Documents listed below:

Product Type: MULTI-PORT MEDICAL DEVICE SERVER - EDS-MD  
Product Number: EDSOR04P-01, EDSOR08P-01, EDSOR16P-01,  
EDSMG04P, EDSMG08P, EDSMG16P  
Rated: 100-240 VAC, 50/60 Hz, 0.4A  
Intended use: Commercial installations, indoor use

#### North America

**Medical Safety:**

- ANSI/AAMI ES60601-1: 2005 + C1:2009 + A2: 2010
- CAN/CSA-C22.2 NO. 60601-1-08

**Non-Medical Safety:**

- UL 60950-1-2011, 2nd Edition
- CAN/CSA C22.2 No. 60950-1-07, 2nd Edition, 2006-07

**Emissions:**

- FCC Part 15, Subpart B, Class A
- ICES-003 Issue 6 Class A

#### European Union

**Medical Safety: Medical Device Directive (93/42/EEC)**

- EN 60601-1: 2006 + AC: 2010 + A1: 2013
- IEC 60601-1: 2005 + A1: 2012

**Non-Medical Safety: Low Voltage Directive (2014/35/EC)**

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

**Emissions: Directives (2014/30/EU)**

- EN 60601-1-2: 2015
- EN 55032: 2012, Class A
- EN 61000-3-2: 2014
- EN 61000-3-3: 2013

**Immunity: Directives (2014/30/EU)**

- EN 60601-1-2: 2015
- EN 55024: 2010
- IEC/EN 61000-4-2: 2009
- IEC/EN 61000-4-3: 2006 + A1: 2008 + A2: 2010
- IEC/EN 61000-4-4: 2012
- IEC/EN 61000-4-5: 2014
- IEC/EN 61000-4-6: 2013
- IEC/EN 61000-4-8: 2009, 2010
- IEC/EN 61000-4-11: 2004

#### Other Countries

• **Australia**

- CISPR 11: 2015 + A1: 2016
- CISPR 32: 2012, Class A Emissions
- AS/NZS CISPR 22: 2009, Class A Emissions
- EN 55032: 2012, Class A

• **Japan**

- VCCI V-3: 2010-04, Class A Emissions
- National Deviation to IEC 60601-1: 1988 + A1: 1991 + A2: 1995 based on JIST 0601-1

"Lantronix, 7535 Irvine Center Drive, Suite 100, Irvine, CA 92618, USA declares that the equipment specified above conforms to the referenced EU Directives and Harmonized Standards."

Signature: 

Date: 9-16-2017

Name: Fathi Hakam

Title: VP of Engineering

CERT-DOC-EDS-MD rev G

Figure C-4 EU Declaration of Conformity

**LANTRONIX<sup>®</sup>**

**CE**

**EU DECLARATION OF CONFORMITY**

**Manufacturer's Name:** LANTRONIX INC.  
**Manufacturer's Address:** 7535 Irvine Center Drive, Suite 100  
Irvine, CA. 92618. USA

**Type of Product:** MULTI-PORT MEDICAL DEVICE SERVER - EDS-MD  
**Product number:** EDSOR04P-01, EDSOR08P-01, EDSOR16P-01,  
EDSMG04P, EDSMG08P, EDSMG16P

**Rated:** 100-240 VAC, 50/60 Hz, 0.4A  
**Intended use:** Commercial installations, indoor use

**Manufacturer's Quality System:**

  
TUV Rheinland

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

**Category of Equipment:** Class 1 (Earthed)

**Applicable EU Directives:**

**Safety: *Medical Safety: Medical Device Directive (93/42/EEC)***

- EN 60601-1: 2006 + AC: 2010 + A1: 2013
- IEC 60601-1: 2005 + A1: 2012

**EMC: *Directive (2014/30/EU)***

- EN 60601-1-2: 2015
- EN 61000-3-2: 2014
- EN 61000-3-3: 2013
- EN 55032: 2012/AC: 2013, Class A Emissions
- EN 55024: 2010
- EN 610000-4-2: 2008, 2009
- EN 61000-4-3: 2006 + A1: 2008 + A2: 2010
- EN 61000-4-4: 2012
- EN 61000-4-5: 2014
- EN 61000-4-6: 2013
- EN 61000-4-8: 2009, 2010
- EN 61000-4-11: 2004

**EU Directive 2011/65/EU for Restriction of Hazardous Substance (RoHS2) with exemption 7(c)-I**

**Statement of Conformity:** The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: \_\_\_\_\_ Date: 9-16-2019

Name: Fathi Hakam Title: VP of Engineering

CERT-DOC-EDS-MD rev G

---

**Manufacturer's Contact:**

Lantronix  
7535 Irvine Center Drive  
Suite 100  
Irvine, CA 92618, USA  
Tel: 949-453-3990  
Fax: 949-453-3995

**RoHS, REACH and WEEE Compliance Statement**

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

## Appendix D: Lantronix Power Cords, Cables, Adapters and Serial Port Pinouts

Lantronix cables and adapters for use with EDS-MD 4, EDS-MD 8 and EDS-MD 16 wired IoT device gateways are listed here according to part number and application.

### Cables and Adapters

**Table D-1 Lantronix Cables and Adapters**

Lantronix P/N	Description	Applications
500-103-R	RJ45-to DB9F	Connects the RJ45 RS232 serial ports of EDS-MD to a DB9M DTE interface of a PC or serial device to check that serial ports in the EDS-MD are functioning properly.
200.2066A	Adapter RJ45-to-DB25M	Allows a standard straight-pinned CAT5 cable to connect the EDS-MD RJ45 serial ports to the DB25F DTE interface of a serial device.
200.2067A	Adapter RJ45-to-DB25F	Allows a standard straight-pinned CAT5 cable to connect the EDS-MD RJ45 serial ports to the DB25M DTE interface of a serial device.
200.2069A	Adapter RJ45-to-DB9M	Allows a standard straight-pinned CAT5 cable to connect the EDS-MD RJ45 serial ports to the DB9F DTE interface of a serial device.
200.2070A	Adapter RJ45-to-DB9F	Allows a standard straight-pinned CAT5 cable to connect the EDS-MD to the DB9M DTE interface of a PC or serial device.
200.2071	Adapter RJ45-to-DB9M	Allows a standard straight-pinned CAT5 cable to connect the EDS-MD RJ45 serial ports to the DB9F DCE interface of a serial device.
200.2072	Adapter RJ45-to-DB9F	Allows a standard straight-pinned CAT5 cable to connect the EDS-MD to the DB9M DCE interface of a PC or serial device.
200.2073	Adapter RJ45-to-DB25M	Allows a standard straight-pinned CAT5 cable to connect the EDS-MD RJ45 serial ports to the DB25F DCE interface of a serial device.
200.2074	Adapter RJ45-to-DB25F	Allows a standard straight-pinned CAT5 cable to connect the EDS-MD RJ45 serial ports to the DB25M DCE interface of a serial device.
930-073-R	Power Cord, Hospital Grade, US	Connects the EDS-MD to an AC power outlet, for the United States.
930-074-R	Power Cord, Hospital Grade, EU	Connects the EDS-MD to an AC power outlet, for Europe.
930-075-R	Power Cord, Hospital Grade, UK	Connects the EDS-MD to an AC power outlet, for the United Kingdom.
930-076-R	Power Cord, Hospital Grade, Australia	Connects the EDS-MD to an AC power outlet, for Australia.
930-077-R	Power Cord, Hospital Grade, Israel	Connects the EDS-MD to an AC power outlet, for Israel.
ADP010104-01	Adapter "Rolled" RJ45-to-RJ45	Allows a standard straight-pinned CAT5 cable to connect the EDS-MD to an RJ45 console port on products from Cisco and other manufacturers.

## Adapters and Serial Port Pinouts

Figure D-2 RJ45 Pinout Diagram

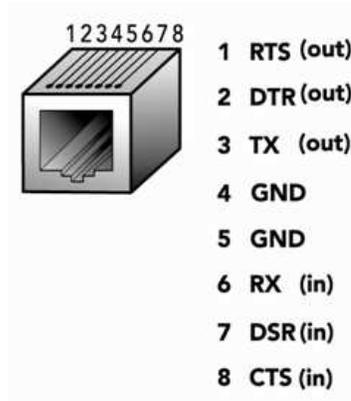
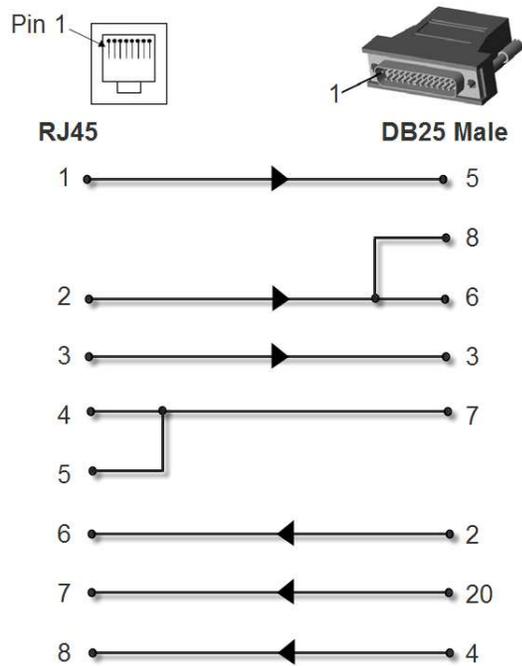
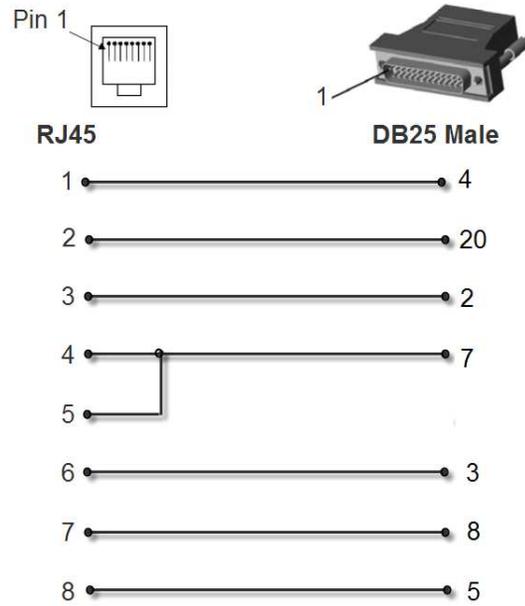


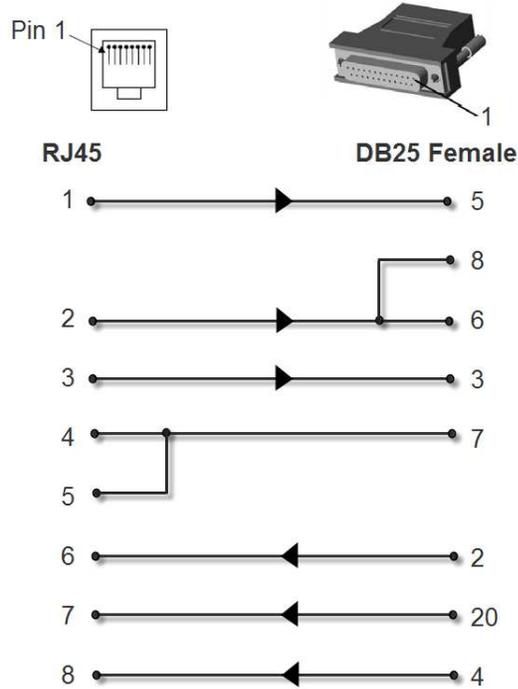
Figure D-3 RJ45 Receptacle to DB25M DTE Adapter (PN 200.2066A)



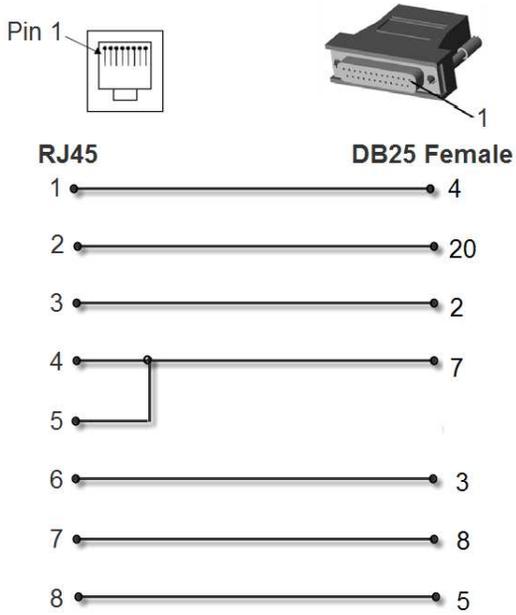
**Figure D-4 RJ45 Receptacle to DB25M DCE Adapter (PN 200.2073)**



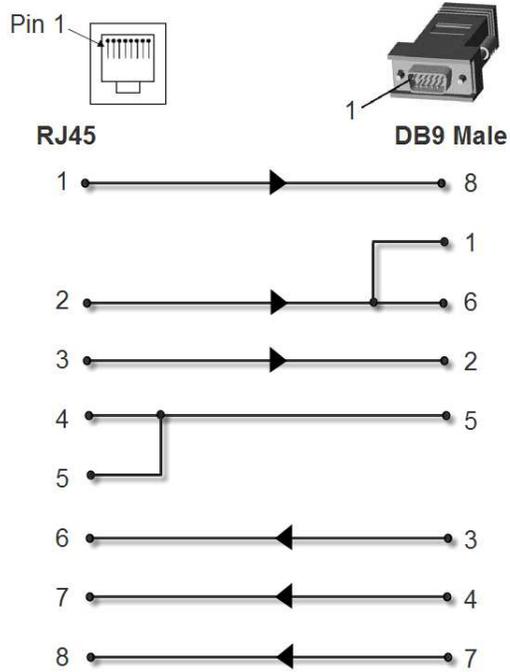
**Figure D-5 RJ45 Receptacle to DB25F DTE Adapter (PN 200.2067A )**



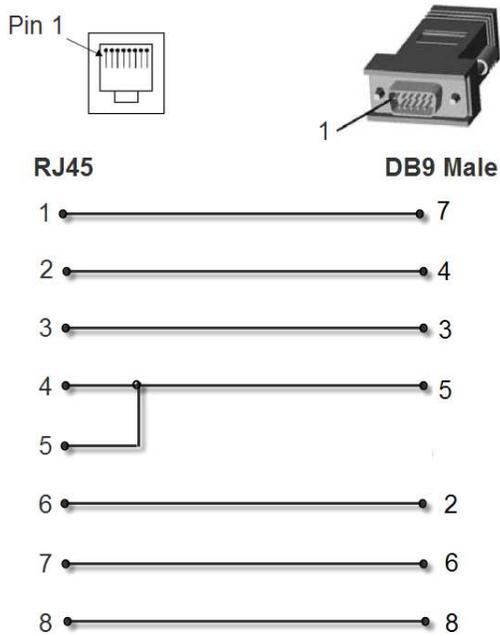
**Figure D-6 RJ45 Receptacle to DB25F DCE Adapter (PN 200.2074)**



**Figure D-7 RJ45 Receptacle to DB9M DTE Adapter (PN 200.2069A)**



**Figure D-8 RJ45 Receptacle to DB9M DCE Adapter (PN 200.2071)**



**Figure D-9 RJ45 Receptacle to DB9F DTE Adapter (PN 200.2070A)**

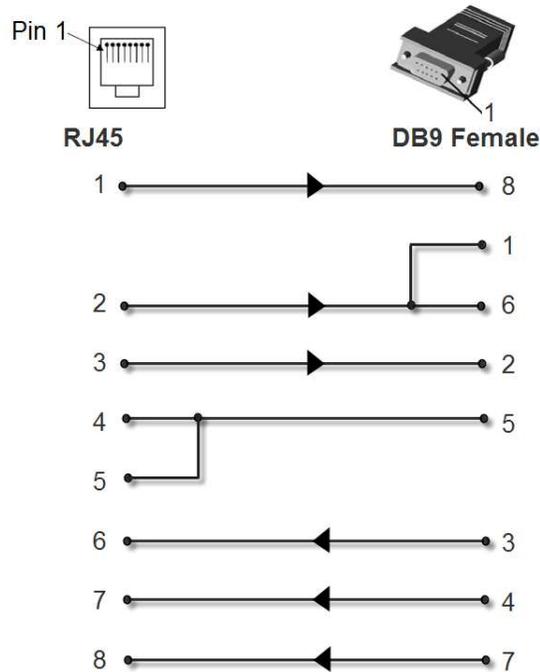


Figure D-10 RJ45 Receptacle to DB9F DCE Adapter (PN 200.2072)

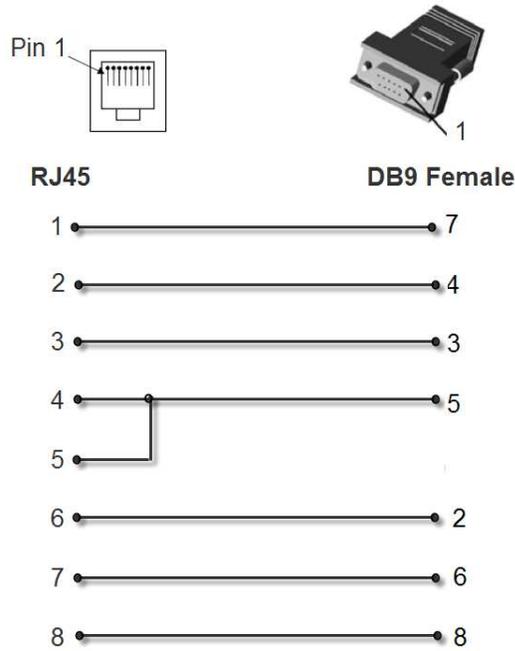
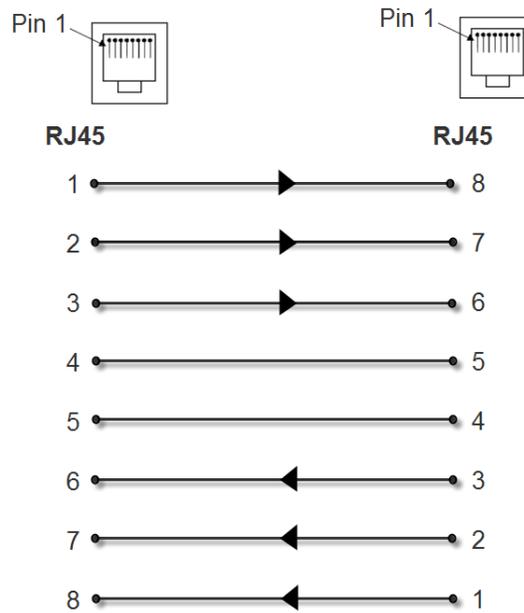


Figure D-11 RJ45 to RJ45 Adapter (ADP010104-01)



**Note:** The cable ends of the ADP010104-01 are an RJ45 socket on one end and a RJ45 plug on the other instead of RJ45 sockets on both ends.