X300 Series IoT Cellular Gateway User Guide

Part Number PMD-00153
Revision B January 2023

Intellectual Property

© 2023 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

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

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

Windows and *Internet Explorer* are registered trademarks of Microsoft Corporation. *Firefox* is a registered trademark of the Mozilla Foundation. *Chrome* is a trademark of Google 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/technical-support/warranty/

Contacts

Lantronix, Inc.
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free:800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about-us/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.

Revision History

Date	Rev.	Comments
July 2022	A	Initial document
January 2023	B	Updated for firmware version 1.9.0.0R26. ◆ Updated quick setup and status based on UI enhancements. ◆ Added X300 and updated X304 model descriptions. ◆ Updated package contents. ◆ Updated ConsoleFlow client configuration options. ◆ Added country code selection for Wi-Fi operation.

For the latest revision of this product document, please check our online documentation at www.lantronix.com/support/documentation.

Contents

1: About this Guide 15

Purpose 15
Summary of Chapters 15
Additional Documentation 17

2: Introduction 18

Key Features 18
- InfiniShield™ Security 18
- Software Features 18
- Lantronix Software Services 19

Applications 19
SKU Information 19
Hardware Components 21
- General Specification 21
- Front Panel 22
- Back Panel 24
- LEDs 25
- Cellular 26
- SIM Slot 27
- Antenna Connections 27
- Certified Antennas 27
- Ethernet Port (LAN) 28
- Serial Port 29
- Power Input 30
- Power Consumption 30
- Reset Button 30
- Product Label 31

3: Installation 32

Package Contents 32
User Supplied Items 32
Accessories 33
Preparing to Install 34
- Enabling DHCP Client on Your Computer 34

SIM Card Management 34
Physical Installation 35
- Insert SIM Card 35
- Connect the Antennas 37
- Connect the AC Power 37
- Connect the Gateway to a Computer 38

Default Configuration 40
Web Admin Page 40
Wireless Access Point SSID 40
Default Interface Configuration 40

4: Web Administration Interface 41

Logging In 42
Change Passwords After Initial Login 43
Logging Out 44

5: Using Lantronix Provisioning Manager 45

Installing Lantronix Provisioning Manager 45
Accessing the Gateway Using Lantronix Provisioning Manager 45

6: Quick Setup 46

Quick Setup 46

7: Status 48

Overview (Page) 48
System Status 48
ConsoleFlow Status 49
Memory Status 50
MWAN Interfaces Status 50
Firewall Status 50
Network Status 51
Cellular Status 52
Network Status 53
Active DHCP and DHCPv6 Leases Status 53
Wireless Status 54
Dynamic DNS Status 54
Routes 55
System Log 56
Kernel Log 56
Processes 56
Realtime Graphs 57
Load 57
Traffic 58
Wireless 58
Connection 59
Load Balancing 61
Interface 61
Detail 61

Diagnostics 61
Troubleshooting 61

8: System 62

System 62
General Settings 62
Logging 63
Time Synchronization 64
Language and Style 65
Administration 65
Router Password 65
SSH Access 65
SSH-Keys 66
Software 66
Configure OPKG 67
Startup 68
Initscripts 68
Local Startup 69
Scheduled Tasks 69
LED Configuration 70
Backup / Flash Firmware 72
Actions 72
Configuration 73
Custom Commands 73
Write Custom Shell Command 73
Run Custom Shell Command 74
Reboot 74
Schedule a Reboot 74

9: VPN 76

IPsec (Internet Protocol Security) 76
OpenVPN 80
OpenVPN Instances 80
Template-based Configuration 82
OpenVPN Configuration File 82

10: Services 83

Agents 83
DOTA 84
Lantronix Server 84
Custom Server 84
Dynamic DNS 86

External Filesystems 89
GPS 90
Description of NMEA Messages 91
GPGGA Format 92
GPRMC Format 93
GPGSV Format 94
GPGSA Format 95
GPVTG Format 96
Keepalived 98
Keepalived Configuration 98
Logs Information 101
Page Selector 101
Reporting Agent 102
Sending Data 103
Data Format 104
Service Actions 104
SMS 105
SMS Configuration 105
SMS AT Commands 105
Ethernet SMS 108
Live Message 109
SNMPD 110
SNMP Architecture 110
SNMP Versions 110
SNMP Configuration 111
SNMPTRAPD 120
SNMP-TRAP Configuration 120
uHTTPd 123
Web Server Configuration 123

11: Network 126

Interfaces 126
Interfaces Overview 126
Interface Status 128
Interface Protocols 129
Protocol Descriptions 130
CELLULAR Interface 140
LAN Interface 141
WWAN and WWAN6 Interface 143
Add Virtual Interface 144
Wireless 148
Wireless Network Configuration 149
DHCP and DNS 152

General Settings 152
Resolv and Host Files 153
TFTP Settings 153
Advanced Settings 154
Static Leases 155
Hostnames 156
Static Routes 156
Static IPv4 Routes 156
Static IPv6 Routes 157
Diagnostics 159
Firewall 160
General Settings 160
Port Forwards 163
Traffic Rules 164
Custom Rules 166
QoS 167
Load Balancing 169
How it works 169
Globals 169
Interfaces 170
Members 172
Policies 173
Rules 175
Notification 176

12: Bluetooth 177

Bluetooth Settings 177
Configure Bluetooth settings 177
Scan for and Pair a Device 177
Bluetooth SPP 178
Configure Bluetooth SPP Connection 179
Configure Tunnel SPP Slave 179
Configure Tunnel SPP Master 179

13: ConsoleFlow 181

Client 181
ConsoleFlow Line 182

14: Discovery 184

Query Port 184

15: Serial 185

Serial Line Statistics 185
Serial Line Configuration 185

16: SSL 187

Credentials 187
Trusted Authorities 188

17: Tunnel 190

Tunnel Statistics 190
Tunnel Modbus RTU to Modbus TCP 190
Tunnel Accept 191
Tunnel Connect 194
Hosts 195
Connecting Multiple Hosts 196
Tunnel Disconnect 197

A: Compliance Information 198

FCC Statement 199
Federal Communication Commission Interference Statement 199
ISED Statement 200
EU Declaration of Conformity 201
EU Statements 204
RF Output Power of X303F202S 210
RF Output Power of X304G002S 211

B: Power Cable Schematic 212

Power Cable Schematic 212

C: List of Acronyms and Protocols 213

D: Lantronix Technical Support 216

List of Figures

Figure 2-1 X300 model Front View 22
Figure 2-2 X303 model Front View 23
Figure 2-3 X304 model Front View 23
Figure 2-4 X300 model Back View 24
Figure 2-5 X303 model Back View 24
Figure 2-6 X304 model Back View 25
Figure 2-7 Ethernet Port 28
Figure 2-8 RJ45 Connector RS-232 / RS- 485 Interface 29
Figure 2-9 DC Input Interface 30
Figure 2-10 Sample Product Label 31
Figure 4-1 Web Admin Interface 41
Figure 4-2 Web Admin Login Page 43
Figure 7-1 IPv4 Firewall Status 51
Figure 7-2 Realtime CPU Load Graph 57
Figure 7-3 Realtime Network Traffic Graph (eth1) 58
Figure 7-4 Realtime Wireless Usage Graph (client) 59
Figure 7-5 Realtime Connection Traffic Graph 60
Figure 10-1 Reporting Agent Data Format (excerpt) 104
Figure 10-2 Service Actions 104
Figure 10-3 VACM Configuration Model 112
Figure 11-1 Interfaces Overview (partial view) 127
Figure 11-2 WAN Interface Status 128
Figure 11-3 LAN Interface (Static Address) Configuration 142
Figure 11-4 WWAN Interface (DHCP client) Configuration 144
Figure 11-5 Network Add New Interface 145
Figure 11-6 Wireless Overview 148
Figure A-1 X300 / X303 EU Declaration of Conformity 201
Figure A-2 X304 EU Declaration of Conformity 202
Figure A-3 X304 UKCA Declaration of Conformity 203
Figure B-1 3-pin Power Cable 212

List of Tables

Table 2-1 X300 Series Models 19
Table 2-2 General Specification 21
Table 2-3 Top Panel LEDs 25
Table 2-4 X300 model Top Panel LEDs 26
Table 2-5 X303 / X304 Cellular Data Rates 26
Table 2-6 X303 / X304 Cellular Bands 26
Table 2-7 Certified Antennas 27
Table 2-8 Ethernet RJ45 Connector Pin Assignment and LEDs 28
Table 2-9 Serial RJ45 Connector Pin Assignment and LEDs 29
Table 2-10 X300 Series Power Consumption 30
Table 3-1 Lantronix Accessories 33
Table 3-2 Default Web Admin Page Credentials 40
Table 3-3 Default Wireless Access Point SSID 40
Table 3-4 Default Network Interface Configuration 40
Table 6-1 Quick Setup Network Configuration 46
Table 7-1 System Status Overview 48
Table 7-2 System Status Overview 49
Table 7-3 Memory Status Overview 50
Table 7-4 Firewall Status 51
Table 7-5 Cellular Status Overview 52
Table 7-6 Network Status Overview 53
Table 7-7 Active DHCP Leases Status Overview 53
Table 7-8 Wireless Status Overview 54
Table 7-9 Routes Status 55
Table 7-10 Processes Status 56
Table 8-1 System General Settings 62
Table 8-2 Syslog Configuration 63
Table 8-3 System Time Synchronization Configuration 64
Table 8-4 Language and Style Configurations 65
Table 8-5 SSH Access Configuration 66
Table 8-6 Software Package Details 67
Table 8-7 OPKG Package Manager Configuration 68
Table 8-8 Initscripts Actions 69
Table 8-9 Cron Shortcuts 70
Table 8-10 Trigger Descriptions 70
Table 8-11 LED Configuration 71

Table 8-12 Backup, Restore, and Flash Operations 72
Table 8-13 Custom Commands Configuration 74
Table 8-14 Schedule Reboot Time Specification 75
Table 9-1 IPsec General Settings 76
Table 9-2 IPsec Advanced Settings 78
Table 10-1 Agent Configurations 83
Table 10-2 DOTA using Lantronix Server 84
Table 10-3 DOTA Custom Server Configuration 85
Table 10-4 Dynamic DNS Client Configuration 86
Table 10-5 External Filesystems Configuration 89
Table 10-6 GPS Service Configuration 90
Table 10-7 GGA Data Format 92
Table 10-8 RMC Data Format 93
Table 10-9 GPGSV Data Format 94
Table 10-10 GSA Data Format 95
Table 10-11 VTG Data Format 96
Table 10-12 Keepalived Configuration 99
Table 10-13 Reporting Agent Configuration 102
Table 10-14 Reporting Agent Data Send Configuration 103
Table 10-15 SMS Service Configuration 105
Table 10-16 SMS AT Command Syntax 105
Table 10-17 Ethernet SMS Configuration 108
Table 10-18 SNMP Security Models and Levels 111
Table 10-19 SNMP General Settings Configuration 114
Table 10-20 SNMP v1/v2/USM VACM Settings 116
Table 10-21 SNMP VACM Settings Engine ID Configuration 118
Table 10-22 SNMP VACM Settings SNMPv3-USM 119
Table 10-23 SNMP Trap Settings Configuration 119
Table 10-24 SNMP-Trap Receiver Configuration 120
Table 10-25 uHTTPd Server Configuration 123
Table 10-26 uHTTPd Self-signed Certificate Configuration 125
Table 11-1 Network Interfaces Overview 127
Table 11-2 Wireless Overview and Associated Stations 128
Table 11-3 Network Interface Protocols 129
Table 11-4 Static Address Protocol Settings 130
Table 11-5 DHCP Client Protocol Settings 132
Table 11-6 DHCPv6 Client Protocol Settings 134
Table 11-7 PPPoE Protocol Settings 135

Table 11-8 UMTS/GPRS/EV-DO Cellular Protocol Settings 136
Table 11-9 QMI Cellular Protocol Settings 138
Table 11-10 VPN Tunnel Protocols 145
Table 11-11 Wireless Overview and Associated Stations 148
Table 11-12 Wireless Device Configuration 149
Table 11-13 Wireless Interface Configuration 150
Table 11-14 General Configuration of DHCP Server and DNS-Forwarder 152
Table 11-15 Resolv and Host File Configuration for DHCP and DNS 153
Table 11-16 TFTP Configuration for DHCP and DNS 153
Table 11-17 Advanced Configuration for DHCP and DNS 154
Table 11-18 DHCP and DNS Static Leases 155
Table 11-19 Hostnames Configuration 156
Table 11-20 Static IPv4 Routes Configuration 156
Table 11-21 Static IPv6 Routes Configuration 157
Table 11-22 Diagnostics - Network Utilities 159
Table 11-23 Cable Diagnostics Status Messages 159
Table 11-24 Firewall Global Settings 160
Table 11-25 Firewall Zones Configuration (LAN) 162
Table 11-26 Firewall Port Forwards 163
Table 11-27 Port Forwarding Configuration for Firewall Zone 163
Table 11-28 Firewall Zone Traffic Rules 164
Table 11-29 Firewall Traffic Rule Configuration 165
Table 11-30 QoS Configure Classes 167
Table 11-31 MWAN Globals Configuration 170
Table 11-32 MWAN Interface 170
Table 11-33 MWAN Interface Configuration 171
Table 11-34 MWAN Members 172
Table 11-35 MWAN Members Configuration 173
Table 11-36 MWAN Policy 174
Table 11-37 MWAN Policy Configuration 174
Table 11-38 MWAN Rules 175
Table 11-39 MWAN Rules Configuration 175
Table 12-1 Bluetooth Settings Configuration 177
Table 12-2 Bluetooth Scan Results 178
Table 12-3 Bluetooth SPP Line Configuration 179
Table 13-1 ConsoleFlow Client Configuration 181
Table 13-2 ConsoleFlow Line 183
Table 15-1 Serial Line Configuration 185

Table 16-1 SSL Credentials - Upload Certificate 187
Table 16-2 SSL Credentials - Create Self-Signed Certificate 188
Table 16-3 SSL Trusted Authority 189
Table 17-1 Tunnel for Modbus RTU to Modbus TCP 190
Table 17-2 Tunnel Accept Mode Configuration 191
Table 17-3 Tunnel Connect Mode Configuration 194
Table 17-4 Host Configuration 195
Table 17-5 Tunnel Disconnect Configuration 197
Table A-1 Regional Certifications 198
Table A-2 Country Transmitter IDs 198
Table A-3 EU Statements 204

1: About this Guide

Purpose

This guide provides the information needed to install, configure, and use the Lantronix X300 series IoT cellular gateways using the web interface. The X300 series gateways are designed for IoT professionals for M2M and enterprise IoT applications requiring faultless connectivity.

The information in this document assumes the reader has knowledge of networking fundamentals and routing concepts for data communication, control, and management functions.

For additional support and product resources, please visit the Lantronix Technical Support portal.

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
Chapter 2: Introduction	Describes the main features of the product and the protocols it supports.
Chapter 3: Installation	Instructions for installing the X300 series gateways. List of accessories for the gateway. Provides the default credentials for access to the web interface and wireless access point.
Chapter 4: Web Administration Interface	Instructions for accessing the web administration interface and using it to configure settings for the X300 series gateways. The configuration chapters (6 -17) provide detailed instructions for using the web interface.
Chapter 5: Using Lantronix Provisioning Manager	Instructions for using Lantronix Provisioning Manager to locate and configure the gateway.
Chapter 6: Quick Setup	Instructions for configuring the Quick Setup.
Chapter 7: Status	Overview of the gateway status pages.
Chapter 8: System	Instructions for configuring the system features, including clock, syslog, SSH access and keys, password, enabling startup scripts, scheduling cron jobs, LED behavior, and executing custom shell commands. Instructions for operations and maintenance, installing software packages, firmware upgrades, configuration backup, restoring configuration, reboot and factory reset.
Chapter 9: VPN	Instructions for configuring and enabling OpenVPN and IPsec tunneling.
Chapter 10: Services	Instructions for configuring and enabling router and gateway services, and for starting and stopping services. Instructions for configuring industrial protocol services.

Chapter	Description
Chapter 11: Network	Instructions for configuring and enabling the wired, wireless, and cellular network interfaces. Instructions for configuring DHCP and DNS, static routes, firewall, QoS, and load balancing. Instructions for defining hostname and running network diagnostic commands.
Chapter 12: Bluetooth	Instructions for configuring and enabling Bluetooth SPP for serial data transmission.
Chapter 13: ConsoleFlow	Instructions for configuring ConsoleFlow client settings.
Chapter 14: Discovery	Instructions for enabling discovery on query port 0x77FE.
Chapter 15: Serial	Instructions for configuring serial settings on the RS-232 and RS-485 lines.
Chapter 16: SSL	Instructions for creating SSL credentials, uploading SSL certificates and private keys from a CA or self-signed, generating self-signed certificates, and uploading trusted authority certificates.
Chapter 17: Tunnel	Instructions for configuring and enabling serial Tunnel connections.
Appendix A: Compliance Information	Provides compliance information.
Appendix B: Power Cable Schematic	Provides information about accessories, cabling, and connectors.
Appendix C: List of Acronyms and Protocols	Provides a glossary of relevant acronyms and protocols.
Appendix D: Lantronix Technical Support	Provides instructions for contacting Latronix Technical Support.

Additional Documentation

Visit the Lantronix web site at https://www.lantronix.com/support/documentation for the latest documentation for this product series.

Document	Description
X300 Series Quick Start Guides	Provides hardware installation instructions, directions to connect the X300 series gateway, and network IP configuration information.
Using the X300 Series SDK Application Note	Describes how to use the SDK to create custom packages and the Image Builder to build custom firmware images.
X300 Series Product Brief	Provides X300 series gateway product overview information and specifications.

2: Introduction

The X303 and X304 models offer LTE-M and LTE Cat 1 cellular communication, Wi-Fi, BLE, Ethernet, and serial interface in a small, industrial-grade form factor. The X300 model offers Wi-Fi, BLE, Ethernet, and serial interface in the same industrial-grade form factor. With built-in security to help prevent cyber-attacks, the X300 series gateway is a robust and reliable solution for mission-critical applications provided with Console Flow, extended warranty, and connectivity services.

Key Features

InfiniShield™ Security

- Built-in security framework for mission-critical applications
- Secure boot, secure firmware updates, secure storage
- Secure communications, secure network attach

Software Features

- Administration and network protocols
  - Web user interface, setup wizard, console log viewer, save/load configuration
  - NTP, SMS/OTA remote configuration, TR-069 capable, Lantronix Provisioning Manager
- Redundancy
  - Ethernet, Cellular, Wi-Fi (configurable as failover or load balancing)
- Resilience
  - Network connectivity watchdog (configurable), internal application watchdog
- Wi-Fi
  - Client or Access point, multiple SSID
  - WPA, WPA-PSK/WPA2-PSK/WPA3-PSK
  - Enterprise Security (WPA2-Enterprise/WPA3-Enterprise)
  - EAP-TLS, EAP-TTLS (MS-CHAPv2), EAP-PEAPv0/EAP-MS-CHAPV2, EAP-PEAPv1, EAP-FAST
  - Bluetooth and Wi-Fi coexistence
- Routing features and protocols
  - DHCP, static routing, port forwarding, traffic routing, static/dynamic DNS, DNS proxy, NAT, STP
  - VPN and tunneling protocols – PPTP client, L2TP, OpenVPN client/server/passthrough, GRE, IPsec up to 4 channels
  - Security – zone-based firewall, VLAN, DMZ, HTTPS local & remote connection, SIM PIN
- Performance and Fault Management
  - Real time processor load and interface (WAN/LAN/Wi-Fi), traffic analysis, ICMP, traceroute, NS lookup

- Essential IoT Applications
  - Serial and Bluetooth SPP to Network tunnels
  - Python runtime and packages available as IPKs for installation
  - Add your own IoT edge applications with the SDK and Image Builder

Lantronix Software Services

- Lantronix ConsoleFlow – Secure cloud platform to manage remote IoT gateways through a single pane of glass.
- Lantronix Connectivity Services – North American and global cellular data plans and VPN security to manage your SIMs and services.
- Lantronix LEVEL Technical Services – Provides dedicated technical support experts to assist your team with technical challenges you may encounter.

Applications

The X300 series gateway is suitable for these application scenarios:

- Industry 4.0
- Energy management
- Smart farming
- Remote asset management

SKU Information

Table 2-1 X300 Series Models

Lantronix Part Number	Description
X300F202S	GATEWAY INCL. 3 YEARS DEVICE MANAGEMENT SERVICE. ROUTERS ◆ MULTI-MODE SERIAL PORT X1; ◆ 1T1R WI-FI 5; BLUETOOTH 5.1; ◆ ETHERNET LAN PORT X1; E ◆ PACK SOFTWARE SUITE
X303F202S	GATEWAY INCL. 3 YEARS DEVICE MANAGEMENT SERVICE. LTE-M ROUTER ◆ MULTI-MODE SERIAL PORT X1; ◆ 1T1R WI-FI 5; BLUETOOTH 5.1; ◆ ETHERNET LAN PORT X1; ◆ EPACK SOFTWARE SUITE
X304G00AS	GATEWAY INCL. 3 YEARS DEVICE MANAGEMENT SERVICE. LTE CAT. 1 ROUTER FOR THE USA, CANADA; ◆ MULTI-MODE SERIAL PORT X1; ◆ 1T1R WI-FI 5; BLUETOOTH 5.1; ◆ ETHERNET LAN PORT X1; ◆ EPACK SOFTWARE SUITE

Lantronix Part Number	Description
X304G002S	GATEWAY INCL. 3 YEARS DEVICE MANAGEMENT SERVICE. LTE CAT. 1 ROUTER FOR EMEA, ASIA PACIFIC; ◆ MULTI-MODE SERIAL PORT X1; ◆ 1T1R WI-FI 5; BLUETOOTH 5.1; ◆ ETHERNET LAN PORT X1; ◆ EPACK SOFTWARE SUITE
X304G007S	GATEWAY INCL. 3 YEARS DEVICE MANAGEMENT SERVICE. LTE CAT. 1 ROUTER FOR JAPAN, SOUTH KOREA; ◆ MULTI-MODE SERIAL PORT X1; ◆ 1T1R WI-FI 5; BLUETOOTH 5.1; ◆ ETHERNET LAN PORT X1; ◆ EPACK SOFTWARE SUITE
X304G00CS	GATEWAY INCL. 3 YEARS DEVICE MANAGEMENT SERVICE. LTE CAT. 1 ROUTER FOR CHINA, THAILAND, INDONESIA, INDIA; ◆ MULTI-MODE SERIAL PORT X1; ◆ 1T1R WI-FI 5; BLUETOOTH 5.1; ◆ ETHERNET LAN PORT X1; ◆ EPACK SOFTWARE SUITE

Hardware Components

General Specification

Table 2-2 General Specification

Component	Specification
Physical	
Casing	Brushed aluminum alloy
Dimensions (W x D x H)	79 x 79 x 23.5 mm
Weight	150 grams, approximately
Environmental	
Operating temperature	-30 °C ~ +70 °C, up to 95% RH
Storage temperature	-40 °C ~ +85 °C, up to 95% RH
Memory	
SPI NOR Flash memory	8MB
Parallel NAND Flash memory	256MB
DDR2 SDRAM	128MB (factory option doubled to 256MB)
Power	
Power	Input voltage: 9V - 30V DC 3-pin Nano-Fit™ header
Digital Input (Ignition)	One (1) digital input, on the middle pin of the 3-pin header Input: 0 V DC ~ 2.5 V DC => ZERO; 3 V DC ~ 50 V DC => ONE
Interfaces	
Ethernet	10/100 BASE-T One (1) LAN port , via RJ-45 header Two (2) LEDs (link, activity)
Wi-Fi	X303: IEEE 802.11ac/a/b/g/n 1T1R Wi-Fi 5 / Bluetooth 5.1, with 1 RP-SMA antenna connector X300 and X304: IEEE 802.11ac/a/b/g/n 2x2 MIMO Wi-Fi 5 / Bluetooth 5.1, with 2 RP-SMA antenna connectors
Dual SIM operation	X303 / X304 only: Universal MFF SIM Auxiliary (external) mini-SIM holder
GNSS	X304 only: Qualcomm's IZat™ gen. 8C gpsOne; via a dedicated SMA connector
User data storage	Internal: via the parallel NAND Flash memory External: One (1) microSD card slot (microSD card not provided)
Serial operation	User selectable as 6 signal RS-232 (Rx, Tx, RTS, CTS, DSR, DTR) or half-duplex RS-485, via RJ-45 header Software configurable baud rate options from 2400 bps to 921600 bps
Digital Input	One (1), via the middle pin of the power header ◆ Input: 0 V dc ~ 2.5 V dc => ZERO; 3 V dc ~ 50 V dc => ONE

Component	Specification
Status LEDs	X303 and X304: Seven (7) LEDs on top panel for network activity and status X300: Four (4) LEDs on top panel for network activity and status
Reset button	Soft Reset (reboot): Short press more than one (1) second and less than 5 seconds Hard Reset (factory reset): Long press more than 5 seconds and less than 20 seconds

Front Panel

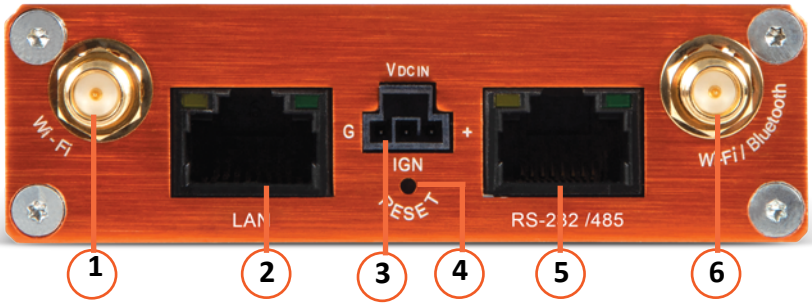
Figure 2-1 X300 model Front View

ID	Connection Name	ID	Connection Name
1	Wi-Fi antenna	5	Serial RS-232/RS-485
2	Ethernet LAN	6	Wi-Fi / Bluetooth antenna
3	DC input	7	LEDs
4	Reset button		

Figure 2-2 X303 model Front View

ID	Connection Name	ID	Connection Name
1	Cellular antenna	5	Serial RS-232/RS-485
2	Ethernet LAN	6	Wi-Fi / Bluetooth antenna
3	DC input	7	LEDs
4	Reset button		

Figure 2-3 X304 model Front View



ID	Connection Name	ID	Connection Name
1	Wi-Fi antenna	5	Serial RS-232/RS-485
2	Ethernet LAN	6	Wi-Fi / Bluetooth antenna
3	DC input		LEDs (on top, not shown here)
4	Reset button		

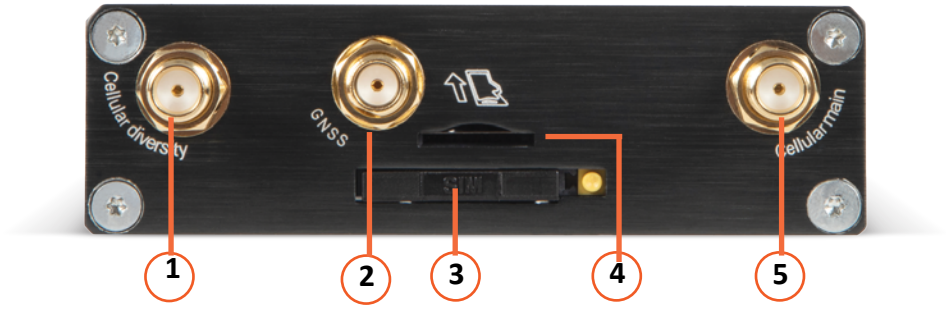
Back Panel

Figure 2-4 X300 model Back View

Figure 2-5 X303 model Back View

ID	Connection Name
1	External SIM slot
2	microSD card slot

Figure 2-6 X304 model Back View



ID	Connection Name	ID	Connection Name
1	Cellular antenna	4	microSD card slot
2	GNSS antenna	5	Cellular antenna
3	External SIM slot		

LEDs

Table 2-3 describes the device status LEDs for X303 and X304 models, as shown in *Figure 2-2*.

Table 2-3 Top Panel LEDs

Name	Color	Status	Description
Alert	Red	OFF	No alert, device is running smoothly
		Flashing	Cellular module reboot, Linux kernel booting
		ON	Hardware fault
Activity	Amber	OFF	Cellular data service is not connected
		Flashing	Data sent and received over cellular connection
		ON	Cellular data service is connected
Network	Amber	OFF	Device is not registered on a cellular network
		Flashing	Registered on roaming cellular network
		ON	Registered on home cellular network
Signal	Amber	OFF	No signal (CSQ=0 to 5, 97, 98, 99)
		Flashing	Weak signal (CSQ > 6 to 12)
		ON	Strong signal (CSQ ≥ 6 to 12)
SIM	Blue	OFF	SIM not in use
		Flashing	External SIM is in use
		ON	Embedded SIM is in use
Wi-Fi	Blue	OFF	Wi-Fi network is inactive
		Flashing	Wi-Fi network connection traffic
		ON	Wi-Fi network link is up and active
Power	Green	OFF	Power off
		ON	Power on

Table 2-4 describes the LEDs for the X300 model, as shown in *Figure 2-1*.

Table 2-4 X300 model Top Panel LEDs

Name	Color	Status	Description
Alert	Red	OFF	No alert, device is running smoothly
		Flashing	Cellular module reboot, Linux kernel booting
		ON	Hardware fault
User-defined	Amber	ON/OFF	User-programmable LED.
Wi-Fi	Blue	OFF	Wi-Fi network is inactive
		Flashing	Wi-Fi network connection traffic
		ON	Wi-Fi network link is up and active
Power	Green	OFF	Power off
		ON	Power on

Cellular

Table 2-5 X303 / X304 Cellular Data Rates

Cellular Type	Uplink / Downlink Maximum Data Rate
2G	236.8 / 296 kbps
3G	5.76 / 42.2 Mbps
LTE-M	Cat M1 [NB1]: 375 / 300 [62.5 / 27.2] kbps updated to Cat M2 [NB2]: 1,000 / 600 [140 / 120] kbps
LTE Cat 1	FDD: 5 / 10 Mbps TDD: 3.1 / 8.96 Mbps

Table 2-6 X303 / X304 Cellular Bands

Model	Part Number	Cellular Type	Bands[1]	Fallback Mode	Bands[1]
X303	X303F202S	LTE Cat M1	85(12)/28/13/20/ 27/26(18,5,19)/8/3/ 66(4)/25(2)/1	2G	5/8/3/2
X304	X304G002S	LTE Cat 1	28/20/8/3/1/7	3G, 2G	8/1; 8/3
	X304G00AS	LTE Cat 1	71/12(17)/13/14/26(5)/ 66(10,4)/25(2)	–	–
	X304G007S	LTE Cat 1	18/5(19)/8/21/3(9)/1/7	–	–
	X304G00CS	LTE Cat 1	5/8/3/1; TDD 40/41[2]	3G, 2G	8/1; 8/3

1. Ranked by increasing frequency
2. More precisely, B41's 2535 MHz ~ 2655 MHz subset, suited to China well

SIM Slot

The X303 and X304 models provide one embedded SIM and one external SIM slot to accommodate one mini SIM card (2FF), as shown in *Figure 2-5* and *Figure 2-6*.

Antenna Connections

Wi-Fi / Bluetooth:

- X300: Two (2) Wi-Fi / Bluetooth, RP-SMA connectors
- X303: One (1) Wi-Fi / Bluetooth, RP-SMA connector
- X304: Two (2) Wi-Fi / Bluetooth, RP-SMA connectors

Cellular / GNSS:

- X300: not applicable
- X303: One (1) cellular, SMA connector
- X304: Two (2) cellular (main and diversity), SMA connectors and one (1) GNSS, SMA connector

Certified Antennas

Table 2-7 lists the antennas that have been certified for the X300 series gateways.

Table 2-7 Certified Antennas

Purpose	Antenna type	Description	Lantronix Part Number	Approved Region
Wi-Fi Antenna	Dipole, swivel type antenna, with RP-SMA(M) connector	Peak gain: 2 dBi, 2.4 Ghz to 2.5 Ghz, 2 dBi, 5.15 Ghz to 5.85 Ghz RoHS compliant	A21H0	FCC, IC, EU, AUS/NZS, JPN, China, Mexico
WWAN Antenna	Dipole, 4G, swivel type blade antenna, with SMA connector, adhesive mount	Performance across LTE frequency bands 698-960, 1710-2170, 2500-2700 MHz Gain: Up to 2 dBi RoHS compliant	A33M0	N/A

Note: *Antenna gain listed above excludes cable loss.*

Antenna Selection

Use the following guidelines in Wi-Fi antenna selection:

- Dipole, peak gain less than 3.8 dBi @ 2.4 GHz ~ 2.5 GHz
- Use the same dipole antenna type as certified module and modem for FCC or external antenna with length greater than 20 cm.

Ethernet Port (LAN)

Figure 2-7 Ethernet Port

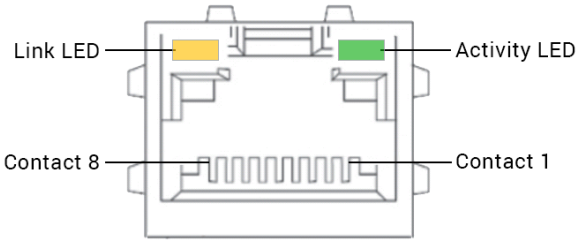


Table 2-8 Ethernet RJ45 Connector Pin Assignment and LEDs

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

Serial Port

One serial RJ45 connector for RS-232 or RS-485 protocol communication.

Figure 2-8 RJ45 Connector RS-232 / RS- 485 Interface

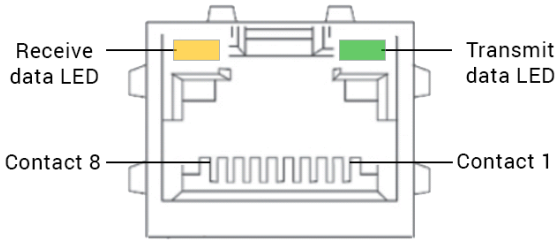


Table 2-9 Serial RJ45 Connector Pin Assignment and LEDs

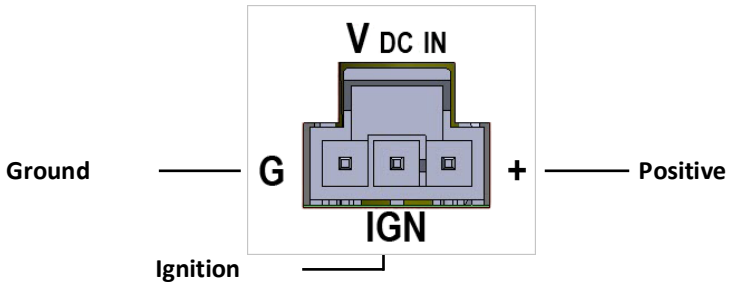
Pin Number / LED	Signal Name for RS-232	Signal Name for RS-485
1	RTS out	TX+ (output from X300)
2	DTR out	Not used / do not connect
3	TX out	TX- (output from X300)
4	GND	GND
5	GND	GND
6	RX in	RX+ (input from X300)
7	DSR in	Not used / do not connect
8	CTS in	RX- (input to X300)
Left LED (Amber)	Receive Data activities (RXD)	Receive Data activities (RXD)
Right LED (Green)	Transmit Data activities (TXD)	Transmit Data activities (TXD)

Power Input

The power input interface is shown in *Figure 2-9*.

For the power cable schematic, see *Power Cable Schematic*.

Figure 2-9 DC Input Interface



Power Consumption

Table 2-10 X300 Series Power Consumption

Device State	Input Voltage			
	10V	12V	24V	30V
Idle state (Wi-Fi, WWAN, WWAN6, LAN & Cellular off)	112 mA	93 mA	52 mA	41 mA
LAN connected (Wi-Fi, WWAN, WWAN6, & Cellular off)	148 mA	110 mA	64 mA	48 mA
WWAN connected (Wi-Fi, LAN, WWAN6 & Cellular off)	113 mA	95 mA	48 mA	40 mA
WWAN6 connected (Wi-Fi, LAN, WWAN & Cellular off)	112 mA	96 mA	48 mA	42 mA
Wi-Fi on (WWAN, WWAN6, LAN, & Cellular off)	162 mA	138 mA	70 mA	58 mA
WWAN, WWAN6, LAN connected, Wi-Fi on, (Cellular standby)	174 mA	144 mA	74 mA	60 mA
Cellular connected (Wi-Fi, LAN, WWAN & WWAN6 off)	164 mA	144 mA	77 mA	54 mA
WWAN, WWAN6, LAN connected, Wi-Fi on, Cellular connected	204 mA	159 mA	83 mA	74 mA

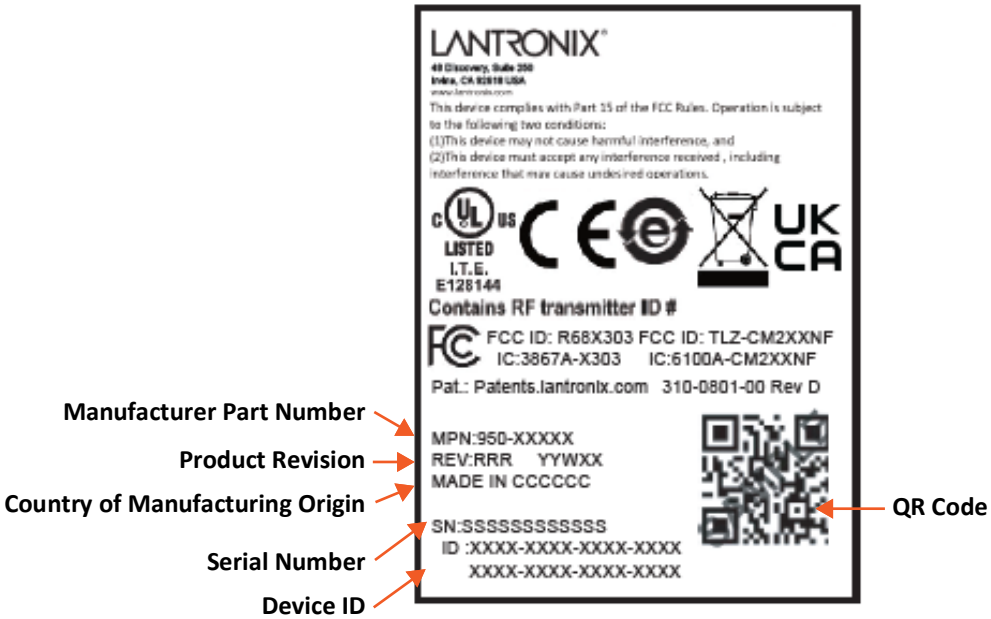
Reset Button

Using a paper clip or similar object to poke through the RESET hole, press the recessed Reset button as shown in *Figure 2-2*.

- To reboot the unit, press and hold the reset button for more than 1 second and less than 5 seconds.
- To reset to factory settings, press and hold the reset button for more than 5 seconds and less than 20 seconds.

Product Label

Figure 2-10 Sample Product Label



3: Installation

Package Contents

- Gateway and accessories:

Component	X300	X303	X304
Gateway model	X300F202S	X303F202S	X304G000S, X304G002S, X304G007S, X304G00AS, X304G00CS
Power supply	ACC-520-165-00	ACC-520-165-00	ACC-520-165-00
Wi-Fi Bluetooth Antenna	A21H0 x2	A21H0 x1	A21H0 x2
Cellular Antenna	N/A	A31M0	A33M0

- X300, X303, or X304 Quick Start Guide
- SIM Insert (printed card with SIM APN and Lantronix Connectivity Services links)

The embedded SIM card is pre-activated by Lantronix and preloaded with an initial amount of data. For more details, see *SIM Card Management on page 34*.

Other accessories must be purchased separately.

Notes:

- *To reduce potential safety issues, only the power adapter provided with the product, a replacement power adapter provided by Lantronix or agency, or a power adapter purchased as an accessory from Lantronix or agency should be used with the product.*
- *If Class I power adapter is used, the power supply cord shall be connected to a socket-outlet with earthing connection*

User Supplied Items

The following items are supplied by the user, if needed. For details about purchasing Lantronix accessories, see *Accessories* below.

- Auxiliary SIM card (2FF), data plan activation required
- Cat 5 Ethernet cable for wired LAN connection
- Serial cable (RS-232 RJ45 connector)
- microSD card for user data storage

The Ethernet cable, serial cable, and microSD card can be acquired from various vendors.

Accessories

Lantronix accessories are listed in *Table 3-1* according to part number and application.

To buy Lantronix accessories, go to https://www.lantronix.com/about-us/contact/.

Table 3-1 Lantronix Accessories

Part Number	Description
Power Cords	
ACC-500-0420-00	POWER CORD WITH 3-PIN NANO-FIT PLUG; 2.5 A FUSE; TWO 1-METRE-LONG AWG20 STRIPPED WIRES (RED, BLACK) FOR POWER
ACC-500-421-00	POWER CORD WITH 3-PIN NANO-FIT PLUG; 2.5 A FUSE; TWO 1-METRE-LONG AWG20 STRIPPED WIRES (RED, BLACK) FOR POWER; ONE 20-CENTIMETRE-LONG AWG20 WIRE (BLUE) FOR IGNITION
Power Supply and Adapters	
ACC-520-0165-00	WORLDWIDE. POWER SUPPLY, WALL CUBE, 12VDC 12W, 4 AC PLUGS, LEVEL 6, WITH PSE, 2X2 3.0MM LATCHED CONN OUTPUT
ACC-520-0166-00	US. POWER SUPPLY, WALL CUBE, 12VDC 12W, US, LEVEL 6, WITH PSE, 2X2 3.0MM LATCHED CONN OUTPUT
Wi-Fi Antenna	
A21H0	2.4/5.8GHZ DIPOLE ANTENNA FOR ISM & WLAN, RP-SMA(M) HINGED (1 for X303, 2 for X304)
4G / GNSS Antenna	
A33M0	THREE IN ONE LTE, 2*LTE+GPS/GLONASS/BD ANTENNA, 3*3000MM RG174 CABLE WITH 3*SMA MALE, ADHESIVE MOUNT
A33H0	THREE IN ONE LTE, 2*LTE+GPS/GLONASS/BD/GALILEO ANTENNA, 3*3000MM RG174 CABLE WITH 3*SMA MALE, ADHESIVE MOUNT. while stocks last
A33H1	THREE IN ONE LTE, 2*LTE+GPS/GLONASS/BD/GALILEO ANTENNA, 3*3000MM RG174 CABLE WITH 3*SMA MALE, ADHESIVE MOUNT.
A32M0	TWO IN ONE LTE, 2*LTE ANTENNA, 2*3000MM RG174 CABLE, SMA MALE. while stocks last
A32H0	TWO IN ONE LTE, 2*LTE ANTENNA, 2*3000MM CABLE, SMA MALE, ADHESIVE MOUNT. while stocks last
A32H1	TWO IN ONE LTE, 2*LTE ANTENNA, 2*3000MM CABLE, SMA MALE, ADHESIVE MOUNT.
A31M0	SINGLE LTE ANTENNA, ADHESIVE REMOTE ANTENNA WITH 3000MM RG174 CABLE, SMA MALE. while stocks last
A31H0	SINGLE LTE ANTENNA,ULTRA WIDEBAND I-BAR ANTENNA, 3000MM CABLE WITH SMA MALE, ADHESIVE MOUNT. while stocks last
A31H1	5G/4G ADHESIVE MOUNT ANTENNA 600-6000MHZ WIDEBAND OPERATION. IP67 RATED ENCLOSURE DIMENSIONS: 105 X 30 X 7.9MM CONNECTOR: SMA MALE STRAIGHT CABLE: 1M OF RG-174 ROHS & REACH COMPLIANT

Preparing to Install

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

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

- Ethernet port or Wi-Fi connectivity and Internet service
- Web browser with recently updated version (Chrome, Safari, Firefox, Edge, Internet Explorer)
- DHCP client is enabled on the computer

Enabling DHCP Client on Your Computer

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

To enable DHCP on Windows 8 or 10:

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

To enable DHCP on Mac OS:

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

SIM Card Management

The Lantronix Connectivity Services embedded SIM card comes pre-activated by Lantronix and preloaded with an initial amount of data. A printed SIM Insert card with the SIM APN on one side and Lantronix Connectivity Services links on the other side is provided. Keep this card for quick reference.

When the purchase order for the gateways is processed, Lantronix creates an account on the Connectivity Services SIM Management portal and enters the SIM cards into the account. A confirmation email with account login details is sent to the contact person on record.

SIM Card Activation

The provided SIM card is pre-activated by Lantronix, but you may need to configure APN in the X300 series software’s cellular network interface SIM settings. To configure the APN, go to Quick Setup or Network > Interfaces and edit the cellular network interface’s SIM settings.

SIM Management Portal

To manage your Lantronix SIM cards, visit the Connectivity Services SIM Management portal at: https://connectivity.lantronix.com

Sign in by entering the user name and password provided by Lantronix.

Here you can view SIM status and usage, manage SIM data limits, manage the SIMs, and access the API documentation.

Before use, the SIM card status will be Pre-active on the SIM Management portal. After it starts transferring data, the status will appear as Active.

Second SIM Card

You may purchase a second SIM card (region specific) from Lantronix Connectivity Services or from a cellular operator for use in the external SIM slot. Before using the SIM card, activate it according to the instructions provided by the vendor.

Lantronix Connectivity Services Links

SIM Management Portal	https://connectivity.lantronix.com
Account	https://shop.lantronix.com/account
Email Support	simhelp@lantronix.com

Physical Installation

Insert SIM Card

Use the embedded, pre-activated SIM card or purchase a SIM card to install in the external SIM slot of the X303 or X304 model gateway. The SIM card must be activated according to vendor instructions before use.

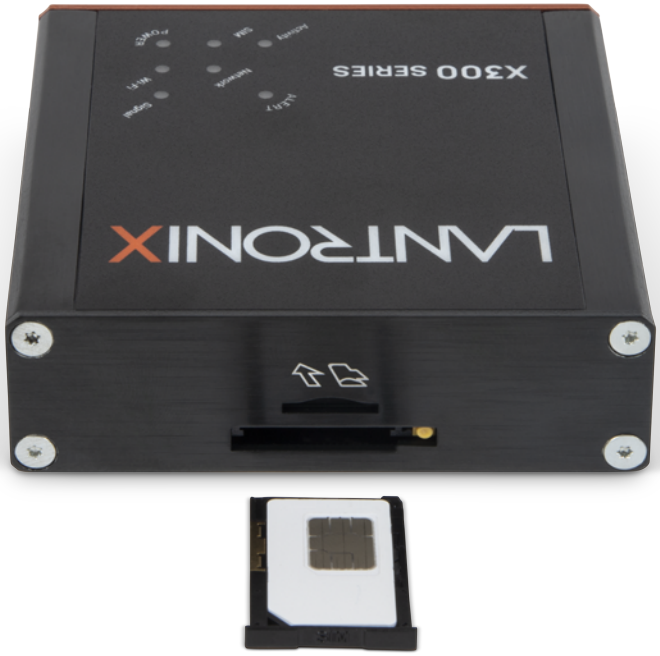
The figures below illustrate installing the SIM card on the X303 model.

To insert the optional SIM card in the external SIM slot:

1. Press the yellow button (using a pen or similar object) to eject the SIM tray.

Press the yellow button to eject the SIM tray.

2. Place the SIM card onto the SIM tray with the contact side up. Note that the tray has a small notch in one of the corners, and the card will only fit one way.



3. Gently slide the SIM tray into the SIM slot and push it to lock it in place.

Connect the Antennas

Ensure that the antenna used is suitable for the cellular frequencies in use, for both the main and auxiliary connectors.

The number and location of the antenna connectors vary by gateway model. Be sure to attach the antennas to the correct antenna connectors according to the connector labels printed on the gateway.

To connect the antennas:

1. Attach the cellular antenna to its antenna connector and tighten it securely.
2. Attach the Wi-Fi / Bluetooth antenna to its antenna connector and tighten it securely.

Cellular **Wi-Fi / Bluetooth**

The X303 model is shown above. The X300 model has one Wi-Fi and one Wi-Fi / Bluetooth antenna connector on the side shown above. The X304 model has two Wi-Fi / Bluetooth antenna connectors on the side shown above and two cellular connectors and one GNSS antenna connector on the opposite side.

Connect the AC Power

To connect the AC power:

1. Connect the power cord to the power supply.

2. Attach the 3-pin connector end of the power cord to the DC input connector on the base unit.

DC input 3-pin connector

The X303 model is shown above. The power input connector is the same for all models.

3. Plug the AC plug on the power supply into a standard AC receptacle.

Connect the Gateway to a Computer

To log into the web administration interface, first connect to the gateway's Wi-Fi access point or connect an Ethernet cable from the gateway's LAN Ethernet port to the computer's LAN Ethernet port.

Connect using Wi-Fi

To connect using Wi-Fi:

1. On your computer, open the Wireless settings and connect to the gateway's Wi-Fi access point. The default access point SSID is:

Parameter	Details
SSID	Lantronix-<model>-<serial-number>
WPA/WPA2 TKIP Key	W1rele$$

2. Open the web browser to 192.168.1.1. The login page appears.
3. Log into the web admin interface. The default username and password credentials are:

User	Default Password
admin	admin
root	L@ntr0n1x

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

Connect using Ethernet

To connect using Ethernet:

1. Connect an RJ-45 terminated Ethernet cable between the LAN Ethernet port on the unit and the LAN Ethernet port on the computer.

2. Open the web browser to 192.168.1.1. The login page appears.
3. Log into the web admin interface. The default username and password credentials are:

User	Default Password
admin	admin
root	L@ntr0n1x

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

Default Configuration

All usernames and passwords are case sensitive.

Web Admin Page

Table 3-2 Default Web Admin Page Credentials

User	Default Password
admin	admin
root	L@ntr0n1x

Note: *Upon first login, you are required to change the factory default passwords before any other gateway configuration can be done. Both the admin and root passwords must be changed.*

Wireless Access Point SSID

Table 3-3 Default Wireless Access Point SSID

Parameter	Details
SSID	Lantronix-<model>-<serial-number>
WPA/WPA2 TKIP Key	W1rele$$

Default Interface Configuration

Table 3-4 Default Network Interface Configuration

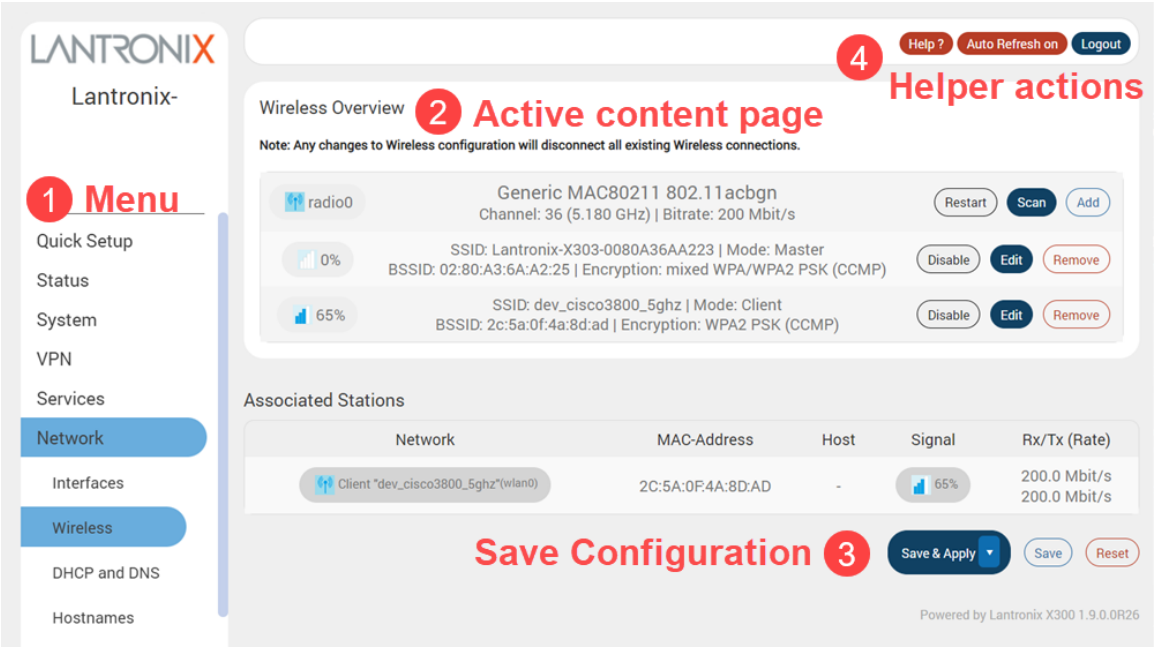
Interface	Details
WAN (Ethernet)	Automatic (DHCP client) Priority source of Internet with cellular backup
LAN (Ethernet)	Active DHCP with starting IP address 192.168.1.100 with pool of 100 clients.
Cellular	No PAP/CHAP authentication
Wireless (LAN)	Wi-Fi enabled as access point

4: Web Administration Interface

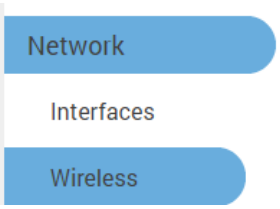
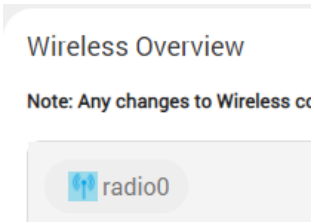
The web admin interface allows the administrator and other authorized users to configure and manage the X300 series gateways using most web browsers (Firefox, Internet Explorer or Safari web applications with the latest browser updates).

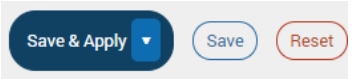
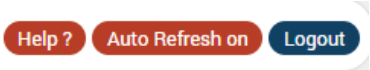
Figure 4-1 shows key components on the web admin interface:

Figure 4-1 Web Admin Interface



How to interact with the web interface:

1	**Menu**  	The menu displays a list of options to configure and operate the gateway. Select a menu option to display the related status and configuration settings in the content pane.
2	**Active content**  	The content pane displays status, configuration settings, and options for interacting with the gateway. It lets you view status, and configure settings on the gateway, or perform maintenance or other operations.

3	**Save Configuration**  	These actions let you save configuration changes or reset unsaved changes on the active page ◆ **Save & Apply** - Applies and saves the changes on the web page to the gateway (in NVRAM) so that the settings will persist when the gateway is rebooted. After clicking this button, wait for the configuration to be applied before closing the browser, otherwise the old configuration will be restored. ◆ **Apply Unchecked** - Click the arrow on the Save & Apply button to reveal this option. Applies and saves the changes on the web page to the gateway (in NVRAM), but will not disrupt the active network interface. Use this if you are changing the interface parameters on which the session is active. ◆ **Save** - Saves the changes on the web page (to RAM) without committing the changes. All saved configuration will be lost when the gateway is rebooted if they are not saved and applied. ◆ **Reset** - Discards the unsaved changes on the page.
4	**Helper actions**  	These actions help you use the web interface. ◆ **Help?** - opens embedded help information for the active page ◆ **Auto Refresh on/off** - lets you enable or disable the UI auto refresh action ◆ **Unsaved changes: <#>** - shows the number of unsaved changes and lets you save & apply the changes to the gateway's configuration or revert the changes back to the saved configuration. ◆ **Logout** - logs you out of the web administration interface.

Logging In

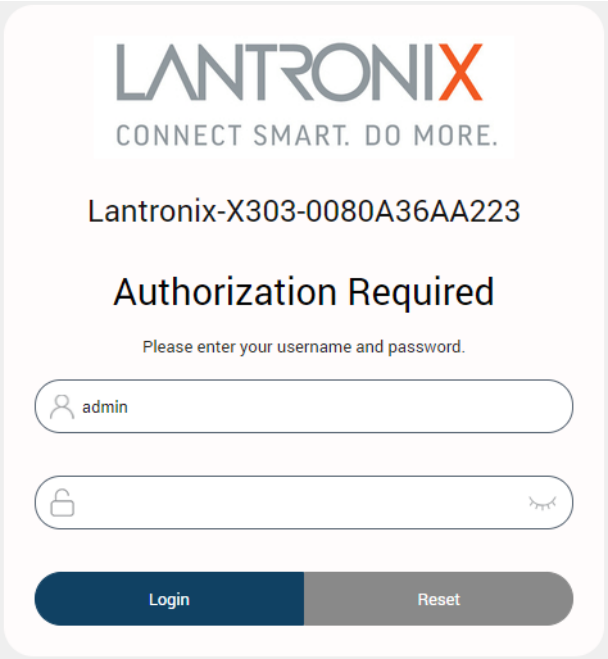
The admin user or root user can log into the web admin interface.

If your gateway is new, please inspect and set up the gateway as described in *Chapter 3: Installation*.

To log into the web interface:

1. Open a web browser on the computer.
2. Enter the default LAN IP address 192.168.1.1. The login screen is displayed.

Figure 4-2 Web Admin Login Page



3. Enter the username and password. If you are logging in for the first time after installation or after factory reset, use the default credentials.
4. Click **Login**.

Change Passwords After Initial Login

After first login with a new device or after resetting the device to factory defaults, you are required to change the factory default passwords for both the admin user and root user before any other gateway configuration can be done.

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

1. Log into the web admin interface as root user. This will allow you to change the passwords for both the root user and the admin user.
2. For the root user, enter the new password and then re-enter it to confirm it.
3. For the admin user, enter the new password and then re-enter it to confirm it.
4. If the country code selection for Wi-Fi operation is displayed, select the country code where the device is being used. This selection ensures that the device will only enable Wi-Fi radio settings that conform with the country's regulatory laws.
5. Click **Save & Apply**.

   This will log you out and return to the login page automatically.

Logging Out

To log out of the web admin interface:

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

5: 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 Gateway Using Lantronix Provisioning Manager

To discover a device on the local network:

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 X300 series gateway in the device list. The device's firmware version, serial number, IP address, and MAC address will be shown. Additional information can be obtained by clicking the **three dot menu** and clicking **Get Device Info**.
4. In order to perform operations on the X300 series gateway such as upgrading the firmware, updating the configuration, or uploading to the file system, click the **checkbox** next to the device and select an operation at the top.

6: Quick Setup

Quick Setup lets you configure the IP network port so that you can configure other gateway settings. To bypass quick setup and directly configure the network interfaces using advanced settings, go to the Network page (see *Chapter 11: Network*).

Quick Setup

Quick Setup > Quick Setup

To configure the network settings:

1. On the Quick Setup page, enter the network and basic configuration of the gateway. See *Table 6-1*.

Table 6-1 Quick Setup Network Configuration

Parameters	Description
Local Area Network (LAN)	
IPv4-Address	Enter an IPv4 address for the LAN interface. This is the IP Address that must be used to access the gateway. The default LAN IPv4 Address is 192.168.1.1.
IPv4-Netmask	Enter the IPv4 netmask of the LAN interface. The default netmask is 255.255.255.0
Cellular	
General Settings	Select which SIM to use, embedded or external SIM.
Embedded SIM Settings (tab)	
Use Custom APN	Select this option to use a custom Access Point Name (APN) for the cellular network data connection.
APN	Displays the APN or custom APN for the connection.
Enable roaming	Displays as Enabled if data roaming is enabled, or disabled otherwise.
External SIM Settings (tab)	
Use Custom APN	Select this option to use a custom Access Point Name (APN) for the cellular network data connection.
APN	Enter the APN used for the cellular data connection.
PIN	SIM card Personal Identification Number (PIN) is used to lock the card, preventing people from making unauthorized phone call or accessing cellular data services. Enter the PIN of the SIM card.
Authentication Type	The authentication method used for the cellular connection. If PAP, PAP/CHAP, or CHAP are selected, enter the username and password.
Username	Enter the PAP/CHAP username.
Password	Enter the PAP/CHAP password.
ConsoleFlow Client	

Parameters	Description
Enable	Select to enable or clear to disable the ConsoleFlow client. For more configuration options, go to **ConsoleFlow > Client**.
Device ID	Read only. Displays the gateway's Device ID. Device ID may be provisioned through Lantronix Provisioning Manager. ***Note:*** *Device ID can only be provisioned once. It will persist across resets.*
Serial Number	Read only. Displays the serial number of the device.
Connection 1	
Host	Enter the host name or IP address of the ConsoleFlow server, used to register the device. It should start with "api."
MQTT Host	Hostname or IP address of MQTT server. It should start with "mqtt."
SSH Access	
Enable	Select to enable or clear to disable SSH access. To configure SSH access, go to **System > Administration**.
Time Synchronization	
Enable NTP client	Select to enable the NTP client on the gateway to synchronize its internal clock every 60 minutes from an NTP server. Clear the check box to disable NTP client. For more configuration options, go to **System > System > Time Synchronization.**
NTP Server candidates	Enter the pool of NTP servers to poll the time from.
Timezone	Select the timezone of the gateway.

7: Status

The Status pages provide a summary view of the vital configurations of the gateway. It includes the following pages:

- *Overview (Page)*
- *Firewall Status*
- *Network Status*
- *Routes*
- *System Log*
- *Kernel Log*
- *Processes*
- *Realtime Graphs*
- *Load Balancing*

Overview (Page)

Status > Overview

The Status Overview page provides a listing of important system parameters.

To view the Status Overview:

1. Go to Status > Overview.
2. Scroll the page to view the rest of the Status Overview sections. Click the following links for details about each of the Status Overview sections.

- *System Status*
- *ConsoleFlow Status*
- *Memory Status*
- *MWAN Interfaces Status*

System Status

The System section provides the gateway's model and software related information.

Table 7-1 System Status Overview

Parameters	Description
Hostname	Name assigned to the gateway for addressing purposes
Model	Model number of the gateway
Part Number	Model part number
UbootVersion	U-Boot version number
Architecture	Architecture type
Firmware Version	Base firmware version number

Parameters	Description
Module Firmware	Modem firmware version
Kernel Version	Linux Kernel version number
Router Time	Day of the week, month, date, time and year configured on the unit. The format is Day Month Date hh:mm:ss Year. The time is displayed in 24-hour clock format.
Uptime	Displays the elapsed time since the unit last rebooted. The format is dd hh mm ss.
Load Average	Average CPU load time over periods of 1, 5, and 15 minute averages
Reboot Cause	Displays the last reboot cause and time whenever possible.
IMEI	15 digit IMEI number An IMEI number (International Mobile Equipment Identity) is a 15 or 17 digit unique number to identify GSM or UMTS mobile devices. It is used to prevent call initiation from a misplaced or stolen GSM or UTMS device, even if someone swaps out the device's SIM card. ***Note:*** *We recommend you record the IMEI number and secure it so that it can be quickly accessed in the event of theft or loss of the unit.*

ConsoleFlow Status

This section describes the ConsoleFlow client status.

Table 7-2 System Status Overview

Parameters	Description
Client State	Displays the current state of the ConsoleFlow client.
Last Status Update	Displays the elapsed time since the ConsoleFlow client sent its status to the server.
Last Content Check	Displays the elapsed time since the ConsoleFlow client requested content check from the server.
Available Firmware Updates	Lists any available firmware updates.
Available Configuration Updates	Lists any available configuration updates.

Memory Status

The Memory section provides information about the available memory.

Table 7-3 Memory Status Overview

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

MWAN Interfaces Status

The MWAN Interface section shows the status of the available and connected WAN options. The interface is green when it is active (it can be online or offline), and red when it is disabled. Online interfaces show tracking status and uptime. Offline interfaces show the downtime.

Firewall Status

Status > Firewall

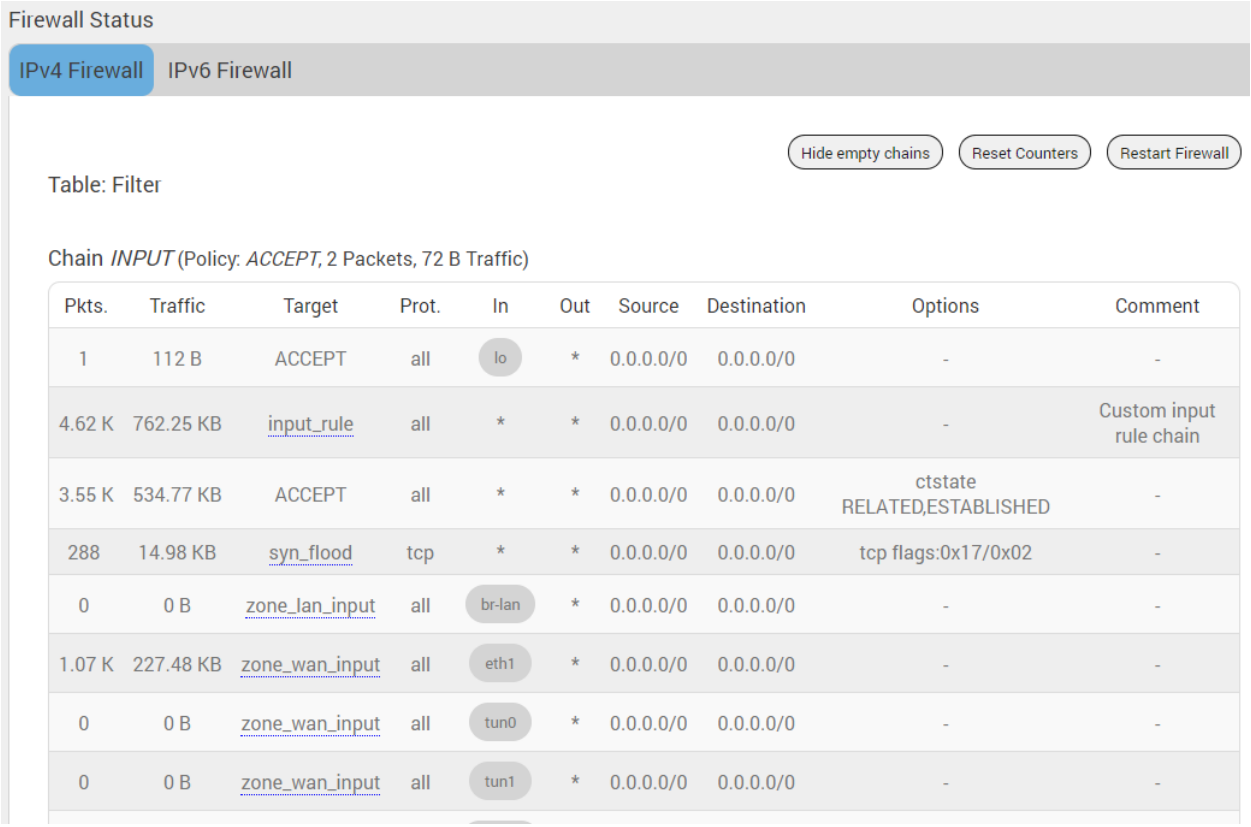
The Firewall Status page provides a listing of the IPv4 firewall or IPv6 firewall rule chains in the Filter, NAT, Mangle, and Raw firewall tables.

You can hide or show empty chains in the firewall list, reset the counters, and restart the firewall.

Hide empty chains	Click to hide the chains that have no rules.
Show empty chains	Click to show all chains.
Reset Counters	Click to reset counters for number of packets and traffic.
Restart Firewall	Click to reload the existing firewall configuration of every interface.

Figure 7-1 shows a portion of the IPv4 Firewall status page, and *Table 7-4* describes the firewall details.

Figure 7-1 IPv4 Firewall Status



Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
1	112 B	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
4.62 K	762.25 KB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
3.55 K	534.77 KB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
288	14.98 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
0	0 B	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
1.07 K	227.48 KB	zone_wan_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	tun0	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	tun1	*	0.0.0.0/0	0.0.0.0/0	-	-

Table 7-4 Firewall Status

Parameters	Description
Rule Chain name and details	Displays the rule chain name, type, and policy details
Pkts	Displays the number of accepted packets.
Traffic	Displays the amount of traffic captured by the filter.
Target	Displays the target action for the traffic processed for a respective rule.
Prot.	Displays the protocols configured in the firewall rule.
In	Input interface.
Out	Output interface.
Source	Displays the source IPv4/IPv6 address.
Destination	Displays the destination IPv4/IPv6 Address.
Options	Displays option details
Comment	Displays comment details

Network Status

Status > Network

Cellular Status

The Cellular section provides the status of the SIM cards in the unit.

Table 7-5 Cellular Status Overview

Parameters	Description
Cellular Data	Displays the cellular data connection status. ◆ CONNECTED – Data communication is connected. ◆ DISCONNECTED – Data communication is not connected.
Signal Strength	Displays the current signal strength. The signal strength range is 0 to 32. ◆ 0: -113 dBm or less (none) ◆ 1: -111 dBm (poor) ◆ 2 to 30: -109 to -53 dBm (fair to good) ◆ 31: -51dBm or greater (excellent) ***Note:*** *Signal strength for a good cellular data connection must be 12 or above.*
Network Status	Displays the registration status of the unit on the current cellular network. ◆ Registered ◆ Not Registered ◆ Registering
Operator Name	Name of the cellular operator in use
Operator Number	Number of the cellular operator in use
Operator Type	Operator type
Roaming Status	The roaming status of the unit: ◆ Home ◆ Roaming ◆ N/A
SIM Status	Displays the availability of SIM card. ◆ No Sim detected – SIM card is not inserted. ◆ READY – SIM card is inserted.
Active SIM Slot	Displays the active SIM, Embedded SIM or External SIM.
IMSI	Displays the International Subscriber Identity (IMSI) number. In case of UMTS, it is read from the SIM card. The IMSI is a 15 digit unique mobile number associated with the cellular network and used to acquire the details of the mobile for identifying the user of a cellular network.
Configured Band	The configured radio frequency bands
Registered Band	The registered radio frequency band
Temperature	Internal temperature of the unit in degrees Celsius
ICCID	Integrated Circuit Card ID (ICCID) – unique serial number that identifies the SIM card.

Network Status

The Network section provides the IPv4 and IPv6 WAN status and the number of active connections.

Table 7-6 Network Status Overview

Parameters	Description
IPv4 Upstream	Displays status of IPv4 WAN connections with following details: ◆ Protocol – Static (manually addressed) or DHCP client (dynamically addressed) ◆ Address – IP address of the WAN interface. ◆ Gateway – IP address of the WAN interface gateway. ◆ DNS 1/2/3 – DNS IP addresses, in order of precedence. ◆ Connected: Duration since connection was established. ◆ Device: the physical interface, cellular, ethernet adapter and so on.
IPv6 Upstream	Displays status of IPv6 WAN connections with following details: ◆ Protocol – Static (manually addressed) or DHCPv6 client (dynamically addressed) ◆ Address – IPv6 addresses of the interface. ◆ Gateway – IP address of the gateway. ◆ DNS 1/2/3 – DNS IP addresses; in order of precedence. ◆ Connected: Duration since connection was established. ◆ Device: the physical interface, cellular, ethernet adapter and so on.

Active DHCP and DHCPv6 Leases Status

The Active DHCP Leases and DHCPv6 Leases shows information about the devices connected to the gateway using a DHCP lease. This includes IPv4 and IPv6 connections.

Table 7-7 Active DHCP Leases Status Overview

Parameters	Description
Host Name	Name of the device (laptop, mobile, etc.) that is connected to the gateway and has been leased an IPv4 address or an IPv6 address by the gateway's DHCP server.
IPv4 Address/IPv6 Address	IPv4 address or IPv6 address assigned to the device.
MAC Address	Applies to IPv4. MAC address of the device.
DUID	Applies to IPv6. DUID (Device Unique Identifier) of the device connected.
Leasetime remaining	The remaining time for which the device can use the DHCP server leased IPv4 address.

Wireless Status

The Wireless section describes the status of the Wi-Fi network used by the gateway and the Wi-Fi associated stations.

Table 7-8 Wireless Status Overview

Parameters	Description
Connection Name	Name of the connection and the details: ◆ Type – The wireless radio chipset ◆ Channel – Wi-Fi channel ◆ Bitrate – Data transfer rate ◆ SSID –Service Set Identifier (SSID) that uniquely names a wireless local area network (WLAN) ◆ Mode – Displays whether the WLAN interface is currently configured as an access point (Master) or as a client of a higher order Wi-Fi network. ***Note:*** *For Wi-Fi WAN (WWAN) operation, the connection mode should be 'Client'.* ◆ BSSID – Displays Basic Service Set Identification (BSSID); 24 bit MAC address of wireless device. ◆ Encryption – Displays the data encryption method. ◆ Associations – Displays the number of associated stations.
Associated Stations	
Network	Mode and name of the network to which the device is connected
MAC Address	MAC address of the computers and/or devices that are connected
Host	Host name of the associated station
Signal/Noise	Signal strength/noise in dBm
RX Rate/Tx Rate	The receive (RX) and transmission (TX) data rates of the associated client. Displays data transfer rate (Mbit/s), channel bandwidth (MHz), Modulation and Coding Scheme index (MCS), and GI time (Guard Interval, for TX rate).
Disconnect	Click to disconnect the associated station from the access point.

Dynamic DNS Status

The Dynamic DNS section shows the Dynamic DNS IPv4 and IPv6 configuration.

Routes

Status > Routes

The Routes status page displays the ARP table and active IPv4 and IPv6 routes.

Table 7-9 Routes Status

Parameters	Description
ARP	
IPv4 Address	Displays the IPv4 address.
MAC Address	Displays MAC address of the peripheral device.
Interface	Displays the interface name connected to the peripheral device.
Active IPv4 Routes	
Network	Displays the network type used by the active IPv4 routes.
Target	Displays the destination IPv4 address.
IPv4 gateway	Displays the IPv4 address gateway used for traffic routing.
Metric	Displays the metric assigned to the interface.
Active IPv6 Routes	
Network	Displays the network type used by the active IPv4 routes.
Target	Displays the destination IPv6 address.
Source	Displays the IPv6 address gateway used for traffic routing.
Metric	Displays the metric assigned to interface.

System Log

Status > System Log

The System Log displays detailed system, traffic, and network activity log information.

Syslog events contain the date, severity, and event details. The format is shown in the following example:

```
Sep 15 22:33:38 Lantronix-X303-0080A36AA223user.info Eventsms: BAND :
All supported bands
```

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

Kernel Log

Status > Kernel log

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

It gets reset on every boot.

Processes

Status > Processes

The Processes log displays a list of active Linux system processes and their resource usage.

Table 7-10 Processes Status

Parameters	Description
PID	Displays the Process identifier (PID) number associated with the process.
Owner	Displays the task owner
Command	Displays the command name
CPU usage %	The CPU usage of the process, displayed as a percentage of the total available CPU resources.
Memory usage %	The amount of the system's working physical memory that the process is currently using, displayed as a percentage.
Actions	**Hang up**—Sends a hang up signal to terminate the process. **Terminate**—Sends a terminate signal to terminate the process. **Kill**—Sends a kill signal to immediately terminate the process. The process will not perform any cleanup operations.

Realtime Graphs

Status > Realtime Graphs

The Realtime graphs display the gateway's activities over time for CPU load, WAN network traffic, wireless usage, and connections.

Load

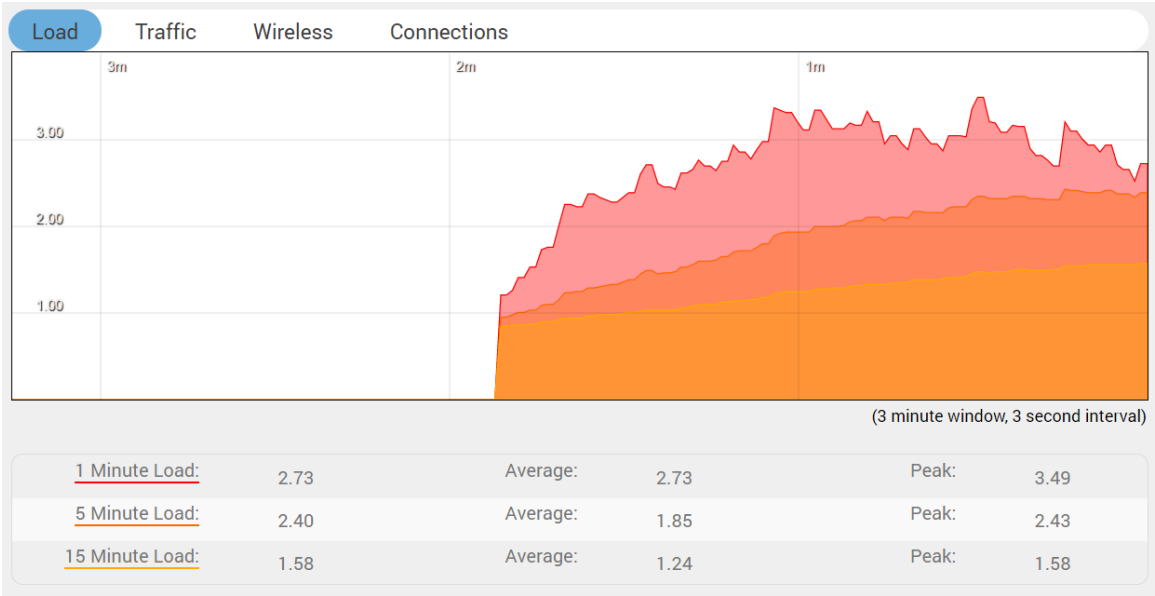
Status Realtime Graphs > Load

The Load graph shows the CPU load average and peak (y-axis, % utilization) over time (x-axis).

Averages are shown for 1-minute (red), 5-minute (orange), and 15-minute (yellow) load.

Figure 7-2 shows a CPU load graph.

Figure 7-2 Realtime CPU Load Graph



Traffic

Status > Realtime Graphs > Traffic

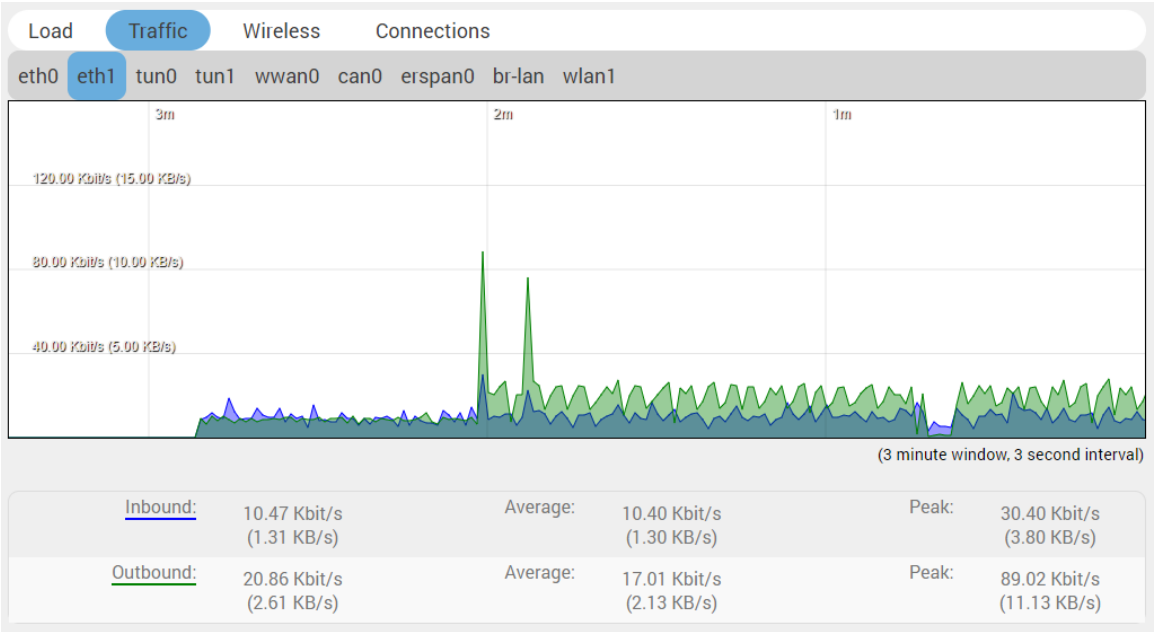
The Traffic graph indicates the WAN-side incoming and outgoing traffic rate (y-axis) on the different interfaces over time (x-axis). The graphs display the average and peak data transfer on the following interfaces (if configured for WAN traffic): eth0, eth1, tun0, tun1, wwan0, can0, erspan0, br-lan, and wlan1.

Average and peak rates are shown for inbound traffic (blue) and outbound traffic (green).

The WAN interface shows average and peak WAN and cellular traffic.

Figure 7-3 shows an example of network traffic for the eth1 interface:

Figure 7-3 Realtime Network Traffic Graph (eth1)



Wireless

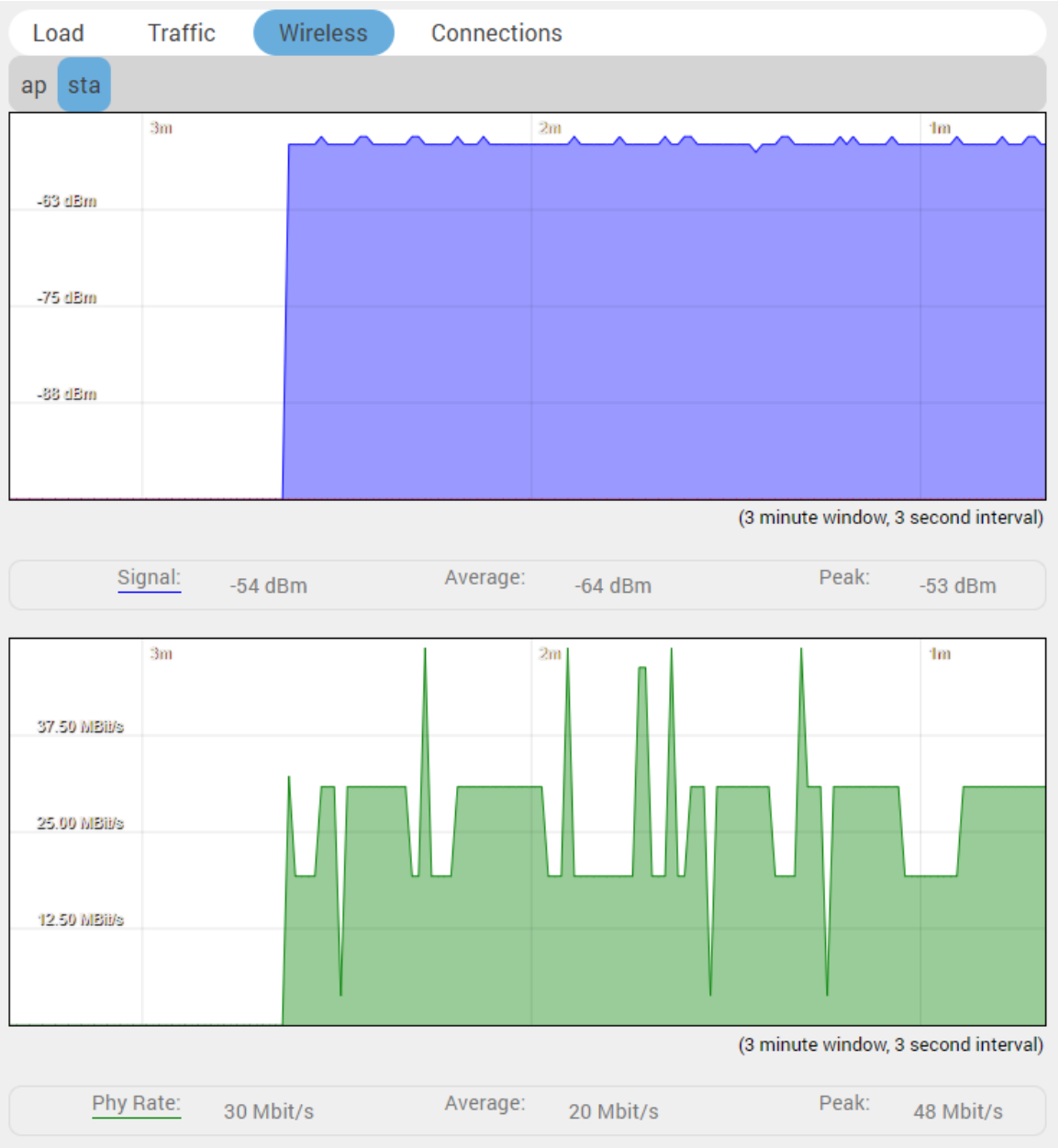
Status > Realtime Graphs > Wireless

The Wireless graph indicates Wi-Fi usage including signal and noise levels (y-axis, dBm) and physical data transfer rate (y-axis, Mbit/sec) over time (x-axis).

The top graph displays signal (blue) and noise (red) levels. The bottom graph displays the physical data transfer rate (green) irrespective of WI-Fi being used as an access point or client.

Figure 7-4 shows the wireless usage graph for a X300 series gateway configured as Wi-Fi client (STA) and connected to an external access point.

Figure 7-4 Realtime Wireless Usage Graph (client)



Connection

Status > Realtime Graphs > Connection

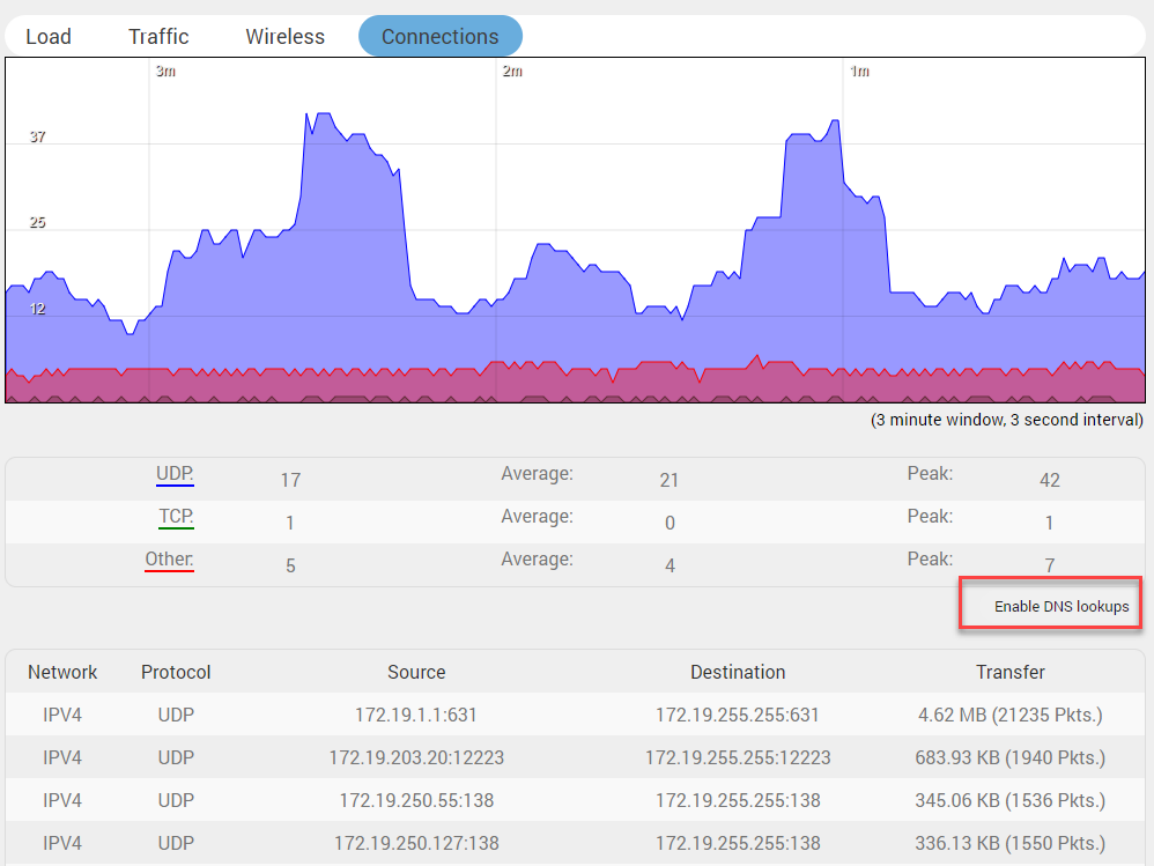
The Connection graph indicates the number of active network connections (x-axis) over time (y-axis). It includes connections originating from the gateway and also connections originating from the LAN or WAN.

The graph displays UDP (blue), TCP (green) and other (red) connections. The table below the graph displays connection details including IPv4/IPv6, protocol, source IP, destination IP, and amount of data transferred.

By default DNS lookup is disabled. You can enable it by clicking the link **Enable DNS lookups** below the graph.

Figure 7-5 shows a realtime connection graph for an idle gateway.

Figure 7-5 Realtime Connection Traffic Graph



Load Balancing

Status > Load Balancing

Interface

Status > Load Balancing > Interface

The Interface page shows the MWAN interfaces, with active interfaces shown in green and disabled interfaces shown in red. The uptime (hh:mm:ss) is displayed for active interfaces.

Detail

Status > Load Balancing > Detail

The Detail page shows MWAN interface (IPv4 and IPv6) details including interface status, current policies, directly connected networks, and active user rules.

Diagnostics

Status > Load Balancing > Diagnostics

The Diagnostics page shows all configured MWAN interfaces and provides diagnostic commands to check the health of the selected MWAN interface.

The following diagnostics commands are supported:

- Ping the default gateway
- Ping tracking IP
- Check IP rules
- Check routing tables
- Hotplug ifup
- Hotplug ifdown

To run a diagnostics command, select the interface and the task and click **Execute**.

Troubleshooting

Status > Load Balancing > Troubleshooting

The Troubleshooting page displays the output of the following IP commands:

- ip a show
- ip route show
- ip route list table 1-250
- iptables -L -t mangle -v -n

8: System

The System pages provide configuration for secure local and remote management of the gateway. The System menu contains the following sections:

- *System*
- *Administration*
- *Software*
- *Startup*
- *Scheduled Tasks*
- *LED Configuration*
- *Backup / Flash Firmware*
- *Custom Commands*
- *Reboot*

System

System > System

This section contains settings that apply to the basic operation of the system, including the hostname, time zone, and system log configuration.

General Settings

System > System > General Settings

General settings let you configure local and router time, hostname, and time zone.

To configure general system settings:

1. Go to System > System > General Settings.
2. Enter the configuration settings. See *Table 8-1*.
3. Click **Save & Apply**.

Table 8-1 System General Settings

Parameters	Description
Local Time	Displays the local time of the user's computer. Sync the local time with browser or with an NTP server. Click **Sync with browser** button to synchronize the gateway's clock with the local computer browser. Click **Sync with NTP-Server** to synchronize the gateway's clock with an NTP server. ***Note:*** *The displayed time is dependent on the configuration of your local computer that is being used as an NTP server.*
Router Time	Displays the current router time according to the configured time zone.

Parameters	Description
Hostname	Displays the hostname for this unit. Do not include the period character "." in the hostname as only the string before the period will be used as the hostname.
Timezone	Select time zone according to the geographical region in which the unit is deployed. The default time zone is UTC.
Set Time Manually	Set the year, month, date, hour, minute and seconds. Click **Apply the time** to save the information.

Logging

System > System > Logging

The system logger provides important debugging and monitoring capabilities. The system logs capture traffic, system, and network activity. The logs are stored in RAM and are reset when the gateway is rebooted.

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

To configure the system log settings:

1. Go to System > System > General Settings.
2. Enter the configuration settings (see *Table 8-2*).
3. Click **Save & Apply**.

Table 8-2 Syslog Configuration

Parameters	Description
System log buffer size	Enter the size of the buffer in Kilobytes (KB) to save logs and status information details. The default system log buffer size is 64 KB. When the buffer is full, records will be overwritten on a first in, first out (FIFO) basis.
External system log server	Enter the IP address of an external syslog server to be used to save the real time logs. By default the logs are written to the local system.
External system log server port	Enter the UDP port number of the external syslog server. The default port is 514.
External system log server protocol	Protocol of the external syslog server. UDP
Write system log to file	File path and file name to write the log messages to. If an external filesystem (SD card or USB flash drive) is mounted, add the mount path and file name here. The logs display application (see *Services > Logs Information*) will download the files written to this file path. Example: /mnt/usbdevice/log.txt

Parameters	Description
Log output level	Select the log severity output level. The level of severity progresses from Info to Emergency. Lower severity levels are more verbose and will include messages from all higher severity levels. Log levels are listed in order of increasing severity: ◆ Debug – Provides debug messages used by the software developer for debugging the application. These logs are typically not useful during operations. ◆ Info – Provides normal operational information messages that are used for general purposes like reporting. ◆ Notice – Provides alerts for peculiar events that are not an error. These logs help to identify potential issues. Since these logs do not indicate errors, immediate action may/may not be necessary. ◆ Warning – Displays warning messages for a potential issue, indicating to take an action. An error may occur if no action is taken against the warning issued. ◆ Error – Displays the messages indicating an error condition. ◆ Critical – Indicates failure in secondary system and must be corrected immediately. ◆ Alert – Problems which should be corrected immediately. ◆ Emergency – System is unusable. ***Note:*** *For help with log errors, contact* Lantronix Technical Support.
Cron log level	Select the minimum level for cron messages to be logged to syslog. ◆ Debug – Helps to debug cron process which has failed during runtime. ◆ Normal – Displays informational messages ◆ Warning – Indicates some issues can happen or error could be generated in cron process. ***Note:*** *For help with Cron log warning messages, contact* Lantronix Technical Support.

Time Synchronization

System > System > Time Synchronization

Select the method that the gateway uses to synchronize its internal clock.

Note: *If all three methods are enabled, the order of precedence is GPS, then NTP, then GSM.*

Table 8-3 System Time Synchronization Configuration

Parameters	Description
GPS Time Synchronization	Select this option for the gateway to synchronize its internal clock using GPS. To use this option, the gateway must support GPS. ***Note:*** *GPS antenna will be needed for GPS time sync.*
Interval	The time in seconds to update time from the GPS frame.
Enable NTP client	This option enables the NTP client on the gateway to synchronize its internal clock every 60 minutes from an NTP server. If enabled, enter the NTP options as needed. To use as NTP client, no change to the firewall is required. ***Note:*** *Enabling NTP Client consumes data.*

Parameters	Description
Provide NTP server	This option enables the NTP server on the gateway. The service will respond to the local network with the time of the gateway. To run as NTP server, open UDP port 123. Disabled by default.
Use DHCP advertised servers	Enables or disables the use of DHCP-provided NTP servers. Enabled by default.
NTP server candidates	Enter the pool of NTP servers to poll the time from.
GSM Time Synchronization	If enabled, the gateway will synchronize using GSM functionality.

Language and Style

System > System > Language and Style

The language and style settings are used to control the look and feel of the web interface.

Table 8-4 Language and Style Configurations

Parameters	Description
Language	Default value is auto.
Design	Default design of user interface is Rosy.
Auto refresh default pollinterval in seconds	Set the auto refresh polling interval between 5 and 50 seconds. Default is 5 seconds. ***Note:*** *Auto refresh can be turned on or off using the Auto Refresh button on the UI.*

Administration

System > Administration

The Administration page allows you to configure the unit's password and SSH access to the device. You can configure various ports and login security.

Router Password

System > Administration > Router Password

This page allows you to change the login password of the current user. If you are logged in as administrator, you can change the administrator password, and if you are logged in as root, you can change the root password and the administrator password.

To change the password:

1. Go to System > Administration.
2. Type the new password and retype it to confirm.
3. Click **Save**.

SSH Access

System > Administration > SSH Access

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

To set up SSH access, an SSH key is required. You can use the default SSH key or generate and upload your own SSH keys.

By default, remote SSH over WAN is disabled. It can be enabled from the web interface (you need to enable port 22 in Firewall settings) or by sending an SMS from a registered admin number. You should disable SSH access on interfaces when it's not needed.

To configure SSH access:

1. Go to System > Administration > SSH Access.
2. Enter the configuration settings (see *Table 8-5*).

Table 8-5 SSH Access Configuration

Parameters	Description
Interface	Select the interface. SSH listens only on the selected interface. ***Note:*** *Unspecified – If this option is selected, SSH listens on all interfaces.*
Port	Provide the listening port of the instance. Default port is 22.
Password Authentication	Select to allow authentication using SSH password.
Allow root logins	Select to allow root user logins to the gateway.
Allow root logins with password	Select to allow root logins and require a password.
GatewayPorts	Select to allow remote hosts to connect to local SSH forwarded ports.
Add Instance	Click to add another SSH instance.

SSH-Keys

System > Administration > SSH-Key

Public SSH keys are used to authenticate with SSH public key authentication. One or more keys are provided by default or you can upload your own keys.

To add a new public SSH key:

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

Software

System > Software

The software package manager lets you install, update, and remove software packages. Software packages can be stored on the Lantronix package server, you can use your own custom package feeds, or you can upload the package from your local machine.

The web interface also lets you view and modify the OPKG package manager configuration files. See *Configure OPKG*.

To manage packages:

1. Go to System > Software.
2. Select the list view:
   - **Available** displays the packages that are stored on the Lantronix package server.
   - **Installed** displays the installed packages on the unit.
   - **Updates** displays the packages for which an update is available from the server.

   Note: *To refresh the list, click* ***Update lists...***
3. To install a package, do one of the following:
   - From the list of Available packages, select the package and click **Install**.
   - Under **Download and install package**, enter the package name (for a package on the download server) or enter the URL (for a package on a custom feed), and click **OK**.
   - Click **Upload Package** and browse to select the package from the local machine.
4. To remove a package, from the list of Installed packages, select the package and click **Remove**.

Table 8-6 Software Package Details

Parameters	Description
Available Memory	
Free space	Indicates the free and used space on the flash memory. The darker line represents the portion of free space.
Available, Installed, or Update Package Details	
Package name	Displays the name of package.
Version	Displays the version of package.
Size (.ipk)	Displays the size of the installed package.
Description	Displays the package description, if one has been provided.

Configure OPKG

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

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

To modify the OPKG configuration:

1. Go to System > Software.

2. Click the **Configure opkg** button.
3. Modify the OPKG configuration (see *Table 8-7*).
4. Click **Save**.

Table 8-7 OPKG Package Manager Configuration

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

Startup

System > Startup

Initscripts

System > Startup > Initscripts

Init scripts are run to start required processes during the boot process. The web interface lets you view and enable or disable installed init scripts. Reboot the gateway for the changes to take effect.

Note: *Disabling an essential script such as a network script may cause your device to become inaccessible.*

- **Enable** and **Disable** actions enable or disable the initscript.
- **Start**, **Restart**, and **Stop** actions perform the specified action on the process immediately.

Table 8-8 describes the initscripts.

Table 8-8 Initscripts Actions

Parameters	Description
Start priority	Displays the priority of when the initscript is run during startup. Order of priority is from 00 to 99.
Initscript	Displays the name of the initscript
Enable/Disable	Displays the current state as Enabled or Disabled. Click the button to disable or enable the initscript.
Start	Starts the initscript immediately
Restart	Restarts the initscript immediately
Stop	Stops the initscript immediately

Local Startup

System > Startup > Local Startup

The local startup file (/etc/rc.local) contains custom commands that are run at the end of the boot process, after the system is initialized. By default, it is empty.

To configure the local startup file:

1. Go to System > Startup > Local Startup.
2. In the editor, type custom commands on any line before the line “exit 0”. Make sure that the file ends with the line “exit 0”.
3. Click **Save**.

Changes will take effect on the next reboot.

Scheduled Tasks

System > Scheduled Tasks

This feature lets you schedule cron jobs to run at a fixed time, date, or interval.

Enter each task on a separate line in the crontab file. Tasks are specified using the following syntax:

```
* * * * * command to execute
- - - - -
| | | | •----day of the week (0-6) (Sunday=0)
| | | •------month (1-12)
| | •--------day of month (1-31)
| •----------hour (0-23)
•------------min (0-59)
```

To configure scheduled tasks:

1. Go to System > Scheduled Tasks.

   Note: *If the editor is empty, you must restart the cron service before creating a scheduled task. To restart the cron service, go to Services > Service Actions in the web interface.*

2. Enter the cron task according to the syntax described above. *Table 8-9* lists available shortcuts.

3. Click **Save**.

Table 8-9 Cron Shortcuts

Shortcut	Equivalent	Description
@reboot	(none)	At system startup
@yearly	0 0 1 1 *	Every year
@annually	0 0 1 1 *	Every year
@monthly	0 0 1 * *	Every month
@weekly	0 0 * * 0	Every week
@daily	0 0 * * *	Every day
@midnight	0 0 * * *	Every day
@hourly	0 * * * *	Every hour

LED Configuration

System > LED Configuration

The X300 series gateway provides 7 LEDs to indicate status and activity. For a description of the default LED behaviors, see *LEDs.*

The LED can be controlled by various system events, which is selected by the trigger option. Depending on the trigger, additional options must be specified. See *Table 8-10* which lists some trigger descriptions. The UI displays some triggers not listed in the table, but these are not recommended to be used.

Note: *LED configuration should be done by experienced personnel. Use care when modifying the LEDs as improper configuration may cause LED indicators to be misread or missed.*

Table 8-10 Trigger Descriptions

Trigger	Description	Examples
none	The LED is always in the default state. This is useful to declare an LED to be always ON.	LED always on: ◆ LED name: any LED ◆ Default: On ◆ Trigger: none
timer	The LED blinks with the configured On/ Off frequency. Options: ◆ On-state delay: time in milliseconds that the LED is On. ◆ Off-state delay: time in milliseconds that the LED is Off.	LED is 100ms On / 200ms Off: ◆ LED name: any LED ◆ Default: On ◆ Trigger: timer ◆ On-State Delay: 100 ◆ Off-State Delay: 200
defaulton	This trigger option is deprecated. Use trigger = none and default = On instead.	

Trigger	Description	Examples
heartbeat	The LED flashes to simulate actual heartbeat thump-thump-pause. The frequency is in direct proportion to 1-minute average CPU load.	LED blinks in heartbeat pattern: ◆ LED name: any LED ◆ Default: Off ◆ Trigger: heartbeat
netdev	Network Activity The LED flashes with link status and/or send and receive activity on the configured interface. Options: ◆ Device: name of the network interface whose status will be indicated ◆ Mode: link, transmit, receive. One or more can be selected	LED blinks when there is a link, transmit or receive activity on the configured network interface (WWAN, LAN, cellular). ◆ LED name: X300-wwanactivity, X300-lanactivity, or X300-network ◆ Default: Off ◆ Trigger: netdev ◆ Device: select the configured interface (for example, “Ethernet adapter: eth1” for WAN) ◆ Mode: Link, Transmit, Receive
usbdev usbport	The LED turns on if a USB device is connected. It is recommended to use usbport rather than usbdev. Options for usbport: ◆ USB Port: select the configured USB port Options for usbdev: ◆ USB device: select the configured USP device	LED turns on if USB device is connected. ◆ LED name: ◆ Default: Off ◆ Trigger: usbport ◆ USP Port: Portusb1-port2

To configure the user-programmable LED:

1. Go to System > LED Configuration.
2. Click **Add LED action** or click **Edit** next to the existing LED action that you want to modify.
3. Enter or modify the configuration settings. See *Table 8-11*.
4. Click **Save**.
5. Click **Save & Apply**.

Table 8-11 LED Configuration

Parameter	Description
Name	Displays the descriptive name of the LED.
LED Name	Displays the LED name by function.
Default state	Displays the default state of the LED before the trigger. Options are On or Off.
Trigger	Displays the trigger event that will toggle the LED state. For descriptions, see *Table 8-10*.

Backup / Flash Firmware

System > Backup / Flash Firmware

The Backup / Flash Firmware page allows you to do backup and maintenance operations to keep the gateway healthy. It includes the following operations:

- Download a backup configuration file - run backups to keep the working configuration data, consisting of all policies and other user related information
- Restore a backup configuration file on the gateway - restore configuration or configure a new gateway with the same settings
- Reset the gateway to factory default settings
- Flash the device firmware

Actions

System > Backup / Flash Firmware > Actions

To perform backup / flash firmware operations:

1. Go to System > Backup / Flash Firmware > Actions.
2. Click the button corresponding to the operation that you want to perform. Follow the prompts for the selected operation. See *Table 8-12*.

Table 8-12 Backup, Restore, and Flash Operations

Parameters	Description
Backup/Restore	
Download Backup	Click **Generate archive** button to download a .tar archive file of the current configuration files.
Reset to defaults	Click **Perform Reset** button to reset the firmware to its default configurations. This is valid only with squashfs images. ***Note:*** *The gateway can also be reset by pressing the reset button on the gateway. Reset button behavior is as follows:* ◆ *Press and hold for more than 5 seconds and less than 20 seconds to reset the gateway to factory settings.* ◆ *Press and hold for more than one second but less than 5 seconds to reboot the gateway.*
Restore backup	Click **Upload archive** button to upload a previously generated backup archive.
Flash image	

Parameters	Description
Image	Click **Flash image** button to upload a sysupgrade compatible image for replacing the running firmware. ***Note:*** *Do not power off the device during the update.* When the image file is uploaded, a file integrity check is done through the use of md5 algorithm. You should verify the md5 value with the one given along with the binary file. When uploading the binary image, the UI will prompt to "Keep settings and retain the current configuration." This is selected by default. If you deselect it, the device configuration will be reset to factory setting after updating to the new firmware.

Configuration

System > Backup / Flash Firmware > Configuration

Add files and directories that should be preserved during a system upgrade to the backup file list. Modified files in /etc/config/ directory and certain other configurations are automatically preserved.

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

To modify the backup file list:

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

Custom Commands

System > Custom Commands

Write and execute custom shell commands from the web interface.

Write Custom Shell Command

This page lets you add or delete custom shell commands.

To write a custom shell command:

1. Go to System > Custom Commands > Configure.
2. Click **Add**.
3. Enter the command details. See *Table 8-13*.
4. Click **Save** or **Save & Apply**.

   The commands will be visible on the dashboard where you can run them.

Table 8-13 Custom Commands Configuration

Parameter	Description
Description	A short text description of the command.
Command	The command to execute on the shell terminal. To specify a file to be executed, the file must be copied to the /usr/sbin directory on the gateway. Files not in env PATH require the complete file path and should be executable.
Custom arguments	Check the box to allow user to provide additional command line arguments while running this command.
Public access	Check the box to allow the command to be executed and the output downloaded without prior authentication.

Run Custom Shell Command

Run custom shell commands. You also have the option to download the results of the command.

To run a custom command:

1. Go to System > Custom Commands > Dashboard.
2. Select the command to be run and click **Run.**

   The command, result, and return code are displayed in a box below the custom command.

Reboot

System > Reboot

Perform a reboot of the gateway. The gateway will restart and reload the configuration. Any unsaved configuration will be lost when the gateway is rebooted.

To reboot the gateway:

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

The gateway will restart and reload the configuration. After the gateway reboots, the login page will be displayed.

Schedule a Reboot

Schedule times when the gateway will reboot itself. You can set the frequency by time of day (hour and minute), day of week, and day of month.

The scheduled item must be enabled in order for the gateway to reboot itself.

To configure the reboot schedule:

1. Go to System > Reboot > Schedule Reboot.
2. Click **Add**.
3. Enter the schedule details (see *Table 8-14*).
4. Click **Save**.

Table 8-14 Schedule Reboot Time Specification

Parameter	Description
Minute	Range: 0-59
Hour	Range: 0-23 0 = midnight
Day of week	Range: 0-6 0 = Sunday
Date	1-31
Month	Range: 1-12

9: VPN

A Virtual Private Network (VPN) tunnel carries traffic of a private network from one endpoint system to another over a public network such as the Internet. The traffic of a private network so carried over a public network does not know about the existence of the intermediate hops between the two endpoints. Similarly, the intermediate hops are also not aware that they are carrying the network packets that are traversing the tunnel. The tunnel may optionally compress and/or encrypt the data, providing enhanced performance and some measure of security.

Note: *The X300 series gateways support additional tunneling protocols. For L2TP, PPtP, or GRE protocol configuration, see Interface Protocols.*

IPsec (Internet Protocol Security)

VPN > IPsec

The IP Security (IPsec) suite of protocols are designed for cryptographically secure communication at the IP layer. The gateway uses standard IPsec protocol to protect traffic. The identity of communicating users is checked with the user authentication based on pre-shared keys (PSK) or X.509 certificates.

The IPsec VPN instance can be started or stopped from the Web UI or by sending an SMS AT+VPN command. See *Table 10-16 SMS AT Command Syntax*.

You can configure a router-to-router VPN connection.

To configure an IPsec instance:

1. Go to VPN > IPsec, and click **Add**.
2. Under Gateway to Gateway, click **Add**.
3. Enter the VPN configuration details on the General Settings (*Table 9-1*) and Advanced Settings (*Table 9-2*) tabs.

Table 9-1 IPsec General Settings

Parameters	Description
Profile Name	Enter the Profile Name to identify the router–to-router IPsec VPN connection.
ProtoType	Gateway to Gateway is selected.
Enable	Check to enable the connection.
Remote IPsec router	Enter the remote WAN IP Address or domain name of the remote IPsec router server.
Remote Address	Enter the remote LAN IP Address and subnet of the remote IPSEC router server for use on the VPN connection.
Remote ID	Enter the ID of the remote network as configured on the remote IPsec router server.

Parameters	Description
Method	Select the interface used to establish the tunnel. ◆ Static – indicates that you will specify the interface to be used to establish the tunnel ◆ Auto – uses the interface that is active from the Load Balancer (MWAN) policies
Route	Available if Static is selected in Method field. Select the interface used to configure IPsec: ◆ Wifi ◆ Cellular
Policy	Available if Auto is selected in Method field. Select the MWAN policy to use.
Interface	Displays the IP address of the interface used for the VPN connection.
Local Address	Enter the local network IP Address and subnet mask of the router for use on the VPN connection.
Local ID	Enter the ID of the local router as configured on the remote IPSEC router server. Note: On the remote server, it may be displayed as "remote ID."
Key Mode	Select the type of Key mode in use for VPN connection: ◆ Pre shared Key ◆ X.509 certificate
Preshared-Key	This field is available if Pre shared Key is selected in the Key Mode field. Enter the key. The peer uses the key to authenticate each other from Internet Key Exchange.
Cert.	This field is available if X.509 Certificate is selected in the Key Mode field. The certificate file must be uploaded to the /etc/ipsec.d/certs directory. Click **Select file...** to browse the local drive and select the file. Click **Upload file...** to upload the file. After the file is uploaded, the Cert. field displays the file name and time stamp of the upload. To delete a file, click **Delete**.
Key	This field is available if X.509 Certificate is selected in the Key Mode field. The key file must be uploaded to the /etc/ipsec.d/private directory. Click **Select file...** to browse the local drive and select the file. Click **Upload file...** to upload the file. After the file is uploaded, the Key field displays the file name and time stamp of the upload. To delete a file, click **Delete**.

Parameters	Description
CA Cert.	This field is available if X.509 Certificate is selected in the Key Mode field. The CA certificate file must be uploaded to the /etc/ipsec.d/cacerts directory. Click **Select file...** to browse the local drive and select the file. Click **Upload file...** to upload the file. After the file is uploaded, the CA Cert. field displays the file name and time stamp of the upload. To delete a file, click **Delete**.
Single hop IP for watchdog	Enter the IP address to be used for monitoring purposes. The application will ping the IP defined here. If the ping fails, it will restart the device. This could be the LAN IP address of the IPsec router server.
Monitor interface ping failure	Select Yes to ping the IP address defined in Single hop IP for watchdog. Select No if you don't want the monitor interface to ping the single hop IP address. The default is No.

Table 9-2 IPsec Advanced Settings

Parameters	Description
IKE Mode	Select the mode that Internet Key Exchange (IKE) protocol uses to authenticate and/or encrypt the peers. ◆ Main ◆ Aggressive
Key Exchange	Select the mode of encryption key exchange between two communicating peers: ◆ IKEV1 ◆ IKEV2 ◆ The default mode is IKEV1.
IKE Encryption	Select the cipher type to use for the Internet Key Exchange (IKE): ◆ Any ◆ AES ◆ AES-128 ◆ AES-192 ◆ AES-256 ◆ 3DES ◆ DES The default cipher type is “Any”.

Parameters	Description
IKE Hash	The IKE hash is used for authentication of packets for the key exchange. Select the IKE Hash type to use for VPN connection: ◆ Any ◆ MD5 ◆ SHA1 ◆ SHA2 256 ◆ SHA2 384 ◆ SHA2 512 The default IKE hash type is “Any”.
IKE DH Group	Select the desired Diffie-Hellman group to use: ◆ Any ◆ Group 1 (768) ◆ Group 2 (1024) ◆ Group 5 (1536) ◆ Group 14 (2048) ◆ Group 15 (3072) ◆ Group 16 (4096) Higher-numbered groups are more secure but also require longer to generate the key. The default group is “Any”.
IPsec Encryption	Select the type of IPsec encryption for VPN connection: ◆ Any ◆ AES ◆ AES-128 ◆ AES-192 ◆ AES-256 ◆ 3DES ◆ DES The default cipher type is “Any”.
IPsec Hash	The IPsec hash is used for authentication of packets for the key exchange. Select the IPsec Hash type to use for VPN connection: ◆ Any ◆ MD5 ◆ SHA1 ◆ SHA2 256 ◆ SHA2-384 ◆ SHA2-512 The default hash type is “Any”.

Parameters	Description
DH Group	Select the desired Diffie-Hellman group to use: ◆ Any ◆ Group 1 (768) ◆ Group 2 (1024) ◆ Group 5 (1536) ◆ Group 14 (2048) ◆ Group 15 (3072) ◆ Group 16 (4096) ◆ Group 17 (6144) ◆ Group 18 (8192) Higher-numbered groups are more secure but also require longer to generate the key. The default group is “Any”.
DPD Keep Alive Time	Enter the time in seconds for interval between Dead Peer Detection keep alive messages.
DPD Timeout	Enter the time in seconds of no response from peer before Dead Peer Detection times out.
IKE Re-key Time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set it to 0.
SA Life Time	Enter the time in seconds for the security association lifetime.
DPD Action	Select the desired Dead Peer Detection action. This action must be taken when a dead IKE peer is detected.

4. Click **Save**. The instance is saved and displayed on the IPsec page.
5. After configuring the profile, click **Connect** to start the IPsec connection for the first time.

OpenVPN

VPN > OpenVPN

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections. It uses the OpenSSL library to provide encryption of both the data and control channels. OpenVPN can run over UDP or TCP transports, multiplexing created SSL tunnels on a single TCP/UDP port.

OpenVPN fully supports IPv6 as the protocol of the virtual network inside a tunnel and the OpenVPN applications can also establish connections via IPv6. It has the ability to work through most proxy servers (including HTTP) and is good at working through network address translation (NAT) and getting out through firewalls. The server configuration has the ability to push certain network configuration options to the clients, including IP addresses, routing commands, and a few connection options.

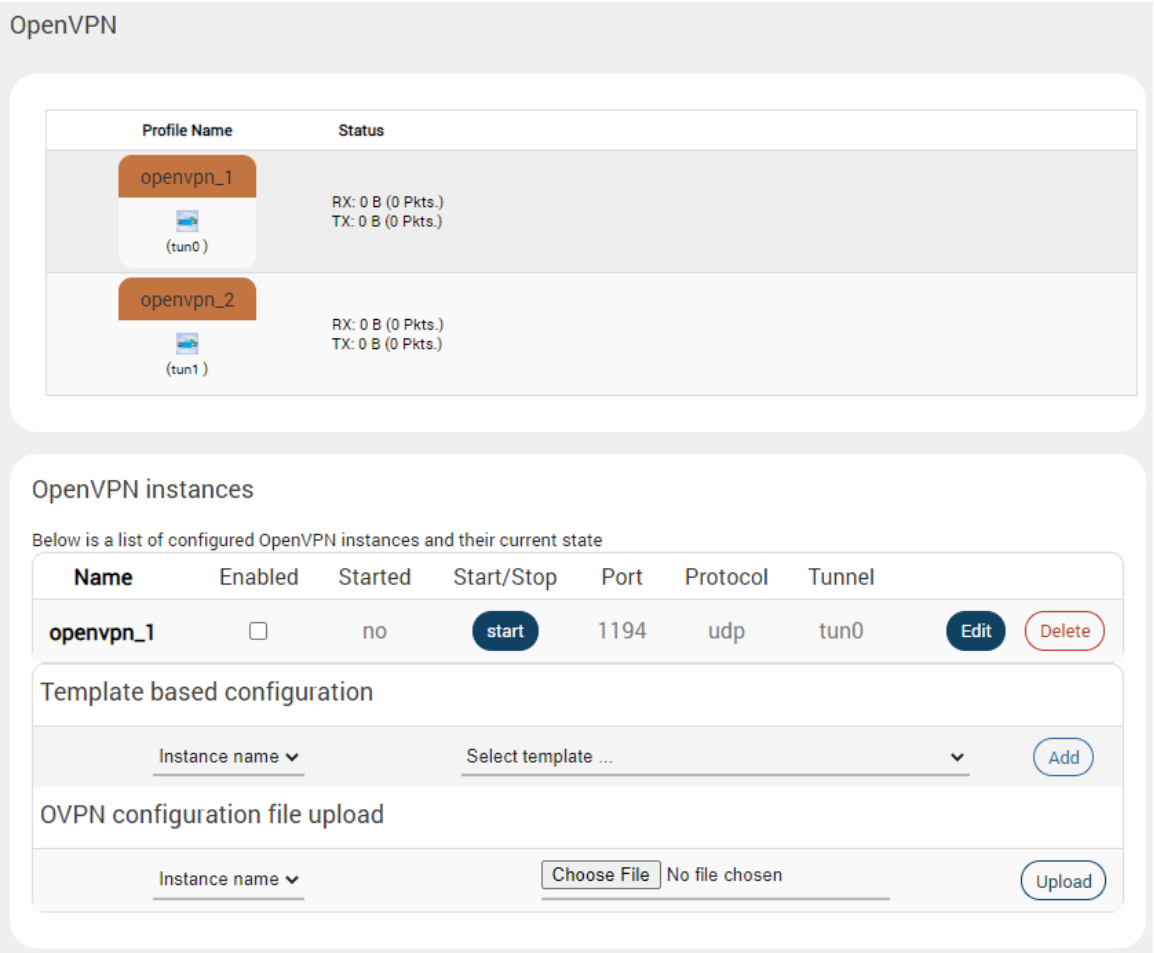
The X300 series gateways support OpenVPN client, server, and pass through.

OpenVPN Instances

The OpenVPN client will attach itself to the configured OpenVPN server over any available WAN, LAN, or Cellular network interface. If the auto-connect function is enabled, OpenVPN will connect over available WAN, switch between WAN connections when one WAN fails-over to another, and also auto start on every reboot.

To create an OpenVPN instance:

1. Go to VPN > OpenVPN. The following page is displayed:



2. Under OpenVPN instances, select the method for the instance configuration:
   - **Template based configuration** – Select the instance name and the template (server or client templates are provided). Click **Add**.
   - **OVPN configuration file upload** – Select the instance name and then choose the OVPN configuration file. Click **Upload**.
3. The instance is added to the list under OpenVPN instances.
4. Choose from the following options:
   - To continue configuring the instance, click **Edit**. See *Template-based Configuration* or *OpenVPN Configuration File* for details respective to the configuration method.
   - To enable the instance, select **Enabled**.
5. Click **Save & Apply**.

Note: *You must manually enter the DNS from Network > DHCP and DNS.*

Template-based Configuration

Predefined templates

Use the following predefined server and client templates to create the initial configuration of the OpenVPN instance:

- Client configuration for an ethernet bridge VPN
- Client configuration for a routed multi-client VPN
- Simple client configuration for a routed point-to-point VPN
- Server configuration for an ethernet bridge VPN
- Server configuration for a routed multi-client VPN
- Simple server configuration for a routed point-to-point VPN

Note: *This document does not cover OpenVPN client/server configuration. Please consult your administrator for configuration details of your VPN or refer to the* OpenVPN online documentation *for information on how to configure the VPN.*

Edit the template-based configuration

After you add the template-based instance, you can edit the instance to configure the appropriate fields and values for the particular VPN connection.

Note the following about editing the template-based instances:

- Click the **Switch to advanced configuration** or **Switch to basic configuration** links at the top of the form to switch the view between basic and advanced configuration.
- Select **Additional Field** at the bottom of the form to select additional configuration fields to add to the form.
- Select **Client** to enable client mode, or leave it blank to enable server mode.
- You should add your CA, certificates, and keys for the instance.
- Click **Save & Apply** when you are finished.

OpenVPN Configuration File

If you use an OVPN configuration file to configure the OpenVPN instance, the configuration file should contain settings for either a server configuration or a client configuration with **.ovpn** as the file extension.

Note: *This document does not cover how to create OpenVPN configuration files. Please refer to the* OpenVPN online documentation *for sample server and client configuration files and information on how to create configuration files.*

Edit the OVPN Configuration File

After you upload the configuration file, you can use the OpenVPN configuration editor on the web interface to modify the configuration. The editor window contains two sections: one to modify the OVPN configuration file and one to add a user and password authentication file with your credentials.

Click **Save** to save changes to the configuration file and close the editor.

10: Services

The X300 series gateways are equipped with services that complement the routing features. These services include:

- *Agents*
- *DOTA*
- *Dynamic DNS*
- *External Filesystems*
- *GPS**
- *Keepalived*
- *Logs Information*
- *Page Selector*
- *Reporting Agent*
- *Service Actions*
- *SMS*
- *SNMPD*
- *SNMPTRAPD*
- *uHTTPd*

Agents

Services > Agents

Agents are customized applications loaded on the gateway that communicate with a specific device or data management platform.

By default, the Lantronix Wireless Automation Server (MWAS) agent is loaded on the gateway, which facilitates bi-directional data communication between devices/PLCs (Programmable Logic Controllers) connected to the gateway and a centralized server through a Kalkitech-compatible server.

[Device/SCADA <=> Kalkitech(sever)] <=> [MWAS(agent) <=> Device/PLC]

Table 10-1 Agent Configurations

Parameters	Description
Agents	Select the Agent from the list: ◆ MWAS – Lantronix Wireless Acquisition System
Enable	Click to enable the selected agent.
LAN IP/URL	Enter the IP address of the field device (PLC).
LAN PORT	Enter the port number of the field device (PLC).
WAN IP/URL	Enter the IP address of the WAN server.
WAN PORT	Enter the port number of the WAN server.
Enable WAN Backup IP	Click to enable the backup server. If enabled, enter the following: ◆ Backup WAN IP/URL – Enter the IP address of backup WAN server. ◆ Backup WAN Port – Enter the port number of backup WAN server.

DOTA

DOTA (download over the air) allows you to remotely update the gateway's firmware using the Lantronix server or your custom server.

Lantronix Server

Services > Dota > Lantronix Server

This page allows you to update the gateway's firmware using the Lantronix DOTA server.

To upgrade the firmware:

1. Go to Services > DOTA > Lantronix Server.
2. Select the channel and click **Check for update** to find available updates. See *Table 10-2*.

   The results of the update check are displayed in the area below the action bar. If an update is available, the firmware file is displayed under Available Firmwares.
3. To update the device, select the firmware file under Available Firmwares and click **Update now**.

   Do not power off the device during the update. After the firmware is updated, the device will reboot.

Table 10-2 DOTA using Lantronix Server

Parameters	Description
Channel	Select the channel on which to look for the firmware update files. The options are Development, Beta, and Released. The default channel option is Released.
Check for update	Click to check for available updates.
Available Firmware	Displays a list of firmware that is available on the server. Select the firmware from this list and click **Update now** to upgrade or downgrade the firmware.
Force Upgrade	Check this box for forceful upgrade or downgrade of the firmware version.
Update now	Click **Update now** to download the firmware selected in the Available Firmware list.

Custom Server

Services > Dota > Custom Server

This page allows you to update the gateway's firmware using a custom DOTA server.

To update firmware using a custom server:

1. Go to Services > DOTA > Custom Server.
2. Enter the server details. See *Table 10-3*.
3. Click **Update now**.

Table 10-3 DOTA Custom Server Configuration

Parameters	Description
Update now	After setting the Custom Server parameters, click **Update now** to download the firmware pointed to by the URL and the filename below.
Custom Server Settings	
Note: If the custom server is not configured, DOTA service will configure the Lantronix server.	
Protocol	Select HTTP or HTTPS as the protocol of the custom server. Enter the configuration depending on the protocol you selected.
URL/IP	Enter the URL or the IP address of the custom DOTA server. The URL, if provided, must include http or https.
Filename	Enter the firmware file name to be accessed for the update.
Username	This field is displayed if the selected protocol was HTTP. Enter the server login username.
Password	This field is displayed if the selected protocol was HTTP. Enter the server login password.
Cert-type	This field is displayed if the selected protocol was HTTPS. Choose the type of certificate file. The options are PEM, DER, or ENG.
Cert	This field is displayed if the selected protocol was HTTPS. Click the **Select file...** button to browse to the SSL certificate file to be uploaded.
Key	This field is displayed if the selected protocol was HTTPS. Click the **Select file...** button to browse to the key file to be uploaded.
Timeout in Minutes	Enter the period of time to wait for the download to complete. The download process will be aborted after the timeout period expires. The default value is 10 minutes.
Retries	Enter the number of retry attempts allowed to check and download the latest firmware file from the server. The default number of retries is 3.

Note: *DOTA update can also be triggered using SMS by sending the SMS AT+DOTA command after setting the custom server configuration from the Web UI (shown above) or by sending the AT+DOTASETTINGS command using SMS from a registered mobile number. For command syntax, see Table 10-16 SMS AT Command Syntax.*

Dynamic DNS

Services > Dynamic DNS

Dynamic Domain Name System (Dynamic DNS or DDNS) offers a method of keeping a static domain/host name linked to a dynamically assigned public IP address allowing your server to be more easily accessible from various locations on the Internet.

The DDNS page lets you configure your DDNS service so that the gateway automatically updates its public IP to your DDNS provider. Before starting this configuration, you should already have registered a DNS name with a compatible DDNS service provider. For a list of compatible DDNS providers, visit: https://openwrt.org/docs/guide-user/services/ddns/client.

To add a DDNS configuration:

1. Go to Services > Dynamic DNS.
2. At the bottom of the Overview section, type the DDNS configuration name and click **Add**.

To edit a DDNS configuration:

1. Go to Services > Dynamic DNS.
2. In the Overview section, select the DDNS configuration that you want to edit and click **Edit**.
3. Edit the configuration settings. See *Table 10-4*.
4. Click **Save & Apply**.

Table 10-4 Dynamic DNS Client Configuration

Parameters	Description
Basic Settings	
Enabled	Select to enable Dynamic DNS. Clear to disable Dynamic DNS. Dynamic DNS allows the gateway to be reached with a fixed hostname while having a dynamically changing IP Address.
Lookup Hostname	Name to identify the host that you want to use on DDNS server. This is the domain name that you registered with your DDNS service provider. The hostname is received from the dynamic DNS service provider.
IP address version	Select the IP address version – IPv4 or IPv6.
DDNS Service Provider [IPv4/ IPv6]	Select the DDNS service provider from the drop down list.
Domain	The domain that you want to update. Usually the same as the lookup hostname.
Username	Username of DDNS account. The username is received from the DDNS service provider.
Password	Password of DDNS account. The password is received from DDNS service provider.
Use HTTP Secure	Select to use HTTPS with the DDNS provider. Otherwise, leave it unchecked.

Parameters	Description
Path to CA-certificate	This field is visible if HTTPS is selected. Enter the directory or file path of the ssl certs. To run HTTPS without verification of server certificates (insecure), enter IGNORE.
Advanced Settings	
IP address source [IPv4/IPv6]	Select the IP Address source: Network, Interface, URL, or Script and enter the appropriate configuration details. Network ◆ Network (IPv4) – Select the software interface to read systems IPv4 address from. Interface ◆ Interface – Select the physical network interface from the options URL ◆ URL to detect – Enter the URL to read systems IP address from. The source IP Address by default is URL. ◆ Event Network (IPv4) – network on which the ddns-updater scripts will be run ◆ Bind Network – leave as “default” or select the network to use for communication. Note that casual users should not change this setting. Script ◆ Script – Enter the script path and file name. ◆ Event Network (IPv4) – network on which the ddns-updater scripts will be run
Force IP Version	Select if you want to force the usage of either IPv4 or IPv6 only. This field is optional.
DNS-Server	Enter DNS server domain name or IP address if you want to override the default DNS server to detect the registered IP. Enter IP address or FQDN.
PROXY-Server	Enter the proxy server to use for detection and updates. Format: [user:password@]proxyhost:port IPv6 address must be given in square brackets: [2001:db8::1]:8080
Log to syslog	Select log level to write log messages to syslog. Critical errors are always logged to syslog. Available options include No logging, Info, Notice, Warning, Error. The default setting is Notice.
Log to file	Select to allow the detailed messages to be written to log files. Log files store up to 250 lines and then are automatically truncated.
Timer Settings	
Check Interval	Specify the time interval to check if the local IP has changed. Values less than 5 minutes (300 seconds) are not supported. Default is 10 minutes.

Parameters	Description
Force Interval	Specify the time interval after which the DDNS server should force update the IP address of your server even if no IP change was detected. The force interval should be greater than the check interval. Enter 0 to force the script to only run once. Default is 72 hours.
Error Retry Counter	The number of retries to attempt before the script stops execution. Default setting is 0 which indicates infinite retries.
Error Retry Interval	If an error occurs on detecting, sending or updating, the script will retry the relevant action according to the specified time interval. Default is 60 seconds.
Log File Viewer	
Read/Reread log file	Click to display the DDNS log file.

External Filesystems

Services > External Filesystems

The X300 series gateway supports an SD(HC)/MMC card or external USB flash drive for external file storage. This page configures the mount settings for the external filesystem.

To configure the external filesystem:

1. Insert the SD card in the SD card slot or the USB flash drive in the USB slot on the gateway.
2. Go to Services > External Filesystems.
3. Configure the external device settings. See *Table 10-5*.
4. Click **Save & Apply**.

Table 10-5 External Filesystems Configuration

Parameters	Description
External device	Select the external device.
Mount point	Enter the mount point directory to the file system, relative to the top level directory. Example: /tmp/usbdevice
Auto mount	Select to mount the device automatically when the gateway boots. If unselected, the device must be mounted manually.
Options	Enter the Linux mount options to be run when the device is mounted. Separate each of the options with a comma. Default mount option: rw, sync

GPS

Services > GPS

The built-in GPS receiver receives GPS data from GPS satellites for synchronizing the GPS time and position data.

Note: *GPS is only available on certain X300 device models.*

Enable GPS

To enable GPS receiver:

1. Go to Services > GPS.
2. Select GPS Enable.
3. Click **Save & Apply**.

The data will be displayed on the page (see *Table 10-6*). It may take some time (about a minute) to receive and display the data.

Send GPS Data to an External Server

The GPS data can be sent in NMEA data format to an external TCP server on a real-time basis. You can also configure the GPS data to be sent to a backup server.

To send the GPS data to an external server:

1. Go to Services > GPS.
2. Select **Enable Data Send** and enter the server settings (see *Table 10-6*).
3. Click **Save & Apply**.

Table 10-6 GPS Service Configuration

Parameters	Description
GPS Parameters	
GPS Enable	Select GPS Enable check box to display current GPS data.
Time (GMT)	Time in hh:mm:ss
Latitude (degree.mmsss)	Latitude in ddmm.mmmm
N/S-Indicator	N = North or S = South
Longitude (degree.mmsss)	Longitude in ddmm.mmmm
E/W-Indicator	E = East or W=West
Position-Fix-Indicator	Indicates the type of signal or technique used by the GPS receiver to determine its location. ◆ **0 –** Fix not available or invalid ◆ **1 –** GPS SPS Mode, fix valid ◆ **2 –** Differential GPS, SPS Mode, fix valid ◆ **3 to 5 –** Not supported ◆ **6 –** Dead Reckoning Mode, fix valid
Number of Satellites Used	Number of satellites used to receive GPS signals. The range for the number of satellite used is 0 to 12.
HDOP	Horizontal Dilution of Precision (HDOP) indicates the relative accuracy of the horizontal position

Parameters	Description
Altitude (in meters)	Altitude above mean sea level
Status	Displays the status. A = Data valid V = Data not valid
Speed	Speed over ground in knots
Course of Ground	Track, or intended direction of travel
Protocol	
Enable Data Send	Select **Enable Data Send** check box to send data to the selected server. It sends the GPS information in NMEA format.
Protocol	Select the TCP protocol only.
IP1/URL1	Enter the primary IP address.
Port1	Enter the port number.
Backup	Click to use a backup server, in case sending the data fails using primary IP address. ◆ IP2/URL2 – Enter the backup IP address. ◆ Port2 – Enter the backup port number.
Polling Interval (in seconds)	The period of time between the end of the timeout period or the completion of the network request and the next request for data on the network.
Send Interval (in seconds)	The period of time to wait between attempts to send GPS data using the primary IP address or backup IP.

Description of NMEA Messages

The X300 series device receives NMEA sentences every second, depending on the configuration. The identifiers for the NMEA messages are listed below. All messages are based on the NMEA standard messages.

GPGGA	GPS Fix Data
GPRMC	Recommended Minimum Specific GPS Data
GPGSV	GPS Satellites in View
GPGSA	GPS DOP and Active Satellites
GPVTG	Course Over Ground and Ground Speed

A full description and definition of the listed messages above is provided in the next sections.

GPGGA Format

The $GPGGA message includes time, position, GPS quality and number of satellites in use.

Example: $GPGGA,120133.0,1907.469671,N,07250.544473,E,1,05,1.0,43.1,M,-64.0,M,,*42

Table 10-7 GGA Data Format

Parameters	Description
MID GGA Parameters	
MID	GGA Protocol Header Example – $GPGGA
UTC Time	Time in hhmms.sss Example – 120133.0
Latitude	Latitude in ddmm.mmmm Example – 1907.469671
N/S-Indicator	N = North or S = South Example – N
Longitude	Longitude in ddmm.mmmm Example – 07250.544473
E/W-Indicator	E = East or W = West Example – E
Position-Fix-Indicator	Indicates ◆ 0 – Fix not available or invalid ◆ 1 – GPS SPS Mode, fix valid ◆ 2 – Differential GPS, SPS Mode, fix valid ◆ 3 to 5 – Not supported ◆ 6 – Dead Reckoning Mode, fix valid Example – 1
Satellite-Used	Number of satellite used to receive GPS signals. The range for the number of satellite used is 0 to 12. Example – 05
HDOP	Horizontal Dilution of Precision Example – 1.0
MSL Altitude	Altitude in meters. Example – 43.1 meters
Units	Example – M meters
Geoid Seperation	Geoid-to-ellipsoid separation. Ellipsoid altitude = MSL Altitude + Geoid Separation Example: -64.0 meters
Units	Example: M meters
Age of Diff.Corr.	Null fields when DGPS is not used.4 The units is sec.
Diff. Ref.Station ID	–
Checksum	*42
<CR><LF>	End of message termination

GPRMC Format

The $GPRMC message includes time, date, position, course, and speed datea.

Example: $GPRMC,120133.0,A,1907.469671,N,07250.544473,E,0.0,0.0,150915,0.3,W,A*1E

Table 10-8 RMC Data Format

Parameters	Description
MID RMC Parameters	
MID	RMC Protocol Header Example – $GPRMC
UTC Time	Time in hhmmss.sss Example – 120133.0
Status(1)	A = Data valid V = Data not valid Example – A
Latitude	Time in ddmm.mmmm Example – 1907.469671
N/S-Indicator	N = North or S = South Example – N
Longitude	Longitude in ddmm.mmmm Example – 07250.544473
E/W-Indicator	E = East or W = West Example – E
Speed Over Ground	Measured in knots. Example – 0.0
Course Over Ground	True. Measured in degrees Example – 0.0
Date	Date in ddmmyy Example – 150915
Magnetic Variation(2)	E = East or W = West Measured in degrees Example – 0.3
East/West Indicator(2)	W = West Example – W
Mode	Indicates ◆ **A –** Autonomous ◆ **D –** DGPS ◆ **E –** DR ◆ **N –** Output Data Not Valid ◆ **R –** Course Position(3) (4) (5) ◆ **S –** Simulator Example **–** A
Checksum	*1E

Parameters	Description
<CR><LF>	End of message termination

(1) A valid status is derived from all the parameters set in the software. This includes the minimum number of satellites required, any DOP mask setting, presence of DGPS corrections, etc. If the default or current software setting requires that a factor is met, and then if that factor is not met the solution will be marked as invalid.

(2) CSR Technology Inc. does not support magnetic declination. All courses over ground data are geodetic WGS84 directions relative to true North.

(3) Position was calculated based on one or more of the SVs having their states derived from almanac parameters, as opposed to ephemerides.

(4) This feature is supported in the GSD4e product only.

(5) This feature is supported in the GSD4e product, version 1.1.0 and later.

GPGSV Format

The $GPGSV includes the number of satellites in view, satellite ID numbers and their evaluation, azimuth and signal-to-noise ratio.

Example: $GPGSV,4,1,16,21,50,358,38,22,28,272,37,29,53,164,36,18,51,319,31,*71E

IMEI number is added at the start of every frame.

Table 10-9 GPGSV Data Format

Parameters	Description
MID GSV Parameters	
MID	GSV Protocol Header Example – $GPGSV
Number of Messages(1)	Total number of GSV messages to be sent in this group Example – 4
Message Number(1)	Message number in this group of GSV messages Example – 1
Satellites in View(1)	16
Satellite ID	Channel (Range 1 – 32) Example – 21
Elevation	Channel 1 (Maximum 90) Example – 50 degrees
Azimuth	Channel (True, Range 0 – 359) Example – 358 degrees
SNR (C/N0)	Range 0 – 99, null when not tracking Example – 38dBHz
….	(Satellite ID, elevation, azimuth, and SNR repeated for each satellite in view)
Satellite ID	Channel 4 (Range 1 – 32) Example – 18

Parameters	Description
Elevation	Channel 4 (Maximum 90) Example – 51 degrees
Azimuth	Channel 4 (True, Range 0 - 359) Example – 319 degrees
SNR (C/N0)	Range 0 – 99, null when not tracking Example – 31 dBHz
Checksum	*71
<CR><LF>	End of message termination

(1)Depending on the number of satellites tracked, multiple messages of GSV data may be required. In some software versions, the maximum number of satellites reported as visible is limited to 12, even though more may be visible.

GPGSA Format

The $GPGSA message includes the list of satellites being used.

Example: $GPGSA,A,3,18,20,21,22,29,,,,,,,2.4,1.0,2.2*36

Table 10-10 GSA Data Format

Parameters	Description
MID GSA Parameters	
MID	GSA Protocol Header Example – $GPGSA
Mode1	**M – Manual:** Forced to operate in 2D or 3D mode **A – 2D Automatic:** Allowed to automatically switch 2D/3D Example – A
Mode2	1 – Fix not available 2 – 2D (<4 SVs used) 3 – 3D (>3 SVs used) Example – 3
Satellite Used(1)	SV on Channel 1 Example – 18
Satellite Used(1)	SV on Channel 2 Example – 20
….	….
Satellite Used	SV on Channel 12
PDOP(2)	Position Dilution of Precision Example: 2.4
HDOP(2)	Horizontal Dilution of Precision Example: 1.0
VDOP(2)	Vertical Dilution of Precision Example: 2.2

Parameters	Description
Checksum	*33
<CR><LF>	End of message termination

(1) Satellite used in solution.

(2) Maximum DOP value reported is 50. When 50 is reported, the actual DOP may be much larger.

GPVTG Format

The $GPVTG message includes course over ground and ground speed.

Example: $GPVTG,0.0,T,0.3,M,0.0,N,0.0,K,A*20

Table 10-11 VTG Data Format

Parameters	Description
MID VTG Parameters	
MID	VTG Protocol Header Example – $GPVTG
Course	Measured heading Example – 0.0 degrees
Reference	True Example – T
Course	Measured heading Example – 0.3 degrees
Reference	Magnetic(1) Example – M
Speed	Measured horizontal speed Example – 0.0 knots
Units	Knots Example – N
Speed	Measured horizontal speed Example – 0.0 km/hr
Units	Kilometers per hour Example – K
Mode	Indicates ◆ **A –** Autonomous ◆ **D –** DGPS ◆ **E –** DR ◆ **N –** Output Data Not Valid ◆ **R –** Course Position(2) (3) (4) ◆ **S –** Simulator Example **–** A
Checksum	*20

Parameters	Description
<CR><LF>	End of message termination

(1) CSR does not support magnetic declination. All “course over ground” data are geodetic WGS84 directions.

(2) Position was calculated based on one or more of the SVs having their states derived from almanac parameters, as opposed to ephemerides.

(3) This feature is supported in the GSD4e product only.

(4) This feature is supported in the GSD4e product, version 1.1.0 and later.

Keepalived

Services > Keepalived

The Keepalived service provides frameworks for load balancing and high availability of the servers connected to the gateway. Keepalived uses Virtual Router Redundancy Protocol (VRRP) to check the health of load balanced routers and elect a router on the network that will serve a particular IP.

In a typical configuration, VRRP groups two or more routers into a virtual router, where one router is the master (active) server and the other is the backup node. The master server has a higher priority than the backup server. The master server transmits multicast VRRP advertisement packets at regular intervals, and the backup servers listen for these advertisement packets. If the backup servers fail to receive three consecutive VRRP advertisements, the backup router with the highest priority becomes the new master router so that the system remains functional.

The configuration for the backup server will be similar to that of the master server, with the exception of the values for priority, state, and interface, depending on the system hardware configuration.

Keepalived Configuration

The Keepalived configuration on the web interface includes the following sections:

- **General** – Keepalived log settings
- **Global** – Keepalived global settings
- **Tracking Scripts** – create tracking script blocks that Keepalived will run to determine the health of the host and increase or decrease the priority of the router by the value of the weight.
- **Tracking Interfaces** – configure which interfaces Keepalived will monitor. If a monitored interface fails, Keepalived will adjust the priority of the host according to the configured weight of the tracking interface.
- **Tracking Processes** – create tracking process blocks that Keepalived can use to monitor the health of the router. If the monitored process stops running, Keepalived will adjust the priority of the host according to the weight of the tracking process. After adding a process, you must restart the Keepalived service.
- **Virtual IP** – configure the Virtual IP address for the VRRP instance.
- **VRRP Instances** – add VRRP instances to be run on interfaces that Keepalived is monitoring. The VRRP instance is defined in the General and Advanced settings. The User Notify settings allow Keepalived to run specified scripts when the router transitions between backup and master states.

To configure Keepalived settings:

1. Go to Services > Keepalived.
2. Edit the configuration settings. See *Table 10-12*.
3. Click **Save & Apply** when you are finished.

Table 10-12 Keepalived Configuration

Parameters	Description
General	
Detailed Log	Select to enable detailed keepalived general/common logs.
Syslog level	Set the log level from 0-4, with 4 being the most detailed.
Keepalived Global	
Vrrp startup delay	Enter the time in seconds to delay before starting VRRP.
Global Router Id/name	Enter the global router ID/name. A default name is provided, but you can modify it if you want. It doesn't have to be the hostname, but it must be unique for each device in a pool.
Keepalived config file	Select the Keepalived configuration file. Settings in the configuration file will supersede settings configured on the Keepalived UI pages except for all scripts loaded in Tracking Scripts, and the User Notify settings in VRRP Instances. The name of the script should match the ones in the configuration file settings.
Remove configuration for Keepalived	Unlink the uploaded keepalived configuration so as to fill the configurations manually.
User	The user for script execution.
Enable Script Security	Select to prevent running any scripts that were configured to be run as root if any part of the path is writable by a non-root user.
Enable dynamic interfaces	Select to enable dynamic interfaces. Once enabled, next to Dynamic interfaces, select Allow or None
Tracking Scripts	
Name of trackscript block	Enter the tracking script block name.
Script	Select the tracking script file to upload it to the router. The file is uploaded to the /usr/sbin/ folder. The script name should start with "keepalived_" and end with ".sh".
Remove script	Click to remove the tracking script.
TrackScript interval	Enter the time interval between script invocations in seconds. Default is 1 second
Weight	Enter the weight to adjust the priority if the tracking script fails. Range is -253 to 253. Positive value will increase the priority. Negative value will decrease the priority. Setting it to zero (0) will ignore the weight, which means that any VRRP instance monitoring the script will transition to the fault state after the fail count number of consecutive failures of the script. A script returning 0 (zero) is success and everything else is fail.
TrackScript pass count	Enter the required number of successes for OK transition.
TrackScript fail count	Enter the required number of fails for NOK transition.
Tracking Interfaces	
Name of interface block	Enter the name of the tracking interface block
Interfaces	Select the interface to monitor for changing the state of the router or decreasing the weight.

Parameters	Description
Weight	Enter the weight to adjust the priority if the interface is present or absent. Range is -253 to 253. Positive value will increase the priority. Negative value will decrease the priority. Default is 0 (zero), which means that the router will fail in case of the interface not running.
Tracking Processes	
Name of process block	Enter the name of the process block.
Process	Enter the name of the process to monitor for running state.
Weight	Enter the weight to adjust the priority if the process is not running. Range is -253 to 253. Positive value will increase the priority. Negative value will decrease the priority. Default is 0 (zero), which means that the router will fail in case of the interface not running.
Virtual IP	
Name of address block	Enter the name of the address block.
Virtual ipaddress	Enter the Virtual IP address and netmask that will be used by the virtual router.
Physical device	Select the device used for the virtual IP.
Scope of the virtual ip	Select the scope. Options include: **global**, site, link, host, nowhere.
VRRP Instances	
VRRP Instances > General Settings	
Enable	Click to enable the VRRP instance. The VRRP instance defines and configures VRRP behavior to run on a specific interface.
Name of Instance	Enter a name for the VRRP instance.
Virtual Router ID	Enter the router ID. This number should be the same for all routers on the virtual router. Unique number from 1 to 155.
Interface to look for	Select the interface that needs to be monitored for switching.
Virtual Router Priority	Enter the priority. The router with the highest priority will be the master.
Delay	Enter the interval in seconds that VRRP will wait between sending advertisement packets. Default is 1 second.
Debug	Enter the debug level, from 1 to 4. Note: Debug level is not implemented yet by Keepalived.
Initial Virtual Router State	Select the initial virtual router state as MASTER or BACKUP. This is for initial state only. As soon as the other routers in the virtual router group come up, an election will be held and the router with the highest priority will become MASTER.
Enable Authentication	Select to enable authentication. Authentication type can be PASS (suggested) or AH – IPsec (not recommended). PASS is a simple text password. This should be the same value on all machines in the virtual router. Only the first eight (8) characters are used. Note: Authentication was removed from the VRRPv2 specification, and use of the option is non-compliant and can cause problems.

Parameters	Description
VRRP Instances > Advanced Settings	
Virtual IPs	Enter the Virtual IP block. The router will assume this IP when it becomes Master and release it when it changes to Backup. Add blocks configured in Virtual IP.
Track Process	Enter the track process block that the VRRP instance will monitor. Add blocks configured in Tracking Process.
Track interface	Enter the track interface block that the VRRP instance will monitor. Add blocks configured in Tracking Interfaces.
Track Script	Enter the tracking script block that the VRRP instance will monitor. Add blocks configured in Tracking Scripts.
VRRP Instances > User Notify Settings	
Notify master Script	Select the notify master script which will be run when the router becomes Master.
Remove master script	Remove the notify master script.
Notify backup Script	Select the notify backup script which will be run when the router becomes Backup.
Remove backup script	Remove the notify backup script.

Logs Information

Services > Logs Information

Logs Information page lets you view the system log file and download them to the local computer. The current log file and up to 3 historical log files may be saved.

The logs configuration is read from the system logging. In order to display and download the log file, the system logging must be configured to write system log to file (see *System > System > Logging*).

To display or download logs:

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

Page Selector

This page allows a root user to hide certain pages from the admin user view.

Reporting Agent

Services > Reporting Agent

The reporting agent captures current device and interface information from the gateway on a periodic basis and sends it to a generic device management server using TCP/UDP/HTTP/HTTPS protocol.

To configure the reporting agent:

1. Go to Services > Reporting Agent.
2. Select **Enable All** to enable collection data on all settings for all interfaces.
3. Select the settings to report for each of the network interfaces (LAN, WAN, Cellular, Wi-Fi, GPS). See *Table 10-13*.
4. Configure and enable the device info, reporting agent, and data send settings. See *Table 10-14*.
5. Click **Save & Apply**.

Table 10-13 Reporting Agent Configuration

Parameters	Description
Enable All	Select check box to enable all settings for all interfaces.
Disable All	Select check box to disable all settings for all interfaces.
LAN Parameters	
LAN	Select to enable reporting of individual LAN settings. ◆ Status ◆ Uptime ◆ IP ◆ Data usage
WAN Parameters	
	Select to enable individual WAN settings. ◆ Status ◆ Uptime ◆ IP ◆ Gateway ◆ DNS ◆ Data usage
Cellular Parameters	
	Select to enable individual Cellular settings. ◆ Status ◆ Uptime ◆ IP ◆ Gateway ◆ DNS ◆ Data usage ◆ RSSI ◆ Roaming Status ◆ Operator Name ◆ Network Status ◆ IMSI

Parameters	Description
Wi-Fi Parameters	
	Select to enable individual Wi-Fi settings. ◆ Status ◆ Uptime ◆ IP ◆ Gateway ◆ DNS ◆ Data usage ◆ Wifi Client Info
GPS Parameters	
	Select to enable individual GPS settings. ◆ Time ◆ Latitude ◆ Longitude ◆ Altitude

Sending Data

Table 10-14 Reporting Agent Data Send Configuration

Parameters	Description
Device Info	Select to allow reporting agent to retrieve device IMEI information.
Reporting Agents	Select the reporting agent. Generic agent is the default selection.
Enable Data Send	Select to enable data send.
Protocol	Select the protocol used in the data transmission. Options are TCP, UDP, HTTP, or HTTPS. Depending on the protocol that you selected, the server fields will vary.
Starting string of the frame	When TCP is selected, a start of frame sequence can be used to indicate the first frame of the data sent by the reporting agent. This string must be less than 20 characters in length.
Ending string of the frame	When TCP is selected, a start of frame sequence can be used to indicate the first frame of the data sent by the reporting agent. This string must be less than 20 characters in length.
IP1/URL1	Enter the IP address or the URL of the destination server.
Port1	Enter the port number (for TCP and UDP).
TCP Timeout	Enter the timeout in seconds to switch between primary and backup IP in case of connectivity failure. TCP user timeout value should be between 10 and 900 seconds.
Backup	This option is available when TCP protocol is selected. Select Backup check box to configure the backup TCP server. ◆ IP2/URL2 ◆ Port2 The backup IP will be used after 3 failed attempts to send data to primary server. Reporting agent will continue to send data to backup server until the backup server fails or the device reboots.
Send Interval in Second	The period of time between two data transmissions.

Data Format

Figure 10-1 shows a portion of the reporting agent data format for a case where all settings were selected.

Figure 10-1 Reporting Agent Data Format (excerpt)

```
@IMEI=352948070039411,Lan Status=Connected,Lan
IP(IPv4)=192.168.1.1,Lan Uptime(Seconds)=329501,Lan TX
bytes=572260469,Lan RX bytes=117212098,Wan Status=Connected,Wan
IP(IPv4)=192.169.1.110,Wan Uptime(Seconds)=329389,Wan
gateway=192.169.1.1,Wan DNS=27.109.1.2 27.109.1.3,Wan TX
bytes=75455301,Wan RX bytes=344481735,Cellular
Status=Enabled,Cellular IP(IPv4)=,Cellular
uptime(Seconds)=,Cellular gateway=,Cellular DNS=,Cellular TX
bytes=208,Cellular RX bytes=0,RSSI(ASU)=99,Roaming Status=N/
A,Operator Name=N/A,Network Status=Not Registered,IMSI=ERROR,Wifi
Status=Enabled,Wifi IP(IPv4)=192.169.2.116,Wifi
Uptime(Seconds)=383,Wifi gateway=192.169.2.1,Wifi
DNS=192.169.2.1,Wifi TX bytes=14135074,Wifi RX bytes=34397774,Wifi
Client
```

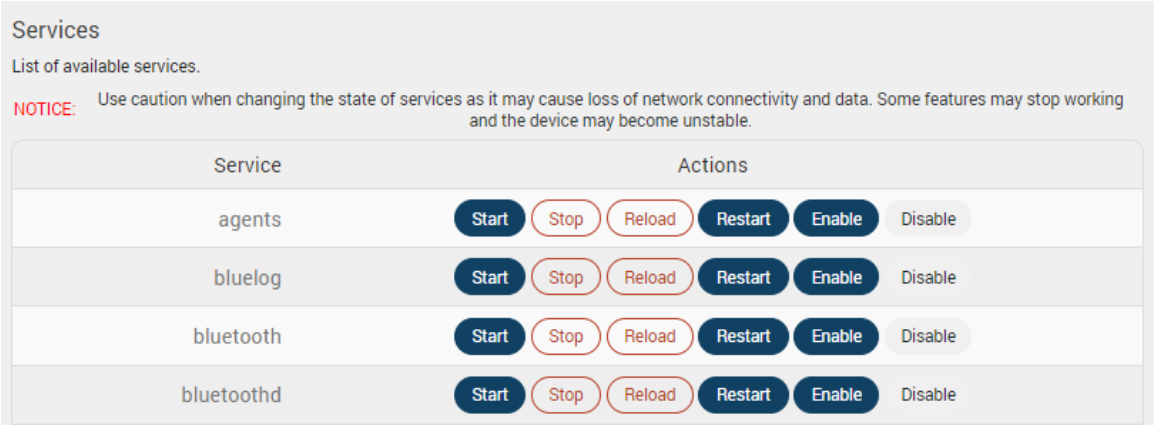
Service Actions

Services > Service Actions

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

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

Figure 10-2 Service Actions



SMS

Services > SMS

The SMS feature lets you send SMS messages to the gateway to request diagnostics information, configure gateway settings, or initiate certain actions such as DOTA upgrade or starting and stopping the VPN.

SMS Configuration

Services > SMS > SMS Configuration

You can configure up to four administrator mobile numbers to receive SMS messages containing gateway diagnostics information after a command is sent by SMS. The mobile number format is as follows: +<countrycode><phonenumber>

You should include the preceding special character “plus (+)”. Example: +9198xxxxxxxx

Table 10-15 SMS Service Configuration

Parameters	Description
SMS Configuration	
Enable	Enable remote SMS configuration.
AT Enable	Enable remote AT commands using SMS
SMS Administrator	Displays up to four Administrators configured to receive the diagnostics via SMS after an SMS command is sent. ***Note:*** *If no number is configured then the gateway will accept SMS from any number.* For each administrator to be configured, enter the mobile number with country code. The format of mobile number must be: +<countrycode><phonenumber> with a preceding special character “plus (+)”. Example: +9198xxxxxxxx

SMS AT Commands

Table 10-16 describes the SMS AT commands in alphabetical order.

Table 10-16 SMS AT Command Syntax

Name	Command Syntax
AT Command	AT#ATCMD='<AT command string>',<Timeout> Description: The command passed in the AT command string will be sent directly to the internal GSM module. Parameters: ◆ AT command string – AT command such as AT+CSQ (signal quality) or AT+CREG? (to check the registration status of GSM module). ◆ Timeout – The timeout value should be an integer in seconds. If the timeout value is set to 0, don't wait for a response. Issue the command and leave it. Example: AT#ATCMD=AT+CSQ,5 – check signal strength

Name	Command Syntax
Cell Diagnostics	AT+CELLDIAG? Description: Get cellular diagnostics
CELL Ping	AT+CELLPING=<IPA> Description: Pings the cellular IP address Parameter: ◆ IPA – IP address of the WAN interface to ping.
DOTA Action	AT+DOTA=<C/M>,<update/check>[,<released/beta/development>,<filename>] Description: Update firmware on gateway or check for available firmware updates from configured server Parameters: ◆ C/M – C for custom server, M for Lantronix server ◆ update/check – whether to update the gateway with the specified filename or to check for available updates ◆ released/beta/development – the release channel on the Lantronix download server ◆ filename – filename of the package to use for the update
DOTA Custom Settings	AT+DOTASETTINGS=<HTTP/HTTPS>,<Server URL>,<File name>,<Username>,<Password>,<Timeout>,<Retry> Description: Update firmware on gateway from a custom server Parameters: ◆ HTTP/HTTPS – protocol of the custom server ◆ Server URL – server URL, must include http: or https: ◆ File name – the name of the file to be accessed for the update ◆ Username – server username ◆ Password – server password ◆ Timeout – period of time to wait for the download to complete (minutes) ◆ Retry Parameters – number of retry attempts for the download
Hardware Information	AT+HWI? Description: Get hardware information
Cellular Settings	AT+IPGPRS=<1/2>,<Apn>,<Username>,<Password>,<Auth-Type>,<Data-Roam> Description: Configure cellular SIM settings Parameters: ◆ 1/2 – SIM slot number ◆ Apn – access point name provided by the cellular network provider ◆ Username – username if auth type is pap, chap, or pap/chap ◆ Password – password if auth type is pap, chap, or pap/chap ◆ Auth-type – none, pap, pap/chap, or chap (auth-type parameter is case sensitive, must be all lowercase) ◆ Data-Roam – 0 for disabled or 1 for enabled

Name	Command Syntax
Install / Update / Remove / Autoremove IPK	AT+IPKDOTA=<Name of IPK file>,<install/upgrade/remove/autoremove>,<For install/upgrade: 0-both default URL and custom URL, 1-default URL, 2-custom URL> Description: Install, update, remove or auto remove packages Parameters: ◆ Name of IPK file – IPK file name that OPKG will install, upgrade, or remove. ◆ install/upgrade/remove/autoremove – action that OPKG will run. ◆ location to check for the package for install or upgrade. This argument is not required for remove or autoremove. ➢ 0 – Both default server URL & custom URL. Both servers should be running, otherwise it will return a failed response. ➢ 1 – default server URL ➢ 2 – custom server URL
Lan Settings	AT+IPLAN=<IPv4 address>,<SubnetMask> Description: Configure LAN IPv4 settings Parameters: ◆ IPv4 address – The IP address of the LAN interface ◆ Subnet mask – Subnet mask of the LAN IP address
LAN Diagnostics	AT+LANDIAG? Description: Get LAN diagnostics
LAN Ping	AT+LANPING=<IPA> Description: Ping LAN IP address Parameter: ◆ IPA – IP address of the LAN interface to ping
OPKG Configuration Settings	AT+OPKGSETTINGS=<Server URL> Description: Set OPKG server Parameter: ◆ Server URL – URL of the package server
Manage Digital Output	AT#OUT=<GPO1/GPO2>,<OPEN/CLOSE> Description: Pull high or push low GPIO pins Parameters: ◆ GPO1/GPO2 – the pin to be configured ◆ OPEN/CLOSE – Set OPEN for low, or CLOSE for high.
Reboot	AT+REBOOT=1 Description: Reboot the gateway
Enable Remote Access	AT+REMACC=<1/0> Description: remote access Parameter: ◆ 1/0 – Set 1 to enable, set 0 to disable remote access
Software Information	AT+SWI? Description: Get software information
WAN Diagnostics	AT+WANDIAG? Description: Get WAN diagnostics

Name	Command Syntax
WAN Ping	AT+WANPING=<IPA> Description: Ping WAN interface Parameter: ◆ IPA – IP address of the WAN interface to ping.
WWAN Ping	AT+WWANPING=<IPA> Description: Ping WWAN interface Parameter: ◆ IPA– IP address of the WAN interface to ping.
Start/Stop VPN	AT+VPN=<VPN Type>,<VPN Name>,<start/stop> Description: Start or stop the VPN instance Parameters: ◆ VPN type – pptp, l2tp, ipsec, openvpn ◆ VPN name – VPN instance name ◆ Start/stop – action to start or stop the VPN Examples: ◆ AT+VPN=ipsec,IPSEC1,start ◆ AT+VPN=ipsec,IPSEC1,stop

Ethernet SMS

Services > SMS > Ethernet SMS

This service enables the device connected on LAN to initiate an SMS using Ethernet port.

Table 10-17 Ethernet SMS Configuration

Parameters	Description
Enable	Check to enable the Ethernet SMS.
Port	Enter the port number. The port number range is from 0 to 65535.

To send an SMS you need to open a TCP client connection on the LAN IP and configured port. Once the connection is created, issue the following commands:

To send an SMS

```
AT#SENDSMS=+<Mobile Number with Country Code><Message end with CTRL+D>
```

To read an incoming SMS

```
AT#READSMS=<ALL/SMS ID><Enter>
```

To delete an SMS

```
AT#DELSMS=<ALL/SMS ID><Enter>
```

The internal SMS buffer is 10 messages – meaning, 11th incoming SMS will be over written on the 1st SMS.

Live Message

Services > SMS > Live Message

Sends SMS from the web interface.

Notes:

- *To activate the Live Message feature, you must first enable the Ethernet SMS feature.*
- *To send SMS, add a # symbol preceding the phone number instead of the + symbol.*

To send SMS from the web interface:

1. Go to Services > SMS > Live Message.
2. Under Send SMS:, type #<mobile number with country code>.
3. Under Message Area: type the message. It can be update 159 characters.
4. Click **SendSMS**.

To read SMS:

On the Live Message page, select the message number (from 1-10 or All) and click **ReadSms**.

To delete an SMS:

On the Live Message page, select the message number (from 1-10 or All) and click **DeleteSms**.

SNMPD

Services > SNMPD

The X300 series gateway uses Net-SNMP to implement SNMP v1, v2c, and v3 using both IPv4 and IPv6 to remotely manage and monitor network components and systems. The implementation includes an SNMP agent for responding to SNMP requests or actions from the SNMP manager, an SNMP-TRAP application for receiving and processing SNMP notifications (or traps), and support for a number of applications to retrieve information from an SNMP capable device (snmpget, snmpgetnext, snmpwalk), retrieve statistics (snmpstatus) or write configuration on the device (snmpset).

The configuration of the SNMP agent and SNMP-TRAP application configuration files (mainly snmpd.conf and snmptrapd.conf) are done using the web interface. Likewise, operations such as enabling or disabling the agent and trap receiver are done using the web interface. Most management operations and monitoring, however, will be done through the SNMP manager.

Prerequisites to use this feature include having knowledge of SNMP and having a network management system (NMS) with which to monitor the network.

For more information about Net-SNMP or SNMP in general, please refer to the Net-SNMP web site.

For information about using SNMP management systems, see the appropriate documentation for your NMS application.

SNMP Architecture

A typical SNMP implementation includes the following components:

- Network management system (NMS) – a combination of hardware devices and software (SNMP manager) used to monitor and administer a network. The manager polls the devices on the network for information about network connectivity, activity, and events.
- Managed device – any device on the network that is managed by the NMS.
- SNMP agent – the SNMP process that resides on the managed device and communicates with the SNMP manager. It responds to requests for information or actions from the manager and generates SNMP notifications (traps). The agent also controls access to the agent's MIB.
- Management Information Base (MIB) – collection of objects that specify the information that the agent provides to the SNMP manager.

SNMP Versions

The X300 series software supports the following versions of SNMP: SNMPv1, SNMPv2c and SNMPv3/USM.

- SNMPv1 – Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings.
- SNMPv2c – The community string-based Administrative Framework for SNMPv2. SNMPv2c is defined in RFCs 1901, 1905, and 1906. Security is based on community strings.
- SNMPv3/USM – SNMPv3 is defined in RFCs 3413-3415. It provides secure access to devices by authenticating and encrypting packets over the network. SNMPv3 provides message integrity, authentication, and encryption security features.

Table 10-18 SNMP Security Models and Levels

SNMP Model	Level	Authentication	Encryption
v1	noAuthNoPriv	Community String	No
v2c	noAuthNoPriv	Community String	No
v3	noAuthNoPriv	Username	No
v3	authNoPriv	MD5 or SHA	No
v3	authPriv	MD5 or SHA	DES or AES

SNMP Configuration

The SNMP agent must be configured to use the version of SNMP that is supported by the management station. An agent can communicate with multiple managers. You can configure the SNMP agent to support communication with one management station using SNMPv1, one using SNMPv2c, and one using SNMPv3.

The web interface allows you to configure the SNMP settings. The configuration specifies directives in the following areas:

- agent behavior
- access control to the agent (VACM)
- system information and monitoring
- active monitoring of the local system

Agent Behavior

The following directives control the behavior of SNMP network service.

- agent address – the listening address on which to receive incoming SNMP requests. The default behavior is to listen on UDP port 161 on all IPv4 interfaces
- EngineID – SNMPv3 only. SNMPv3 requires an SNMP agent to define a unique engine ID to respond to SNMP requests.

For configuration details, see *Table 10-19 on page 114*.

View-based Access Control Model (VACM)

SNMP v1/v2c/v3-USM follow the VACM model. VACM determines whether to allow access to a managed object in a local MIB by a remote principal. VACM makes use of a MIB that defines the access control policy for the agent and makes it possible to use remote configuration.

The SNMP service uses four keywords to set up VACM:

- **Com2sec** – maps a v1 and v2c community string and a source IP or network to a security name.
- **Group** – maps a security name/security model pair to a group name.
- **View** – maps an OID subtree family and bitstring value (mask-optional), or MIB view, to a view name.
- **Access** – maps a group name to a minimum access level (noauth, auth, or priv) and read/write/notify scope for a specified security model (v1, v2c, v3/usm, or any).

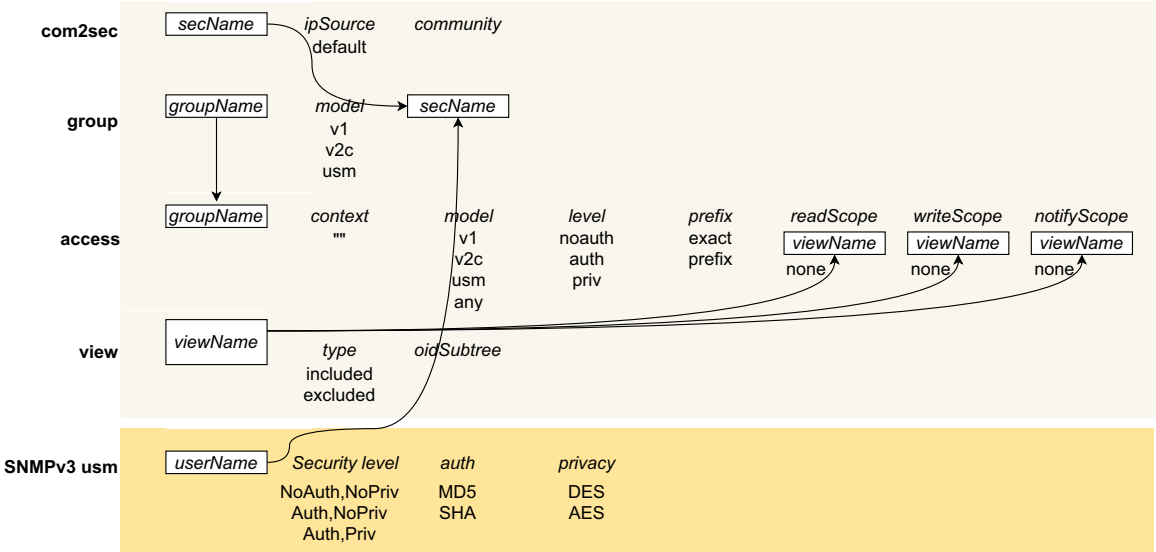
In summary:

- The Access and View keywords determine what access is being controlled.

- The Group and com2sec keywords determine who has this access.

Figure 10-3 shows how the fields map in the VACM configuration model.

Figure 10-3 VACM Configuration Model



For SNMP v1/v2c/USM VACM configuration details, see *Table 10-20 on page 116*.

SNMPv3 with User-based Security Model (USM)

SNMPv3 with USM contains a private list of users and keys specific to the SNMPv3 protocol. To use this model, the SNMPv3 USM users must be created and added to the VACM group table (as security name).

For SNMPv3 with USM user configuration details, see *Table 10-22 on page 119*.

System Information and Monitoring

System information includes system group information and monitoring information, which is described below. The system group information, such as name, location, contact, and description, are retrieved from the underlying network management system.

The agent is built with support for monitoring the local system. The following directives can be specified:

- Process monitoring – provides information about individual processes running on the local system
- Disk usage monitoring – provides information about disk usage for specified disks or all disks
- System load monitoring – provides information about system load average and swap space
- Log file monitoring – monitors the file size of specified log files

For system information and monitoring configuration details, see *Table 10-19 on page 114*.

Active Monitoring

The agent can be configured to generate trap notifications based on the following directives:

- Authentication failure trap – generate authentication failure traps

- Default monitors – configure the Event MIB tables to monitor various UCD-SNMP-MIB tables for problems
- Link up/link down notifications – monitor for network interfaces being taken up or down and triggering a linkUp or linkDown notification as appropriate
- Where to send the trap notifications – determine where to send the notifications such as to the localhost or to the SNMP manager.

For Trap sender configuration, see *Table 10-23 on page 119*.

Configure SNMPv1 or SNMPv2

To configure SNMPv1 or SNMPv2c:

1. Go to Services > SNMPD.
2. Enter the configuration settings as required according to the SNMP version (v1/v2c/v3-USM) you have chosen. Click **Save** before moving between tabs on the SNMP page.
3. To configure SNMP general settings including agent behavior and system information/ monitoring, select the General Settings tab. See *Table 10-19*.
4. To configure VACM access control settings, select the VACM tab. See *Table 10-20*.

   Note: *You do not need to configure the EngineID or SNMPv3 with USM settings.*

5. To configure SNMP agent trap sender, select the Trap Settings tab. See *Table 10-23*.

   Note: *To configure SNMP-TRAP application, see* *SNMPTRAPD on page 120*.

6. On the General Settings tab, select **Enable** if it is not already selected.
7. Click **Save & Apply**.

Configure SNMPv3 with USM

To configure SNMPv3 with USM:

1. Go to Services > SNMPD.
2. Enter the configuration settings as required according to the SNMP version (v1/v2c/v3-USM) you have chosen. Click **Save** before moving between tabs on the SNMP page.
3. To configure SNMP general settings including agent behavior and system information/ monitoring, select the General Settings tab. See *Table 10-19*.
4. To configure VACM access control settings, select the VACM tab. See *Table 10-20*.
5. To configure Engine ID settings for SNMPv3, select the VACM tab. See *Table 10-21*.
6. To create users for SNMPv3 with USM, select the VACM tab. See *Table 10-22*.
7. To configure SNMP agent trap sender, select the Trap Settings tab. See *Table 10-23*.

   Note: *To configure SNMP-TRAP application, see* *SNMPTRAPD on page 120*.

8. On the General Settings tab, select **Enable** if it is not already selected.
9. Click **Save & Apply**.

Table 10-19 SNMP General Settings Configuration

Parameters	Description
Enable	Select to enable the SNMPD application.
EngineID	Displays the SNMP engine ID, which is required to respond to SNMPv3 requests. This value is auto-generated when the agent is first started.
agentaddress	Defines a list of listening addresses on which to receive incoming SNMP requests. The default agent behavior is listening on all interfaces on UDP port 161. This is equivalent to the following directive: agentaddress udp:161 or simply agentaddress 161 To configure this field, specify one or more listening addresses using the format: [<transport-specifier>:]<transport-address> Examples: ◆ UDP:161, UDP6:161 – accept requests on all IPv4 and IPv6 interfaces on UDP port 161 ◆ localhost:161 – accept requests on the local loopback interface on UDP port 161 ◆ 127.0.0.1 – accept requests on the local loopback interface (UDP is implied) ◆ UDP:161, UDP6:161, TCP:161, TCP6:161 – accept requests on all IPv4 and IPv6 interfaces on UDP port 161 and TCP port 161 Other combinations are also valid.
System Information	Displays the system group information. System name, contact and location can be set through the SNMP Manager. ◆ sysName – default is Lantronix ◆ sysContact – default is root@localhost ◆ sysLocation – default is Unknown ◆ sysDescription – default 'uname -s -n -r -v -m' command output is not writable using a set request.
Process Monitoring	
Process Monitoring	Monitors the processes running on the local system and registers a command that can be run to fix errors. This table displays the processes that are being monitored and provides options to add, edit or delete items from the monitoring table. ◆ Click **Add** to add an entry to the process monitoring table. Enter the process name and other details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Process Name	Name of the process that is being counted.
Max Process	Maximum number of processes that should be running. Generates an error flag if the number of processes detected is greater than the maximum specified.
Min Process	Minimum number of processes that should be running. Generates an error flag if the number is less than the minimum.
Enable Fix Action	Tells the agent to attempt to fix the problem by calling the operation specified in the fix action. The command will not be invoked automatically.
Program Name (Procfix action)	The command that gets run when the error is detected and the fix action field is enabled.
Arguments	Arguments that support the command.

Parameters	Description
Disk Usage Monitoring	
Disk Usage Monitoring	Monitors the minimum threshold specified in KB or as a percentage of the total disk space and registers an error if the available disk space is less than the minimum required space configured for it. Disk usage monitoring section also allows for monitoring of all disks found on the system according to a specified percentage threshold. (See Include all disks.) This table displays the disks being monitored for disk usage and provides options to add, edit, or delete items from the monitoring table. ◆ Click **Add** to add an entry to the disk usage monitoring table. Enter the partition and space details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Partition	Path where the disk is mounted.
Minimum Space	Minimum space or minimum percentage must be configured. ◆ Minimum space required on the disk in KB before the errors are triggered. ◆ Minimum space required on the disk as a percentage of the total disk space before the errors are triggered.
Include All disks	Enables monitoring of all disks found on the system.
Minimum Percent	Minimum space required as a percentage of total disk space of all disks before the errors are triggered. ***Note:*** *The threshold for individual disks can be configured using the partition directives above.*
System Load Monitoring	
Load Monitoring	Displays the system load monitoring details if configured. Monitors the load average of the local system.
Enable Load Monitoring	Enables monitoring of system load averages
1 - Minute Max. Load	The one-minute maximum load average before errors are triggered.
5 - Minute Max. Load	The five-minute maximum load average before errors are triggered.
15 - Minute Max. Load	The fifteen-minute maximum load average before errors are triggered.
Swap Space Threshold (in KB)	Amount of swap space (in KB) available on the local system. The default threshold is 16 MB and it is enabled by default. If the available swap space is less than 16 KB if not user-configured, or less than the configured value, and if Default Monitoring is enabled, it will generate a notification to SNMP traps.
Log File Monitoring	
Log File Monitoring	Monitors the size of the log files and registers an error if the size exceeds the maximum size configured for it. Limit: Up to 20 files can be monitored. This table displays log files being monitored for file size limits and provides options to add, edit or delete items from the monitoring table. ◆ Click **Add** to add an entry to the log file monitoring table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
File Path	File path and name of the file to be monitored.

Parameters	Description
Maximum Size	Maximum file size in KB before errors are triggered.

Table 10-20 SNMP v1/v2/USM VACM Settings

Parameters	Description
Com2Sec Configuration	
Com2Sec Configuration	The com2sec directive maps a v1/v2c community string and a source IP or network address to a security name (username). This table displays com2Sec entries and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the com2sec table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Security Name	Username specifies the security name to which this source and community string are to be mapped. Security name can contain alphanumeric characters, dash, underscore, or period. No spaces or other special characters allowed.
Source	Source can be one of the following: ◆ restricted source – a specific hostname or address ◆ subnet – represented as IP/Mask (10.10.10.10/255.255.255.0) or IP in CIDR notation (10.10.10.10/8) or the IPv6 equivalents ◆ global – use “default” ◆ localhost – use “localhost” or 127.0.0.1
Community	Specifies the community (user credential) to use for SNMP requests. The same community string can be specified in separate com2sec directives.
Group Configuration	
Group Configuration	The group directive maps a security name in the specified security model (see *Table 10-18 on page 111*) into a named group. This table displays groups and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the group table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table. ***Note:*** ➢ Several group directives can specify the same group name, allowing a single access setting to apply to several users and/or community strings. ➢ All members of one group have the same access rights. ➢ A user cannot belong to more than one group for each of the security models. ➢ Groups must be set up for the community-based models separately. You would typically create two group directives for a single com2sec directive, one for v1 and one for v2c.
Group Name	Group name can contain alphanumeric characters, dash, underscore, or period. No spaces or other special characters allowed.

Parameters	Description
Version	◆ v1 ◆ v2c ◆ usm
Security Name	Security name should be one of the security names defined in the com2sec configuration.
Access Configuration	
Access Configuration	The access directive maps a group name to an access level (noauth, auth, or priv) and read/write/notify scope for a specified security model (v1, v2c, v3/usm, or any). The table displays access entries and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the access table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Group Name	Group name should be one of the group names defined in Group configuration.
Context	Default context is the empty string “”, which equates to “none”. For v1 or v2c, context will be empty (“none”).
Version	◆ v1 ◆ v2c ◆ usm ◆ any This value should match the SNMP version of clients that will connect to this agent.
Level	◆ noauth ◆ auth – (authNoPriv) use strong authentication ◆ priv – (authPriv) use strong authentication and encryption For v1 or v2c, set the level to noauth. For usm, set the level to at least the minimum level required. The SNMPv3–USM security level must be configured to this level or higher.
Match	Specifies how the context should be matched against the context of the incoming request. ◆ exact – context name must match exactly (default) ◆ prefix – only the first part of the context name must match
Read	Specifies the view to be used for GET requests. ◆ unspecified – if left unspecified, it will be treated as none - no access ◆ none – no access ◆ custom – name of the view from the view table
Write	Specifies the view to be used for SET requests. ◆ unspecified – if left unspecified, it will be treated as none - no access ◆ none – no access ◆ custom – name of the view from the view table
Notify	Specifies the view to be used for TRAP/INFORM requests. ◆ unspecified – if left unspecified, it will be treated as none - no access ◆ none – no access ◆ custom – name of the view from the view table
View	

Parameters	Description
View	Creates a named view, which determines what part of the MIB the access control is applied to. The table displays view entries and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the view table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
View Name	View name can contain alphanumeric characters, dash, underscore, or period. No spaces or other special characters allowed.
Type	Specifies whether to include or exclude the elements of the subtree from the MIB view. ◆ included – the MIB view includes all the elements of the subtree ◆ excluded – the MIB view excludes all the elements of the subtree
OID	The OID defining the root of the subtree to include or exclude from the named view.
Mask (optional)	List of hex octets optionally separated by '.' or ':' with the set bits indicating which subidentifiers in the view OID to match against. Recommended to ignore this field.

Table 10-21 SNMP VACM Settings Engine ID Configuration

Parameters	Description
Engine ID Configuration	EngineID is required to respond to SNMPv3 requests. This ID is determined automatically, but can be configured manually. The string must be consistent through time and should not change or conflict with another agent's engineID. For this reason, it is recommended that you use the default values unless you know what you are doing.
Enable	Enables the engineID.
engineID	Specifies that the engineID should be built from the given text string. Default: lantronix
engineIDType	Specifies that the engineID should be built from given type. Type 1 – IPv4 address Type 2 – IPv6 address Type 3 – MAC address (default)
engineIDNic	Specifies that the engineID should use the following interface when determining the MAC address. Only required if engineIDType 3 is specified. Default: eth0

Table 10-22 SNMP VACM Settings SNMPv3-USM

Parameters	Description
SNMPv3 with USM Configuration	Create one or more SNMPv3 users. The table displays SNMPv3 with USM users and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the table. Enter the details as shown below. ◆ Click **Edit** to modify an entry. ◆ Click **Delete** to delete an entry from the table.
User Name	Map the security name from the VACM com2sec table here.
Security Level	Security level can be: ◆ NoAuth,NoPriv – no authentication or privacy protocol ◆ Auth,NoPriv – has authentication (MD5|SHA), no privacy protocol ◆ Auth,Priv – has authentication (MD5|SHA), and has privacy protocol (DES|AES).
Auth Protocol	Select the authentication protocol. ◆ MD5 ◆ SHA SHA authentication requires SSL.
Auth Password	Enter the MD5 or SHA passphrase to use for authentication. The passphrase must be at least 8 characters.
Priv Protocol	Select the privacy protocol. ◆ DES ◆ AES DES and AES require SSL.
Priv Password	Enter the privacy protocol passphrase. The passphrase must be at least 8 characters.

Table 10-23 SNMP Trap Settings Configuration

Parameters	Description
Enable	
Authentication Failure Trap Enable	If enabled, generates authentication failure traps. This is disabled by default.
Enable Default Monitors	Monitors the UCD-SNMP-MIB tables for problems. The monitored events (process, load, disk usage, log file) should first be configured on the General Settings page. By default, the agent will check the default monitors once on startup and then every 10 minutes.
Enable Link Up/Down Notification	Monitors the ifTable for changes in network interfaces link status and generates linkUp or linkDown notifications as appropriate.
Trap Configuration	
Version	Specifies the SNMP version. Can be v1, v2c, or v3. ◆ For v1, community and host are required. ◆ For v2c, type, community, and host are required. ◆ For v3, type, username, security level, and host are required.

Parameters	Description
Type	Select the type as trap or inform. For information about SNMPv3 notification behavior and the difference between traps and informs, see the following tutorial: http://www.net-snmp.org/tutorial/tutorial-5/commands/snmptrap-v3.html To use type inform, the SNMP manager must also support inform messages.
User Name	Username is the SNMP v3 security name, as defined in VACM settings.
Security Level	Security level can be: ◆ NoAuth,NoPriv – no authentication or privacy protocol ◆ Auth,NoPriv – has authentication (MD5|SHA), no privacy protocol ◆ Auth,Priv – has authentication (MD5|SHA), and has privacy protocol (DES|AES). If Auth,NoPriv or Auth,Priv are selected, additionals fields will be displayed. Enter the authentication and privacy protocol details as needed.
Community	Defines the v1 or v2c community string to be used when sending traps.
Host	Defines the IP address and port that the trap should be sent to. Typically, this could be localhost:162 or the IP and port of the SNMP manager. The well known SNMP Trap port is port 162.

SNMPTRAPD

Services > SNMPD TRAPD

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

SNMP-TRAP Configuration

To configure SNMP-TRAP settings:

1. Go to Services > SNMPTRAPD.
2. Enter the configuration settings. See *Table 10-24*.
   - Logging – Notifications can be written to the syslog or to a file path on the gateway.
   - Notification processing – notifications can sent to a notification handler or to a notifications receiver.
3. Under General, select **Enable** if it is not already selected.
4. Click **Save & Apply**.

Table 10-24 SNMP-Trap Receiver Configuration

Parameters	Description
General	

Parameters	Description
Enable	Enables the SNMPTRAP application.
Ignore Authorization Failure	Select to ignore authentication failure traps.
SNMP-TRAP daemon configuration	
Version	Specifies the SNMP version. Can be v1, v2c, or v3. ◆ For v1, community and host are required. ◆ For v2c, type, community, and host are required. ◆ For v3, type, username, security level, and host are required.
Community	Specifies the community used for v1 and v2c authorization. Notifications using the specified community will be allowed to be processed per the notification handling configuration.
User Name	Enter the SNMP v3 username, as defined in VACM settings.
Type	Select the type as trap or inform. For information about SNMPv3 notification behavior and the difference between traps (unacknowledged) and informs (acknowledged), see the following tutorial: http://www.net-snmp.org/tutorial/tutorial-5/commands/snmptrap-v3.html
EngineID	Specifies the EngineID value. For use only with SNMPv3 traps.
Security Level	Security level can be: ◆ NoAuth,NoPriv – no authentication or privacy protocol ◆ Auth,NoPriv – has authentication (MD5|SHA), no privacy protocol ◆ Auth,Priv – has authentication (MD5|SHA), and has privacy protocol (DES|AES). Enter the authentication and privacy protocol type and passphrase as appropriate for the selection.
Source	Used for v1 and v2c authorization. The source field specifies that the configuration should only apply to notifications received from the listed sources.
OID	Specifies the OID defining the root of the subtree to add to or exclude from the named view.
Logging Configuration	
Log	Enables log.
Logging Location	Specifies where to log the notifications, either to a local file on the gateway or to the syslog. Select one: ◆ Specific file – enter the file path. ◆ syslog
Format1	Specify the format used to display SNMPv1 traps. If no format is defined, the default Net-SNMP format will be provided. For information about the format specification, see http://www.net-snmp.org/docs/man/snmptrapd.html.
Format2	Specify the format used to display SNMPv2c and SNMPv3 traps. SNMP v2c and v3 use the same PDU format. If no format is defined, the default Net-SNMP format will be provided. For information about the format specification, see http://www.net-snmp.org/docs/man/snmptrapd.html.
Notifications Handling	
Execute	Pass the details of the trap to a specified handler program.

Parameters	Description
Execute OID	Invokes the specified program with the given arguments whenever a notification is received that matches the OID token. For SNMPv2c and SNMPv3 notifications, this token will be compared against the snmpTrapOID value taken from the notification. For SNMPv1 traps, the generic and specific trap values and the enterprise OID will be converted to the equivalent OID per RFC 2576. If the OID field is the token default then the program will be invoked for any notification not matching another OID-specific traphandle entry.
Program	Program name with path specified followed by a space separated arguments if any. For example, /usr/bin/xyz 1 2 3
Net	Forward the trap to another notification receiver ***Note:*** *Do not use this directive for SNMPv3.*
Net OID	See description for Execute OID above.
Destination	Forwards notifications that match the specified OID to another receiver.

uHTTPd

Services > uHTTPd

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

Web Server Configuration

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

To configure the HTTP/S server:

1. Go to Services > uhttpd.
2. Edit the configuration settings for the gateway. See *Table 10-25*.
3. If you upload a new X.509 certificate and private key in the general web server settings, you will need to configure the uHTTPd Self-signed Certificate Parameters section. See *Table 10-26*.
4. Click **Save & Apply**.

Note: *If you want to create a new server instance, go to the bottom of the Main instance (on the General Settings tab), enter a name and click **Add**. For configuration details, see Table 10-25.*

Table 10-25 uHTTPd Server Configuration

Parameters	Description
General Settings	
HTTP listeners (address:port)	Either HTTP listener or HTTPS listener is required. Enter the ports and addresses to listen on for HTTP access. Use 0.0.0.0/[::] to bind to all devices present. Enter a specific IP address to restrict binding to a specific interface.
HTTPS listener (address: port)	Either HTTP listener or HTTPS listener is required. Enter the ports and addresses to listen on for HTTPS access. Use 0.0.0.0/[::] to bind to all devices present. Enter a specific IP address to restrict binding to a specific interface.
Redirect all HTTP to HTTPS	Select this option to redirect all HTTP to HTTPS.
Ignore private IPs on public interface	Select to ignore requests from private IP addresses (RFC1918) directed to the server's public IPs. The default setting is to ignore the requests from private IPs.
HTTPS Certificate (DER Encoded)	Upload the HTTPS cert file. Click the icon to expand the directory structure (from root).
HTTPS Private Key (DER Encoded)	Upload the HTTPS private key file. Click the icon to expand the directory structure (from root).
Remove old certificate and key	Click to remove old certificate and key files
Remove configuration for certificate and key	Click to remove the cert, key, and configuration information.

Parameters	Description
Full Web Server Settings	
Index page(s)	Enter the index file to use for directories. Usually index.html or index.php.
CGI filetype handler	Enter the interpreter to associate with file endings in the cgi scripts directory.
Do not follow symlinks outside document root	If selected, the HTTP/HTTPS server will not follow symbolic links outside the document root.
Do not generate directory listings	If selected, the HTTP/HTTPS server will not generate directory listings.
Aliases	Maps URL to filesystem locations outside the document root. The format should be /old/path=/new/path
Realm for Basic Auth	Enter the realm for basic authentication when prompting the client for credentials. The default is "Lantronix", which is the local hostname.
Config file (e.g. for credentials for Basic Auth)	Enter the path of the configuration file for credentials for basic authentication and additional settings. The server will not use HTTP authentication if this field is blank.
404 Error	Enter the virtual URL of file or CGI script to handle 404 (file not found) request. It must begin with a forward slash '/'.
Advanced Settings	
Document root	Enter the directory path to the server document root. By default the document root is /www.
Path prefix for CGI scripts	Enter the prefix for CGI scripts, relative to the document root. Leave it blank to disable CGI support.
Virtual path prefix for Lua scripts	Enter the prefix for sending requests to the embedded Lua interpreter, relative to the document root. Leave it blank to disable Lua support.
Full real path to handler for Lua scripts	Enter the full path to the Lua handler script to initialize Lua runtime on server start. This field is required if Lua prefix is given, otherwise it's optional.
Virtual path prefix for ubus via JSON-RPC integration	Enter the URL prefix for ubus via JSON-RPC handler, relative to the document root. Leave it blank to disable UBUS.
Override path for ubus socket	Enter the override ubus socket path
Enable JSON-RPC Cross-Origin Resource Support	Select to enable CORS HTTP headers on JSON-RPC API. By default, this setting is disabled.
Disable JSON-RPC authorization via ubus session API	If selected, do not authenticate JSON-RPC requests against the UBUS session API. By default the requests are authenticated.
Maximum wait time for Lua, CGI, or ubus execution	Enter the maximum wait time for CGI, Lua or ubus requests in seconds. If no output is generated within the timeout period, the requested executables are terminated. Default is 60 seconds.
Maximum wait time for network activity	Enter the maximum wait time for network activity. If no network activity occurs within the timeout period, the requested executables are terminated and the connection is shut down. Default is 30 seconds.
Connection reuse	Sets the time limit for connection reuse.

Parameters	Description
TCP Keepalive	Number of unanswered keep alive requests allowed. Default: 1
Maximum number of connections	Enter the maximum number of concurrent connections allowed. If the limit is reached, further TCP connection attempts are queued until the number of connections is below the limit. Default: 100
Maximum number of script requests	Enter the maximum number of concurrent requests. If the limit is reached, further requests are queued until the number of requests drops below the limit. Default: 6
Maximum wait time for rpc timeout in seconds per requests	Enter the maximum wait time for RPC timeout in seconds. Default: 55

Self-Signed SSL Certificate Parameters

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

Table 10-26 uHTTPd Self-signed Certificate Configuration

Parameters	Description
uHTTPd Self-signed Certificate Parameters	
Valid for # of Days	Enter the validity time (number of days) of the generated certificate. Default: 730 days
Length of key in bits	Enter the length of the generated RSA key in bits Default: 2048
Server hostname	Enter the server hostname covered by the certificate. Default: Lantronix
Country	Country of the certificate issuer
State	State of the certificate issuer
Location	Location/city of the certificate issuer

11: Network

The software provides the administrator several options to customize the Network configuration adhering to the organization's requirements. The following sections are available to configure the Network parameters:

- *Interfaces*
- *Wireless*
- *DHCP and DNS*
- *Hostnames*
- *Static Routes*
- *Diagnostics*
- *Firewall*
- *QoS*
- *Load Balancing*

Interfaces

Network > Interfaces

The Interfaces section provides the overview and status of the network interfaces for LAN, Cellular, and WWAN. It also provides the configuration parameters for each of these interfaces, which allow you to configure or update the interface according to your requirements.

Additionally, you can add new virtual interfaces, such as GRE, L2TP, PPP, or PPtP VPN instances.

The Network Interfaces section contains the following pre-configured interfaces:

- *CELLULAR Interface*
- *LAN Interface*
-
- *WWAN and WWAN6 Interface*

Interfaces Overview

Network > Interfaces

Figure 11-1 shows a summary view of the network interfaces and interface status.

Figure 11-1 Interfaces Overview (partial view)

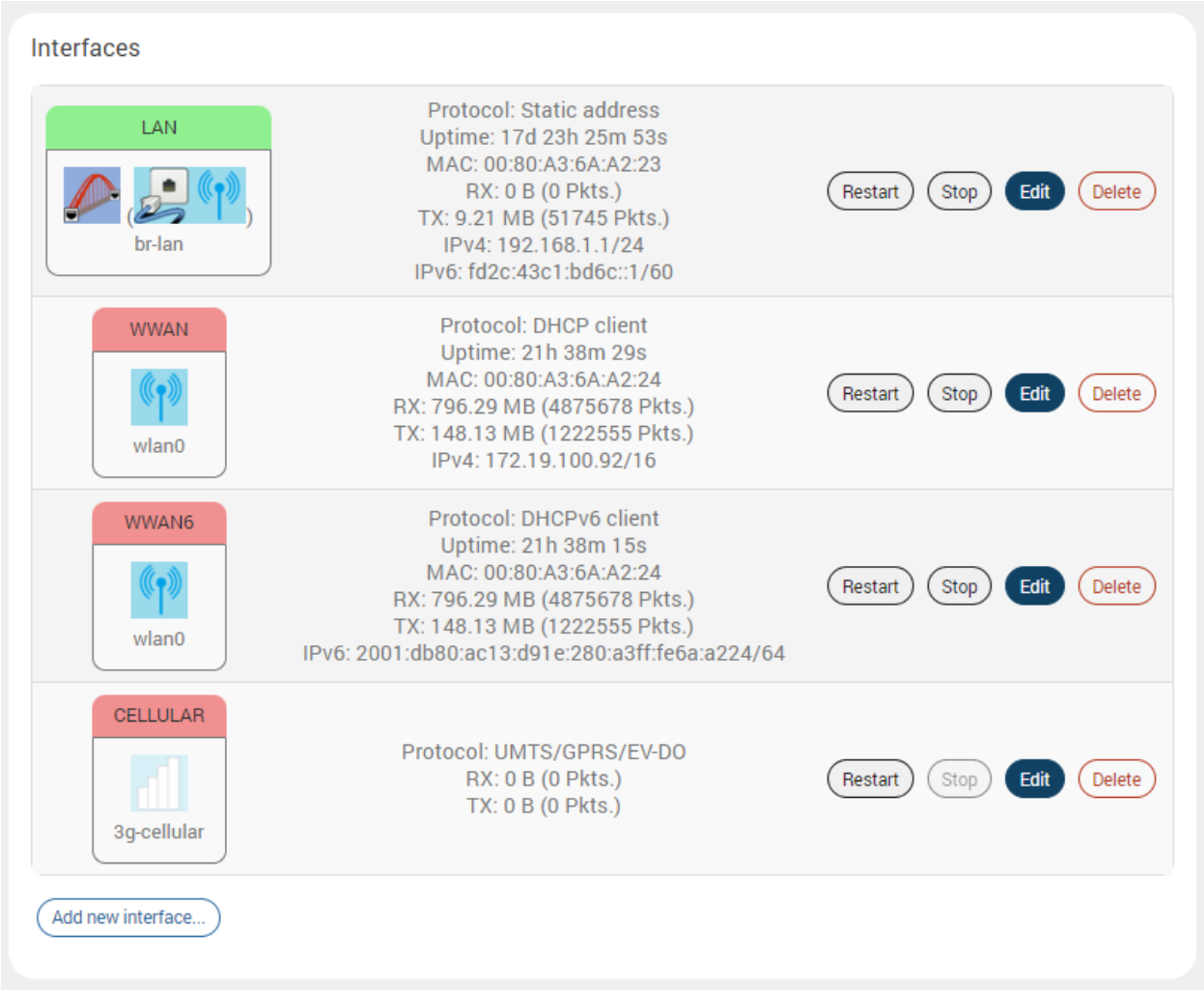


Table 11-1 Network Interfaces Overview

Parameters	Description
Interfaces Overview	
Network	Displays the network name and image representing the interface. ***Note:*** *When Wi-Fi is configured as Client, the WWAN interface will become active.*
Status	Displays the status of the interface. See *Interface Status*.

Parameters	Description
Actions	Select the action to be taken for the interface. ◆ **Restart** – Connects the interface or reconnects the already started interface. ◆ **Stop** – Stops the interface. ◆ **Edit** – Allows you to edit the interface settings. ◆ **Delete** – Deletes the interface. ***Note:*** *Default interfaces have predefined configurations and should not be deleted.*
Add new interface	Click **Add new interface** to add a virtual interface. See *Add Virtual Interface*.
Global Network Options	
IPv6 ULA-Prefix	Displays the IPv6 Unique Local Address (ULA)-Prefix
Network Watchdog	
Enable	Select this box to enable or clear the box to disable the network watchdog. The network watchdog monitors the connectivity of all WAN (external network) interfaces. In the absence of connectivity resulting in Network down, the gateway resets itself. By default, the network watchdog is in enabled mode.
Time	If the network watchdog is enabled, enter the watchdog timeout in minutes.

Interface Status

Figure 11-2 WAN Interface Status

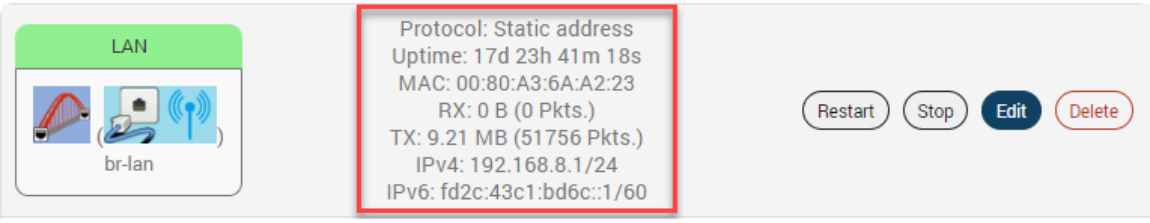


Table 11-2 Wireless Overview and Associated Stations

Parameters	Description
Protocol	Protocol assigned to the interface
Uptime	Amount of time that the interface has been active since the last reconnection.
MAC Address	MAC address of the physical interface. ***Note:*** *MAC address is displayed for LAN, WAN, WWAN, and OpenVPN interfaces.*
RX	Number of received bytes over the interface for the current session.
TX	Number of transmitted bytes over the interface for the current session.
IPv4	IPv4 address
IPv6	IPv6 address

Interface Protocols

The protocol assigned to each interface defines rules for exchanging information on the interface. *Table 11-3* shows the available protocol options for each of the interfaces. When configuring an interface, please make sure that the protocol selection is appropriate for the interface.

Legend: ✓ = protocol can be assigned ✗ = protocol should not be assigned

Table 11-3 Network Interface Protocols

Interface Protocols	LAN	WWAN	Cellular
Static Address	✓	✓	✗
DHCP client	✗	✓	✗
DHCPv6 client	✗	✓	✗
GRE	✗	✗	✗
L2TP	✗	✗	✗
Unmanaged	✓	✓	✗
PPP	✗	✗	✗
PPPoE	✗	✗	✗
PPtP	✗	✗	✗
UMTS/GPRS/EV-DO	✗	✗	✓
QMI Cellular	✗	✗	✓
Relay Bridge	✗	✗	✗

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

Most of the other protocols listed in *Table 11-3* are used for VPN configuration. For example, use L2TP protocol to configure an L2TP VPN connection. For descriptions on these protocols, see *Add Virtual Interface*.

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

Protocol Descriptions

Static Address

Table 11-4 describes the Static Address protocol settings.

Table 11-4 Static Address Protocol Settings

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

Parameters	Description
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value represents auto MTU size
Use gateway metric	Enter the gateway metric. It ensures a separate routing entry for the respective interface in the main routing table. The default metric is 5.
Physical Settings	
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. ◆ Enable STP – Check to enable the Spanning Tree Protocol over the bridge. ◆ Enable IGMP snooping – Check to enable IGMP snooping on the bridge.
Interface	Select the interface to be configured. Select more than one interface, if parameter creating a bridge over multiple interfaces is enabled.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.
DHCP > General Setup **DHCP Server - DHCP Server is used only for LAN interfaces**	
Ignore Interface	Check to disable the DHCP interface. ***Note:*** *If DHCP server is disabled for the interface, all the LAN devices connected to the gateway should have a static LAN IP configured.*
Start	Lowest leased address as offset from the network address. ***Note:*** *If your LAN IP address is 192.168.1.1 and the parameter Start is configured as 100, then the starting IP Address of the leased IP Address range is 192.168.1.100*
Limit	Maximum number of leased addresses that can be configured. Example ◆ If your LAN IP Address is 192.168.1.1, the parameter Start is configured as 100, and parameter Limit is configured as 150, then a total of 150 devices are configured. Thus the leased IP Address range is 192.168.1.100 to 192.168.1.249.
Lease time	Remaining time until the device can use the DHCP server leased IP Address. ***Note:*** *IP address allocated by the gateway will disappear from the Wi-Fi / Overview / Associated stations list only after individual lease time for each IP expires.*
DHCP > Advanced Settings	
Dynamic DHCP	Check to allocate DHCP IP addresses dynamically to the clients. When unchecked, service will be provided only to the clients having the static IP Address.

Parameters	Description
Force	Check to override the current configured Server and use DHCP server.
IPv4-Netmask	Enter the IPv4 netmask. This netmask will override the netmask used by the clients. In normal scenario netmask is calculated from the subnet.
DHCP-Options	Define additional DHCP options Example: ◆ “6,192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients.
DHCP > IPv6 Settings	
Router Advertisement-Service	Select the Router Advertisement-Service mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Service	Select the DHCPv6-Service mode; disabled, server mode, relay mode, hybrid mode.
NDP-Proxy	Select the NDP mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Mode	Select the DHCPv6-Service mode: ◆ Stateless ◆ Stateful ◆ Stateless + Stateful ◆ Stateful only
Always announce default router	Select to Announce as default router even if no public prefix is available.
Announced DNS servers	Add the DNS servers
Announced DNS domains	Add the DNS domains.

DHCP Client

Table 11-5 describes the DHCP Client protocol settings.

Table 11-5 DHCP Client Protocol Settings

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

Parameters	Description
Use broadcast flag	Check to use the broadcast flag. This flag is generally used by the ISP's.
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for WAN interface is checked by default. If unchecked, the advertised DNS server addresses are ignored.
Use gateway metric	Enter the gateway metric. The Load Balancer uses these Metric values to determine priority of a WAN. The default metric is 4.
Client ID to send when requesting DHCP	Enter the Client ID that shall be sent when requesting DHCP.
Vendor Class to send when requesting DHCP	To allocate DHCP IP Addresses based on Vendor Class.
Override MAC address	Click to override the default MAC Address for the WAN Interface. On factory reset, it will be set to default MAC address.
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value represents auto MTU size
Physical Settings	
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. Enable STP – Check to enable the Spanning Tree Protocol over the bridge. Enable IGMP snooping – Check to enable IGMP snooping on the bridge.
Interface	Select the interface to be configured. Select more than one interface if parameter creating a bridge over multiple interfaces is enabled.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

DHCPv6 Client

Table 11-6 describes the DHCPv6 Client protocol settings.

Table 11-6 DHCPv6 Client Protocol Settings

Parameters	Description
General Settings	
Protocol	DHCPv6 Client – Address and netmask are assigned by DHCP
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
Request IPv6-address	Enter the behavior for requesting addresses. Options are try (default), force, and disabled
Request IPv6-prefix of length	Enter the IPv6 address prefix length in bits. Options are: ◆ Unspecified ◆ Automatic (default) ◆ disabled – use if you want single IPv6 address for the AP without a subnet for routing ◆ 48, 52, 56, 60, 64 –hinted prefix length ◆ custom – enter custom prefix length
Advanced Settings	
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Custom delegated IPv6 prefix	Enter the custom IPv6 prefix to be used.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for WAN interface is checked by default. If unchecked, the advertised DNS server addresses are ignored.
Client ID to send when requesting DHCP	Enter the Client ID that shall be sent when requesting DHCP.
Override MAC address	Click to override the default MAC Address for the WAN Interface. On factory reset, it will be set to default MAC address.
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value means auto MTU size
Physical Settings	
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. ◆ Enable STP – Check to enable the Spanning Tree Protocol over the bridge. ◆ Enable IGMP snooping – Check to enable IGMP snooping on the bridge.

Parameters	Description
Interface	Select the interface to be configured. Select more than one interface, if parameter creating a bridge over multiple interfaces is enabled.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

PPPoE

Table 11-7 describes the PPPoE protocol settings.

Table 11-7 PPPoE Protocol Settings

Parameters	
General Settings	
Protocol	PPPoE – Point to Point Protocol over Ethernet
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
PAP/CHAP username	Enter the PAP/CHAP username. The default password is admin.
PAP/CHAP password	Enter the PAP/CHAP password.
Access Concentrator	Enter the access concentrator name.
Service Name	Enter the service name. ***Note:*** *Access Concentrator name and Service Name gets auto populated from the PPPoE Access Point router if they are not explicitly provided*
Advanced Settings	
Use builtin IPv6 management	Allows to use the built in IPv6 management configuration
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. This is the default.
Obtain IPv6-Address	Allow IPv6 negotiation on the PPP link
Use default gateway	Select to use the default gateway. If unselected, no default route will be configured.
Use DNS servers advertised by peer	Select to use DNS servers advertised by peer, otherwise ignore advertised DNS servers.
Use gateway metric	Enter gateway metric.
LCP echo failure threshold	Enter the number of LCP echo request failures allowed before considering the peer dead. Set to zero (0) to ignore failures.

Parameters	
LCP echo interval	The LCP echo interval in seconds. LCP echo failure threshold must be set, otherwise this value is ignored.
Host-Uniq tag content	Enter the custom Host-Uniq tag to be used.
Inactivity timeout	Enter the inactivity timeout in seconds, Close the connection if the timeout is reached or enter zero (0) to ignore inactivity timeout.
Override MTU	Enter MTU size in bytes. The default is 1500 bytes.
Physical Settings	
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. ◆ Enable STP – Check to enable the Spanning Tree Protocol over the bridge. ◆ Enable IGMP snooping – Check to enable IGMP snooping on the bridge.
Interface	Select the interface to be configured. Select more than one interface, if parameter creating a bridge over multiple interfaces is enabled.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

UMTS/GPRS/EV-DO Cellular

Table 11-8 describes the UMTS/GPRS/EV-DO Cellular protocol settings.

Table 11-8 UMTS/GPRS/EV-DO Cellular Protocol Settings

Parameters	Description
General Settings	
Protocol	Modems using the UMTS/GPRS/EV-DO protocols
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
Modem device	Displays the modem device
SIM to use	Indicates which SIM to use, Embedded SIM or External SIM
Advanced Settings	
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.
Obtain IPv6-Address	Click to enable IPv6 negotiation on PPP link.

Parameters	Description
Modem init timeout	Enter the maximum wait time in seconds for the modem to become ready. The default modem initiation timeout 20 seconds.
Use default gateway	Click to configure a default gateway route. If unchecked, no default route is configured.
Use gateway metric	Enter the gateway metric. Default is 5
Use DNS servers advertised by peer	Click to enable, otherwise leave box unchecked to ignore the advertised DNS servers.
LCP echo failure threshold	Enter the number of LCP echo failures after which the peer is presumed to be dead. Enter 0 to ignore failures.
LCP echo interval	Send LCP echo requests at the given interval in seconds. Failure threshold must be configured for this to be effective.
Inactivity timeout	Number of seconds for inactivity timeout. Enter 0 to persist the connection.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – custom to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box.
Embedded SIM / External SIM Settings	
PDP Type	IP stack mode ◆ IPv4 ◆ IPv6 ◆ IPv4/IPv6
Service Type	◆ Automatic ◆ Cat M1 ◆ GSM
APN	Enter the Access Point Name provided by the cellular network operator.
PIN	Enter the PIN code to unlock the SIM card
PUK	Enter the PUK (personal unblocking key) used to unblock the SIM card if the PIN code has been repeatedly entered incorrectly
Authentication Type	Enter the authentication method used for the cellular connection. ◆ PAP/CHAP ◆ PAP (requires username and password) ◆ CHAP (requires username and password) ◆ None
Enable roaming	Enable data roaming on the cellular interface
Cid	Enter Cid value. It is usually okay to leave as the default value.

QMI Cellular

Table 11-9 describes the QMI Cellular protocol settings.

Table 11-9 QMI Cellular Protocol Settings

Parameters	Description
General Settings	
Protocol	QMI Cellular – USB modems using QMI protocol
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
Cellular Module	Displays the cellular module name
Modem device	Displays the modem device
PDP Type	Enter the IP stack mode as IPv4, IPv6, or IPv4/IPv6 (dual stack)
SIM to use	Indicates which SIM to use. Embedded SIM or External SIM
Advanced Settings	
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.
Enable IPv6 negotiation	Click to enable IPv6 negotiation on PPP link.
Modem init timeout	Enter the maximum wait time in seconds for the modem to become ready. The default modem initiation timeout 20 seconds.
Use default gateway	Click to configure a default gateway route. If unchecked, no default route is configured.
Use gateway metric	Enter the gateway metric. Default is 5
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes, which is the maximum size. A blank value means use auto MTU size.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – custom to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box.
SIM Settings	
PDP Type	IP stack mode ◆ IPv4 ◆ IPv6 ◆ IPv4v6 (for dual-stack)

Parameters	Description
Service Type	◆ Automatic ◆ LTE Only
APN	Enter the Access Point Name provided by the cellular network operator.
PIN	Enter the PIN code to unlock the SIM card
PUK	Enter the PUK (personal unblocking key) used to unblock the SIM card if the PIN code has been repeatedly entered incorrectly
Authentication Type	Enter the authentication method used for the cellular connection. ◆ PAP (requires username and password) ◆ CHAP (requires username and password) ◆ None
Enable roaming	Enable data roaming on the cellular interface
Cid	Enter Cid value. It is usually okay to leave as the default value.

CELLULAR Interface

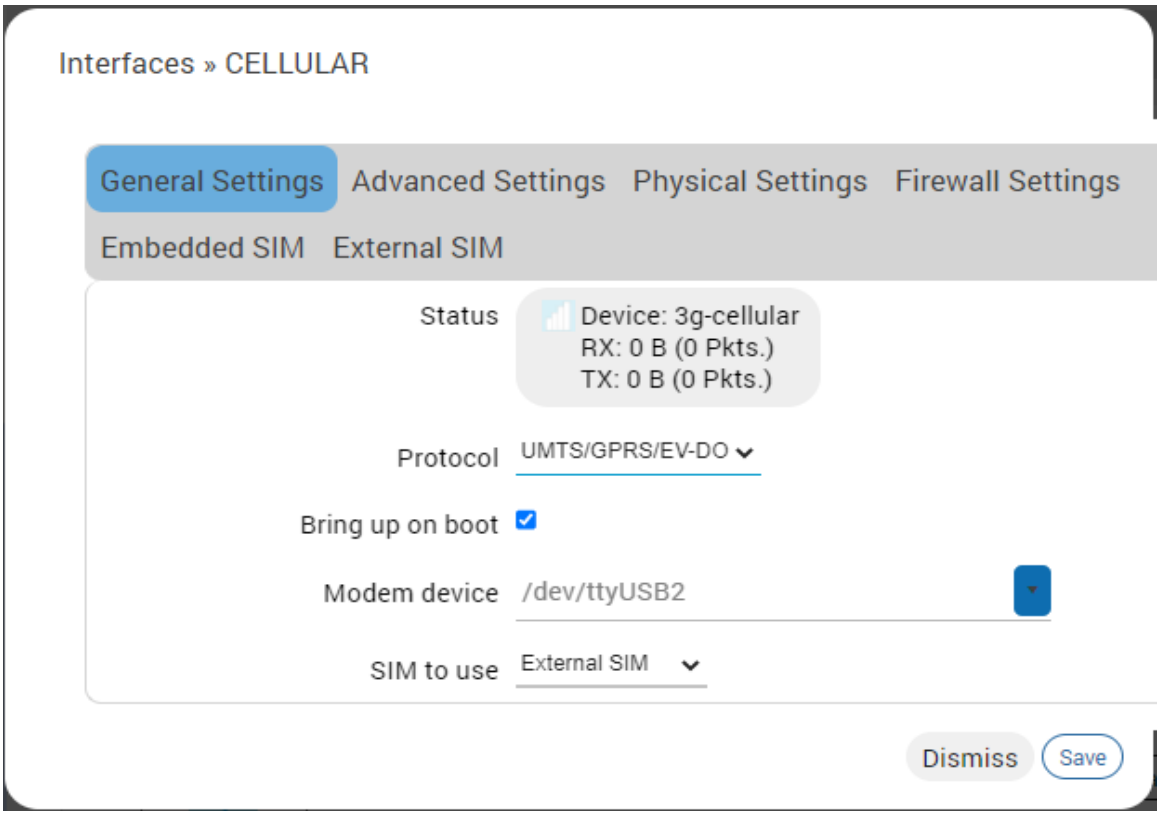
Network > Interfaces > CELLULAR

This page allows you to configure the Cellular interface parameters. When the Cellular interface is first enabled or when the gateway is factory reset, the gateway detects the module and assigns the appropriate protocol.

For descriptions of the protocol settings, see *UMTS/GPRS/EV-DO Cellular*.

To edit the interface:

1. Go to Network > Interfaces, select CELLULAR and click **Edit**.



2. Configure the interface settings.

   Note:

   - *General Settings – Protocol should not be changed for the cellular interface.*
   - *Firewall Settings – Firewall zone should be set as WAN zone.*
   - *SIM1 / SIM2 Settings – Configure the SIM settings according to the SIM slot.*

3. Click **Save**.
4. Click **Save & Apply** to save the configuration on the gateway.

LAN Interface

Network > Interface > LAN

This page allows you to configure the LAN interface. The LAN interface should use Static Address. Gateway may be used but is not required. DHCP server may be used to dynamically assign an IP address to clients connecting to the LAN. If DHCP server is disabled for the interface, all the LAN devices connected to the gateway should have a static LAN IP configured.

DHCP Server

The X300 series gateway can act as the DHCP server and assign IP addresses to devices connecting to the LAN network. The DHCP server maintains a database of available IP addresses and configuration information. When it receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, allocates an IP address or prefix appropriate for the client, and sends configuration information appropriate for that client.

DHCP servers typically grant IP addresses to clients for a limited interval called a lease. DHCP clients are responsible for renewing their IP address before that interval has expired, and must stop using the address once the interval has expired, if they have not been able to renew it. DHCP is used for IPv4 and IPv6. While both versions serve the same purpose, the details of the protocol for IPv4 and IPv6 are sufficiently different that they should be considered separate protocols.

Interface configuration settings are determined mainly by the protocol selection. For a description of the protocol settings, see *Static Address.*

To edit the interface:

1. Go to Network > Interfaces, select LAN and click **Edit**.

Figure 11-3 LAN Interface (Static Address) Configuration

Interfaces » LAN

General Settings | Advanced Settings | Physical Settings | Firewall Settings | DHCP Server

Status
Device: br-lan
Uptime: 17d 23h 51m 23s
MAC: 00:80:A3:6A:A2:23
RX: 0 B (0 Pkts.)
TX: 9.21 MB (51763 Pkts.)
IPv4: 192.168.8.1/24
IPv6: fd2c:43c1:bd6c::1/60

Protocol: Static address

Bring up on boot: ☑

IPv4 address: 192.168.8.1

IPv4 netmask: 255.255.255.0

IPv4 gateway: 172.19.0.1 (wwan)

IPv4 broadcast: 192.168.8.255

Use custom DNS servers:

IPv6 assignment length: 60

Assign a part of given length of every public IPv6-prefix to this interface

IPv6 assignment hint: 0

Assign prefix parts using this hexadecimal subprefix ID for this interface.

IPv6 suffix: ::1

Optional. Allowed values: 'eui64', 'random', fixed value like '::1' or '::1:2'. When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like '::1') to form the IPv6 address ('a:b:c:d::1') for the interface.

Dismiss | Save

2. Configure the interface settings respective to the gateway model number.
   - For protocol settings, see *Static Address*.

     Note:

     - *General Settings – Protocol should be Static Address for the LAN interface. Gateway is not required.*
     - *Physical Settings – By default, the LAN interface bridges the eth0.1 and wlan0 physical interfaces.*
     - *Firewall Settings – Firewall zone should be set as LAN zone.*
     - *DHCP Server – DHCP server can be used to assign IP address to clients connecting to the LAN. To enable the DHCP server, make sure that the check box "Ignore Interface" is not selected, and configure the other DHCP settings.*
3. Click **Save**.
4. Click **Save & Apply** to save the configuration.

WWAN and WWAN6 Interface

Network > Interface > WWAN or WWAN6

This page allows you to configure the WWAN and WWAN6 interface parameters. The WWAN interface becomes active when the wireless interface is configured as lient. The wireless interface is configured on the Network > Wireless page.

The WWAN interface supports IPv4 or dual mode IPv4/IPv6. WWAN6 interface supports IPv6 mode. Otherwise, the WWAN and WWAN6 interfaces provide similar functionality and are configured in a similar manner.

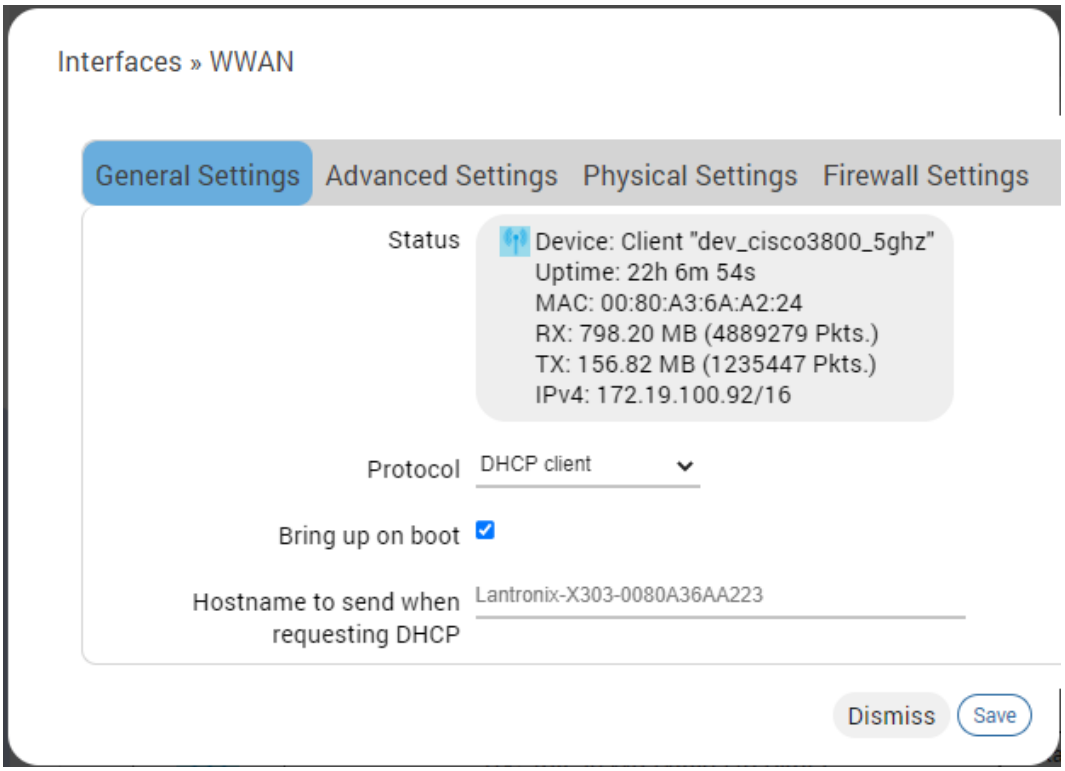
The WWAN or WWAN6 interface will use either Static Address, DHCP client, or DHCPv6 client protocol. On the WWAN interface, if you assign Static Address as the protocol, IPv4 gateway is required for external interface, but should not be used for internal use. DHCP server should be disabled.

Interface configuration settings will vary depending on the assigned protocol. For descriptions of the protocol settings, see *Static Address*, *DHCP Client*, or *DHCPv6 Client*.

To edit the interface:

1. Go to Network > Interfaces, select WWAN and click **Edit**.

Figure 11-4 WWAN Interface (DHCP client) Configuration



2. Configure the interface settings respective to the gateway.
   - For protocol settings, see *Static Address* or *DHCP Client*.
   - General Settings – To change the WWAN protocol, select the protocol and click the **Switch Protocol** button. If Static IP address protocol is selected, IPv4 gateway is required for external interface, but should not be used for internal use.
   - Advanced Settings – Similar to WAN DHCP settings, except the metric is fixed by default for other features to work as per requirement.
   - Firewall Settings – Firewall zone should be set as WAN zone.
   - DHCP Server – DHCP server should be disabled.
3. Click **Save**.
4. Click **Save & Apply** to save the configuration.

Add Virtual Interface

The virtual network interface allows you to configure a new interface such as a VPN tunnel that encapsulates data inside a transport protocol. The supported tunneling protocols include GRE, L2TP, PPP, and PPtP.

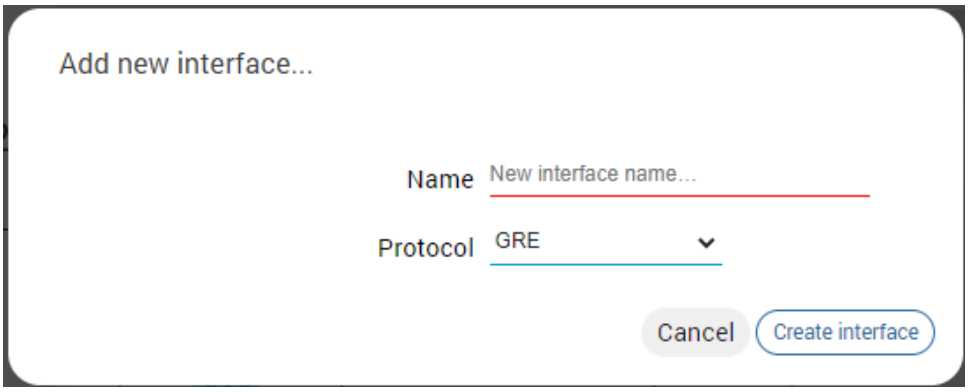
The virtual interface can be created for other reasons, such as to configure a relay bridge to extend the wireless network.

Note: *Adding a virtual interface may require modifications to the load balancer configuration. For load balancer configuration, see Load Balancing. For additional support and knowledge base articles, please visit Lantronix Support.*

To add a new interface:

1. Go to Network > Interfaces, scroll to the bottom of the list of interfaces and click **Add new interface.**

Figure 11-5 Network Add New Interface



2. Enter the interface name. The name must include only alpha numeric characters and special character underscore (_).
3. Select the protocol to assign to the interface.
4. Click **Create interface**.
5. Configure the interface settings relative to the selected protocol.
   - The first field below the protocol selection is Bring up on boot. This is enabled by default and will start the interface when the gateway is booted.
   - For the remaining configuration details, see *Table 11-10*.
6. Click **Save** to save the new interface.
7. Click **Save & Apply** to apply the configuration to the gateway.

Table 11-10 VPN Tunnel Protocols

Protocol	Description
GRE	

Protocol	Description
GRE General Settings	◆ Bring up on boot – Start the interface when the device is booted. Selected by default. ◆ Enable GRE tunnel – Enable the interface. ◆ GRE Server Address – Enter the WAN IP address or domain name of the remote GRE server. ◆ Local Address – Enter the WAN IP address of the gateway ◆ Local Tunnel Address – Enter the local IP address of the gateway on the GRE tunnel ◆ Remote Tunnel Address – Enter the remote IP address on the GRE tunnel ◆ Keepalive Interval (in minutes) – The amount of time before sending a keepalive probe packet to check the connection ◆ Keepalive Retries – The number of unanswered echo requests before considering the peer dead ◆ Interface – Enter the interface to bind to GRE. GRE cannot move from one interface to another. It must be bound to a particular interface.
GRE Advanced Settings	◆ Use builtin IPv6 management – Allows to use the built in IPv6 management configuration ◆ Force link – Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. This is the default.
GRE Firewall Settings	Select the WAN zone as the firewall zone.
L2TP	
L2TP General Settings	◆ Bring up on boot – Start the interface when the device is booted. Selected by default. ◆ L2TP Server – Enter the public IP address of the VPN server for L2TP connection ◆ PAP/CHAP username – Enter the PAP/CHAP username. The default password is admin. ◆ PAP/CHAP password – Enter the PAP/CHAP password.
L2TP Advanced Settings	Advanced settings are similar to those of PPPoE with a few exceptions as noted below. For configuration details, see *UMTS/GPRS/EV-DO Cellular*. ◆ Keepalive Requests is similar to LCP echo failure threshold. ◆ Checkup Interval is similar to Inactivity timeout. ◆ L2TP does not include fields for LCP echo interval or Host-Uniq tag content.
L2TP Firewall Settings	Select the WAN zone as the firewall zone.
PPP	
PPP General Settings	◆ Modem device – Select the modem device from the list. ◆ PAP/CHAP username – Enter the PAP/CHAP username. The default password is admin. ◆ PAP/CHAP password – Enter the PAP/CHAP password.
PPP Advanced Settings	Advanced settings are similar to those of PPPoE. For configuration details, see *UMTS/GPRS/EV-DO Cellular*.
PPP Firewall Settings	Select the WAN zone as the firewall zone.
PPtP	

Protocol	Description
PPtP General Settings	***Note:*** *Enabling PPtP will also enable a 20 mins PPtP watchdog which will reboot the gateway in absence of an active PPtP connection for a period of 20 mins.* ◆ VPN Server – Enter the public IP Address or DNS name of the remote VPN Server for the PPTP connection. ◆ PAP/CHAP username – Enter the PAP/CHAP username. ◆ PAP/CHAP password – Enter the PAP/CHAP password. The default password is admin. ◆ Interface – Select the interface that the device will use to initiate the PPtP connection. ◆ Unspecified – use the active interface to make the connection.
PPtP Advanced Settings	Advanced settings are similar to those of PPPoE. For configuration details, see *UMTS/GPRS/EV-DO Cellular*. One additional setting is described below: ◆ Use mppe – Select to enable encryption if this setting is enabled on the remote server.
PPtP Firewall Settings	◆ Select the WAN zone as the firewall zone.

Relay Bridge

The Relay Bridge protocol provides an option to implement bridge behavior (on IPv4 only) to extend the wireless network. The virtual interface must have a local IPv4 address to access the bridge connection and relay between two networks.

Wireless

Network > Wireless

The Wireless interface on the gateway can operate in two modes:

- Client mode – The gateway will act as a Wi-Fi client to existing wireless networks. The gateway will accept Internet access through wireless access provided by another service provider and then distribute the access to the machines connected to the gateway on its LAN interface.
- Access point (Master) mode – The gateway will act as a wireless access point to provide a wireless LAN network that wireless clients may join.

The gateway can act as Wi-Fi master and client at the same time provided that the gateway's Wi-Fi client is connected to any AP.

Figure 11-6 and *Table 11-11* describe the Wireless Overview and Associated Stations.

Figure 11-6 Wireless Overview

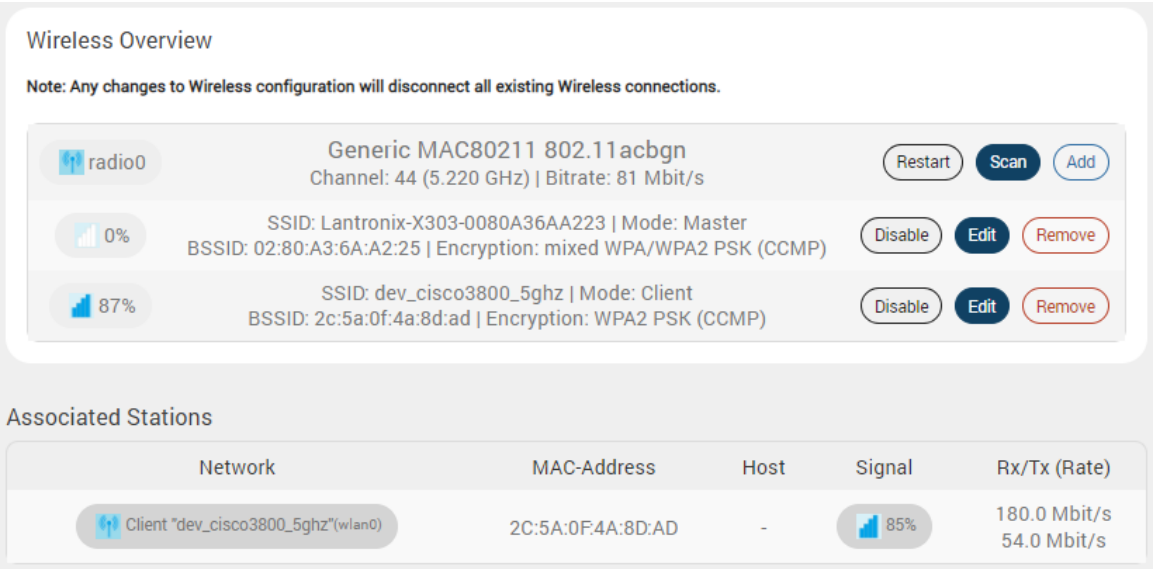


Table 11-11 Wireless Overview and Associated Stations

Parameters	Description
Wireless Overview	Displays status and details about the wireless radio and wireless instances. The gateway provides the following interaction with the wireless radio: ◆ **Restart** – restart the radio ◆ **Scan** – scan for available wireless connections and join a network. This also adds a new client instance. ◆ **Add** – add a new instance The gateway provides the following interaction on the wireless interface instances: ◆ **Disable/Enable** – disable or enable the instance ◆ **Edit** – edit the instance configuration settings ◆ **Remove** – delete the instance

Parameters	Description
Associated Stations	Displays details about associated wireless stations such as network, MAC address, host, signal and Rx/Tx (rate).

Wireless Network Configuration

Note: *When Wi-Fi is configured as Client, the WWAN interface will become active.*

Wi-Fi Client

To join a wireless network in client mode:

1. Go to Network > Wireless.
2. Click **Scan** to find available wireless networks. The scan results will display a list of networks.
3. Select the network that you want to connect to and click **Join Network**.
4. On the wireless configuration window, enter the settings to join the network based on the network's encryption method (WPA, WPA2, WPA3 SAE, mixed WPA/WPA2). The assigned firewall zone should be WAN. If you select Replace wireless configuration, all existing networks will be deleted from the radio. Click **Submit**.
5. Configure the wireless network client. For details, see *Table 11-12* and *Table 11-13*.
6. Click **Save**.

   The client instance is created and the access point to which it is associated appears under Associated Stations.
7. Click **Save & Apply**.

Wireless Access Point

To configure the wireless instance as an access point:

1. Go to Network > Wireless.
2. If an access point exists and you want to edit it, click **Edit**.
3. If no access point exists, click **Add** to create an instance.
4. Configure the device and interface settings, selecting Access point as the Wi-Fi interface mode. For configuration details, see *Table 11-12* and *Table 11-13*.
5. Click **Save**.
6. The access point instance is created or modified.
7. Click **Save & Apply**.

Table 11-12 Wireless Device Configuration

Parameters	Description
General Setup	

Parameters	Description
Status	Displays the following details: ◆ Mode – Master (access point) or Client ◆ SSID – Service Set Identifier (SSID) is a public identifier up to 32 characters that uniquely names a Wi-Fi connection. ◆ BSSID – Basic Service Set Identification (BSSID); 24 bit MAC Address of Wireless Access Point ◆ Encryption – data encryption method ◆ Channel – wireless channel and frequency band ◆ Tx-Power – transmit power in dBm ◆ Signal/Bitrate – signal strength in dBm and bitrate in Mbit/sec ◆ Country – country code
Wireless network is enabled/ disabled	The field label displays the state of the wireless network as either enabled or disabled. Click **Enable** or **Disable** to update the network operation state.
Operating Band	By default, 'auto' lets the wireless device select the operating band to use. Alternatively, choose the band and channel. Channels are defined in 5 MHz increments and are 20 MHz wide. It's recommended to select 'auto' or to select channels that don't overlap with channels used by other access points in the immediate area of the access point that you are configuring.
Roaming	
Roaming State	Enable or disable the roaming state, which allows the wireless client to make roaming choices of which AP to associate to.
Level	Select preconfigured roaming settings or select Custom to configure custom settings for the client.
Time interval for consecutive scans	The interval in seconds between scans.
RSSI Delta for 2.4G	The RSSI delta for 2.4G represents the roaming threshold at which the client will roam to the target AP.
RSSI Delta for 5G	The RSSI delta for 5G represents the roaming threshold at which the client will roam to the target AP.
Scan Threshold for 2.4G	The 2.4G scanning threshold in dbm, after which the client will scan for potential target APs.
Scan Threshold for 5G	The 5G scanning threshold in dbm, after which the client will scan for potential target APs.

Table 11-13 Wireless Interface Configuration

Parameters	Description
General Setup	
Mode	Select the Wi-Fi Interface mode. ◆ Access Point – gateway will act as an access point (master mode) ◆ Client – gateway will act as a wireless client The default mode is Access Point.
ESSID	Displays the device name assigned to the gateway.

Parameters	Description
Priority	The order of preference in which the gateway will attempt to join the configured wireless networks. The range is from 1 to 8 with 1 being the highest priority and 8 being the lowest priority.
BSSID	This field is displayed for Client only. Basic Service Set Identifier (BSSID) – 48-bit MAC address for the access point of the BSS. This can be left blank.
Network	Select LAN for the Access Point or WWAN for Client Mode to configure the gateway as LAN or WWAN respectively.
Hide ESSID	Select Hide ESSID, to hide ESSID when client machines scan for available Wi-Fi networks.
Wireless Security	
Encryption	Select the Encryption mode for Wi-Fi network. Available Options: ◆ WPA3 Transition Mode (strong security) ◆ WPA2-EAP (strong security) ◆ WPA3 SAE (strong security) ◆ WPA2-PSK/WPA-PSK Mixed mode (medium security) ◆ WPA-PSK (medium security) ◆ WPA-EAP (medium security) ◆ Open (no security) The default encryption mode for access point configuration is WPA2-PSK/WPA-PSK Mixed mode. WPA3 only applies to the STA (client) interface
Cipher	For all encryption modes except No Encryption. Select the cipher suitable to the gateway. Options: ◆ Auto ◆ Force CCMP (AES) ◆ Force TKIP ◆ Force TKIP and CCMP (AES) The default cipher is auto mode.
Key	Enter the key respective to cipher type
Enable key reinstallation (KRACK) countermeasures	This setting is displayed only if the interface is an Access Point. Select to enable KRACK countermeasures. This setting is disabled by default.
MAC-Address Filter	
MAC-Address Filter	Allows or blocks certain client MAC Addresses. Default is disabled. This setting applies only to Access point mode. Options: ◆ Disable ◆ Allow listed only – If this option is selected, choose the client MAC Addresses to allow. ◆ Allow all except listed – If this option is selected, choose the client MAC Addresses to block.

DHCP and DNS

Network > DHCP and DNS

Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices to communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server. The DHCP client then uses this information to configure its host. Once the configuration process is complete, the host is able to communicate on the network.

For details about basic setup of DHCP server on the LAN side see *DHCP Server*.

The DHCP and DNS page allows you to configure advanced options such as custom DNS servers, custom lease files, advanced TFTP settings and MAC Address-based IP Address allocation.

To configure:

1. Go to Network > DHCP and DNS.
2. Enter the configuration settings. See *Table 11-14* to *Table 11-18*.
3. Click **Save & Apply**.

General Settings

Network > DHCP and DNS > General Settings

Table 11-14 General Configuration of DHCP Server and DNS-Forwarder

Parameters	Description
Server Settings	
Domain required	Check to allow forwarding of DNS request only if they have domain name.
Authoritative	Check to authorize the DHCP in the local network.
Local server	Enter the local server domain specification. These domain names are only resolved using DHCP or host files.
Local domain	Enter the local domain suffix appended to DHCP names and host file entries.
Log queries	Log the DNS request received in the syslog server.
DNS forwardings	Enter the DNS Server names to forward the received DNS requests.
Rebind protection	Check to discard upstream RFC1918 responses
Allow localhost	Check to allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services
Domain whitelist	Enter the list of domain name to allow RFC1918 responses.
Local Service Only	Select to accept DNS queries only from hosts whose address is on a local subnet.
Non-wildcard	Select to bind only configured interface addresses, instead of the wildcard address.
Listen Interfaces	Restrict listening to the specified interfaces.
Exclude Interfaces	Prevent listening on the specified interfaces.
Active DHCP Leases	

Parameters	Description
Hostname	Name of the device that is connected to the gateway and has been leased an IP Address by DHCP server.
IPv4-Address	IPv4 Address assigned to the device connected to the gateway.
MAC-Address	MAC address of the device connected to the gateway.
Leasetime remaining	Remaining time until which the device can use the DHCP server leased IP Address.
Active DHCPv6 Leases	
Hostname	Name of the device that is connected to the gateway and has been leased an IPv6 Address by DHCPv6 server.
IPv6-Address	IPv6 Address assigned to the device connected to the gateway.
DUID	DUID (Device Unique Identifier) of the device connected to the gateway
Leasetime remaining	Remaining time until which the device can use the DHCPv6 sever leased IPv6 Address.
Static Leases	
Hostname	Name of the device that is connected to the gateway and has been assigned a static IP Address.
MAC-Address	MAC address of the device connected to the gateway.
IPv4-Address	IPv4 Address to be assigned to the device connected to the gateway.
IPv6-Suffix (hex)	IPv6 Address to be assigned to the device connected to the gateway.

Resolv and Host Files

Network > DHCP and DNS > Resolv and Host File

Table 11-15 Resolv and Host File Configuration for DHCP and DNS

Parameters	Description
Use /etc/ethers	Check to use /etc/ethers for configuring the DHCP-Server.
Leasefile	Enter the directory path name where given DHCP-leases will be stored.
Ignore resolve file	Check to ignore the resolved file.
Resolve file	Enter the local DNS file.
Ignore /etc/hosts	Check to ignore the hosts file.
Additional Hosts file	Enter the additional host files.

TFTP Settings

Network > DHCP and DNS > TFTP Settings

This page provides settings to configure the gateway as a Trivial File Transfer Protocol (TFTP) server, which can be used to serve files for download to a remote TFTP client.

Table 11-16 TFTP Configuration for DHCP and DNS

Parameters	Description
Server Settings	

Parameters	Description
Enable TFTP server	Check to enable TFTP server. By default, the TFTP server is in disabled. ◆ TFTP server root – Enter the Root directory for the files served using TFTP. ◆ Network boot image – Enter the Filename of the boot image which is advertised to the clients.

Advanced Settings

Network > DHCP and DNS > Advanced Settings

Table 11-17 Advanced Configuration for DHCP and DNS

Parameters	Description
Server Settings	
Suppress logging	Suppress logging of the routine operation of DHCP. Errors and problems will still be logged.
Allocate IP Sequentially	Force DHCP server to allocate IP addresses sequentially, starting from the lowest available address. In this mode, clients that allow a lease to expire are more likely to move IP address.
Filter private	Check to deny the reverse lookups for local networks.
Filter useless	Check to deny the requests that cannot be answered by public name servers. By default the request are forwarded.
Localize queries	Check to localize hostname depending on the requesting subnet if multiple IP Addresses are available.
Expand hosts	Check to add local domain suffix to names served from hosts files.
No negative cache	Check to deny caching the negative replies, e.g. for non-existing domains.
Additional Servers file	List of DNS servers to forward requests to.
Strict order	DNS servers will be queried in the order of the resolve file.
All Servers	Select to query all upstream DNS servers.
Bogus NX Domain Override	Enter the hostname that supply bogus NX domain results.
DNS server port	Enter the listening port for inbound DNS queries. The default DNS server port is 53.
DNS query port	Enter the fixed source port number for outbound DNS queries. The default DNS query port is “any”
Max. DHCP leases	Enter the maximum number of allowed DHCP leases that are active. By default unlimited DHCP leases are allowed.
Max. EDNS0 packet size	Enter the maximum allowed size of EDNS.0 UDP packets. The default EDNS.0 UDP packet size is 1280.
Max. concurrent queries	Enter the maximum number of concurrent DNS queries allowed. By default 150 concurrent DNS queries are allowed.

Parameters	Description
Size of DNS query cache	Enter the maximum number of cached DNS entries. By default, 150 DNS entries are cached. Maximum is 10000. A value of zero (0) means no caching.

Static Leases

Network > DHCP and DNS > Static leases

Table 11-18 DHCP and DNS Static Leases

Parameters	Description
Add	Click to add a static lease.
Active DHCP Leases	
Hostname	Name of the device that is connected to the gateway and has been leased an IP Address by DHCP server.
IPv4-Address	IPv4 Address assigned to the device connected to the gateway.
MAC-Address	MAC address of the device connected to the gateway.
Leasetime remaining	Remaining time until which the device can use the DHCP server leased IP Address.
Active DHCP6 Leases	
Hostname	Name of the device that is connected to the gateway and has been leased an IPv6 Address by DHCPv6 server.
IPv6-Address	IPv6 Address assigned to the device connected to the gateway.
DUID	DUID (Device Unique Identifier) of the device connected to the gateway
Leasetime remaining	Remaining time until which the device can use the DHCPv6 sever leased IPv6 Address.
Static Leases	
Hostname	Name of the device that is connected to the gateway and has been assigned a static IP Address.
MAC-Address	MAC address of the device connected to the gateway.
IPv4-Address	IPv4 Address to be assigned to the device connected to the gateway.
IPv6-Suffix (hex)	IPv6 Address to be assigned to the device connected to the gateway.

Hostnames

Network > Hostnames

Allows you to enter host names for the devices on the LAN.

To add a host name:

1. Go to Networks > Hostnames.
2. Click **Add**.
3. Enter the hostname and the IP address of the host. See *Table 11-19*.
4. Click **Save**.
5. Click **Save & Apply**.

Table 11-19 Hostnames Configuration

Parameters	Description
Hostname	Enter the Hostname. The hostname can contain any combination of alphabetic characters, numbers, dashes, and underscores. No other special characters are allowed.
IP address	Enter the IP Address of the host.

Static Routes

Network > Static Routes

Configure static routes to define the explicit path between two different networks located in two different domains. Static routes must be manually reconfigured when network changes occur.

To configure static routes:

1. Go to Networks > Static Routes.
2. Select IPv4 or IPv6 tab.
3. Click **Add**.
4. Enter the configuration settings. For IPv4 static routes, see *Table 11-20* and for IPv6 static routes, see *Table 11-21*.
5. Click **Save**.
6. Click **Save & Apply**.

Static IPv4 Routes

Table 11-20 Static IPv4 Routes Configuration

Parameters	Description
General Settings	
Interface	Select the interface name of the parent interface this route belongs to.
Target	Enter the target host IPv4 Address or Network address if the target is a network.

Parameters	Description
IPv4-Netmask	Enter the IPv4 Netmask of the static route.
IPv4-Gateway	Enter the IPv4 gateway. If gateway is not entered, the gateway from the parent interface is used.
Advanced Settings	
Metric	Enter the metric of the static route.
MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. A blank value represents auto MTU size.
Route type	Select the route type. Available options: ◆ unicast – route entry describes real paths to the destinations covered by the route prefix. ◆ local – destinations are assigned by this host. Packets are looped back and delivered locally. ◆ broadcast – destinations are broadcast addresses. Packets are sent as link broadcasts. ◆ multicast – special type used for multicast routing. ◆ unreachable – these destinations are unreachable ◆ prohibit – these destinations are unreachable. ◆ blackhole – these destinations are unreachable. Packets are discarded silently. Local senders get an ENVAL error. ◆ anycast – these destinations are anycast addresses assigned to this host.
Route table	Define the table ID to use for the route. The table ID can be either a numeric table index ranging from 0 to 65535 or a symbolic alias declared in /etc/iproute2/rt_tables. The following special aliases are also recognized: local (255), main (254), default (253).
Source Address	Specify the preferred source address when sending to destinations covered by the target.
On-Link route	If enabled, the gateway is on link even if the gateway doesn't match any interface prefix.

Static IPv6 Routes

Table 11-21 Static IPv6 Routes Configuration

Parameters	Description
General Settings	
Interface	Select the interface name of the parent interface this route belongs to.
Target	Enter the target host IPv6 Address or Network CIDR if the target is a network.
IPv6-Gateway	Enter the IPv6 gateway for the static route. If gateway is not entered, the gateway from the parent interface is used.
Advanced Settings	
Metric	Enter the metric of the static route.

Parameters	Description
MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value represents auto MTU size
Route type	Select the route type. Available options: ◆ unicast – route entry describes real paths to the destinations covered by the route prefix. ◆ local – destinations are assigned by this host. Packets are looped back and delivered locally. ◆ broadcast – destinations are broadcast addresses. Packets are sent as link broadcasts. ◆ multicast – special type used for multicast routing. ◆ unreachable – these destinations are unreachable ◆ prohibit – these destinations are unreachable. ◆ blackhole – these destinations are unreachable. Packets are discarded silently. Local senders get an ENVAL error. ◆ anycast – these destinations are anycast addresses assigned to this host.
Route table	Define the table ID to use for the route.
Source Address	Specify the preferred source address when sending to destinations covered by the target.
On-Link route	If enabled, the gateway is on link even if the gateway doesn't match any interface prefix.

Diagnostics

Network > Diagnostics

~~This page lets you run~~ The diagnostics feature allows you to run network utilities and cable diagnostics commands from the web interface.

Table 11-22 describes each of the network utilities.

Table 11-23 describes the cable diagnostics status messages.

Note: *The cable diagnostics command will bring down the Ethernet port link, which will take more time to complete the test. Cable diagnostics is only accurate for cable lengths of 7 - 120 meters.*

Table 11-22 Diagnostics - Network Utilities

Network Utility	Description
Ping	IP Address or fully qualified domain name to be pinged. Ping determines network connection between gateway and host on the network. The output shows if the response was received, packets transmitted and received, and packet loss if any.
Traceroute	IP Address or fully qualified domain name Traceroute displays all the routers present between the destination IP address and the gateway. The output shows all the gateways through which data packets pass on way to the destination system from the source system, maximum hops and total time taken by the packet to return measured in milliseconds.
Nslookup	IP Address or fully qualified domain name that needs to be resolved. Name lookup is used to query the Domain Name Service for information about domain names and IP addresses. It sends a domain name query packet to a configured domain name system (DNS) server. If you enter a domain name, you get back the IP address to which it corresponds. If you enter an IP address, you get back the domain name to which it corresponds. A message stating “Unknown Host” indicates that the Internet Name does not exist.

Table 11-23 Cable Diagnostics Status Messages

Status message	Description
<interface name:> No cable faults detected	The cable link is good.
<interface name:> Open circuit detected in cable	There is no cable.
<interface name:> Open circuit detected in cable Distance to cable fault is ~<disance> meter(s).	Open ended cable.
<interface name:> Short circuit detected in cable. Distance to cable fault is ~<distance> meter(s).	There is an issue with the cable.

Status message	Description
<interface name:> Short cable (less than 10 meters) detected.	Short cable detected.
<interface name:> Cable diagnostic test failed	The cable has failed the diagnostic test. Possible failure reasons include: interface is busy, link partner is not configured for auto-negotiation, or link partner is busy establishing the link.

Firewall

Network > Firewall

The firewall policy helps secure the network. The X300 series gateways follow a zone based firewall concept. Every interface of the gateway, whether physical or virtual, needs to be assigned to a firewall zone, and all traffic routed through that interface is bound by the assigned policy. At a minimum, there are two firewall zones, the LAN zone and WAN zone, with one or more interfaces assigned to each zone.

By default, there is a minimal firewall configuration predefined in the gateway. The minimal configuration consists of global firewall settings, and two zones, the LAN zone and WAN zone which serve as a source or destination for port forwarding, rules, and redirects. This configuration may be sufficient for your needs with little modification. Otherwise, you can use the web interface to modify the firewall configuration.

This section assumes that the reader has knowledge of implementing firewall policies or will consult their network administrator to set up the firewall policies.

Note: *Create a backup of the firewall configuration before making any changes.*

General Settings

The General settings page consists of the global settings and zones. The global firewall settings are default firewall settings that do not belong to any zone.

Firewall Global Settings

To configure firewall global settings:

1. Go to Network > Firewall.
2. In the top section of the General Settings page, if desired, modify global firewall settings. See *Table 11-24*.
3. Click **Save & Apply** to save the changes and reload the firewall.

Table 11-24 Firewall Global Settings

Parameters	Description
General Settings	
Enable SYN-flood protection	Check to enable SYN-flood protection. SYN-flood protection will enable spamming detection and block whenever there is a spam attack.

Parameters	Description
Drop invalid packet	Check to drop the invalid packets that are not matching any active connection.
Input	Select to accept or reject the inbound traffic to all the interfaces.
Output	Select to accept or reject the outbound traffic from all the interfaces.
Forward	Select to accept or reject the forwarded traffic from all the interfaces.

Firewall Zones

Two firewall zones, the LAN zone and WAN zone, are predefined in the gateway. All traffic from LAN to WAN has no restrictions but all incoming traffic from WAN source is blocked unless a port forwarding rule is set or unless a particular port is opened.

A zone section groups one or more interfaces and serves as source or destination for forwarding, rules, and redirects. A zone is defined by the following rules:

- Masquerade (NAT) of outgoing traffic (WAN) is controlled on a per zone basis on the outgoing interface.
- INPUT rules describe what happens to traffic trying to reach the gateway through an interface in that zone.
- OUTPUT rules zone describe what happens to traffic originating from the gateway going through an interface in that zone.
- FORWARD rules describe what happens to traffic passing between different interfaces in that zone.

Packet filtering actions

- ACCEPT – traffic is allowed to pass as if there is no firewall in place. If the port at the destination is closed, a response will be returned as if a Reject rule is in place.
- DROP – the firewall discards the packet and sends no response back to the source host that sent the packet. The source host will wait for a response until a timeout occurs and may attempt to retry the connection after timeout occurs.
- REJECT – the firewall discards the packet and sends a response back to the source host that the port is closed. Doing so can hint to the source that packet filtering firewall is in place.

In general, use REJECT to deny traffic from trusted hosts by gracefully informing them that traffic is not allowed to pass. Use DROP to deny traffic from untrusted hosts or when you don't want expose information about the destination host.

To configure firewall zones:

1. Go to Network > Firewall.
2. To add and configure a new firewall zone, click **Add**.
3. To modify settings for an existing firewall zone, click **Edit**.
4. Enter or modify the firewall zone settings. See *Table 11-25*.
5. Click **Save**.

Table 11-25 Firewall Zones Configuration (LAN)

Parameters	Description
General Settings	
Name	Enter the name of the zone.
Input	Select to accept, reject or drop the inbound traffic to all the configured zones.
Output	Select to accept, reject or drop the outbound traffic from all the configured zones.
Forward	Select to accept, reject or drop the forwarded traffic from all the configured zones.
Masquerading	Check to allow IP Masquerading (NAT).
MSS clamping	Check to allow MSS clamping.
Covered networks	Select the network interfaces that must be included in the zone configuration.
General Settings / Inter-Zone Forwarding	
Allow forward to destination zones	Select to allow or deny forwarding traffic to the configured destination zone.
Allowed forward from source zones	Select to allow or deny forwarding traffic from the configured source zone.
Advanced Settings	
Covered devices	List of raw network device names attached to this zone
Covered subnets	List of IP subnets attached to this zone.
Restrict to address family	Select IP Address family for configuring firewall for LAN zone from available options. Available Options ◆ IPv4 ◆ IPv6 ◆ IPv4 and IPv6
Restrict Masquerading to given source subnets	Enter the source subnet to which the masquerading must be restricted.
Restricts Masquerading to given destination subnets	Enter the destination subnet to which the masquerading must be restricted.
Enable logging on this zone	Check to enable logging of all the activities on the Zone.
Conntrack Settings	
Allow "invalid" traffic	Select to allow invalid traffic. More specifically, when selected, no rules can be installed that reject forwarded traffic with conntrack state equal to invalid. Disabled by default.
Automatic helper assignment	Automatically assign conntrack helpers for the zone.
Conntrack Settings	
Extra source arguments	Extra arguments passed directly to iptables for source classification rules.
Extra destination arguments	Extra arguments passed directly to iptables for destination classification rules

Port Forwards

Network > Firewall > Port Forwards

Port forwarding allows remote computers to connect to a specific host within the LAN by opening the WAN port and redirecting the connection (and data) on that port to an internal LAN IP and port. By default, all WAN side ports are closed.

To view port forwarding entries, go to Firewall > Port Forwards. See *Table 11-26* for a description. You can also edit, reorder or delete the entries from this view.

Table 11-26 Firewall Port Forwards

Parameters	Description
Match	Displays the WAN TCP/UDP ports for matching the conditions before forwarding it to LAN device.
Forward to	Displays the destination IP Address to which the traffic must be forwarded.
Enable	Check to enable the Port Forwarding rule.

Add Port Forwarding Rule

To add a port forwarding rule:

1. Go to Network > Firewall > Port Forwards.
2. At the bottom of the Port Forwards table, click **Add**.
3. Enter the configuration settings. See *Table 11-27*.
4. Click **Save**.

Table 11-27 Port Forwarding Configuration for Firewall Zone

Parameters	Description
Port Forwards General Settings	
Name	Enter the name of the Port Forwarding rule.
Protocol	Select the protocol. Available options: ◆ TCP ◆ TCP + UDP ◆ UDP ◆ ICMP ◆ unspecified ◆ custom
Source Zone	Specify the traffic source zone. This must refer to one of the firewall zones, usually WAN.
External Port	Enter the WAN port of the external network.
Destination zone	Specify the traffic destination zone. This must refer to one of the firewall zones, usually LAN.
Internal IP address	Enter the LAN IP address of the internal network.
Internal port	Enter the LAN port number of the internal network.
Port Forwards Advanced Settings	

Parameters	Description
Source MAC Address	The rule will match incoming traffic from the specified source mac address.
Source IP Address	The rule will match incoming traffic from the specified source IP address.
Source port	The rule will match incoming traffic from the specified source port number.
External IP Address	Enter the external IP address of the gateway.
Enable NAT Loopback	Enable NAT loopback to allow one machine on the LAN network to access another machine on the LAN through the external IP address of the gateway
Extra arguments	Passes additional arguments to iptables. Should be used with care.

Traffic Rules

Network > Firewall > Traffic Rules

Traffic rules are security policies that allow or restrict access to specific ports or hosts. Rule actions can be configured to accept, drop, or reject traffic.

The following describes good practices for configuring traffic rules.

- Block all traffic by default and explicitly enable specific traffic to known services.
- Allow specific traffic, using the principle of least privilege.
- Specify source IP address. It's okay to specify "any" if the service should be accessible to everyone on the Internet, otherwise, specify the source address.
- Specify the destination IP address.
- Specify the destination port. The value of the destination port should never be "any".

Rule and zone matching

The source and destination zones are tied to the target action.

- If source and destination are given, the rule matches forwarded traffic.
- If only source is given, the rule matches incoming traffic.
- If only destination is given, the rule matches outgoing traffic.
- If neither source nor destination are given, the rule defaults to an outgoing traffic rule.

To view traffic rules, go to Network > Firewall > Traffic Rules. See *Table 11-28* for a description. You can also enable or disable the traffic rule from this page view.

Table 11-28 Firewall Zone Traffic Rules

Parameters	Description
Name	Displays the name of the traffic rule.
Match	Displays the details of the traffic rule configuration and the conditions in which the rule is applicable.

Parameters	Description
Action	Action to be taken on the traffic when the rule conditions are satisfied. Indicates whether the rule is for incoming, forwarded, or outgoing traffic.
Enable	Select the box to enable the traffic rule. If the rule is enabled, clear the box to disable the rule.
Edit	Click to edit the traffic rule settings.
Delete	Click to delete the traffic rule.
Add	Click to add a new traffic rule. This button appears at the bottom of the Traffic Rules page.

Add Traffic Rule

To add a traffic rule:

1. Go to Network > Firewall > Traffic Rules.
2. At the bottom of the Traffic Rules table, click **Add**.
3. Enter the configuration settings. See *Table 11-29*.
4. Click **Save**.

Table 11-29 Firewall Traffic Rule Configuration

Parameters	Description
General Settings	
Name	Enter the name of the traffic rule.
Protocol	Select the protocol from the available options. Available options ◆ TCP – Allows only TCP traffic to the open port ◆ UDP – Allows only UDP traffic to the open port ◆ TCP+UDP – Allows both TCP and UDP traffic to the open port
Source zone	Select the traffic source zone. This is usually WAN zone.
Source address	Match incoming traffic from the specified source IP address
Source port	Match incoming traffic from the specified source port
Destination zones	Select the destination firewall zone. If specified the rule applies to forwarded traffic, otherwise it is treated as an input rule.
Destination address	Match incoming traffic directed to the specified destination IP address. If no destination zone is specified, the rule is treated as an input rule.
Destination port	Match incoming traffic directed to the specified destination port.
Action	Sets the target parameter to indicate the firewall action. Options include: ◆ Accept ◆ Reject ◆ Drop ◆ Mark ◆ Notrack.
Advanced Settings	

Parameters	Description
Restrict to address family	Enter the protocol family to generate iptables rules for. Options include: ipv4, ipv6, or any.
Source MAC address	Match incoming traffic from the specified MAC address.
Extra arguments	Enter extra arguments to pass to iptables. This can be used to specify additional match options.
Time Restrictions	
Week Days	If specified, only match traffic during the given days of the week.
Month Days	If specified, only match traffic during the given days of the month.
Start Time (hh.mm.ss)	Specify a time to start matching traffic.
Stop Time (hh.mm.ss)	Specify a time to stop matching traffic.
Start Date (yyyy-mm-dd)	Specify a date to start matching traffic.
Stop Date (yyyy-mm-dd)	Specify a date to stop matching traffic.
Time in UTC	Select to interpret all time values as UTC time instead of local time.

Custom Rules

Network > Firewall > Custom Rules

The shell script allows you to add custom iptable commands that will be executed after the firewall is restarted, immediately after the default ruleset has been loaded.

To configure custom rules:

1. Go to Network > Firewall > Custom Rules.
2. Enter the custom iptable rule command after the commented lines. Each rule should be on a separate line.
3. Click **Save**.

QoS

Network > QoS

QoS allows you to prioritize specific flows in network traffic to manage handling and allocation of network capacity. Assign traffic to target classes and allocate the amount of bandwidth that is given to those classes. QoS service provides the following functionality:

- Configure two to four predefined **classes** with rate, priority, and packet latency (delay) settings
- Configure one or more **interfaces** (WAN, WWAN, LAN, cellular, VPN) with global connection characteristics such as upload and download speed limits. Each interface can have its own buffer.
- Configure **classification rules** to allocate packets to the configured classes (targets). Traffic is differentiated by source and destination IP addresses, protocols, and ports.

You can configure up to four QoS classes, although you can achieve results by configuring as few as two classes. The predefined classes to limit traffic are Priority, Normal, Express, and Bulk, as well as classes to limit ingress traffic, which are appended with the _down suffix. If the classes to limit ingress traffic are configured, then the original classes will limit egress traffic only. Otherwise, if they are not configured, then Priority, Normal, Express, and Bulk will limit both ingress and egress traffic.

To enable QoS:

Enable QoS by interface. Go to Network > QoS > Interfaces.

To configure QoS:

1. Go to Network > QoS.
2. Enter the QoS configuration settings. See *Table 11-30*.
3. To enable QoS, go to the Interfaces tab and select **Enable** to apply QoS to the interface.
4. Click **Save & Apply**.

Table 11-30 QoS Configure Classes

Parameters	Description
Configure Classes	
Name	Class name. ◆ Priority ◆ Express ◆ Normal ◆ Bulk When configured, these classes will limit both egress (outgoing from the host) and ingress (incoming to the host) traffic. Classes to limit ingress traffic: ◆ Priority_down ◆ Normal_down ◆ Express_down ◆ Bulk_down If Priority_down or Normal_down are configured, then Priority or Normal will limit egress traffic only.
Packet Size	Maximum packet size in bytes, up to 1500 bytes.

Parameters	Description
Average Minimum Rate	Average rate for this class, expressed as the percentage of bandwidth
Priority	Priority of the class, expressed as percentage. The sum priority of all classes should not exceed 100.
Packet Delay in ms	The amount of time, in milliseconds, that the packet will wait in queue before it is transmitted.
Max Rate in percentage	Maximum rate, expressed as percentage of total bandwidth
Interfaces	
Name	Displays the name of the interface that QoS will be configured on. Click **Add** to add an interface to the list.
Enable	Select to enable or clear to disable QoS on the interface.
Classification Group	One classification group “Default” is defined.
Calculate Overhead	Select to enable or clear to disable. Decreases upload and download ratio to prevent link saturation.
Half-duplex	Limit the interface to half-duplex mode.
Download Speed (kbit/sec)	Enter the download limit for the interface.
Upload Speed (kbit/sec)	Enter the upload limit for the interface.
Classification Rules	
Target	Select the target class. There can be one rule set for each class. If a target is deleted and you want to configure it, click **Add**.
Source Host	Enter the source IP address or IP and mask (CIDR notation). All packets that match this source host value will be included in the QoS target class.
Destination Host	Enter the destination IP address or IP and mask (CIDR notation). All packets that match this destination host value will be included in the QoS target class.
Protocol	Packets matching this protocol will be included in the target class
Ports	Packets matching this port or range of ports will be included in the target class.
Number of bytes	Packets matching this will be included in the target class.
Comment	Description field.

Load Balancing

Network > Load Balancing

Load balancing is a mechanism that enables balancing traffic between various links. It distributes traffic among various links, optimizing utilization of all the links to accelerate performance and reduce operating costs. Interfaces are assigned a priority by means of a metric.

How it works

Load balancing is determined by the load metric, in other words, the weight. Each link is assigned a relative weight and the gateway distributes traffic across links in proportion to the ratio of weights assigned to each individual link. This weight determines how much traffic will pass through a particular link relative to the other links.

Weights can be selected based on:

- Link capacity (for links with different bandwidth)
- Link/Bandwidth cost (for links with varying cost)

Note: *The default configuration of the load balancer is in Failover Mode with the highest priority given to WAN, then WWAN and then Cellular.*

MWAN Concept

On X300 series gateways, one or more sources of Internet can be used at the same time. In failover mode, the gateway uses one source of Internet and fails over to another according to defined priorities. Once the source with a higher priority is online, the same will be used as a primary source of Internet.

Priority can be defined by setting the metric. The lower the metric, the higher the priority.

The decision of when to failover or rollback is dependent on which interfaces are online and which ones are offline. Online and offline interface status is based on the PING responses to a particular server at a particular time interval. You can speed up the failover by sending PING packets in a shorter interval and you can add reliability by adding multiple server candidates.

Load balancing is where two or more sources of Internet are used at the same time and the load is split between the multiple interfaces in the ratio of their assigned weights.

The gateway supports a feature called WAN affinity whereby a particular source IP, Destination IP or a data type can be bound to a particular interface. To accomplish this, you need to create members which correspond to physical interfaces, assign the members in a particular policy, create rules and assign a policy to the rules.

In summary:

- Members correspond to physical interfaces with an assigned metric and weight
- Policy consists of a member or group of members
- Rules specify which traffic will use a particular policy

Globals

Network > Load Balancing > Globals

To configure MWAN global settings:

1. Go to Network > Load Balancing > Globals.

2. Enter or modify the settings. See *Table 11-31*.
3. Click **Save & Apply**.

Table 11-31 MWAN Globals Configuration

Parameters	Description
Firewall mask	Enter the firewall mask value in hexadecimal, starting with 0x.
Logging	Select to enable global firewall logging and select the log level.
Update Interval	Enter the update interval for the interface routing table. Default is 5 seconds.
Routing table lookup	Enter an additional routing table to be scanned for connected networks

Interfaces

Network > Load Balancing > Interfaces

To view and add MWAN interfaces:

1. Go to Network > Load Balancing.
2. The MWAN Interfaces table is displayed. See *Table 11-32*.
3. Go to the bottom of the table, enter the interface name and click **Add**.
4. Enter the interface settings. See *Table 11-33*.
5. Click **Save & Apply**.

Note: *Configuring a large number of tracking IP addresses, a high ping count, or a low ping interval time will result in faster switchover but will consume more data.*

Table 11-32 MWAN Interface

Parameters	Description
MWAN Interfaces	Displays the interfaces and provides options to add, edit, or delete items from the table. ◆ Enter the interface name (must match an existing interface name) and click **Add** to add member. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Name	Name of the available Interface.
Enabled	Displays the Interface status. Yes for enabled No for disabled
Tracking method	Displays the method used to track the interface.
Tracking source	Displays the tracking source as address or interface.
Tracking reliability	Displays the number of tracking IP addresses. The acknowledgment/ responses from these tracking IP addresses are considered to determine the interface as up or down.
Ping interval	Displays the time in seconds between sending two successive ping packets.

Parameters	Description
Interface down	Displays the number of consecutive failed attempts after which the interface is declared offline.
Interface up	Displays the number of consecutive successful pings after which the interface is declared online.
Metric	Metric assigned to the interface.

Edit MWAN Interface

To edit MWAN interface settings:

1. Go to Network > Load Balancing > Interfaces.
2. To modify an interface, select the interface and click **Edit**.
3. Modify the settings. see *Table 11-33*.
4. Click **Save & Apply**.

Table 11-33 MWAN Interface Configuration

Parameters	Description
Enabled	Enable the Interface. ◆ No – Interface do not participate in Load Balancing. ◆ Yes – Interface is enabled and can connect to Internet. Once enabled it can be tracked using ping configuration.
Initial State	Offline – traffic goes via this interface only if the load balancer has checked the connection first. Online – the interface is marked as online immediately. Default is Online
Internet Protocol	Displays the internet protocol of the interface as IPv4 or IPv6.
Tracking hostname or IP address	IP Address to which the ping requests are sent from the interface to determine if the interface is up or down. Leave the field blank to assume the interface is always online.
Tracking method	Select the tracking method in use. Default is ping.
Tracking source	Select the tracking source to use. Options are Interface or Address
Tracking reliability	Enter the number of responses that must be received from tracking IP Addresses to consider the Interface as up.
Ping count	Enter the number of ping packets that will be sent. The default ping count is 5.
Ping size	Size of the ping request in bytes. Default value is 56.
Max TTL	Displays the Max Time to Live (Max TTL) timer value to be included in the packets that tells the recipient how long to hold or use the packet before expiring or discarding the packet or data.
Check link quality	Select to check link quality otherwise leave box unselected.

Parameters	Description
Ping timeout	Enter the time to wait for a response to ping request sent before declaring the interface unreachable. The wait time is in seconds. The default value depends on the interface used. Cellular will have different values to reduce data consumption.
Ping interval	Specifies the time in seconds between sending ping packets. The default ping interval is 5 seconds.
Interface down	The number of consecutive failed attempts after which the interface is declared down. The default value depends on the interface used. Cellular will have different values to reduce data consumption.
Interface up	The number of consecutive successful attempts to determine the reliability of the network connection through the interface. The default value depends on the interface used. Cellular will have different values to reduce data consumption.
Metric	Displays the Interface Metric. The route with least metric is considered as best route. The default metric assigned to the interface is 1. For load balancing between two interfaces, both the interfaces must have the same metric value on the Member configuration page.

Members

Network > Load Balancing > Members

MWAN Members are profiles corresponding to individual interfaces where you can set metric and weight.

To view and add MWAN members:

1. Go to Network > Load Balancing > Members.
2. The MWAN Members table is displayed. See *Table 11-34*.
3. To add a member profile, at the bottom of the table enter the name and click **Add**.
4. Enter the settings. See *Table 11-35*.
5. Click **Save & Apply**.

Table 11-34 MWAN Members

Parameters	Description
MWAN Members	Displays the members and provides options to add, edit, or delete items from the table. ◆ Enter a name and click **Add** to add member. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table. ◆ The buttons to the left of the Edit button can be used to reorder the items in the list. This does not change the configuration.
Name	Displays the interface member notation number.
Interface	Displays the name of the interface associated with the member.

Parameters	Description
Metric	Displays the metric assigned to the interface. The interface with the lowest metric has the highest priority and all data is always routed through it. ***Note:*** *If two or more interfaces have same metric configured and that metric is lowest compared to other interfaces, then the data/load is balanced and data/load is distributed among the two interfaces in the ratio of the respective weight.*
Weight	Displays the weight assigned to the interface. Members with the same metric will distribute load based on the weight value.
Add	Enter the name of the new interface to be added.

Edit MWAN Member

To edit an MWAN member:

1. Go to Network > Load Balancing > Members.
2. Select the member and click **Edit**.
3. Modify the configuration settings. See *Table 11-35*.
4. Click **Save & Apply**.

Table 11-35 MWAN Members Configuration

Parameters	Description
Interface	Select the name of the interface.
Metric	Enter the interface metric. The route with lowest metric is considered as best route. For load balancing between two interfaces, both the interfaces must have the same metric value.
Weight	Enter the interface weight. The default weight assigned to the interface is 2. For load balancing between two interfaces, both the interfaces must have the same metric value. The route with higher weight carries more traffic. Also the connections will be distributed amongst the interfaces with the same weight and not the actual data traffic.

Policies

Network > Load Balancing > Policies

Policies define how traffic is routed through the different WAN interfaces. Policy consists of a member or group of members. If a policy has one member, traffic will only go out through that member. If a policy has more than one member, members within the policy with a lower metric have precedence and are used first. Members with the same metric will be load balanced based on the assigned weight values.

Policy can also be configured to use one member and then fail over to another.

To view and add MWAN policies:

1. Go to Network > Load Balancing > Policies.

2. The MWAN Policies table is displayed. See *Table 11-36*.
3. To add a policy, at the bottom of the table enter the name and click **Add**.
4. Enter the settings. See *Table 11-37*.
5. Click **Save & Apply**.

Table 11-36 MWAN Policy

Parameters	Description
MWAN Policies	Displays the policies and provides options to add, edit, or delete items from the table. ◆ Enter a name and click **Add** to add policy. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Name	Name of the policy. The name must be 15 characters or less, and may contain characters A-Z, a-z, 0-9, _ and no spaces. Policies must not share the same name as configured interfaces, members or rules.
Members assigned	Interface members to which the policy is applied.
Last resort	Displays the failover routing behavior when all WAN policy members are offline.
Errors	Displays if an error has occurred during the Policy configuration. Error messages are displayed as warnings.

Edit MWAN Policy

To edit MWAN policy:

1. Go to Network > Load Balancing > Policies.
2. Select the policy and click **Edit**.
3. Modify the configuration settings. See *Table 11-37*.
4. Click **Save & Apply**.

Table 11-37 MWAN Policy Configuration

Parameters	Description
Member used	Select the interface to apply the policy on for traffic passing through the interface.
Last Resort	Select the failover routing behavior when all WAN policy members are offline. Available options: ◆ unreachable (reject) ◆ blackhole (drop) ◆ default (use main routing table)

Rules

Network > Load Balancing > Rules

A rule specifies what traffic to match and what policy to assign for that traffic.

The MWAN Rules page displays the rules and provides options to add, edit, or delete items from the table. The Rules page also lists key points to consider when configuring rules.

To add MWAN rules:

1. Go to Network > Load Balancing > Rules.
2. The MWAN Policies table is displayed. See *Table 11-38*.
3. At the bottom of the Rules table, add a rule name and click **Add**.
4. Modify the configuration settings. See *Table 11-39*.
5. Click **Save & Apply**.

Table 11-38 MWAN Rules

Parameters	Description
MWAN Rules	Displays the rules and provides options to add, edit, or delete items from the table. ◆ Enter a name and click **Add** to add rule. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Name	Displays the rule name.
Source address	Displays the Source IP address.
Source port	Displays the Source port number.
Destination address	Displays the Destination IP address.
Destination port	Displays the Destination port number.
Protocol	Displays the protocols on which the rule is applicable.
Policy assigned	Policy to be applied to the rule.
Errors	Displays if an error has occurred during the rule configuration. Error messages are displayed as warnings.

Edit MWAN Rule

To edit MWAN rules:

1. Go to Network > Load Balancing > Rules.
2. Select the rule name and click **Edit**.
3. Modify the configuration settings. See *Table 11-39*.
4. Click **Save & Apply**.

Table 11-39 MWAN Rules Configuration

Parameters	Description
Source address	Enter the Source IP Address.

Parameters	Description
Source Port	Enter the Source Port number.
Destination address	Enter the Destination IP Address.
Destination port	Enter the Destination Port number.
Protocol	Select the protocols on which the rule is applicable.
Sticky	Select Yes to allow traffic from the same source IP address within the timeout limit to use the same WAN interface as the previous session. Otherwise, select No.
Sticky timeout	Enter the stickiness timeout value in seconds. If no value is entered, this defaults to 600.
IPset	Enter the name of the IPset rule. IPset lets you route traffic over WAN interfaces based on a set of IP addresses. When the ipset option is configured, the rule will match traffic directed at the given destination IP address to the ipset set.
Logging	Select Yes to enable firewall logging. The global load balancing logging setting must also be enabled. Otherwise, select No.
Policy assigned	Policy to be applied to the rule.

Notification

Network > Load Balancing > Notification

MWAN Notification lets you write custom MWAN actions, to be executed with each netifd hotplug interface event on interfaces for which MWAN is enabled. The file is interpreted as a shell script, and is preserved during sysupgrade.

The script must start with the line “#!/bin/sh” (without quotation marks).

Commented lines (starting with #) will not be executed.

Three main environment variables are passed to the script. They are described below:

```
# $ACTION
#       <ifup>          Is called by netifd and mwan3track
#       <ifdown>        Is called by netifd and mwan3track
#       <connected>     Is only called by mwan3track if tracking was
                        successful
#      <disconnected> Is only called by mwan3track if tracking has failed

# $INTERFACE           Name of the interface which went up or down
                      (e.g. "wan" or "wwan")

# $DEVICE             Physical device name which interface went up or down
                      (e.g. "eth0" or "wwan0")
```

12: Bluetooth

The X300 series gateways support dual-mode Bluetooth BR/EDR (Classic Bluetooth) and BLE wireless connectivity. The Serial Port Profile (SPP) is included for Bluetooth BR/EDR. Bluetooth SPP allows two Bluetooth devices to connect and exchange serial data using the Bluetooth SPP profile for tunneling.

Bluetooth Settings

The Bluetooth Settings page lets you configure Bluetooth settings and scan for and pair to Bluetooth devices.

Configure Bluetooth settings

To configure Bluetooth settings:

1. Go to Bluetooth > Settings.
2. Next to Bluetooth State, select or clear the box to enable or disable Bluetooth.
3. Enter the configuration settings. See *Table 12-1*.

Table 12-1 Bluetooth Settings Configuration

Parameters	Description
Bluetooth State	Select to enable or clear to disable Bluetooth.
Device name	Displays the Bluetooth device name. The name can be edited. ***Note:*** *Changing the device name will disconnect any existing Bluetooth SPP master or slave connections.*
Device Address	Displays the Bluetooth device address.
Paired devices	Displays the paired devices. Click **Unpair** to unpair the device.
Allow Discovery	Select to allow the gateway to be visible to other Bluetooth devices during a scan. Clear the box if you do not want the gateway to be visible to other Bluetooth devices during a scan.
Scan	Click **Scan** to scan for nearby discoverable Bluetooth devices. A device must be discoverable in order to pair to it.

4. Click **Save & Apply**.

Scan for and Pair a Device

To scan for and pair to nearby devices:

1. On the Bluetooth Settings page under Scan, click **Scan**. The scan will take a few seconds to complete.
2. The Bluetooth Scan Result page shows the discovered devices and contains the following details:

Table 12-2 Bluetooth Scan Results

Parameters	Description
Device Address	Displays the Bluetooth device address.
Device Name	Displays the Bluetooth device name.
Type	Displays the Bluetooth service type that the device advertises. BR/EDR – the device advertises Bluetooth BR/EDR service type and supports SPP. BLE (Public or Random) – the device advertises BLE service type.
RSSI	Displays the signal strength of the Bluetooth device.
Pair	Click **Pair** to pair the device. The device that initiates the pairing, in this case the X300 series gateway, acts as the master device, and the paired device acts as the slave device.
Refresh	Click **Refresh** to run the scan again.
Dismiss	Click **Dismiss** to close this page.

3. Click **Pair**.

   The paired device appears under Paired devices.

To unpair a device:

1. On the Bluetooth Settings page under Paired Devices, view the paired devices.
2. In the row containing the device to be unpaired, click **Unpair**.

Bluetooth SPP

Bluetooth SPP page allows you to configure the Bluetooth SPP connection and tunnel.

To use Bluetooth SPP, the Bluetooth device and the gateway must first be paired. The master device makes the RFCOMM connection. Once the Bluetooth connection is established, you should configure a tunnel on the Bluetooth SPP line to enable serial data transmission.

Either device in the Bluetooth connection can be the master or the slave, and either can be the tunnel server or client.

The following describes the Bluetooth SPP roles:

- Master – The master is the device that initiates the pairing with the other Bluetooth device. The master device can:
  - establish the RFCOMM connection with the paired device
  - disconnect the RFCOMM connection
  - be configured in tunnel accept (server) or tunnel connect (client) mode
- Slave – The slave is the device that is paired. The slave device can:
  - disconnect the RFCOMM connection
  - be configured in tunnel accept (server) or tunnel connect (client) mode

Configure Bluetooth SPP Connection

To configure the Bluetooth SPP connection:

1. Select the Master 1 or Slave tab depending on whether the gateway is the master or slave device.
2. Enter the line configuration settings. See *Table 12-3*.
3. To establish the connection, click the RFCOMM **Connect** button. To end a connection, click the **Disconnect** button.

Table 12-3 Bluetooth SPP Line Configuration

Parameters	Description
Name	Displays the line name. The name can be edited.
State	Select to enable or clear to disable the line.
Protocol	Select the protocol. ◆ Tunnel – the line will use tunnel over Bluetooth SPP connection. Tunnel will use the settings configured under the Server or Client tab to select tunnel accept or tunnel connect mode. ◆ None – no protocol will be used.
Gap Timer	Set the number of milliseconds to delay from the last character received before the driver forwards the received serial bytes. By default, the delay is four character periods at the current baud rate (minimum 1 msec). Gap timer range is 1 to 5000 milliseconds (default value is 4000 msec).
Threshold	Enter the number of threshold bytes which need to be received in order for the driver to forward received characters. Default value is 56 bytes.
RFCOMM	Click **Connect** to establish the connection or **Disconnect** to end the connection. The master device can connect and disconnect, while the slave device can only disconnect.

Configure Tunnel SPP Slave

To configure the Tunnel SPP Slave:

1. Go to Tunnel > Tunnel SPP Slave.
2. Enter the Accept configuration if the connection attempt originates from the network (see Table 17-2, “Tunnel Accept Mode Configuration,” on page 191), or enter the Connect configuration if the connection attempt originates from the gateway (Table 17-3, “Tunnel Connect Mode Configuration,” on page 194)
3. Click **Save & Apply**.
4. On the remote device, configure the tunnel server or client settings appropriate for the connection.

Configure Tunnel SPP Master

To configure the Tunnel SPP Master:

1. Go to Tunnel > Tunnel SPP Master.
2. Enter the Accept configuration if the connection attempt originates from the network (see

Table 17-2, “Tunnel Accept Mode Configuration,” on page 191), or enter the Connect configuration if the connection attempt originates from the gateway (Table 17-3, “Tunnel Connect Mode Configuration,” on page 194)

3. Click **Save & Apply**.
4. On the remote device, configure the tunnel server or client settings appropriate for the connection.

13: ConsoleFlow

The X300 series gateways come integrated with ConsoleFlow® cloud platform to allow for the remote management of devices. To set up the ConsoleFlow client, you need to configure the following settings:

- ConsoleFlow Client – to connect to the ConsoleFlow cloud platform.
- Line 1 and Line 2 – to enable remote management and data access to your application or device attached on the serial line.

Client

To configure the ConsoleFlow client:

1. Go to ConsoleFlow > Line 1.

   This page displays the configuration and status for the ConsoleFlow client.

2. Enter the client and connection configuration information. See *Table 13-1*.
3. Click **Save & Apply**.

Table 13-1 ConsoleFlow Client Configuration

ConsoleFlow Client	Description
Enable	Select to enable or clear to disable the ConsoleFlow client.
Device ID	Read only. Displays the gateway's Device ID. Device ID may be provisioned through Lantronix Provisioning Manager. ***Note:*** *Device ID can only be provisioned once. It will persist across resets.*
Serial Number	Read only. Displays the serial number of the device.
Device Name	Enter the ConsoleFlow Device Name.
Device Description	Enter the ConsoleFlow Device Description.
Status Update Interval	Enter the frequency that the gateway updates the device status to ConsoleFlow. The valid range is between 1 minute and 1440 minutes (1 day).
Content Check Interval	Enter the frequency that the gateway checks ConsoleFlow for updates to configuration or firmware. The valid range is between 1 hour and 2160 hours (90 days).
Apply Firmware Updates	Select to allow firmware updates to be applied via ConsoleFlow. Enabled by default.
Apply Configuration Updates	Select the option to indicate when to apply configuration updates. ◆ **Always**: signifying configuration updates will always apply. ◆ **Never**: never apply configuration updates.
Reboot After Update	Automatically reboot device after configuration update.
Allow Remote Connections	Select to allow remote connections or clear to disable. Enabled by default.
Remote Access Local Port	Local port for remote access connection

ConsoleFlow Client	Description
Active Connection	Select the connection instance to use when connecting to ConsoleFlow. You can configure two connections. The configuration options for Connection 1 and Connection 2 are listed below.
Connection 1/Connection 2	
Connect to	Select Cloud or On-premise connection.
Host	Enter the host name or IP address of the ConsoleFlow server, used to register the device.
Port	Enter the ConsoleFlow port. Default: 443
Secure Port	Select to enable or clear to disable the ConsoleFlow client secure port 443.
Validate Certificates	Select to enable or clear to disable the validation of the ConsoleFlow server certificates. To validate certificates, both MQTT Security and Secure Port must be enabled.
Local Port	Local port for Consoleflow MQTT client. When configured, a total of 32 consecutive ports will be reserved.
Enable MQTT	Select to enable or clear to disable MQTT.
MQTT Host	Hostname or IP address of MQTT server.
MQTT Port	Enter the port number of the ConsoleFlow MQTT server. When configured, a total of 32 consecutive ports will be reserved.
MQTT Security	Select to enable SSL for MQTT.
MQTT Local Port	Local port for ConsoleFlow MQTT client. When configured, a total of 32 consecutive ports will be reserved.
Use Proxy	Select to enable the use of a proxy for this connection. If enabled, complete the proxy fields displayed under the Use Proxy field. Disabled by default.
Proxy Type	Proxy server type. The supported type is SOCKS5.
Proxy Host	Hostname or IP address of the proxy server to be used.
Proxy Port	Port of the proxy server to be used. Default port is **80**.
User Name	Username for the proxy server.
Password	Password for the proxy server.

ConsoleFlow Line

Configure ConsoleFlow Line settings to enable remote management and data access to your application or device attached on the serial line. The gateway offers 1 (one) line for configuration.

To configure ConsoleFlow Line settings:

1. Go to ConsoleFlow > Line 1.

   This page displays the configuration and status for ConsoleFlow Line.

2. Enter the following information. See *Table 13-2*.
3. Click **Save & Apply**.

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

Table 13-2 ConsoleFlow Line

ConsoleFlow Line	Description
Enable	Select to enable or clear to disable the ConsoleFlow line client.
Project Tag	Enter the ConsoleFlow project tag string, as provided by the ConsoleFlow project administrator.
Status Update Interval	Enter the frequency in minutes that the gateway updates the device status to ConsoleFlow. The valid range is between 1 minute and 1440 minutes (1 day).
Content Check Interval	Enter the frequency in hours that the gateway checks ConsoleFlow for updates to configuration or firmware. The valid range is between 1 hour and 2160 hours (90 days).
Command Delimiter	Enter the command delimiter for attached serial devices. **Note:** *Send delimiter before command and after response is received.*

14: Discovery

Network discovery allows your computer to locate other computers and devices on the network. This setting also allows other computers to see your computer. If enabled, the device responds to auto-discovery messages on port 0x77FE.

Query Port

This page displays the current query port statistics and the configuration option to enable or disable discovery.

Query port is enabled by default.

To enable or disable query port discovery:

1. Go to Discovery > Query Port.
2. Under Configuration, select or clear **Enable**.
3. Click **Save & Apply**.

15: Serial

The X300 series gateways offer one serial port that uses a standard RS-232 interface. Serial settings such as baud rate, parity, data bits, stop bits, and flow control apply to this line.

For wiring configuration details for the RS-485 port in half-duplex mode, see *B: Power Cable Schematic.*

The default serial settings:

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

Serial Line Statistics

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

To view line statistics, go to Serial and select Serial 1.

Serial Line Configuration

To configure Serial line settings:

1. Go to Serial > Serial 1.
2. Enter the line configuration settings. See *Table 15-1*.
3. Click **Save & Apply**.

Table 15-1 Serial Line Configuration

Parameters	Description
Name	Descriptive name.
Enabled	Select to enable the line on the serial port.
Interface	◆ RS232. ◆ RS485 Half-Duplex ◆ RS485 Full-Duplex
Termination	Termination of the RS485 bus, if available. ◆ Enabled ◆ Disabled
Is baudrate custom	If using a custom baud rate, select the box and add a value between 2400 bps and 921600 bps.

Parameters	Description
Baud Rate	Select the desired baud rate from the drop-down list. Baud rate options: 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600
Parity	Select parity from the drop-down list: ◆ None ◆ Even ◆ Odd
Data Bits	Select data bits from the drop-down list: ◆ 7 ◆ 8
Stop Bits	Select the stop bits from the drop-down list. ◆ 1 ◆ 2
Flow Control	Select the flow control from the drop-down list. ◆ None ◆ Hardware ◆ Software
Gap Timer	Set the number of milliseconds to delay from the last character received before the driver forwards the received serial bytes. By default, the delay is four character periods at the current baud rate (minimum 1 msec). Gap timer range is 1 to 5000 milliseconds (default value is 4000 msec).
Threshold	Set the number of threshold bytes which need to be received in order for the driver to forward received characters. Default value is 56 bytes.
Mode	Select the mode of serial communication: ◆ None – can be used if ConsoleFlow line is configured ◆ Tunnel – (see *Chapter 17: Tunnel*) ◆ Tunnel/Modbus RTU to Modbus TCP – (see *Tunnel Modbus RTU to Modbus TCP*) ◆ Managed Device

16: SSL

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

SSL certificates identify the X300 series gateway to peers and are used with some methods of wireless authentication. Provide a name at upload time to identify certificates on the gateway.

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

Credentials

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

To configure a new credential:

1. Go to SSL > Credentials.
2. Type the name for your credential in the Credential Name field.
3. Enter the fields under Upload Certificate (see *Table 16-1*) or Create New Self-Signed Certificate (see *Table 16-2*).
4. Click **Save & Apply**. The process to create a self-signed certificate can take up to 30 seconds, depending on the length of the key.

   The newly created credential is displayed at the top of the SSL Credentials page.

To view a credential:

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

To delete a credential:

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

Table 16-1 SSL Credentials - Upload Certificate

Field	Description
SSL Certificate	Click the **Select file...** button to browse to the SSL certificate to be uploaded. RSA or DSA certificates are allowed.

Field	Description
Certificate Type	Select the certificate type to upload: ◆ PEM ◆ PKCS7 ◆ PKCS12 For PKCS certificates, enter a password. Ensure that the certificate is formatted properly with a valid open and close tag.
SSL Private Key	Click the **Select file...** button to browse to the SSL private key to be uploaded. The key must belong to the entered certificate. Ensure that the private key associated to the selected certificate and that it is formatted properly with a valid open and close tag.
Key Type	Select the key type being uploaded: ◆ PEM ◆ Encrypted PEM ◆ PKCS12 For encrypted PEM or PKCS12 key types, enter a password.

Table 16-2 SSL Credentials - Create Self-Signed Certificate

Field	Description
Country (2 Letter code)	Enter the 2 letter code for the country where the organization is located. This is a two-letter ISO code (e.g., “US” for the United States).
State/Province	Enter the state or province where the organization is located.
Locality (City)	Enter the city where the organization is located.
Organization	Enter the organization name to which the gateway belongs.
Organization Unit	Enter the organization unit which specifies the department or organization to which the gateway belongs.
Common Name	Enter a network name for the gateway when installed in the user’s network (usually the fully qualified domain name). It is identical to the name that is used to access the gateway with a web browser without the prefix `http://`. In case the name given here and the actual network name differ, the browser will pop up a security warning when the gateway is accessed using HTTPS.
Expires	Type the date that the self-signed certificate expires in **mm/dd/yyyy** format.
Type	Select **RSA**, **DSA**, or **ECDSA**.
Key length	Select the key length in bits.

Trusted Authorities

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

To upload an authority certificate:

1. Go to SSL > Trusted Authorities.

2. Enter the Upload Certificate fields. See *Table 16-3*.
3. Click **Save & Apply**.

Table 16-3 SSL Trusted Authority

Field	Description
SSL Certificate	Click the **Select file...** button to browse to an existing SSL authority certificate. RSA or DSA certificates are allowed. The format of the authority certificate can be PEM or PKCS7. PEM files must start with "`-----BEGIN CERTIFICATE-----`" and end with "`-----END CERTIFICATE-----`". Some certificate authorities add comments before and/or after these lines. Those comments must be deleted before upload.
Certificate Type	Select the certificate type through the drop-down list. This field may automatically update, depending upon extension of the certificate entered.
Clear	Click to clear the fields.

To delete an existing certificate authority:

1. Go to SSL > Trusted Authorities.
2. Under Current Certificate Authorities, click the **Delete** button next to the name of the authority.

17: Tunnel

Tunneling allows serial devices to communicate over a network without being aware of the devices that establish the network connection between them. The Tunnel settings allow you to configure how the serial network tunneling operates. Tunneling is available on the serial line.

Tunnel Statistics

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

To view tunnel statistics, go to Tunnel and select Tunnel 1, Tunnel SPP Slave, or Tunnel SPP Master.

Tunnel Modbus RTU to Modbus TCP

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

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

To configure the serial interface:

1. Go to Serial and select Serial 1.
2. Configure the serial port settings.
3. Select Mode as Tunnel/Modbus RTU to Modbus TCP.
4. Click **Save & Apply**.

To configure the TCP interface:

1. Go to Tunnel and select Tunnel 1.
2. Under Modbus RTU to Modbus TCP, select **Enable** and then enter the configuration settings. See *Table 17-1*
3. Click **Save & Apply**.

Table 17-1 Tunnel for Modbus RTU to Modbus TCP

Field	Description
Enable	Select to enable and configure the Modbus RTU to Modbus TCP settings.
Protocol	TCP option is selected.
Mode	◆ **Server** - the gateway acts as a server and listens for the TCP connection from the external Modbus master. TCP Port number is required. ◆ **Client** - the gateway acts as a TCP client and sends the TCP connection request to the external Modbus master. The IP address and TCP port of the Modbus master is required.

Field	Description
IP	IP address of the external Modbus master on the LAN or WAN interface.
Port	Modbus TCP port number that the server is listening on. The default Modbus TCP port number is 502.
Backup Server Enable	If client mode is selected, select the box to configure a backup Modbus master. Enter the backup server's IP address and port number.
Socket Timeout Enable	Select to configure socket timeout. Enter the inactivity timeout period in seconds.

Tunnel Accept

In Accept mode, the gateway listens (waits) for incoming connections from the network.

A remote node on the network initiates the connection. The configurable local port is the port that the remote device connects to for this connection. There is no remote port or address. Serial data can still be received while waiting for a network connection, keeping in mind serial data buffer limitations.

To configure Accept mode:

1. Go to Tunnel > Tunnel 1, Tunnel SPP Slave, or Tunnel SPP Master.
2. Under Accept, enter the Accept mode configuration settings.
3. Click **Save & Apply**.

Table 17-2 Tunnel Accept Mode Configuration

Field	Description
Mode	Set the method used to start a tunnel in Accept mode. ◆ **Disable** – do not accept an incoming connection. ◆ **Always** – accept an incoming connection (*default*). ◆ **Any Character** – start waiting for an incoming connection when any character is read on the serial line. ◆ **Start Character** – start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. Use the default Start Character <control>B, or enter a custom start character. The Flush Start Character setting flushes the start character when a new connection is made.
Local Port	Set the port number for use as the network local port. The default local port number correlates with the tunnel instance. ◆ Tunnel 1: 10001 ◆ Tunnel SPP Slave: 10002 ◆ Tunnel SPP Master: 10003

Field	Description
Protocol	Select the desired security protocol: ◆ SSL ◆ TCP (*default protocol*) ◆ TCP AES ◆ Telnet Configure the protocol fields as determined by the protocol selection.
Secure Protocols	When using SSL, select the secure protocols and the SSL credential. This configuration field becomes available when Protocol options are: ◆ SSL3 ◆ TLS1.0 ◆ TLS1.1 (default selected) ◆ TLS1.2 (default selected) ◆ TLS1.3 (default selected)
TCP Keep Alive	The TCP keep alive time is the time in which probes are periodically sent to the other end of the connection to ensure the other side is still connected. Enter the TCP Keep Alive time in milliseconds. Set to 0 to disable TCP Keep Alive, and blank the field to restore the default.
TCP Keep Alive Interval	Enter the time, in milliseconds, to wait between Keep Alive probes in order to keep the TCP connection up during idle transfer periods. Blank the display field to restore the default.
TCP Keep Alive Probes	Enter the number of TCP Keep Alive probes to send before closing the connection if no response is received. The probes are sent after the initial TCP Keep Alive probe is sent. Valid values are between 1 and 16. Blank the field to restore the default.
AES Encrypt Key	Enter the AES Encrypt Key. This configuration field becomes available when the TCP AES protocol is selected.
AES Encrypt Key Type	Select **Text** or **Hexadecimal** to indicate format. This configuration field becomes available when the TCP AES protocol is selected.
AES Decrypt Key	Enter the AES Decrypt Key. This configuration field becomes available when the TCP AES protocol is selected.
AES Decrypt Key Type	Select **Text** or **Hexadecimal** to indicate format. This configuration field becomes available when the TCP AES protocol is selected.

Field	Description
Initial Send	Enter the **Initial Send** data to be sent out the network upon connection establishment before any data from the Line. It may contain one or more **Directives** of the form `%<char>`. The Initial Send string can be entered in **Text** or **Binary** form. The Binary form allows square braces `[]` to enclose one or more character designations separated by commas. Use straight decimal numbers up to 255 or hexadecimal numbers prefixed with `0x` up to `0xFF` within the square braces. To specify an open brace in binary mode, use two in a row. Example The selection (in binary mode): `AB[255,0xFF]C[[D]` results in a string containing binary values where the dots appear: `AB...C[D]` **Directives** ◆ `%i` local IP address ◆ `%m` MAC address ◆ `%n` network interface name ◆ `%p` local port ◆ `%s` serial number ◆ `%%` %
Initial Send Type	The format of the initial send data. ◆ **Text** ◆ **Binary**
Flush Serial	Set whether the serial line data buffer is flushed upon a new network connection. Choices are: ◆ **Enabled** – serial data buffer is flushed on network connection ◆ **Disabled** – serial data buffer is not flushed on network connection (*default*)
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ◆ **Enabled** – if Enabled, incoming characters from the serial line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the serial line if hardware or software flow control is configured. ◆ **Disabled** – this is the default setting; incoming characters from the serial line are sent on into the network. Any buffered characters are sent first.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: ◆ **Enabled** – if Enabled, incoming characters from the network will not be forwarded to the serial line. Instead, they will be buffered and will eventually flow off the network side. ◆ **Disabled** – this is the default setting; incoming characters from the network are sent on into the serial line. Any buffered characters are sent first.
Password	The password can be up to 31 characters in length. Valid characters are alphanumeric characters and punctuation. When set, clients must send the correct password string to the device within 30 seconds from opening network connection in order to enable data transmission. The password sent to the device must be terminated with one of the following: ◆ 0A (Line Feed) ◆ 00 (Null) ◆ 0D 0A (Carriage Return/Line Feed) ◆ 0D 00 (Carriage Return/Null) If, **Prompt for Password** is set to **Enabled** and a password is provided, the user will be prompted for the password upon connection.

Tunnel Connect

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

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

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

To configure Tunnel Connect mode:

1. Go to Tunnel > Tunnel 1.
2. Under Connect, enter the connect mode configuration settings. See *Table 17-3*.
3. Under Connect Host, configure 1 to 4 Hosts. See *Table 17-4 Host Configuration*.
4. Click **Save & Apply**.

Table 17-3 Tunnel Connect Mode Configuration

Field	Description
Connect Mode	Set the method to be used to attempt a connection to a remote host or device. Choices are: ◆ **Disable** – an outgoing connection is never attempted. (*default*) ◆ **Always** – a connection is attempted until one is made. If the connection gets disconnected, the gateway retries until it makes a connection. ◆ **Any Character** – a connection is attempted when any character is read on the serial line. ◆ **Start Character** – a connection is attempted when the start character for the selected tunnel is read on the serial line.
Host Mode	If more than one host is configured, set the method to be used to access multiple hosts. **Sequential –** A tunnel will connect to hosts in sequential order. Host 1 will be attempted first. If that fails, it will proceed in order to Host 2, 3, and then 4. When a connection drops, the cycle starts again with Host 1 and proceeds in order. (default setting) **Simultaneous –** A tunnel will connect to all hosts accepting a connection. Simultaneous connections occur at the same time to all listed hosts. The gateway supports a maximum of 4 host connections.
Local Port	Enter an alternative local port. The local port is set to <Random> by default but can be overridden. Blank the field to restore the default.
Reconnect Timer	Set the value of the reconnect timeout (in milliseconds) for outgoing connections established by the gateway. Valid range is 1 to 65535 milliseconds. Default is 15000.

Field (continued)	Description
Flush Serial	Set whether the serial line data buffer is flushed upon a new network connection. Choices are: ◆ **Enabled** – serial data buffer is flushed on network connection ◆ **Disabled** – serial data buffer is not flushed on network connection (*default*)
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ◆ **Enabled** – If Enabled, incoming characters from the serial line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the serial line if hardware or software flow control is configured. ◆ **Disabled** – this is the default setting; incoming characters from the serial line are sent on into the network. Any buffered characters are sent first.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: ◆ **Enabled** – If Enabled, incoming characters from the network will not be forwarded to the serial line. Instead, they will be buffered and will eventually flow off the network side. ◆ **Disabled** – this is the default setting; incoming characters from the network are sent on into the serial line. Any buffered characters are sent first.

Hosts

The Connect mode supports up to 4 hosts. Hosts may be accessed sequentially or simultaneously.

Notes:

Configure the keep alive timeout to be larger than the user timeout.

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

The user timeout will not be an exact limit; in practice, it will always take somewhat longer for the connection to be closed.

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

Table 17-4 Host Configuration

Host Field	Description
Address	Enter the destination IP address for the connection.

Host Field	Description
Port	Enter the TCP or UDP port number on the target host for the connection.
Protocol	Select the desired security protocol. ◆ SSL ◆ TCP ◆ TCP AES ◆ Telnet ◆ UDP ◆ UDP AES Configure the remaining protocol fields as determined by the protocol selection.
Secure Protocols	When using SSL, select the secure protocols and the SSL credential. Protocol options are: ◆ SSL3 ◆ TLS1.0 ◆ TLS1.1 (default selected) ◆ TLS1.2 (default selected) ◆ TLS1.3 (default selected)
TCP Keep Alive	Enter the time, in milliseconds, the gateway waits during a silent TCP connection before the first Keep Alive probe is sent to the remote host in order to keep the TCP connection up during idle transfer periods. Set to 0 to disable TCP Keep Alive, and blank the field to restore the default.
TCP Keep Alive Interval	Enter the time, in milliseconds, to wait between Keep Alive probes in order to keep the TCP connection up during idle transfer periods. Blank the display field to restore the default.
TCP Keep Alive Probes	Enter the number of TCP Keep Alive probes to send before closing the connection if no response is received. The probes are sent after the initial TCP Keep Alive probe is sent. Valid values are between 1 and 16. Blank the field to restore the default.
TCP User Timeout	Specify the amount of time the TCP segments will be retransmitted before the connection is closed.
AES Encrypt Key	Enter the AES Encrypt Key. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
AES Encrypt Key Type	Select **Text** or **Hexadecimal** to indicate format
AES Decrypt Key	Enter the AES Decrypt Key. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
AES Decrypt Key Type	Select **Text** or **Hexadecimal** to indicate format
Initial Send	Enter the Initial Send character to be sent out the network upon connection establishment before any data from the Line. It may contain one or more **Directives** of the form `%<char>`. This configuration field becomes available when the TCP, UDP, or UDP AES protocol is selected.
Initial Send Type	Select **Text** or **Hexadecimal** to indicate format.
Credentials	If SSL is the selected protocol, select an existing credential from the drop-down list. Go to SSL > Credentials to create, view, or edit SSL credentials. See *Credentials on page 187*.
Validate Certificate	Select to enable validation of the SSL certificate on the server. This configuration field becomes available when the SSL protocol is selected.

Connecting Multiple Hosts

The Connect Mode supports up to 4 hosts. Hosts may be accessed sequentially or simultaneously.

- **Sequential** – A tunnel will connect to hosts in sequential order. The host specified as Host 1 will be attempted first. If that fails, it will proceed to Host 2, 3, and 4. When a connection drops, the cycle starts again with Host 1 and proceeds in order. Sequential is the default Host Mode.
- **Simultaneous** – A tunnel will connect to all hosts accepting a connection. Simultaneous connections occur at the same time to all listed hosts. The gateway can support a maximum of 4 connections.

Tunnel Disconnect

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

To configure Disconnect settings:

1. Go to Tunnel > Tunnel 1, Tunnel SPP Slave, or Tunnel SPP Master.
2. Under Disconnect, enter the configuration settings.
3. Click **Save & Apply**.

Table 17-5 Tunnel Disconnect Configuration

Field	Description
Stop Character	Enter the Stop Character which, when received on the serial line, disconnects the tunnel. The Stop Character may be designated as a single printable character or as a control character. Control characters may be input in any of the following forms: `<control>J` or `0xA` (hexadercimal) or `\10` (decimal). To disable the Stop Character, blank the field, which sets it to <None>.
Flush Stop Character	Set whether to flush the stop character when the tunnel is disconnected. Options: ◆ **Enabled** ◆ **Disabled** (default)
Timeout	Enter the number of milliseconds a tunnel may be idle before disconnection. To disable the timeout, set the field to zero (0).
Flush Serial Data	Set whether to flush the Serial Line when the Tunnel is disconnected. Choices are: ◆ **Enabled** ◆ **Disabled** (default)

A: Compliance Information

(According to ISO/IEC Guide and EN 45014)

Manufacturer's Name & Address:

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

Product Family:

X300 Series

Conforms to the following standards or other normative documents:

Table A-1 Regional Certifications

Country /	Specification
USA	FCC 47 CFR part 15 Subpart B FCC 47 CFR part 15 Subpart 22H, 24E, 27 & 90 FCC 47 CFR Part 15 Subpart E
Canada	ISED RSS-130 Issue 2 RSS-132 Issue 3 RSS-133 Issue 6 RSS 139 Issue 3
EU	EU Declaration of Conformity See *Figure A-1*.
Australia, New Zealand	AS/NZS CISPR 32:2015
Safety	UL/EN 62368-1 CAN/CSA C22.2 62368-1-14
Cellular Certification	PTCRB, AT&T

Table A-2 Country Transmitter IDs

Country	Specification
USA FCC ID	Cellular Module: ◆ X303F202S: R68X303 ◆ X304G00AS: R68X304 Wi-Fi Module: TLZ-CM2XXNF
Canada IC ID	Cellular Module: ◆ X303F202S: 3867A-X303 ◆ X304G00AS: 3867A-X304 Wi-Fi Module: 6100A-CM2XXNF

FCC Statement

Federal Communication Commission Interference Statement

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

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

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

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

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

Operations are restricted to indoor usage only.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Antenna Installation

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and

2) The transmitter module may not be co-located with any other transmitter or antenna.

ISED Statement

This device complies with RSS-247 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-247 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This device is intended only for use under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and

2) The transmitter module may not be co-located with any other transmitter or antenna.

Cet appareil est conçu uniquement pour les intégrateurs OEM dans les conditions suivantes: (Pour utilisation de dispositive module)

1) L'antenne doit être installée de telle sorte qu'une distance de 20 cm est respectée entre l'antenne et les utilisateurs, et

2) Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

EU Declaration of Conformity

Figure A-1 X300 / X303 EU Declaration of Conformity

LANTRONIX®

CE

EU DECLARATION OF CONFORMITY

EU-type examination certificate no.

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

Product Type: Gateway
Product Family: X300 Series
Model name: X303F202S, X300F202S
Rated: 9-30 VDC
Intended use: Commercial installations, indoor use
Modules: B+C
Notified Body: Telefication B.V.
Notified Body number: 0560

Manufacturer's Quality System:

TÜVRheinland

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

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)
- EN 62368-1:2014/A11:2017

EMC Directive (2014/30/EU)
- EN 301 489-1 V2.2.3 (2019-11)
- EN 301 489-17 V3.2.4 (2019-11)
- Draft EN 301 489-52 V1.1.2 (2020-12)
- EN 61000-3-2:2019
- EN 61000-3-3:2013+A1:2019
- EN 55032:2015/A11:2020

RF Radio Directive (2014 / 53 / EU)
- EN 301 908-1 V13.1.1 (2019-11)
- EN 301 908-13 V13.1.1 (2019-11)
- EN 301 511 V12.5.1 (2017-03)
- EN 300 328 V2.2.2 (2019-07)
- EN 301 893 V2.1.1 (2017-05)

Healthy Directive (2014 / 53 / EU)
- EN 62311:2020

RoHS
1) 2011/65/EU Restriction of the use of Hazardous Substances in EEE (RoHS)
2) 2015/863/EU Change of Annex II from 2011/65/EU
3) Directive 2018/736/EU and 2018/741/EU
- EN 63000-2018

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

Signature: _____ Date: May 6, 2022

Name: _____ Fathi Hakam _____ Title: VP of Engineering

CERT-00XXX rev A

Figure A-2 X304 EU Declaration of Conformity

EU DECLARATION OF CONFORMITY

Certificate no.222140460/AA/00

Manufacturer's Name: LANTRONIX INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 USA
Product Type: X300 Series IOT Cellular Gateway
Product Family: X304G002S, X304xxxxx (x can be any character or blank)
Rated: 9-30VDC
Intended use: Commercial installations, indoor use

Manufacturer's Quality System:

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

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)
- **EN 62368-1:2020+A11:2020**

EMC Directive (2014/53/EU)
- **EN 301 489-1 V2.2.3**
- **EN 301 489-17 V3.2.4**
- **EN 301 489-19 V2.2.0**
- **EN 301 489-52 V1.2.1**
- **EN 55032:2015+A11:2020 class A**
- **EN 55035:2017+A11:2020**
- **EN 61000-3-2:2014**
- **EN 61000-3-3:2013**
- **EN 61000-4-2:2009**
- **EN 61000-4-3:2006+A1:2008+A2:2010**
- **EN 61000-4-4:2012**
- **EN 61000-4-5:2014+A1:2017**
- **EN 61000-4-6:2014+AC:2015**
- **EN 61000-4-11:2004+A1:2017**

RF Radio Directive (2014 / 53 / EU)
- **EN 303 413 V1.2.1**
- **EN 300 328 V2.2.2**
- **EN 301 893 V2.1.1**
- **EN 301 908-1 V15.1.1**
- **EN 301 908-2 V11.1.1**
- **EN 301 908-13 V11.1.1**
- **EN 62311:2020**

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

1) 2011/65/EU Restriction of the use of Hazardous Substances in EEE (RoHS)
2) 2015/863/EU Change of Annex II from 2011/65/EU
3) Directive 2018/736/EU and 2018/741/EU
EN 6300-2018

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

Signature: _____ Date: August 30, 2022

Name: _____Fathi Hakam _____ Title: VP of Engineering

CERT-DoC X304 rev A

Figure A-3 X304 UKCA Declaration of Conformity

UKCA DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX INC.
Manufacturer's Address: 48 Discovery, Suite 250, Irvine, CA 92618 USA
Product Type: X300 Series IOT Cellular Gateway
Product Family: X304G002S, X304xxxxx (x can be any character or blank)
Rated: 9-30VDC
Intended use: Commercial installations, indoor use

Manufacturer's Quality System:

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

Safety
- **BS EN 62368-1:2020+A11:2020**
- **EN 62368-1:2020+A11:2020**

EMC
- **EN 301 489-1 V2.2.3**
- **EN 301 489-17 V3.2.4**
- **EN 301 489-19 V2.2.0**
- **EN 301 489-52 V1.2.1**
- **BS EN 55032:2015+A11:2020 class A**
- **EN 55032:2015+A11:2020 class A**
- **BS EN 55035:2017+A11:2020**
- **EN 55035:2017+A11:2020**
- **EN 61000-3-2:2014**
- **EN 61000-3-3:2013**
- **EN 61000-4-2:2009**
- **EN 61000-3:2006+A1:2008+A2:2010**
- **EN 61000-4-4:2012**
- **EN 61000-4-5:2014+A1:2017**
- **EN 61000-4-6:2014+AC:2015**
- **EN 61000-4-11:2004+A1:2017**

RF
- **EN 303 413 V1.2.1**
- **EN 300 328 V2.2.2**
- **EN 301 893 V2.1.1**
- **EN 301 908-1 V15.1.1**
- **EN 301 908-2 V11.1.1**
- **EN 301 908-13 V11.1.1**
- **EN 62311:2020**

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

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

Signature: _____ Date: August 29, 2022

Name: _____Fathi Hakam_____ Title: VP of Engineering

EU Statements

Table A-3 EU Statements

Code	Language	Statement
bg	Bulgarian	Lantronix, Inc., декларира, че този X300 Series отговаря на основните изисквания и други приложими разпоредби на Директива 2014/53 / ЕС. Пълният текст на декларацията на ЕС за съответствие е достъпен на следния интернет адрес: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Известие на ЕС за ограничения при употреба: Това устройство е ограничено само за вътрешна употреба. Може да не се работи на открито.
cs	Česky [Czech]	Lantronix, Inc. tímto prohlašuje, že tento X300 Series je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU. Úplné znění ES prohlášení o shodě je k dispozici na této internetové adrese: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Oznámení EU o omezení používání: Toto zařízení je omezeno pouze na použití uvnitř. Nesmí být provozován venku.
da	Dansk [Danish]	Undertegnede Lantronix, Inc. erklærer herved, at følgende udstyr X300 Series overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. Den fulde tekst til EU-overensstemmelseserklæringen er tilgængelig på følgende internetadresse: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU-meddelelse om begrænsninger i brug: Denne enhed er kun begrænset til indendørs brug. Det betjenes måske ikke udendørs.
de	Deutsch [German]	Hiermit erklärt Lantronix, Inc., dass sich das Gerät X300 Series in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet. Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse abrufbar: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU-Hinweis zu Nutzungsbeschränkungen: Dieses Gerät darf nur in Innenräumen verwendet werden. Es darf nicht im Freien betrieben werden.

Code	Language	Statement
et	Eesti [Estonian]	Käesolevaga kinnitab Lantronix, Inc. seadme X300 Series vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. EL-i vastavusdeklaratsiooni täielik tekst on saadaval järgmisel Interneti-aadressil: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EL-i teade kasutuspiirangute kohta: seda seadet saab kasutada ainult siseruumides. Seda ei tohi õues kasutada.
en	English	Hereby, Lantronix, Inc., declares that this X300 Series is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU Notice of Restrictions on Use: This device is limited to indoor use only. It may not be operated outdoors.
es	Español [Spanish]	Por medio de la presente Lantronix, Inc. declara que el X300 Series module cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU. El texto completo de la declaración de conformidad de la UE está disponible en la siguiente dirección de Internet: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Aviso de restricciones de uso de la UE: este dispositivo está limitado solo para uso en interiores. No puede ser operado al aire libre.
el	Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Lantronix, Inc. ΔΗΛΩΝΕΙ ΟΤΙ X300 Series ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕU. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ διατίθεται στην ακόλουθη διεύθυνση διαδικτύου: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Ειδοποίηση της ΕΕ για περιορισμούς χρήσης: Η συσκευή αυτή περιορίζεται μόνο σε εσωτερικούς χώρους χρήσης. Μπορεί να μην λειτουργεί σε εξωτερικούς χώρους.

Code	Language	Statement
fr	Français [French]	Par la présente Lantronix, Inc. déclare que l'appareil X300 Series est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU. Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante : https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Avis de restrictions d'utilisation de l'UE: Cet appareil est limité à une utilisation en intérieur uniquement. Il ne doit pas être utilisé à l'extérieur.
is	Icelandic	Hér með lýsir Lantronix, Inc. því yfir að X300 Series sé í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53 / ESB. Í heildartexta ESB-samræmisyfirlýsingarinnar er að finna á eftirfarandi internetfangi: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Tilkynning ESB um takmarkanir á notkun: Þetta tæki er eingöngu takmarkað við notkun innanhúss. Það má ekki nota það úti.
it	Italiano [Italian]	Con la presente Lantronix, Inc. dichiara che questo X300 Series è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU. Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Avviso di restrizioni d'uso dell'UE: questo dispositivo è limitato esclusivamente all'uso in interni. Potrebbe non essere utilizzato all'aperto.
lv	Latviski [Latvian]	Ar šo Lantronix, Inc. deklarē, ka X300 Series atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. Pilns ES atbilstības deklarācijas teksts ir pieejams šādā tīmekļa vietnē: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads ES paziņojums par lietošanas ierobežojumiem: šo ierīci var izmantot tikai iekštelpās. To nedrīkst darbināt ārpus telpām.
lt	Lietuvių [Lithuanian]	Šiuo Lantronix, Inc. deklaruoja, kad šis X300 Series atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas. Visą ES atitikties deklaracijos tekstą galite rasti šiuo interneto adresu: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads ES pranešimas apie naudojimo apribojimus: Šis prietaisas skirtas naudoti tik patalpose. Jo negalima naudoti lauke.

Code	Language	Statement
nl	Nederlands [Dutch]	Hierbij verklaart Lantronix, Inc. dat het toestel X300 Series overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op het volgende internetadres: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU kennisgeving van gebruiksbeperkingen: dit apparaat is beperkt tot gebruik binnenshuis. Het mag niet buitenshuis worden gebruikt.
mt	Malti [Maltese]	Hawnhekk, Lantronix, Inc., jiddikjara li dan X300 Series jikkonforma malħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU. It-test sħiħ tad-dikjarazzjoni ta 'konformità tal-UE huwa disponibbli fl-indirizz tal-internet li ġej: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Avviż tal-UE dwar Restrizzjonijiet fuq l-Użu: Dan l-apparat huwa limitat għal użu ġewwa biss. Ma jistax jitħaddem barra.
hu	Magyar [Hungarian]	Alulírott, Lantronix, Inc. nyilatkozom, hogy a X300 Series megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak. Az EU-megfelelőségi nyilatkozat teljes szövege a következő internetes címen érhető el: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU értesítés a korlátozásokról: Ez az eszköz csak beltéri használatra korlátozódik. Lehet, hogy szabadban nem üzemeltethető.
no	Norwegian	Lantronix, Inc. erklærer herved at denne X300 Series er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53 / EU. Den fullstendige teksten til EU-samsvarserklæringen er tilgjengelig på følgende internettadresse: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EUs merknad om bruksbegrensninger: Denne enheten er bare begrenset til innendørs bruk. Det kan hende at den ikke brukes utendørs.

Code	Language	Statement
pl	Polski [Polish]	Niniejszym Lantronix, Inc. oświadcza, że X300 Series jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU. Pełny tekst deklaracji zgodności UE jest dostępny pod następującym adresem internetowym: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Zawiadomienie UE o ograniczeniach użytkowania: To urządzenie jest przeznaczone wyłącznie do użytku w pomieszczeniach. Nie można go obsługiwać na zewnątrz.
pt	Português [Portuguese]	Lantronix, Inc. declara que este X300 Series está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU. O texto completo da declaração UE de conformidade está disponível no seguinte endereço na Internet: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Aviso da UE de restrições de uso: Este dispositivo está limitado apenas ao uso interno. Não pode ser operado ao ar livre.
ro	Romanian	Prin prezenta, Lantronix, Inc., declară că acest X300 Series respectă cerințele esențiale și alte dispoziții relevante din Directiva 2014/53 / UE. Textul complet al declarației de conformitate a UE este disponibil la următoarea adresă de internet: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Notificarea UE privind restricțiile de utilizare: Acest dispozitiv este limitat numai la uz interior. Este posibil să nu funcționeze în aer liber.
sr	Serbian	Овиме, Лантроник, Инц., изјављује да је овај X300 Series у складу са суштинским захтевима и осталим релевантним одредбама Директиве 2014/53 / ЕУ. Комплетан текст ЕУ изјаве о усаглашености доступан је на следећој Интернет адреси: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Обавештење ЕУ о ограничењима употребе: Овај уређај је ограничен само на унутрашњу употребу. Можда се не користи на отвореном.
sl	Slovensko [Slovenian]	Lantronix, Inc. izjavlja, da je ta X300 Series v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU. Celotno besedilo izjave EU o skladnosti je na voljo na naslednjem spletnem naslovu: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Obvestilo EU o omejitvah uporabe: Ta naprava je omejena samo na notranjo uporabo. Morda ga ne uporabljate na prostem.

Code	Language	Statement
sk	Slovensky [Slovak]	Lantronix, Inc. týmto vyhlasuje, že X300 Series enterprise Wi-Fi IoT module spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU. Úplné znenie EÚ vyhlásenia o zhode je k dispozícii na tejto internetovej adrese: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Oznámenie EÚ o obmedzeniach pri používaní: Toto zariadenie je obmedzené iba na použitie v interiéri. Nesmie sa používať vonku.
fi	Suomi [Finnish]	Lantronix, Inc. vakuuttaa täten että X300 Series tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. EU-vaatimustenmukaisuusvakuutuksen koko teksti on saatavana seuraavassa Internet-osoitteessa: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU: n ilmoitus käyttörajoituksista: Tämä laite on rajoitettu vain sisäkäyttöön. Sitä ei saa käyttää ulkona.
sv	Svenska [Swedish]	Härmed intygar Lantronix, Inc. att denna X300 Series står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU. Den fullständiga texten till EU-försäkran om överensstämmelse finns på följande internetadress: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU-meddelande om begränsningar för användning: Den här enheten är endast begränsad till inomhusbruk. Det får inte användas utomhus.

AT	BE	BG	CH	CY	CZ
DE	DK	EE	EL	ES	FI
FR	HR	HU	IE	IS	IT
LI	LT	LU	LV	MT	NL
NO	PL	PT	RO	SE	SI
SK	TR	UK(NI)			

Caution:This device operates in the 5150 – 5350 MHz frequency range, and is restricted to indoor use only. Outdoor operation in this range is prohibited.

RF Exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

RF Output Power of X303F202S

Bluetooth BR/EDR

Frequency (MHz)	Maximum E.I.R.P (dBm)	Maximum E.I.R.P (mW)	E-Field Strength (V/m)	E-Field Strength (V/m)Limit	Pass/Fail
2402-2480	3.620	2.301	1.31	61	Pass

Note: The conducted output power is refer to report No.: 2180380R-RFCEBT2V01 from the DEKRA.

Bluetooth LE

Frequency (MHz)	Maximum E.I.R.P (dBm)	Maximum E.I.R.P (mW)	E-Field Strength (V/m)	E-Field Strength (V/m)Limit	Pass/Fail
2480	7.260	5.321	2.00	61	Pass

Note: The conducted output power is refer to report No.: 2180380R-RFCEBLEV01 from the DEKRA.

802.11n (40M)

Frequency (MHz)	Maximum E.I.R.P (dBm)	Maximum E.I.R.P (mW)	E-Field Strength (V/m)	E-Field Strength (V/m)Limit	Pass/Fail
2462	19.810	95.719	8.47	61	Pass

Note: The conducted output power is refer to report No.: 2180380R-RFCEWL2V01 from the DEKRA.

802.11n (40M)

Frequency (MHz)	Maximum E.I.R.P (dBm)	Maximum E.I.R.P (mW)	E-Field Strength (V/m)	E-Field Strength (V/m) Limit	Pass/Fail
5310	22.900	194.984	12.093	61	Pass

Note: The conducted output power is refer to report No.: 2180380R-RFCEWL5V01, 2180380R-RFCEOTHV09 from the DEKRA.

Band	Output Power (dBm)	Antenna Gain (dBi)	E-Field Strength (V/m)	E-Field Strength Limit (V/m)	Pass/Fail
GSM 900	32.98	2.13	17.438	40.79	Pass
DCS 1800	30.23	3.79	15.381	56.86	Pass
LTE Band 1	23.26	3.37	18.579	60.25	Pass
LTE Band 3	23.67	3.79	20.442	56.86	Pass
LTE Band 8	23.79	2.13	17.121	40.79	Pass
LTE Band 20	23.56	1.29	15.137	39.66	Pass
LTE Band 28	23.67	3.25	19.210	36.46	Pass

Note: The conducted output power is refer to original module report.

RF Output Power of X304G002S

Mode	Frequency (MHz)	Peak Power (dBm)	Antenna Gain (dBi)	R (cm)	E Field Strength (V/m)	Limit (V/m)
BLE	2480	3.21	2.00	20.0	1.58	61
2.4GHz	2472	16.11	2.00	20.0	6.97	61
5GHz	5320	15.77	2.00	20.0	6.70	61

Note: The conducted output power is refer to report No.: 2240750R-RFCEBLEV01-A, 2240750R-RFCEWL2V01-A 2240750R-RFCEWL5V01-A from the DEKRA.

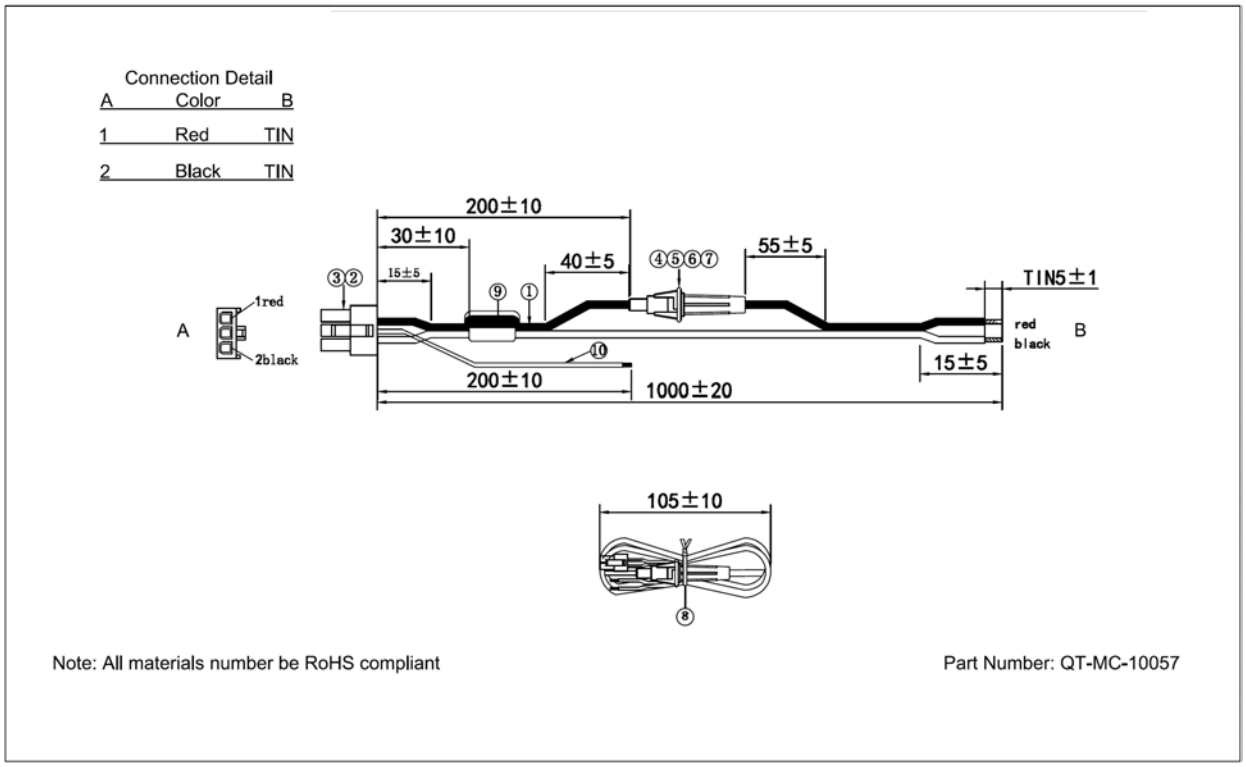
Band	Output Power (dBm)	Antenna Gain (dBi)	E-Field Strength (V/m)	E-Field Strength Limit (V/m)	Pass/Fail
WCDMA Band 1	24.00	2.50	18.303	60.25	Pass
WCDMA Band 8	24.00	1.00	15.400	40.79	Pass
LTE Band 1	24.00	2.50	18.303	60.25	Pass
LTE Band 3	24.00	2.50	18.303	56.86	Pass
LTE Band 7	24.00	2.50	18.303	61.00	Pass
LTE Band 8	24.00	2.50	18.303	61.00	Pass
LTE Band 20	24.00	1.00	15.400	40.79	Pass
LTE Band 28	24.00	1.00	15.400	39.66	Pass

B: Power Cable Schematic

Power Cable Schematic

3-pin power cable schematic

Figure B-1 3-pin Power Cable



C: List of Acronyms and Protocols

Acronym	Description
2G	2nd Generation
3G	3rd Generation
AES	Advanced Encryption Standard
AP	Access Point (or wireless access point) is a device that provides wireless service for clients within its coverage area.
APN	Access Point Name is the name of an access point for the cellular network data connection.
ASDU	Application Service Data Unit is the IEC-101/IEC-104 data structure that holds application layer information to exchange between a control center and a remote terminal unit.
CHAP	Challenge handshake protocol is used by PPP to authenticate users and can be used with many VPNs.
CSQ	Cellular Signal Strength (CSQ). It ranges from 0 to 32.
DHCP	Dynamic Host Configuration Protocol is a standardized networking protocol used by hosts to dynamically discover and lease an IP address, and learn the correct subnet mask, default gateway, and DNS server IP address.
DIO	Digital Input/Output
DLMS	Device Language Message Specification is a set of standards for electricity meter data exchange.
DMZ	Demilitarized Zone is a physical or logical sub network that contains and exposes an organization's external-facing services to a larger and un-trusted network, usually the Internet.
DNP3	Distributed Network Protocol version 3 is a protocol used for automation and remote control communication with serial and TCP/IP capabilities used in SCADA environments.
DNS	Domain Name System is an application layer protocol used throughout the Internet for translating hostnames into their associated IP addresses.
DynDNS, DDNS	Dynamic DNS is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DNS configuration of its configured hostnames, addresses or other information.
EDGE	Enhanced Data rates for GSM Evolution (EDGE) is a backwards-compatible extension of GSM that provides higher data transmission rates than GSM
GPRS	General packet radio service is a packet oriented mobile data standard on the 2G and 3G cellular communication network's GSM
GPS	Global Positioning Satellite
GSM	Global system for mobile communications
HT Physical mode	High Throughput Physical Mode
IEC-101/IEC-104	IEC-101 (serial) and IEC-104 (TCP) are part of the IEC 60870-5 set of standards that define systems or methods used for telecontrol in electrical engineering and power system automation applications.

Acronym	Description
ICMP	Internet Control Message Protocol (ICMP) is a TCP/IP network layer protocol that reports errors and provides other information relevant to IP packet processing.
IGMP	Internet Group Management Protocol is a communications protocol used by hosts and adjacent gateways on IP networks to establish multicast group memberships
IKEv1 and IKEv2	Internet Key Exchange (version 1 or version 2) is an encryption key exchange mode used between two peers.
IPsec	Internet Protocol Security is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
ISP	Internet service provider
L2TP	Layer Two Transport Protocol
LAN	Local Area Network
LED	Light emitting diode
M2M	Machine to machine
MAC address	Media Access Control address is a unique identifier (6 bytes) assigned to a network interface for use as a network address.
MD5	MD5 is a message digest algorithm used as a checksum to verify data integrity
Modbus	Modbus is a data communication protocol used for connecting industrial electronic devices.
MTU	Maximum transmission unit of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards
MWAN	multiple WAN interface
NAT	Network Address Translation is a method of translating IP addresses that are not globally unique into public addresses in the globally routable address space.
NMS	Network Management System. Component in SNMP architecture that includes SNMP manager.
NTP	Network Time Protocol is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks
PAP	Password Authentication Protocol is a password based protocol used by PPP (point to point protocol) to authenticate users and can be used with many VPNs. PAP is considered less secure than CHAP or some other authentication protocols.
PDU	Protocol Data Unit
PoE	Power over Ethernet describes standards for passing electric power and data over Ethernet cabling between the Power Sourcing Equipment (PSE) and the Powered Device (PD).
PLC	Programmable Logic Controller
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol

Acronym	Description
PSK	Pre-shared key
QoS	Quality of Service
RF	Radio Frequency
RTU	Remote terminal unit
Rx	Reception
SCP	Secure Copy Protocol
SHA1/SHA2	Secure Hash Algorithm is an encryption cipher type
SIM	Subscriber identity module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SPI	Serial Peripheral Interface
SSH	Secure Shell
SSID	Service Set Identifier
SSL/TLS	Secure Sockets Layer/Transport Layer Security are encryption-based security protocols designed to provide data security for Internet communications.
STP	Spanning Tree Protocol is a network protocol that prevents loops when switches or bridges are interconnected through multiple paths.
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
Tx	Transmission
UDP	User Datagram Protocol
VPN	Virtual private network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area network
WPA/WPA2/WPA3	Wi-Fi Protected Access® (WPA) family of technologies are security protocols for wireless networks.

D: Lantronix Technical Support

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

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

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

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