LANTRONIX®

SGX™ 5150, SGX™ 5150 MD, and SGX™ 5150 XL IoT Device Gateway User Guide

Part Number 900-776-R
Revision J June 2021

Intellectual Property

Lantronix and *ConsoleFlow* are registered trademarks of Lantronix, Inc. in the United States and other countries.

Patented: http://patents.lantronix.com; additional patents pending.

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

Warranty

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

Contacts

Lantronix, Inc.
7535 Irvine Center Drive
Suite 100
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support Online: www.lantronix.com/support

Sales Offices

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

Open Source Software

Some applications are Open Source software licensed under the Berkeley Software Distribution (BSD) license, the GNU General Public License (GPL) as published by the Free Software Foundation (FSF), and the Python Software Foundation (PSF) License Agreement for Python 2.7.9 (Python License). Lantronix grants you no right to receive source code to the Open Source software. Your use of each Open Source component or software is subject to the terms of the applicable license. The BSD license is available at http://opensource.org/licenses. The GNU General Public License is available at http://www.gnu.org/licenses/. The Python License is available at https://www.python.org/download/releases/2.7/license/.Your use of each Open Source component or software is subject to the terms of the applicable license.

wpa_supplicant: http://w1.fi/cgit/hostap/plain/wpa_supplicant/README

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

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

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

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

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

Linux kernel version 3.10.0.

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

Disclaimer

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
October 2016	A	Initial document for firmware release 8.0.0.0.
November 2016	B	Updated user guide to include software features available in all SGX 5150 device gateway models. The user will experience differing featuer availability depending on the model type installed.
March 2017	C	Updated user guide GRE section.
January 2018	D	Updated to firmware version 8.1.0.1 and updated installation and compliance information.
January 2019	E	Adds support for the SGX 5150 MD model and updates to firmware 8.2.0.3. ➢ Adds support for bridging mode. ➢ Adds support for smart roaming. ➢ Adds support for Secure Boot. ➢ Adds the Developing Applications Using Yocto SDK chapter.
April 2019	F	Adds support for the SGX 5150 XL model and updates documentation for firmware 8.4.0.0.
August 2019	G	Updated for firmware release 8.7.0.0.
January 2020	H	Updated for firmware release 9.0.0.0. ➢ Added Tunnel Buffering configuration. ➢ Replaced DeviceInstaller information with Lantronix Provisioning Manager information. ➢ Updated default password information.
June 2021	J	Updated for firmware release 9.9.0.0. ➢ Updated Access Point settings. ➢ Added EAPoL settings to Wired Network (eth0) Link configuration. ➢ Replaced MACH10 information with ConsoleFlow information. ➢ Added early initialization to Line configuration.

Table of Contents

Intellectual Property 2
Warranty 2
Contacts 2
Open Source Software 2
Disclaimer 3
Revision History 3
Table of Contents 4
List of Figures 11
List of Tables 12

1: Using This Guide 16

Purpose and Audience 16
Summary of Chapters 16
Explanations of Symbols on Product and Product Packaging 17
SGX 5150 MD - Important Safety Information 18
- Medical Power Supply Adapter for SGX 5150 MD 18
- Power Plug 18
- Input Supply 19
- Grounding 19
- Fuses 19
- Wall Mounting 19
- Port Connections 19
- Equipment Classifications 20
- Environmental Conditions for Transport and Storage 20
- Cleaning Instructions 20
- Product End-Of-Life Disposal 21
- Electromagnetic Interference 21

Additional Documentation 21

2: Introduction 22

Key Features 22
Applications 23
Use Cases 24
Protocol Support 24
Troubleshooting Capabilities 25
Configuration Methods 25
Addresses and Port Numbers 25
- Hardware Address 25
- IP Address 26
- Port Numbers 26

Product Information Label 26

3: Installation of the SGX 5150, SGX 5150 MD, & SGX 5150 XL 28

Package Contents 28
User-Supplied Items 28
Hardware Components 29
Front Panel 29
Back Panel 31
USB Connection 32
Power 32
Ethernet Ports 33
Wi-Fi Protected Setup (WPS) 34
Reset Button 34
To Start WPS 34
Installing the SGX 5150 34
Optional SGX 5150 Bracket 37
Wireless Quick Connect 38

4: Using Lantronix Provisioning Manager 39

Installing Lantronix Provisioning Manager 39
Accessing the SGX 5150 Using Lantronix Provisioning Manager 39

5: Configuration Using Web Manager 40

Accessing Web Manager 40
Status Page 41
Web Manager Components 43
Navigating Web Manager 44

6: Network Settings 46

Access Point 46
To View or Configure Access Point Settings 48
Bridge 48
Bridge Status and Configuration 49
To View or Configure Bridge Settings 51
Wired (eth0) Network 51
Interface Status and Configuration 51
To Configure Network Interface Settings 53
Link Status and Configuration 53
To Configure Network Link Settings 55
QoS Statistics and Configuration 55
To View and Configure Wired Network QoS Settings 56
Wired (eth0) Network Failover 56

To View and Configure Wired Network Failover Settings 57
Wireless (wlan0) Network 57
Wireless (wlan0) Network Interface 57
To View or Configure Wireless Network Interface Settings 59
Wireless (wlan0) Network Link 59
Smart Roam 61
To View or Configure Network Link Settings 61
Wireless (wlan0) Network QoS 62
To View or Configure Wireless Network QoS Settings 63
Wireless (wlan0) Network Failover 63
To View or Configure Wireless Network Failover Settings 64
Wired (usb0) Network 64
Interface (usb0) Status and Configuration 64
To Configure Network Interface Settings 66
QoS Statistics and Configuration 66
To View and Configure Wired Network (USB) QoS Settings 67
Wired (usb0) Network Failover 67
To View and Configure Wired (USB0) Network Failover Settings 68
Protocol Stack 68
IP Settings 68
To Configure IP Protocol Stack Settings 69
ICMP Settings 69
To Configure ICMP Protocol Stack Settings 69
ARP Settings 69
To Configure ARP Network Stack Settings 70
VPN 70
Configuring VPN Settings 72
Wi-Fi Protected Setup 72
To Initiate WPS 73
To Show WPS Status 73
WLAN Scan/QuickConnect 73
To View WLAN Link Scan and Status Information 74
WLAN Profiles 74
Configuring WLAN Profile Settings 75

7: Filesystem 79

File Transfer and Modification 80
To View, Transfer, or Modify Filesystem Files 80

8: Diagnostics 81

DNS 81
Accessing the DNS Settings 81
Hardware 82

To View Hardware Information 82
IP Sockets 82
To View the List of IP Sockets 82
Log 83
To Configure the Diagnostic Log Output 83
Memory 83
To View Memory Usage 83
Ping 84
To Ping a Remote Host 84
Processes 84
To View Process Information 84
Routes 85
Threads 85
To View Thread Information 85
Traceroute 85
To Perform a Traceroute 86

9: Administration 87

Actions 88
To Configure Action Settings 89
Python 89
Applications 90
To Configure Application Settings 91
Bluetooth 91
Bluetooth Status and Configuration 91
To View and configure Bluetooth settings: 91
Bluetooth Serial 92
Bluetooth Serial Statistics and Configuration 92
To View and configure Bluetooth settings: 92
CLI 93
CLI Status and Configuration 93
To View and Configure Basic CLI Settings 93
Clock 94
To Specify a Clock-Setting Method 94
ConsoleFlow 95
Configure ConsoleFlow Client 95
Configure ConsoleFlow Line 96
To Configure ConsoleFlow 97
Discovery 97
To Configure Discovery 97
Email 98
To View, Configure and Send Email 98
FTP 99

To Configure FTP Settings 99
Gateway 99
Status 99
WAN 100
MAC Address Filters 101
IP Address Filters 101
To Configure Gateway WAN Settings 101
Port Forwarding 102
To Configure Gateway Port Forwarding Settings 102
Static Routes 103
To Configure Gateway Static Route Settings 104
DHCP Server 104
To Configure Gateway DHCP Server Settings 105
Static Lease Listing 105
Routing Protocols 105
To Configure Gateway Routing Protocol Settings 106
Virtual IP 106
To Configure Gateway Virtual IP 107
GRE 107
To Configure GRE Settings 108
Host 108
To Configure Host Settings 109
HTTP 109
Interface Status, Configuration and Authentication 109
To View or Configure HTTP Authentication 110
To Configure HTTP Authentication 111
Line 112
Line Status and Configuration 112
To View and Configure Line Configuration and Command Mode 113
Modbus 114
Serial Transmission Mode 114
Modbus Statistics 114
Modbus Configuration 114
To View and Configure the Modbus Server 115
RSS 115
To Configure RSS Settings 116
Security 116
To Configure Security Settings 117
SFTP 117
To Configure SFTP Settings 117
SMTP 118
To Configure SMTP Settings 118
SNMP 118

To Configure SNMP Settings 119
SSH 120
SSH Server: Host Keys 120
SSH Server: Authorized Users 121
SSH Client: Known Hosts 121
SSH Client: Users 122
To Configure SSH Settings 123
SSL 123
Credentials 123
To Create a New Credential 124
To Delete a Credential 124
To Configure an SSL Credential to Use an Uploaded Certificate 125
To Configure an SSL Credential to Use a Self-Signed Certificate 126
Trusted Authorities 126
To Upload an Authority Certificate 126
CSR (Certificate Signing Request) 127
Syslog 128
To Configure Syslog Settings 128
System 129
To access System settings: 130
Terminal 131
To Configure the Terminal Network Connection 131
To Configure the Terminal Line or USB Connection 132
Tunnel 132
Tunnel Statistics 132
To View Tunnel Statistics 132
Serial Settings 132
To Configure Tunnel Serial Settings 133
Packing Mode 133
To Configure Tunnel Packing Mode Settings 134
Accept Mode 134
To Configure Tunnel Accept Mode Settings 137
Connect Mode 137
To Configure Tunnel Connect Mode Settings 140
Connecting Multiple Hosts 140
Host List Promotion 141
Disconnect Mode 141
To Configure Tunnel Disconnect Mode Settings 141
Modem Emulation 142
To Configure Tunnel Modem Emulation Settings 142
USB 143
USB Statistics 143
To View USB Statistics 143

USB Configuration 143
To Configure USB Settings 144
USB Command Mode 144
To Configure USB Command Mode 144
User Management 145
To Configure User Management 147
XML 147
To Export Configuration 148
To Export Status 149
To Import Configuration 149
Quick Setup 151
To Utilize Quick Setup 151

10: Developing Applications Using Yocto SDK 154
Using Lantronix PremierWave BSP Yocto Project 154
Summary 154
Prerequisites 154
Build the ROM Image and SDK 154
Install SDK 154
Use SDK to Build/Test Your Application 155
Add/Update Your Application into the ROM Image 155
Upload/Program Firmware into Gateway 156
Examples 156
Secure Boot 156
Firmware Filenames 156
Preparing the SGX 5150 for OEM Secure Boot 157
Releasing Custom Firmware 157
Integration with Microsoft Azure 158
Environment Setup for Microsoft Azure 158
Using Lantronix Beacon Scanner 159
Installing Lantronix Beacon Scanner 159
Using Lantronix Beacon Scanner 159

Lantronix Technical Support 161

Compliance 162
SGX 5150 Regulatory Domains 169
RoHS, REACH and WEEE Compliance Statement 170

List of Figures

Figure 2-1 Serial to Wi-Fi or Ethernet ____ 24
Figure 2-2 Ethernet to Wi-Fi Bridge ____ 24
Figure 2-3 Product Label SGX 5150 MD ____ 27
Figure 2-4 Product Label SGX 5150 and SGX 5150 XL ____ 27
Figure 3-5 Front Panel ____ 29
Figure 3-6 Back Panel for SGX 5150 MD ____ 31
Figure 3-7 Back Panel for non-medical SGX 5150 ____ 31
Figure 3-8 RJ45 Serial Port ____ 32
Figure 3-9 Wi-Fi Protected Setup ____ 34
Figure 3-10 SGX 5150 Dimensions in Inches (in) and Millimeters (mm) ____ 36
Figure 3-11 Optional Bracket Installation ____ 37
Figure 5-12 Status Page (Section 1 of 2) ____ 41
Figure 5-13 Status Page (Section 2 of 2) ____ 42
Figure 5-14 Components of the Web Manager Page ____ 43
Figure 5-15 Expandable Menu Bar Selections ____ 43
Figure 10-16 Environment Setup for Microsoft Azure ____ 158
Figure B-1 SGX 5150 Suppliers Declaration of Conformity ____ 163
Figure B-2 SGX 5150 MD Suppliers Declaration of Conformity ____ 165
Figure B-3 EU Declaration of Conformity ____ 166

List of Tables

Table 1-1 Product and Packaging Symbols ____ 17
Table 3-2 SGX 5150 LEDs and Descriptions ____ 29
Table 3-3 “STATUS” LED ____ 29
Table 3-4 “WLAN” LED ____ 30
Table 3-5 Signal Strength Indicator at 2.4 GHz ____ 30
Table 3-6 Signal Strength Indicator at 5 GHz ____ 30
Table 3-7 Serial RJ45 Connector Pinout and LEDs ____ 31
Table 3-8 USB Type C Connector Pinout ____ 32
Table 3-9 SGX 5150 - Power Input Interface ____ 32
Table 3-10 SGX 5150 MD - Power Input Interface ____ 33
Table 3-11 Ethernet RJ45 Connector Pinout ____ 33
Table 3-12 Left Ethernet LED ____ 34
Table 3-13 Right Ethernet LED ____ 34
Table 5-14 Web Manager Pages ____ 44
Table 6-15 Access Point Settings ____ 46
Table 6-16 Bridge Settings ____ 49
Table 6-17 Wired (eth0) Network Interface ____ 51
Table 6-18 Link (eth0) Configuration ____ 53
Table 6-19 Wired (eth0) Network QoS Settings ____ 56
Table 6-20 Wired (eth0) Network Failover Settings ____ 57
Table 6-21 Wireless (wlan0) Interface Configuration ____ 58
Table 6-22 Wireless (wlan0) Link Configuration ____ 60
Table 6-23 Smart Roam Settings ____ 61
Table 6-24 Wireless (wlan0) Network QoS Settings ____ 62
Table 6-25 Adding or Deleting Wireless (wlan0) Network QoS Settings ____ 62
Table 6-26 Wireless (wlan0) Network Failover ____ 63
Table 6-27 Wired (usb0) Network Interface ____ 64
Table 6-28 Wired (usb0) Network QoS Settings ____ 67
Table 6-29 Wired (usb0) Network Failover Settings ____ 67
Table 6-30 IP Protocol Stack Settings ____ 68
Table 6-31 ICMP Protocol Stack Settings ____ 69
Table 6-32 ARP Protocol Stack Settings ____ 70
Table 6-33 VPN Settings ____ 70
Table 6-34 Wi-Fi Protected Setup ____ 73
Table 6-35 WLAN Scan/Quick Connect Results ____ 74
Table 6-36 WLAN Profiles ____ 75

Table 6-37 Individual WLAN Profile Settings 75
Table 7-38 File Modification Settings 79
Table 7-39 USB Auto Mount Configuration Settings 79
Table 7-40 File Transfer Settings 80
Table 8-41 DNS Settings 81
Table 8-42 Log Settings 83
Table 8-43 Ping Configuration 84
Table 8-44 Traceroute Settings 85
Table 9-45 Action Settings 88
Table 9-46 Script Settings 90
Table 9-47 Bluetooth Configuration 91
Table 9-48 Bluetooth Serial Configuration 92
Table 9-49 CLI Configuration Settings 93
Table 9-50 Clock Settings 94
Table 9-51 ConsoleFlow Client Configuration 95
Table 9-52 ConsoleFlow Line 96
Table 9-53 Discovery Settings 97
Table 9-54 Email Configuration 98
Table 9-55 FTP Settings 99
Table 9-56 WAN Configuration 100
Table 9-57 Adding or Deleting MAC Address Filters 101
Table 9-58 Adding or Deleting IP Address Filters 101
Table 9-59 Port Forwarding Rules List 102
Table 9-60 Adding a New Port Forwarding Rule 102
Table 9-61 Static Route Settings 103
Table 9-62 Routing Table 103
Table 9-63 Adding a New Static Route 103
Table 9-64 DHCP Settings 104
Table 9-65 Static Lease Listing 105
Table 9-66 Add a Static Lease 105
Table 9-67 Routing Protocol Settings 106
Table 9-68 Existing Virtual IP Settings 107
Table 9-69 Add a Virtual IP 107
Table 9-70 GRE Settings 107
Table 9-71 Host Settings 108
Table 9-72 HTTP Configuration 109
Table 9-73 HTTP Authentication 111
Table 9-74 Line Configuration Settings 112

Table 9-75 Line Command Mode Setting 113
Table 9-76 Byte Header of Modbus Application Protocol 114
Table 9-77 Modbus Transmission Modes 114
Table 9-78 Modbus Configuration 115
Table 9-79 RSS 116
Table 9-80 SMTP Settings 118
Table 9-81 SNMP Settings 119
Table 9-82 SSH Server Host Keys 120
Table 9-83 SSH Server Authorized Users 121
Table 9-84 SSH Client Known Hosts 121
Table 9-85 SSH Client Users 122
Table 9-86 Create New Keys 122
Table 9-87 SSL Credential - Upload Certificate 124
Table 9-88 SSL Credential - Create New Self-Signed Certificate 125
Table 9-89 SSL Trusted Authority 126
Table 9-90 SSL CSR (Certificate Signing Request) 127
Table 9-91 System Settings 129
Table 9-92 Terminal on Network and Line Settings 131
Table 9-93 Tunnel Serial Settings 133
Table 9-94 Tunnel Packing Mode Settings 133
Table 9-95 Tunnel Accept Mode Settings 135
Table 9-96 Tunnel Connect Mode Settings 137
Table 9-97 Host Settings 138
Table 9-98 Tunnel Disconnect Mode Settings 141
Table 9-99 Tunnel Modem Emulation Settings 142
Table 9-100 USB Configuration 143
Table 9-101 USB Command Mode 144
Table 9-102 Administrator Settings 145
Table 9-103 Current Users List 145
Table 9-104 New User Settings 145
Table 9-105 Current Roles List 146
Table 9-106 New Role Settings 146
Table 9-107 Configuration from Filesystem 150
Table 9-108 Line(s) from single line Settings on the Filesystem 150
Table 9-109 Administrator Settings 151
Table 9-110 Bridge 1(br0) Configuration 151
Table 9-111 Wi-Fi Protected Setup 152
Table 9-112 Current Configuration 152

Table 9-113 Available Networks _____ 152
Table 10-114 Lantronix Beacon Scanner commands _____ 159
Table B-1 EU Declaration of Conformity _____ 167
Table B-1 Country Transmitter IDs _____ 168
Table B-2 SGX 5150 Module RF Output Power _____ 168
Table B-3 20 MHz Channels _____ 169
Table B-4 40 MHz Channels _____ 170
Table B-5 80 MHz Channels _____ 170

1: Using This Guide

Purpose and Audience

This document provides information needed to configure, use, and update the Lantronix® *SGX™ 5150, SGX™ 5150 MD, and SGX™ 5150 XL IoT Device Gateway.* It is intended for system integrators who are configuring this product.

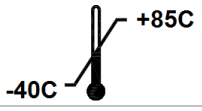
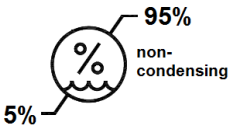
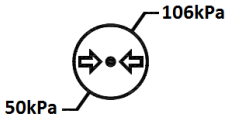
Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
2: Introduction	Describes main features of the product and the protocols it supports. Includes technical specifications.
3: Installation of the SGX 5150, SGX 5150 MD, & SGX 5150 XL	Instructions for installing the SGX 5150, SGX 5150 MD, and SGX 5150 XL.
4: Using Lantronix Provisioning Manager	Instructions for viewing the current configuration using Lantronix Provisioning Manager.
5: Configuration Using Web Manager	Instructions for accessing Web Manager and using it to configure settings for the SGX 5150, SGX 5150 MD, and SGX 5150 XL gateway.
6: Network Settings	Instructions to view and configure Access Point, Bridge, Wired Network (eth0), Wireless Network (wlan0), Wired Network (usb0), Protocol Stack, VPN, Wi-Fi Protected Setup, WLAN Scan/ QuickConnect, and WLAN Profiles settings.
6: Network Settings	Instructions to view and configure Access Point, Bridge, Wired Network (eth0), Wireless Network (wlan0), Wired Network (usb0), Protocol Stack, VPN, Wi-Fi Protected Setup, WLAN Scan/ QuickConnect, and WLAN Profiles settings.
7: Filesystem	Instructions to view and configure the filesystem.
8: Diagnostics	Instructions to view and configure DNS, Hardware, IP Sockets, Log, Memory, Ping, Processes, Routes, Threads, and Traceroute information.
9: Administration	Instructions to view and configure Actions, Applications, Bluetooth, Bluetooth Serial, CLI, Clock, ConsoleFlow, Discovery, Email, FTP, Gateway, GRE, Host, HTTP, Line, Modbus, RSS, Security, SFTP, SMTP, SNMP, SSH, SSL, Syslog, System, Terminal, Tunnel, USB, User Management, XML, and Quick Setup information.
10: Developing Applications Using Yocto SDK	Instructions for developers to use the Yocto SDK to create custom firmware.
A: Lantronix Technical Support	Instructions for contacting Lantronix Technical Support.
B: Compliance	Provides SGX 5150, SGX 5150 MD, and SGX 5150 XL compliance information.

Explanations of Symbols on Product and Product Packaging

Table 1-1 Product and Packaging Symbols

Symbol	Meaning
	**User Manual** Indicates the user manual should be referenced for operating instructions
	**Warning** Indicates the user should refer to user manual to avoid accidents and failures
	**Temperature Range** Indicates the recommended temperature range for transport and storage
	**Humidity Range** Indicates the humidity range recommended for transport and storage
	**Atmospheric Pressure Range** Indicates the atmospheric pressure range for transport and storage
	**Fragile** Indicates that the product is fragile and should be handled with care
	**Keep Dry** Keep the product in a dry place
	**Avoid Sunlight** Keep product out of sunlight
	**Manufacturer**
	**Product Manufacture Date**

Symbol	Meaning
SN	**Product Serial Number**

SGX 5150 MD - Important Safety Information

This section describes the safety precautions that should be followed when installing and operating the SGX 5150 MD for use in medical environments.

Caution: ***IMPROPER USES OF THE PRODUCT MAY CAUSE SAFETY HAZARDS, UNIT FAILURES, AND VOID OF WARRANTY.***

Warning:

- The SGX 5150 MD is not suitable for use in the presence of a flammable anesthetic mixture including air, oxygen or nitrous oxide. To avoid the risk of electric shock, the Power Supply Adapter of the SGX 5150 MD must only be connected to a supply main with protective earth.
- The SGX 5150 MD is not to be used in life support or as a life sustaining product.
- No modification of this equipment is allowed. Use only the external Power Supply Adaptor shipped together with SGX 5150 MD. The operation of device, connected systems, and user/operator safety may be compromised if not using the correct Power Supply as required.
- Do not remove the cover of the SGX 5150 MD or the Power Supply Adaptor. There are no user-serviceable parts inside. Opening or removing the cover may expose you to dangerous voltage that could cause fire or electric shock.
- Do not operate the SGX 5150 MD if the housing of the SGX 5150 MD or of Power Supply Adaptor is broken.
- Interconnection of the SGX 5150 MD wireless IoT gateway for medical devices with other medical devices, medical systems, or other non-medical devices shall be evaluated to the requirements of Clause 16 of IEC 60601-1 in the end use application.
- Refer all servicing to Lantronix.

Medical Power Supply Adapter for SGX 5150 MD

- The required Power Supply Adapter for medical applications part number is SL Power ME10A1272F02 (Lantronix Part Number 520-160-R).

Power Plug

- When disconnecting the power cord from the wall ac socket, pull on the plug, not the cord.
- Always connect the power cord to a properly wired and grounded power source. Do not use adapter plugs or remove the grounding prong from the cord.
- Only use a power cord with a voltage and current rating greater than the voltage and current rating marked on the unit.

Notes:

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

Input Supply

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

Grounding

- Maintain reliable grounding of this product.

Fuses

- There is no fuse. If the SGX 5150 MD fails to power on, return it to Lantronix for servicing.

Wall Mounting

If a wall-mounted with SGX 5150's optional bracket (see Figure 3-16), the following items must be considered:

- Do not install the unit in such a way that a hazardous stability condition results because of uneven loading. A drop or fall could cause injury.
- Make sure to install the SGX 5150 MD unit in an environment with an ambient temperature less than the maximum operating temperature of the SGX 5150 MD device. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature specified by the manufacturer.
- Maintain reliable earthing of wall-mounted equipment. Give particular attention to supply connections other than direct connections to the branch circuit (e.g. use of power strips) because of the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

  Note: *Before operating the SGX 5150 MD device, make sure the device mounting is secured.*

Port Connections

- Only connect the network port to an Ethernet network that supports 10 Base-T/100 Base-TX using CAT5/CAT5E/CAT6 cables.
- Only connect device ports to equipment with serial ports that support EIA-232 (formerly RS-232C), and USB port to intended USB Device/Host port as appropriate by applications.

Warning on USB Port:

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

Warning on Ethernet Port:

The integration of the SGX 5150 MD wireless IoT gateway into an IT network may constitute a Medical Electrical (ME) System. It is recommended that the system leakage current be measured to verify that the basic requirement for the safety of the ME System, after installation or subsequent modification of the system, does not result in an unacceptable risk.

The integration of the SGX 5150 MD into a IT network may result in unforeseen risks associated with the interconnection of the SGX 5150 MD Programmable Electronic Subsystem PESS)/ Programmable Electrical Medical Systems (PEMS) to IT Networks. Connection of equipment containing PEMS to an IT NETWORK/DATA COUPLING that includes other equipment could result in previously unidentified risks to patients, operators or third parties. The entity accountable for the use and maintenance of an ME EQUIPMENT or an ME SYSTEM should identify, analyze, evaluate and control these RISKS. Subsequent changes to the IT NETWORK/DATA COUPLING could introduce new RISKS and require additional analysis. Changes to the IT NETWORK/DATA COUPLING include:

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

Equipment Classifications

- Classification according to the type of protection against electric shock:

  SGX 5150 MD: Class III

  Power Supply: Class I or Class II
- Classification according to the degree of protection against electric shock: No Applied Parts
- Classification according to the degree of protection against ingress of water: IP20
- Classification according to the mode of operation: Continuous Operation

Environmental Conditions for Transport and Storage

- Ambient Temperature Range -40°C to +85°C.
- Humidity Range 5% to 95% non-condensing
- An atmospheric pressure range of 50 kPa to 106 kPa

Cleaning Instructions

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

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

Product End-Of-Life Disposal

- Product's service life is estimated at 5 years or more.
- When the product is no longer usable or repairable, dispose the product properly according to local laws.

Electromagnetic Interference

This equipment has been tested and found to comply with the EMC limits for the Medical Device Directive 93/42/EEC (EN 55032 Class B and EN 60601-1-2). These limits are designed to provide reasonable protection against harmful interference in a typical medical installation. The equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to other devices in the vicinity. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference with other devices, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Additional Documentation

Visit the Lantronix Web site at www.lantronix.com/support/documentation for all the latest Lantronix documentation including the following documents related to this product.

Document	Description
SGX 5150 IoT Device Gateway Command Reference	Instructions for accessing command mode (the command line interface) using a Telnet connection, SSH connection or through the serial port. Detailed information about the commands, XML configuration, and status are provided.
SGX 5150 IoT Device Gateway Quick Start Guide	Instructions for getting the SGX 5150 unit up and running.
Lantronix Provisioning Manager Online Help	Instructions for using the Lantronix Provisioning Manager application that discovers, configures, updates, and managers Lantronix devices.
Com Port Redirector Quick Start and Online Help	Instructions for using the Windows operating system-based utility to create virtual com ports.
Secure Com Port Redirector User Guide	Instructions for using the Windows operating system-based utility to create secure virtual com ports.

2: Introduction

The SGX 5150 is a turnkey WLAN IoT device gateway that securely connects deployed devices to the enterprise network through serial, USB or Ethernet interfaces. It simplifies enterprise Wi-Fi® deployments and accelerates the availability of connected devices within enterprise, medical/ healthcare and industrial automation applications.

Note: *This user guide describes all software features supported in the Lantronix SGX 5150 device gateway models available for purchase. Depending on the specific SGX 5150 device gateway model you have purchased, some descriptions may not apply. Commands within this document apply to the SGX 5150, SGX 5150 MD, and SGX 5150 XL unless otherwise noted.*

Key Features

- **Power Supply:**

  SGX 5150: Flexible power options and input voltage range: one barrel connector for 9-30 VDC power source, USB type C VBUS 5V, and optional PoE power input via Ethernet RJ45 interface

  SGX 5150 MD: To comply with IEC 60601-1 requirement, please use the Medical 12VDC Power Supply 520-160-R as indicated in the Important Safety Information section.

  SGX 5150 XL: Flexible power options and input voltage range: one barrel connector for 9-30 VDC power source and optional PoE power input via Ethernet RJ45 interface

- **Controller:** 32-bit ARM9 microprocessor running at 400 megahertz (Mhz) with 32 Kilobyte (KB) configurable cache
- **Memory:** 400 MHz ARM9, 64 MB SDRAM and 128 MB NAND flash. 8 GB eUSB flash drive on the SGX 5150 XL.
- **Ethernet:**

  - One RJ45 10Base-T/100Base-TX Ethernet port

  - Auto sensing

  - Automatic MDI/MDI-X crossover

  - Full duplex IEEE 802.3x flow control

  - Half-duplex back pressure flow control

  - Hardware Optional PoE Power Input (Class 2)
  Supports inputs at both Spare Pins or Ethernet Center Taps

- **Wireless:**

  - 5G Wi-Fi (IEEE 802.11ac)
    - 1x1 ac (MCS0 - MCS9)
    - 20, 40 and 80 MHz Channels with optional SGI
  - IEEE 802.11 n
    - 1x1 n (MCS0 - MCS7)
    - 20 MHz and 40 MHz channel width with optional SGI

- Advanced 802.11 n/ac Features
  - Tx/Rx Low Density Party Check (LDPC)
  - Rx Space Time Block Coding (STBC)
- Compatible with IEEE 802.11 a/b/g and supports IEEE 802.11 d/h
- Bluetooth/WLAN Coexistence
- Dual band 2.4 GHz and 5 GHz
  - 2.412 GHz - 2.484 GHz - Channels 1 - 14
  - U-NII-1 (5.15 – 5.25 GHz) Channels 36, 40, 44, 48
  - U-NII-2 (5.25 – 5.35 GHz) Channels 52, 56, 60, 64
  - U-NII-2e (5.47 – 5.725 GHz) Channels 100 – 140
  - U-NII-3 (5.725 – 5.825 GHz) Channels 149 - 165

- **Serial Ports:** Two 300 to 921 kbaud with options of RS-232 serial ports or multi-protocol RS232/422/485 serial ports
- **USB Ports:** One USB 2.0 high speed interfaces via USB type C connector
- Configuration via CLI, XML and HTTP
- Ethernet to wireless tunneling
- Built-in site survey tool
- **Temperature Range:**

  - Operates over a temperature range of -40°C to +70°C (-40°F to 158°F) for non-medical SGX 5150
  - Operates over a temperature range of 0 to 45°C (32F to 113F) for SGX 5150 MD
  - The storage temperature range is -40C to 85°C (-40°F to 185°F)

- **Physical Specifications:**

  - Housing material: 6000 series aluminum extrusion alloy
  - See *Figure 3-10* for physical dimensions

Applications

- Home energy management systems
- Medical device and clinical information system (CIS) integration
- Asset and warehouse management
- Mobile driven human-machine interface (HMI) and instrumentation
- Industrial machines - weighing scales, automation controllers

Use Cases

Figure 2-1 Serial to Wi-Fi or Ethernet

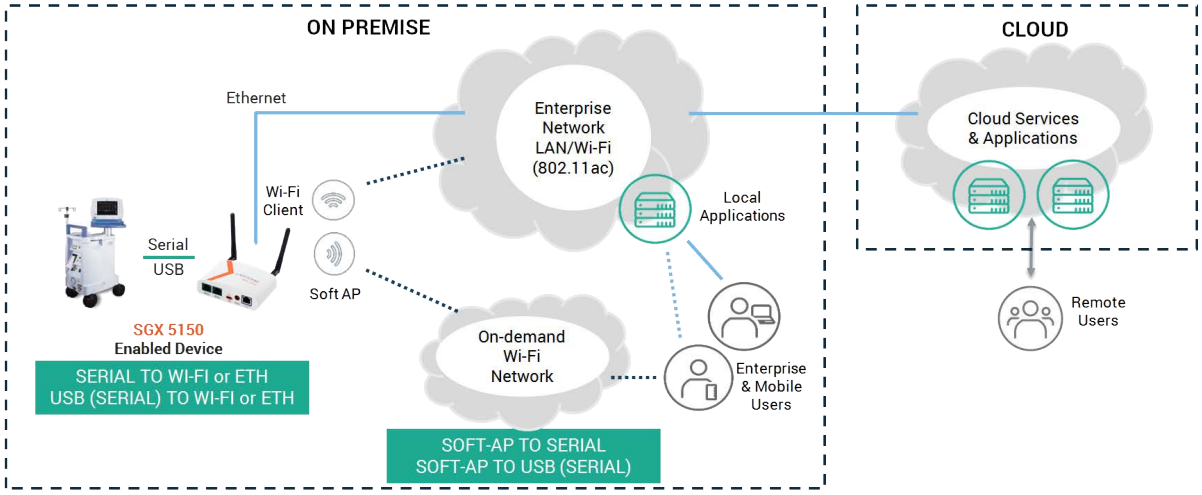
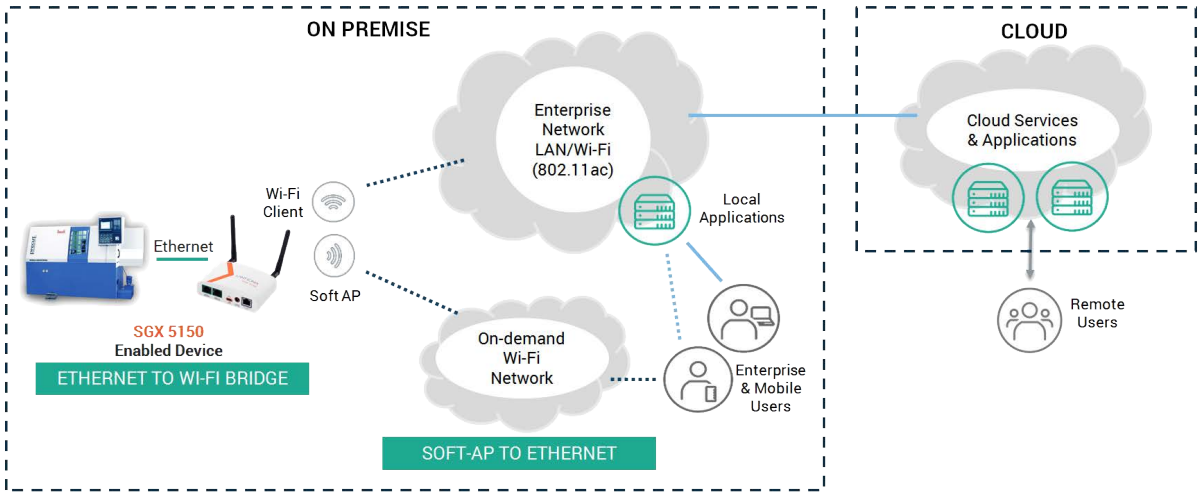


Figure 2-2 Ethernet to Wi-Fi Bridge



Protocol Support

The SGX 5150 contains a full-featured IP networking and wireless software stack:

- DHCP Client, DHCP Server, DHCPv6 Client
- uPnP (Discovery), LCAP (77FE), Telnet, SSH, SSLv3/TLSv1.0/TLSv1.1/TLSv1.2, (S)FTP, HTTP(S)
- IPv4/IPv6, TCP, UDP, ICMP, ARP, Auto-IP, DNS, SNMP v1/v2/v3
- WPA/WPA2 Personal, WPA2 Enterprise (EAP-TLS, EAP-TTLS, EAP-PEAPv0/v1, EAP-FAST)

Troubleshooting Capabilities

The SGX 5150 offers a comprehensive diagnostic tool set that lets you troubleshoot problems quickly and easily. Diagnostic tools available in the CLI or Web Manager allow you to:

- View critical hardware, memory, buffer pool, IP socket information and routing table
- Perform ping and traceroute operations
- Conduct forward or reverse DNS lookup operations
- View all processes currently running on the SGX 5150 including CPU utilization
- View system log messages

Configuration Methods

After installation, the SGX 5150 requires configuration. For the unit to operate correctly on a network, it must have a unique IP address on the network. There are five basic methods for logging into the SGX 5150 and assigning IP addresses and other configurable settings:

- **Web Manager:** View and configure all settings easily through a web browser using the Lantronix Web Manager. See *Chapter 5: Configuration Using Web Manager*.
- **Lantronix Provisioning:** Obtain basic information about the device such as firmware version, IP address, and serial number. Update the firmware, configure the device using XML files, or upload to the file system.
  See *Chapter 4: Using Lantronix Provisioning Manager*.
- **Command Mode:** Two methods for accessing Command Mode (CLI) include making a Telnet or SSH connection, or connecting a PC or other host running a terminal emulation program to the unit's serial port. See the *SGX 5150 IoT Device Gateway Command Reference* for instructions and available commands.
- **XML:** The SGX 5150 supports XML-based configuration and setup records that make device configuration transparent to users and administrators. XML is easily editable with a standard text or XML editor. See the *SGX 5150 IoT Device Gateway Command Reference* for instructions and commands.
- **Web API:** The Web APIs are RESTful APIs that allow access to a subset of gateway functions through a standard HTTP request. They can be used to export and import configuration, export status, take a status action, and manipulate the file system. See the SGX 5150 IoT Device Gateway Command Reference for details and a list of actions.

Addresses and Port Numbers

Hardware Address

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

Sample ways hardware address may be represented:

- `00-80-A3-14-1B-18`
- `00:80:A3:14:1B:18`

IP Address

Every device connected to an IP network must have a unique IPv4 address. This address references the specific unit.

Port Numbers

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

The following is a list of the default server port numbers running on the SGX 5150:

- TCP Port 22: SSH Server (Command Mode configuration)
- TCP Port 23: Telnet Server (Command Mode configuration)
- TCP Port 80: HTTP (Web Manager Configuration)
- TCP Port 21: FTP
- TCP Port 443: HTTPS
- TCP Port 30179: UPnP Discovery
- UDP Port 30718: Lantronix Discovery Protocol

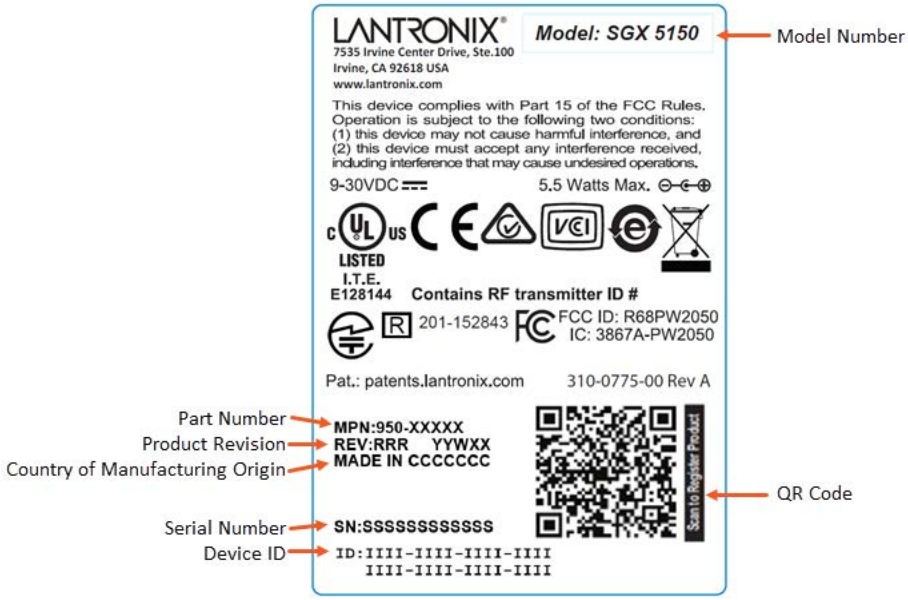
Product Information Label

The product information label on the SGX 5150 gateway contains the following information about the specific unit:

- Model Name
- Product Part Number
- QR Code
- Product Revision
- Country of Manufacturing Origin
- Serial Number
- Device ID

Figure 2-3 Product Label SGX 5150 MD

Figure 2-4 Product Label SGX 5150 and SGX 5150 XL



3: Installation of the SGX 5150, SGX 5150 MD, & SGX 5150 XL

This chapter describes how to install the SGX 5150 device gateway. It contains the following sections:

- *Package Contents*
- *User-Supplied Items*
- *Hardware Components*
- *Installing the SGX 5150*

Warning: ***This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.***

警告　この装置は、クラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　ＶＣＣＩ－Ｂ

Package Contents

The SGX 5150 package includes the following items:

- SGX 5150 IoT device gateway
- 2 external antennas with RP-SMA connectors
- Type A to type C USB cable

  Note: *This cable is compliant to the specification mandated 56k Ω pull-up.*
- *SGX 5150 IoT Device Gateway Quick Start Guide*

Notes:

- *An IEC 60601-1 certified SGX 5150 MD is in most cases shipped with a medical power supply adapter. The SGX 5150 MD is for use only with the SL Power P/N: ME10A1272F02 (Lantronix Part Number 520-160-R).*
- *For non-medical SGX 5150 no external power supply is provided.*
- *For SGX 5150 XL, an external 12V power supply is provided.*

User-Supplied Items

To complete your installation, you need the following items:

- RS-232/422/485 serial device(s) requiring network connectivity
- A serial cable for each serial device

- A null modem cable to connect the serial port to another DTE device.
- A straight-through modem cable to connect the serial port to a DCE device

- An available connection to your Ethernet network and an Ethernet cable
- Power Supply for non-medical SGX 5150
  - USB VBUS power via a USB-C cable for SGX 5150, OR
  - Optional 12 VDC (10W, 2.1 mm barrel connector) wall cube power supply (Lantronix part number 520-154-R or equivalent).
  - Due to the additional power required for the internal eUSB flash drive on the SGX 5150 XL, an external 12VDC power supply, which is provided, is required.

Hardware Components

Front Panel

Figure 3-5 Front Panel

Table 3-2 SGX 5150 LEDs and Descriptions

LED Name	LED Color for SGX 5150 MD	LED Color for SGX 5150	Description
STATUS	Orange	Orange	LED for diagnostics. See *Table 3-3*.
WLAN	Orange	Orange	LED to indicate the status of WLAN and WPS. See *Table 3-4*.
SIGNAL	Orange	Orange	LEDs to indicate received RF signal strength. See *Table 3-5* and *Table 3-6*.

Table 3-3 "STATUS" LED

Indications	"STATUS" LED Pattern
WLAN and LAN Links established	Steady on
No IP obtained from eth0 network	Long, long, short, short, short, two seconds off, then pattern repeats
No IP obtained from wlan0 network	Long, long, long, short, short, short, two seconds off, then pattern repeats

Indications	"STATUS" LED Pattern
No IP obtained from the usb0 network	Long, long, long, long, long, short, short, two seconds off, then pattern repeats
No eth0 link	Long, long, short, short, two seconds off, then pattern repeats
No wlan0 link	Long, long, long, short, short, two seconds off, then pattern repeats
No usb0 link	Long, long, long, long, long, short, two seconds off, then pattern repeats

Table 3-4 "WLAN" LED

The WLAN link LED is used to indicate WLAN and WPS status. See below for LED patterns.

WLAN/WPS Status	Blink Pattern
WLAN Link established	Steady on
WPS is enabled and on	Short, two seconds off, then pattern repeats
WPS has a profile error	Long, long, long, short, short, two seconds off, then pattern repeats
WPS has a timeout error	Long, long, long, short, short, short, short, two seconds off, then pattern repeats

Notes:

- *A "long" blink is 0.7 seconds ON followed by 0.3 seconds OFF*
- *A "short" blink is 0.2 seconds ON followed by 0.2 seconds OFF*

Table 3-5 Signal Strength Indicator at 2.4 GHz

Received RF Signal Strength	Blink Pattern
Greater than -60 dbM	Three LEDs on
Greater than -70 dbM and less than -60 dbM	Two LEDs on
Greater than -80 dbM and less than -70 dbM	One LED on
Less than -80 dBm	All LEDs OFF

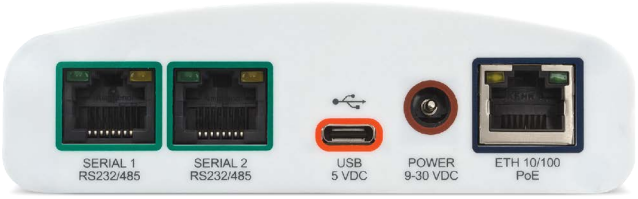
Table 3-6 Signal Strength Indicator at 5 GHz

Received RF Signal Strength	Blink Pattern
Greater than -60 dbM	Three LEDs on
Greater than -65 dbM and less than -60 dbM	Two LEDs on
Greater than -70 dbM and less than -65 dbM	One LED on
Less than -70 dBm	All LEDs OFF

Back Panel

Figure 3-6 Back Panel for SGX 5150 MD

Figure 3-7 Back Panel for non-medical SGX 5150



Serial Interface

One or two serial ports are available for the SGX 5150. Data rates can be configured for speeds between 300 and 921 kbaud. Hardware protocol options include the following:

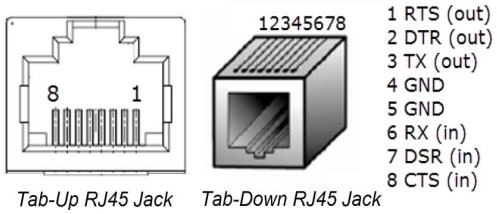
- Two RJ45 RS232 Serial Ports, or
- Two RJ45 Multi-protocol RS232/422/485 ports, or
- One RJ45 RS232 Serial Port

Note: *Multi-protocol ports come with configurable terminations 120 ohm on TX+/- and RX+/-.*

Table 3-7 Serial RJ45 Connector Pinout and LEDs

Pin Number	Signal Name for RS-232	Signal Name for RS-422/485 (4 wire)	Signal Name for RS485 2-Wire
1	RTS (output from SGX)	TX+ (output from SGX)	TX+/RX+
2	DTR (output from SGX)	Not used/do not connect.	Not used/do not connect
3	TXD (output from SGX)	TX- (output from SGX)	TX-/RX-
4	GND	GND	GND
5	GND	GND	GND
6	RXD (input to SGX)	RX+ (input to SGX)	Not used/do not connect
7	DCD (input to SGX)	Not used/do not connect.	Not used/do not connect
8	CTS (input to SGX)	RX- (input to SGX)	Not used/do not connect
Right LED	Yellow for Transmit Data activities (TXD)	Yellow for Transmit Data activities (TXD)	Yellow for Transmit Data activities (TX)
Left LED	Green for Receive Data activities (RXD)	Green for Receive Data activities (RXD)	Green for Receive Data activities (RX)

Figure 3-8 RJ45 Serial Port



Tab-Up RJ45 Jack *Tab-Down RJ45 Jack*

Note: *For the proper operation of the RS422/485 4-wire, the 2-wire modes, as well as the RS232 mode, a GND (Ground) wire must be connected between the equipment.*

USB Connection

One USB 2.0 HS/FS port with USB type C connector is available on the SGX 5150 and can be configured in two ways:

- As a USB device (default setting) where the SGX 5150 can be powered by a VBUS 5V.
- As a USB configurable host where the SGX 5150 can provide VBUS 5V 0.5A if powered by a Lantronix provided wall adapter or PoE (hardware optional).

Table 3-8 USB Type C Connector Pinout

Upper Row Pin Number	Lower Row Pin Number	Signal Name
A1	B1	Ground
A2	B2	No Connection
A3	B3	No Connection
A4	B4	VBUS 5V
A5		CC1
	B5	CC2
A6	B6	Data+
A7	B7	Data-
A8	B8	No Connection
A9	B9	VBUS 5V
A10	B10	No Connection
A11	B11	No Connection
A12	B12	Ground

Power

Table 3-9 SGX 5150 - Power Input Interface

Power Input	Description
Barrel Connector	◆ Center contact fork type for better grip ◆ 9-30 VDC Input with center = (+) ◆ Reverse polarity protection up to 30 VDC
USB Type C Connector	◆ USB VBUS 5V powering (default setting) ◆ SGX can provide VBUS 5V 0.5A out if configured as USB host, and powered by Lantronix provided wall adaptor, or PoE power source class 2 (hardware optional)
Ethernet PoE RJ45 Connector	◆ PoE power module is optional ◆ Must provide class 2 PoE power source ◆ Supports power inputs at both spare pins or Ethernet center taps with full bridge diodes for polarity in-discrimination

Power Input	Description
Power Consumption for SGX 5150 and SGX 5150 MD	◆ 1.9 W typical if configured as USB Device or USB Host - but not providing VBUS 5V power ◆ 5.5 W maximum if configured as USB Host and providing out VBUS 5V power ◆ The internal hardware configuration allows more than one or all power sources applied at the same time
Power Consumption for SGX 5150 XL	◆ 2.5 W typical if configured as USB Device or USB Host - but not providing VBUS 5V power ◆ 6.0 W maximum if configured as USB Host and providing out VBUS 5V power ◆ The internal hardware configuration allows more than one or all power sources applied at the same time.

Table 3-10 SGX 5150 MD - Power Input Interface

Power Input	Description
Barrel Connector	◆ Center contact fork type for better grip ◆ 12 VDC Input with center = (+)
USB Type C Connector	◆ SGX can provide VBUS 5V 0.5A out if configured as USB host, and powered by Lantronix provided Medical Power Supply
Power Consumptions	◆ 1.9 W typical if configured as USB Device, or USB Host - but not providing VBUS 5V power ◆ 5.5 W maximum if configured as USB Host and providing out VBUS 5V power

Ethernet Ports

The Ethernet port has two LEDs (see *Table 3-6*) that indicate the status of the connection as described in *Table 3-12* and *Table 3-13* below.

Table 3-11 Ethernet RJ45 Connector Pinout

Pin Number	Signal Name
1	ETX+
2	ETX-
3	ERX+
4	Spare pin for PoE power input_1
5	Spare pin for PoE power input_1
6	ERX-
7	Spare pin for PoE power input_2
8	Spare pin for PoE power input_2
Right LED	See *Table 3-12*.
Left LED	See *Table 3-13*.

Table 3-12 Left Ethernet LED

Color/Status	Solid Light
Yellow	100 Mbps activity
OFF	10 Mbps activity

Table 3-13 Right Ethernet LED

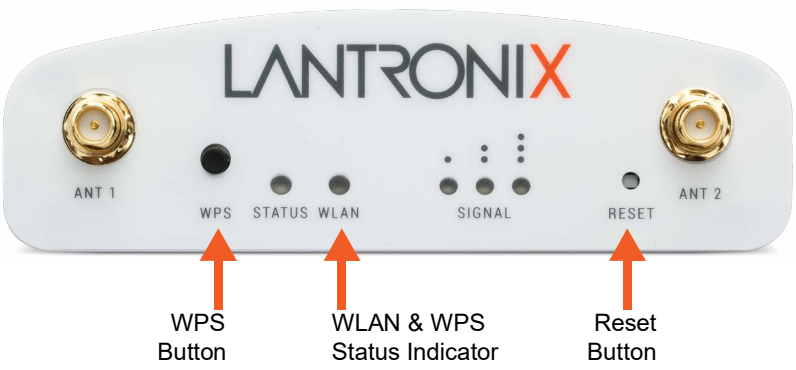
Color/Status	Blinking Light
Green	Link Up
OFF	No Link

The Ethernet port can conect to an Ethernet (10 Mbps) or fast Ethernet (100 Mbps) network.

Wi-Fi Protected Setup (WPS)

Using WPS, you have the option of connecting to SGX 5150 devices with a router or access point in a single operation instead of manually creating a profile with a network name (SSID), setting up wireless security parameters and updating the choice list.

Figure 3-9 Wi-Fi Protected Setup



Reset Button

Using a paper clip or similar object to poke through the RESET hole, press the recessed Reset button as shown in *Figure 3-9* for 6 seconds to reset the SGX 5150 configuration parameters to factory defaults and reboot.

To Start WPS

Press and hold the WPS button for minimum of 5 seconds (see *Figure 3-9*), the unit will start Wi-Fi protected setup.

Installing the SGX 5150

Be sure to place or mount the SGX 5150 gateway securely on a flat horizontal or vertical surface. The gateway comes with brackets for mounting it, for example, on a wall. If using AC power, do not use outlets controlled by a wall switch.

Observe the following guidelines when connecting the serial devices:

- The SGX 5150 serial ports support RS-232 or multi-protocol RS232/422/485 serial ports.
- Use a null modem cable to connect the serial port to another DTE device. Use a straight-though (modem) cable to connect the serial port to a DCE device.
- Connect your RJ-45 Ethernet cable to the RJ-45 port of the unit.

Perform the following steps to install your device:

1. Attach the two antennas to the SGX 5150 gateway.
2. Connect the equipment to the numbered device port (Serial 1/Serial 2) using appropriate cables and adapters.
3. Mount or place the SGX 5150 gateway securely.
4. Supply power to the SGX 5150 and connect it to the user device by using the supplied type A to type C USB cable. As soon as you plug the gateway into power, it powers up automatically, the self-test begins, and LEDs would indicate the gateway's status.

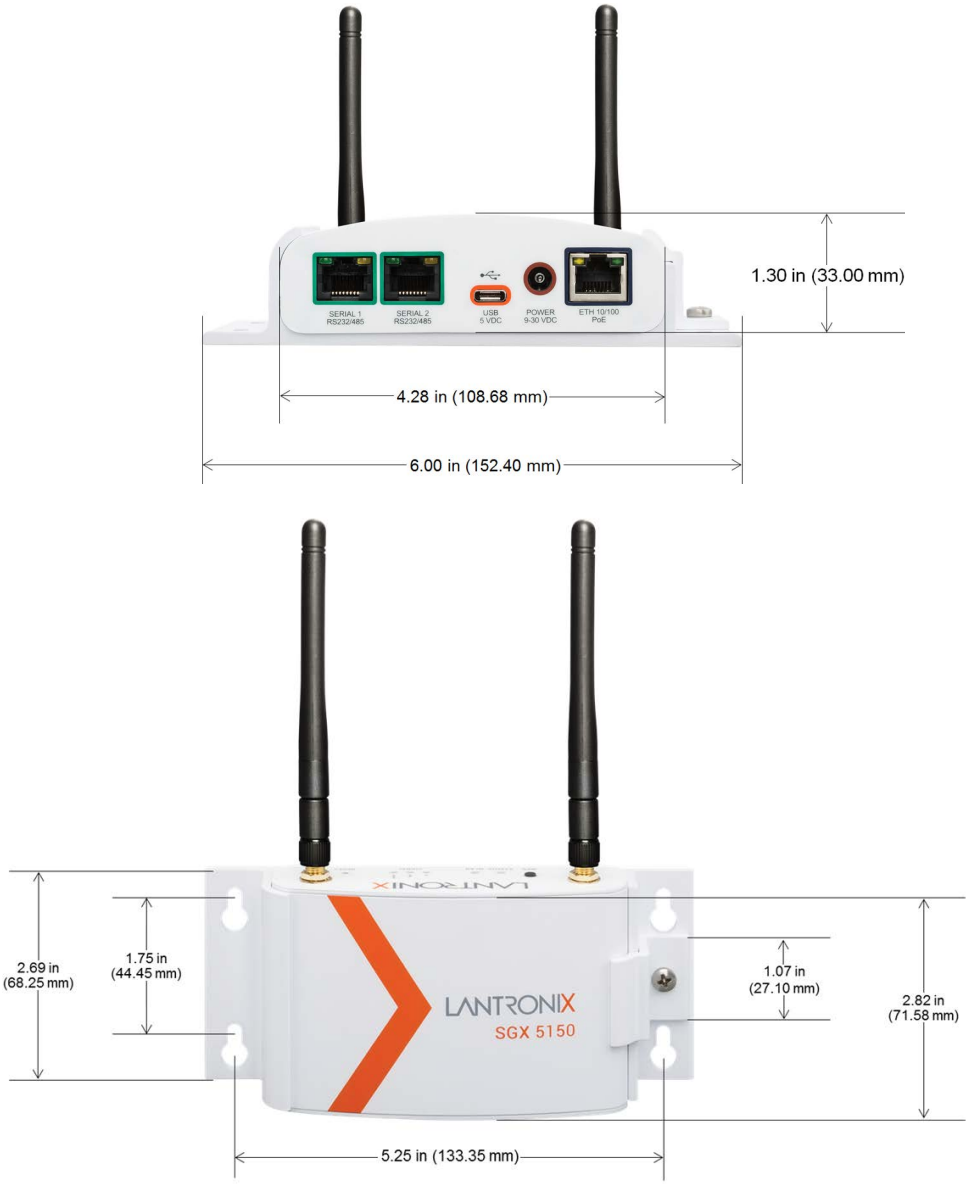
Notes:

- *The SGX 5150 supports a power range of 9 to 30 VDC and can be powered up via the barrel-power adapter or USB port.*
- *For the SGX 5150 MD it is required 12VDC from the Medical Power Supply Lantronix PN 520-160-R connected at barrel connector.*

5. Via the computer connected on the same network, you can follow one of two paths to device discovery and initial network configuration as outlined below.

Note: *Antennas must be installed prior to powering on the unit. Do not remove or connect the antennas while the unit power is on or proper wireless signals may not be transmitted or received as intended.*

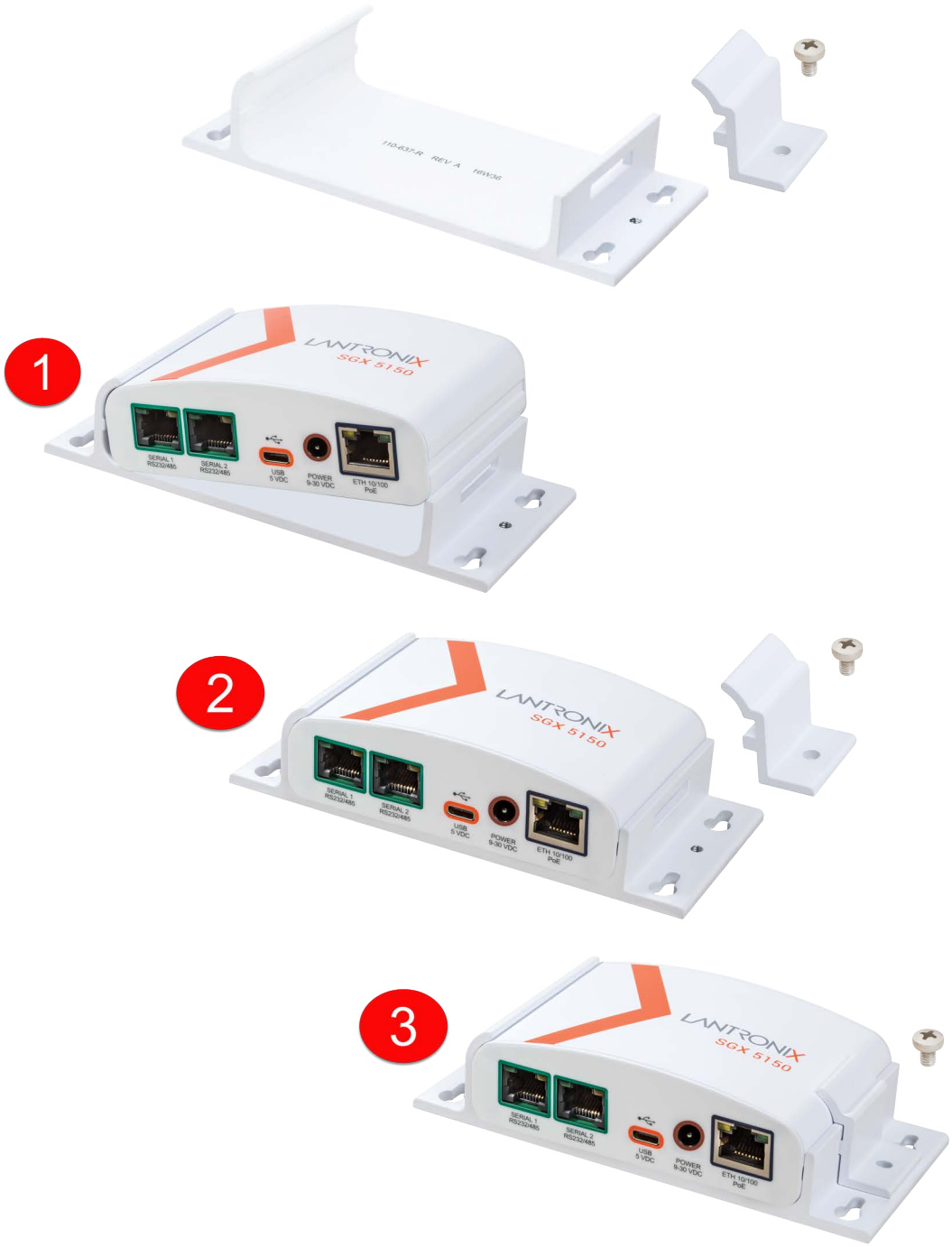
Figure 3-10 SGX 5150 Dimensions in Inches (in) and Millimeters (mm)



Optional SGX 5150 Bracket

A bracket accessory for securing the SGX 5150 IoT device gateway can be purchased at the Lantronix Online Store at https://store.lantronix.com/ or by calling Lantronix Sales at 800-422-7055. Purchased brackets will come with an installation guide.

Figure 3-11 Optional Bracket Installation



Wireless Quick Connect

Continue with these steps for Wireless Quick Connect after installing the SGX 5150 IoT device gateway.

1. From your Wi-Fi device, connect to `SSID sgx5150_*`, where * is your gateway 12-digit serial number.
2. From your browser, connect to `192.168.0.1` using these default login credentials:
   - The default User ID is "`admin`"
   - The default password is the last 8 characters of the Device ID (for devices manufactured after January 1, 2020) or "`PASS`" (for all older units)

   Note: *For security purposes, please change the admin password during initial setup.*
3. Select **Wireless Quick Connect**, choose the appropriate network name for the gateway connection, and follow the prompts for your wireless network required security parameters.
4. Click **Apply** to save and complete the wireless network setup.

4: Using Lantronix Provisioning Manager

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

Installing Lantronix Provisioning Manager

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

Accessing the SGX 5150 Using Lantronix Provisioning Manager

Note: For detailed instructions, see the Lantronix Provisioning Manager online help.

1. Launch Lantronix Provisioning Manager
2. If this is the first time you have launched Lantronix Provisioning Manager, you may need to proceed through an initial setup.
3. Locate the SGX 5150 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 SGX 5150 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.

5: Configuration Using Web Manager

This chapter describes how to configure the SGX 5150 unit using Web Manager, the Lantronix browser-based configuration tool. The device's configuration is stored in non-volatile memory and is retained across device reset and during loss of power to the device. All changes take effect immediately, unless otherwise noted. This chapter contains the following sections:

- *Accessing Web Manager*
- *Status Page*
- *Web Manager Components*
- *Navigating Web Manager*

Accessing Web Manager

Web Manager is normally accessed through a standard web browser but you can also access Web Manager through SoftAP. See the *SGX 5150 IoT Device Gateway Quick Start Guide* for instructions on accessing Web Manager through SoftAP. The quick start guide is available at www.lantronix.com/support/documentation.

To access Web Manager through a web browser:

1. Open a standard web browser. Lantronix supports the latest versions of Internet Explorer®, Firefox®, Safari®, or Chrome™ web browsers.
2. Enter the IP address or host name of the SGX 5150 unit in the address bar. The IP address may have been assigned automatically by DHCP. If you do not know the IP address, you can find it by using Lantronix Provisioning Manager. See *Chapter 4: Using Lantronix Provisioning Manager on page 39*.
3. Enter your username and password. The factory-default username is "**admin**" and the factory default password is the last 8 characters of the Device ID (for devices manufactured after January 1, 2020) or "**PASS**" (for all older units). The Status web page (see *Figure 5-12*) displays current configuration and status details for the device, network and line settings.

Status Page

This page appears upon logging into Web Manager and when you click the **Status** tab.

Figure 5-12 Status Page (Section 1 of 2)

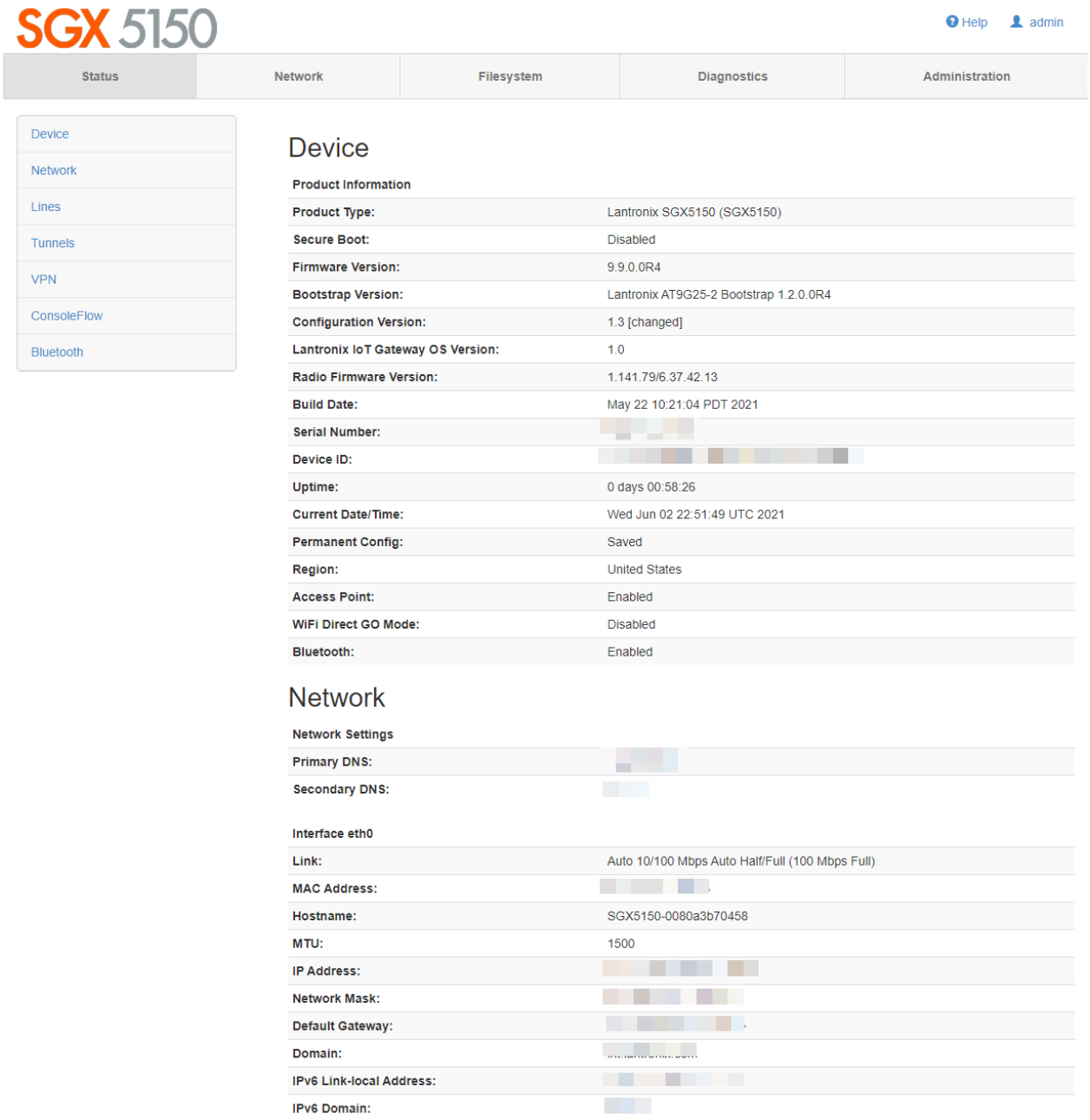
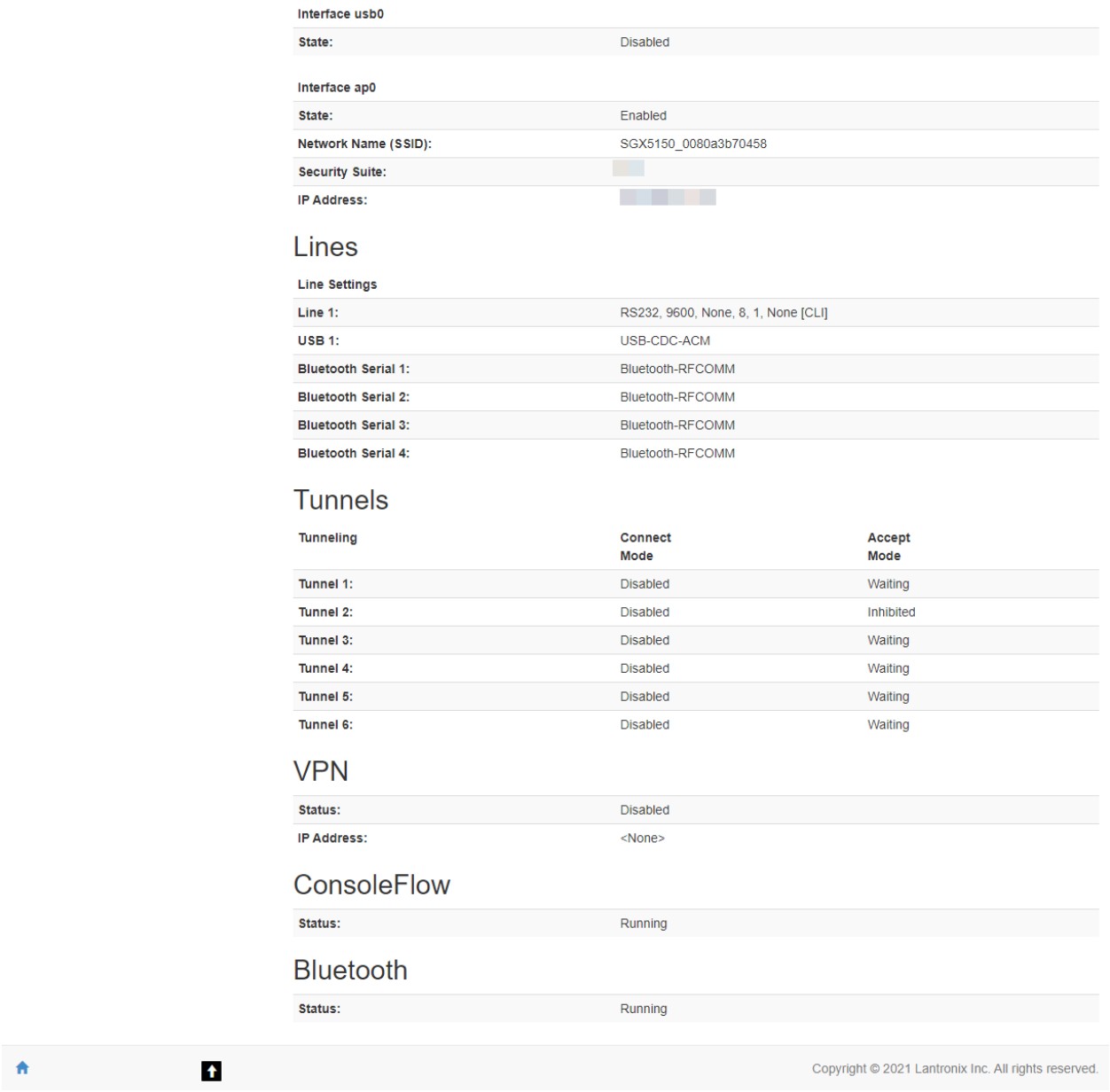


Figure 5-13 Status Page (Section 2 of 2)



Interface usb0	
State:	Disabled

Interface ap0	
State:	Enabled
Network Name (SSID):	SGX5150_0080a3b70458
Security Suite:	
IP Address:	

Lines

Line Settings	
Line 1:	RS232, 9600, None, 8, 1, None [CLI]
USB 1:	USB-CDC-ACM
Bluetooth Serial 1:	Bluetooth-RFCOMM
Bluetooth Serial 2:	Bluetooth-RFCOMM
Bluetooth Serial 3:	Bluetooth-RFCOMM
Bluetooth Serial 4:	Bluetooth-RFCOMM

Tunnels

Tunneling	Connect Mode	Accept Mode
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Inhibited
Tunnel 3:	Disabled	Waiting
Tunnel 4:	Disabled	Waiting
Tunnel 5:	Disabled	Waiting
Tunnel 6:	Disabled	Waiting

VPN

Status:	Disabled
IP Address:	<None>

ConsoleFlow

Status:	Running

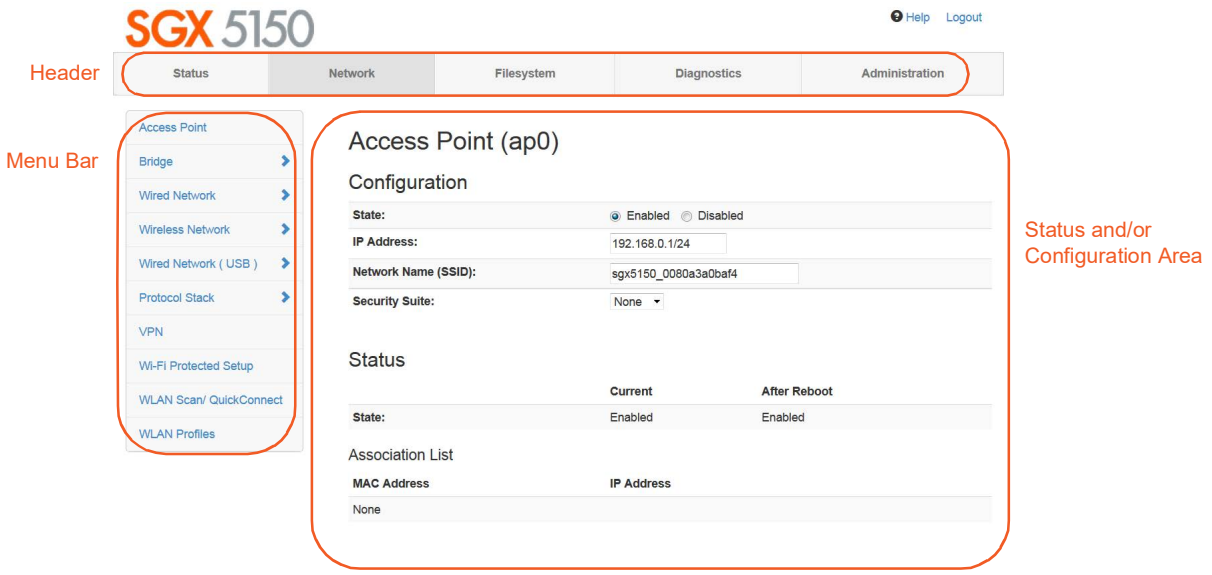
Bluetooth

Status:	Running

Web Manager Components

The layout of a typical Web Manager page is below.

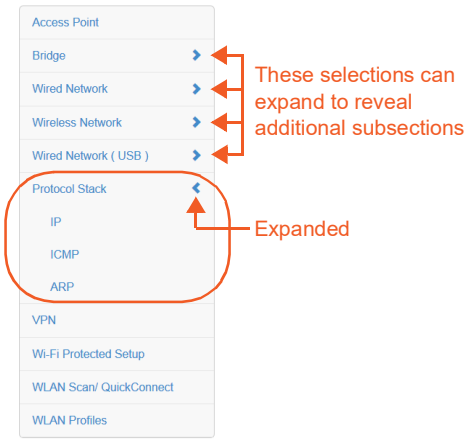
Figure 5-14 Components of the Web Manager Page



Web Manager pages have these sections:

- The **Status**, **Network**, **Filesystem**, **Diagnostics** and **Administration** tabs located in the **header** at the top of the page provide direct access to each Web Manager page of the same name. All the functionality is accessible through Web Manager and is divided between these tab/pages.
- Each Web Manager page accessed through the header tabs reveal a page-specific **menu bar** on the left side organizing available sections for that page.
  - The menu bar accessed via the **Network** and **Administration** tabs contain selections that can further expand to reveal additional subsections. A right-pointing blue arrow indicates a particular selection can be expanded to reveal subsections.
  - Expand or collapse an expandable menu bar section by clicking on it.
- The main body area of the page contains either view-only **Status info** or **Configuration options** according to the tab, menu bar selection or subsection selected.

Figure 5-15 Expandable Menu Bar Selections



- When a parameter is changed on a page, a **Submit** button will appear at the bottom of the page. Click on this button to save the change.
- A **Logout** link is available at the upper right corner of every Setup and Admin page. In Chrome or Safari, it is necessary to close out of the browser to completely logout. If necessary, reopen the browser to log back in.

Navigating Web Manager

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

Table 5-14 Web Manager Pages

Web Manager Page	Description	Page
Status	Shows Product Information, Alarms, Network, Line Tunnels, VPN, ConsoleFlow, and Bluetooth settings.	*41*
Access Point	Allows you to configure an access point and shows the current operational state of existing access points.	*41*
Action	Allows you to view and configure the actions for a specific alarm or report.	*88*
Applications	View and configure application running scripts.	*90*
Bluetooth	Allows you to view statistics and lets you enable or disable Bluetooth.	*91*
Bluetooth Serial	View and configure Bluetooth SPP profile settings for tunneling or command mode.	*92*
Bridge	Allows you to configure a bridge and shows the current operational state of the bridge.	*48*
CLI	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	*93*
Clock	Allows you to view and configure the current date, time and time zone as it displays in web manager.	*94*
ConsoleFlow	Shows the configuration and status for the ConsoleFlow client.	*95*
Diagnostics	Lets you perform various diagnostic procedures.	*81*
Discovery	Allows you to view and modify the configuration and statistics for device discovery.	*97*
DNS	Displays the current status of the DNS subsystem.	*81*
Email	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	*98*
Filesystem	Shows file system statistics and lets you browse the file system to view a file, create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.	*79*
FTP	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	*99*
Gateway	Shows statistics and lets you change the current configuration for the gateway.	*99*
GRE	Allows you to view and configure GRE settings.	*107*
Hardware	Shows hardware status and configuration options.	*82*
HTTP	Shows Hyper Text Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	*109*
IP Sockets	Shows IP socket status and lets you change hardware configuration.	*82*
Line	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	*112*
Log	Shows and allows changes with logs.	*83*
Memory	Shows memory status and lets you change hardware configuration.	*83*

Web Manager Page	Description	Page
Modbus	Shows the current connection status of the Modubs servers listening on the TCP ports and configure Modbus TCP server.	*114*
Network	Shows status and lets you configure the network interface.	*46*
Ping	Shows how to ping a network host with a DNS hostname or IP address.	*84*
Processes	Shows the processes currently running on the system.	*84*
Protocol Stack	Lets you perform lower level network stack-specific activities.	*68*
QuickConnect	Lets you change configuration settings for the Quick Connect.	*73*
Quick Setup	Shows the quick setup configuration options for the device.	*151*
Routes	Shows the current system routing table.	*85*
RSS	Shows RSS status and configuration optinos.	*115*
Security	Shows configuration and statistics for security.	*116*
SFTP	Shows SFTP status and configuration options.	*117*
SMTP	Shows SMTP status and configuration options.	*118*
SNMP	Shows SNMP status and configuration options.	*118*
SSH	Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	*120*
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	*123*
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	*128*
System	Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.	*129*
Terminal	Lets you change current settings for a terminal.	*131*
Threads	Shows thread ID numbers, names and CPU usage.	*85*
Traceroute	Shows how to perform a traceroute to a network host.	*85*
Tunnel	Lets you change the current configuration settings for an incoming tunnel connection.	*132*
USB	Shows USB status, command mode, and configuration options.	*143*
User Management	Shows the configuration of users.	*145*
VPN	Lets you view and configure VPN settings.	*70*
Wi-Fi Protected Setup	Lets you connect the device to router or access point via Wi-Fi Protected Setup (WPS).	*72*
WLAN Profiles	Lets you view, edit, delete and create a WLAN profile on a device.	*74*
WLAN Scan	Shows a scan of wireless devices within range of the device.	*73*
XML	Lets you export XML configuration and status records, and import XML configuration records.	*147*

6: Network Settings

Network settings for the SGX 5150 can be viewed and modified under the Network tab in the Web Manager user interface. This chapter describes the following network settings:

- *Access Point*
- *Bridge*
- *Wired (eth0) Network*
- *Wireless (wlan0) Network*
- *Wired (usb0) Network*
- *Protocol Stack*
- *VPN*
- *Wi-Fi Protected Setup*
- *WLAN Scan/QuickConnect*
- *WLAN Profiles*

Access Point

Configure software-enabled access point interface (SoftAP) on this page. Access point status information displays at the bottom half of the page.

Warning: ***If the SGX 5150 is connected to a 5 GHz access point on the WLAN, the SoftAP interface will not be accessible to devices that support only 2.4 GHz.***

Table 6-15 Access Point Settings

Access Point Field	Description
State	Select to enable or disable the access point. If enabled, the DHCP server will assign IP addresses to the access point clients.
Multicast Forwarding	Select to enable or disable forwarding of multicast packets.
Mode	Select the desired mode from the drop-down menu: ◆ **Always Up:** the SoftAP interface will always be up, allowing clients to connect at any time. Default selection. ◆ **Triggered:** in response to an external trigger event, the SoftAP interface will come up for a user-configurable amount of time (the 'First Client Connect Timeout' and the 'Last Client Disconnect Timeout') and allow clients to connect.

Access Point Field	Description
First Client Connect Timeout	Enter the number of seconds for the First Client Connect Timeout. Upon receiving an external trigger event the SoftAP interface will stay up this amount of time waiting for a client to connect. If, at the end of the First Client Connect Timeout no clients have connected, the SoftAP interface will immediately go back down. If, during the First Client Connect Timeout at least one client has attached, the SoftAP interface will remain up until the last client has disconnected. After the last client has disconnected, the SoftAP interface will remain up for a user-configurable amount of time (the 'Last Client Disconnect Timeout'), giving clients an opportunity to reconnect. ***Note:*** *This field appears when Triggered mode is selected.*
Last Client Disconnect Timeout	Enter the number of seconds for the Last Client Disconnect Timeout. After the last client has disconnected the SoftAP interface will stay up this amount of time, giving clients an opportunity to reconnect. If, at the end of the Last Client Disconnect Timeout no clients have reconnected, the SoftAP interface will immediately go down. If, during the Last Client Disconnect Timeout at least one client has attached, the SoftAP interface will remain up until the last client has disconnected. ***Note:*** *This field appears when Triggered mode is selected.*
SoftAP Trigger	Click the **Trigger** button to provide an external trigger event to bring the SoftAP interface up. ***Note:*** *This button and the timeout settings appear when Triggered mode is selected.*
Channel Selection	Select the desired channel from the drop-down menu through which the SoftAP will operate: ◆ **Automatic**: Allow the radio to select the channel for the SoftAP. ◆ **Configured**: Specify the channel on which the SoftAP should operate. ***Note:*** *The Configured setting will only control the channel on which the SoftAP operates as long as the station (STA) interface is not connected to an access point. Once the STA interface has established an association with an access point, the SoftAP will move to the STA interface's channel (determined by the access point.) The channel selected by the user will be validated by the UI against a list of channels supported by the radio. To prevent inconsistent channel/band combinations the UI will coordinate the 'SoftAP channel' and 'WLAN Band' settings.*
Channel	Enter the Channel number to be configured. ***Note:*** *This field appears when a Configured channel selection is selected.*
IP Address	Enter the IP address of the SoftAP interface.
Network Name (SSID)	Specify the network name/SSID of the access point. The SSID update will take effect after the SGX 5150 gateway is rebooted.
Security Suite	Select a security suite (None, WPA, or WPA2) to be used with the access point.
Key Type	Select Passphrase (default) or Hex key type. ***Note:*** *This field appears when WPA or WPA2 security suite is selected.*
Key	Enter a hex key if WPA or WPA2 security suite is selected. ***Note:*** *This field appears when WPA or WPA2 security suite and Hex key type are selected.*

Access Point Field	Description
Passphrase	Enter a passphrase if WPA or WPA2 security suite is selected above. ***Note:*** *This field appears when WPA or WPA2 security suite and Passphrase key type are selected.*
Show Password (check box)	Check to make the key or passphrase entered to the left visible. ***Note:*** *This field appears when WPA or WPA2 security suite is selected.*
DNS Redirect	Enter the name to the IP address of the Access Point. DNS names are case insensitive.
SSID Broadcast	If enabled, the gateway will broadcast its SSID in the beacons that are sent out. Enabled by default.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View or Configure Access Point Settings

Using Web Manager

- To view access point statistics and configuration options, on the **Network** page, click **Access Point**.

Using the CLI

- To enter the command level: `enable > config > access point`

Using XML

- Include in your file: `<configgroup name="access point">`

Bridge

The SGX 5150 bridges traffic between an Ethernet or USB RNDIS (usb0) and WLAN interface. For example, br0 is a bridge between eth0 and wlan0. For USB RNDIS interface, USB 1 must be configured as an Ethernet device.

When a bridge is enabled, the *Wired (eth0) Network* configuration is used for configuring direct connections into the SGX 5150 gateway over the primary interface; the *Wireless (wlan0) Network* configuration is ignored. Both the Ethernet and WLAN link configurations are used the same as when the bridge is disabled.

Bridging MAC Address specifies the MAC address of bridgeable traffic between the Ethernet and WLAN interfaces. When bridging is active, this MAC Address will be used as the MAC address of the WLAN interface. Packets received on the Ethernet interface from this address will be bridged to the WLAN interface (except traffic directed at the Primary Interface). If this field is not configured, then the SGX 5150 gateway waits for the first packet to arrive on the Ethernet interface and uses the source address as the bridging address.

Bridging IP Address specifies the IP address of the bridged client.

When bridging is active, this IP Address will be used to create a static route between the SGX 5150 gateway and the bridged client.

This route is required for connecting to the bridged client from devices connected via the access point network and from this SGX 5150 gateway.

If Auto Detect IP Address is enabled, then the SGX 5150 gateway will attempt to learn the IP Address by using the source or destination IP address of packets arriving on the Ethernet interface.

Warning: ***Running processes may be impacted while the SGX 5150 gateway monitors Ethernet traffic to determine the wired host IP address.***

During initialization, the bridging subsystem enables and controls both eth0 and wlan0 networks. These are important aspects to keep in mind:

- If the eth0 physical link is inactive, wlan0 is the primary interface.
- If the eth0 physical link is active, eth0 is the primary interface.

When the eth0 link is active, the wlan0 link is established. Additionally, the bridging MAC address is acquired using preconfiguration or auto-detection, and bridging enters the Active state. If either link goes down, bridging reverts to the Inactive state.

When in the Active state, all packets that arrive on the wlan0 interface are bridged out (through) the eth0 interface. Similarly, all packets that arrive on the eth0 interface are bridged out (through) the wlan0 interface. However, exceptions to this behavior include:

- Ethernet packets directed specifically to the Ethernet (eth0) MAC address are terminated internally and are not bridged to WLAN.
- An ARP request for the primary interface IP address is terminated internally and is not bridged to the WLAN.

Ethernet packets that do not originate from the bridging MAC Address are discarded.

Bridge Status and Configuration

View-only status information on the Bridge1 (br0) Status page displays whether bridging is currently enabled, active, and the following (if any): Ethernet link, WLAN link, primary interface, bridging MAC, Ethernet MAC, WLAN MAC, bridging IP address, and bridging IPv6 address. Ethernet to WLAN and WLAN to Ethernet statistics are provided for unicast, nonunicast, discards and octets.

See *Table 6-16* for the bridge settings that can be modified on the Bridge1 (br0) Configuration page.

Table 6-16 Bridge Settings

Bridge Fields	Description
State	Select to enable or disable bridging. When a bridge is Enabled, the Ethernet Network Interface Configuration is used for configuring direct connections into the SGX 5150 gateway over the primary Interface. The WLAN Network Interface Configuration is ignored. Both the Ethernet and WLAN Link Configurations are used the same as when the bridge is disabled. In Bridge Statistics: ◆ **Enable State** shows whether the bridge is currently enabled. If the state is changed, it will not be reflected here until the next reboot. ◆ **Active State** shows the current state of the bridge. The bridge may be Active or Inactive, depending on the state of the bridge and the physical links.

Bridge Fields	Description
Bridging Mode	Select either Host, Network, or Static Network. ◆ In **Host** mode, a single device is connected via Ethernet. Default. ◆ In **Network** mode, multiple devices can be connected via Ethernet through a switch. DHCP server with DHCP relay must be enabled. ◆ In **Static Network** mode, multiple devices with static IP addresses can be connected via Ethernet through a switch. If the DHCP server with DHCP relay is also enabled, the SGX 5150 will act as a DHCP relay agent.
Transparent Mode	Select to enable or disable transparent mode. This can only be enabled if Bridging Mode is **Host**. ◆ If **Enabled**, the SGX 5150 can no longer be accessed via telnet or web manager from a PC and is invisible to the network. The connected device and the SGX 5150 will share a MAC address. Default. ◆ If **Disabled**, the SGX 5150 will be accessible to a PC on the network via telnet or Web Manager.
Network Access for Gateway	Select to enable or disable network access for the gateway. This can only be enabled if Transparent Mode is **Enabled**. ◆ If **Enabled**, the SGX 5150 gateway will share the Ethernet IP address of the bridged client in addition to the MAC address. WLAN Network Interface Configuration must match the bridged client Ethernet configuration. Local ports must be configured to distinguish network traffic destined for the SGX 5150 gateway. Any port configured on the SGX 5150 gateway must be different from those in use by services on the bridged client. Default. ◆ If **Disabled**, the SGX 5150 will not be accessible over the network.
Ethernet Interface	Select interface from drop-down menu: ◆ eth0 (default) ◆ usb0
Bridging MAC Address	Enter the bridging MAC address which specifies the MAC address of bridgeable traffic between the Ethernet and WLAN interfaces. When bridging is active, this MAC Address will be used as the MAC address of the WLAN interface. Packets received on the Ethernet interface from this address will be bridged to the WLAN interface (except traffic directed at the primary interface). If this field is not configured, then the SGX 5150 gateway waits for the first packet to arrive on the Ethernet interface and uses the source address as the bridging address.
Bridging IP Address	Enter the bridging IP address which specifies the IP address of the bridged client. When bridging is active, this IP address will be used to create a static route between this SGX 5150 gateway and the bridged client. This route is required for connecting to the bridged client from devices connected via the access point network and from this gateway.
Auto Detect IPv4 Address	Select to enable or disable auto detection of IPv4 addresses. If enabled, the SGX 5150 gateway will attempt to learn the IP addresses by using the source or destination IP address of packets arriving on the Ethernet interface. ***Warning:*** ***Running processes may be impacted while the SGX 5150 gateway monitors Ethernet traffic to determine the wired host IP address.***
Auto Detect IPv6 Address	Select to enable or disable auto detection of IPv6 addresses. If enabled, the SGX 5150 gateway will attempt to learn the IP addresses by using the source or destination IP address of packets arriving on the Ethernet interface. ***Warning:*** ***Running processes may be impacted while the SGX 5150 gateway monitors Ethernet traffic to determine the wired host IP address.***

Bridge Fields	Description
Bridging IPv6 Address	Enter the bridging IPv6 address.
Initial Scan Interval	Indicate the interval, in seconds, the SGX 5150 gateway will attempt to learn the IP address initially.
Scan Interval	Indicate how often the SGX 5150 gateway will attempt to learn if the IP address has changed. ***Warning:*** ***Running processes may be impacted while the SGX 5150 gateway monitors Ethernet traffic to determine the wired host IP address.***
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View or Configure Bridge Settings

Using Web Manager

- To view the Bridge status, on the **Network** page, click **Bridge** > **Statistics**.
- To configure Bridge settings, on the **Network** page, click **Bridge** > **Configuration** in the links.

Using the CLI

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

Using XML

- Include in your file: `<configgroup name="bridge" instance="br0">`

Wired (eth0) Network

Network interface settings apply to both the wired Ethernet (eth0) and wireless WLAN (wlan0) interfaces, but are configured independently for each interface. The wired network pages are described in this section.

Interface Status and Configuration

Table 6-17 displays the wired interface status and configuration information. The view-only status information is available on the Wired (eth0) Network Interface Status page. This same information is configurable on the Wired (eth0) Network Interface Configuration page.

Table 6-17 Wired (eth0) Network Interface

Field/Button	Description
State	Select to enable or disable the interface
Hostname	Enter the hostname for the interface. It must begin with a letter or number, continue with a sequence of letters, numbers, or hyphens, and end with a letter or number. This setting will take effect immediately, but will not register the hostname with a DNS server until the next reboot.

Field/Button	Description
Priority	Priority ranges from 0-10. The IP stack will give the interface with the lowest numerical value highest priority and the highest numerical values lowest priority when sending data. This setting only applies when the SGX 5150 gateway is not in bridging mode and both interfaces are connected to the same IP subnet.
MTU	When DHCP is enabled, the MTU size is (usually) provided with the IP address. When not provided by the DHCP server, or using a static configuration, this value is used. The MTU size can be from 576 to 1500 bytes, the default being 1500 bytes.
IPv4 State	Select to enable or disable.
DHCP Client	Select to turn **On** or **Off**. At boot up, after the physical link is up, the *SGX 5150 unit* will attempt to obtain IPv4 settings from a DHCP server and will periodically renew these settings with the server. ***Note:*** *Overrides the configured IPv4 address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the SGX 5150 gateway. Within Web Manager, click* ***Renew*** *to renew the DHCP lease.*
IP Address	Enter the static IPv4 address to use for the interface. You may enter it alone or in CIDR format. ***Note:*** *This setting will be used if Static IP is active (DHCP is Disabled). Changing this value requires you to reboot the SGX 5150 gateway. When DHCP is enabled, the SGX 5150 unit tries to obtain an IPv4 address from a DHCP server. If it cannot, the SGX 5150 unit generates and uses an Auto IP address in the range of 169.254.xxx.xxx, with a network mask of 255.255.0.0.*
Default Gateway	Enter the IPv4 address of the router for this network. ***Note:*** *This setting will be used if Static IP is active (DHCP is* ***Disabled****).*
Domain	Enter the domain name suffix for the interface. ***Note:*** *This setting will be used when either static IP or auto IP is active, or if DHCP is active and no domain suffix was acquired from the server****.***
DHCP Client ID	Enter the ID if the DHCP server requires a DHCP client ID option. The DHCP server's lease table shows IP addresses and MAC addresses for devices. The lease table shows the client ID, in hexadecimal notation, instead of the SGX 5150 unit MAC address.
Primary DNS	Enter the IP address of the primary domain name server (DNS.) ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
Secondary DNS	Enter the IP address of the secondary domain name server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
IPv6 State	Select to enable or disable.
IPv6 DHCP Client	Select to turn **On** or **Off**. At bootup, after the physical link is up, the SGX 5150 unit will attempt to obtain IPv6 settings from a DHCPv6 server and will periodically renew these settings with the server. ◆ **On:** enables the SGX 5150 server to obtain IPv6 setting from a DHCPv6 server upon bootup. ◆ **Off:** enables the SGX 5150 server to obtain IPv4 settings from a DHCP server upon bootup. ***Note:*** *Overrides the configured IP address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the SGX 5150 gateway. Within Web Manager, click Renew to renew the DHCPV6 lease.*

Field/Button	Description
IPv6 Auto Configuration	Select to turn **On** or **Off** IPv6 auto configuration.
IPv6 IP Address	Enter the static IPv6 address to use for the interface. ***Note:*** *This setting is used if Static IPv6 is active (DHCPv6 is Disabled). Changing this value requires a reboot. When DHCPv6 is enabled, the SGX 5150 unit tries to obtain an IPv6 address from a DHCPv6 server. If it cannot, then SGX 5150 unit generates and uses a Link local IPv6 address.*
IPv6 Default Gateway	Enter the default IPv6 default gateway.
IPv6 Domain	Enter the domain name suffix for the interface. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no Domain Suffix was acquired from the server.*
IPv6 Primary DNS	Enter the IP address of the primary domain name server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
IPv6 Secondary DNS	Enter the IP address of the secondary domain name server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure Network Interface Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Link Status and Configuration

Table 6-18 displays the wired link status and configuration information. The view-only status information is available on the Wired (eth0) Network Ethernet Link page. This same information is configurable on the Wired (eth0) Network Ethernet Link Configuration page.

Table 6-18 Link (eth0) Configuration

Field/Button	Description
Speed	Select the Ethernet link speed. (Default is **Auto**.) ◆ **Auto** = Auto-negotiation of Link Speed ◆ **10 Mbps** = Force 10 Mbps ◆ **100 Mbps** = Force 100 Mbps

Field/Button	Description
Duplex	Select the Ethernet link duplex mode. (Default is **Auto**.) ◆ **Auto** = Auto-negotiation of Link Duplex ◆ **Half** = Force Half Duplex ◆ **Full** = Force Full Duplex
EAPoL	Select to enable or disable EAPoL (Extensible Authentication Protocol) authentication. If Enabled, the EAPoL Security Configuration fields are displayed.
EAPol Security Configuration	
IEEE 802.1X	Choose an IEEE 802.1X authentication type: ◆ EAP-TLS ◆ EAP-TTLS ◆ PEAP ◆ FAST
Validate Certificate	Validate the certificate installed on the PremierWave 2050 gateway by selecting **Enabled** in the Validate Certificate field which appears. Validates the certificate installed on the gateway with the one received from the RADIUS server. ***Note:*** *This field appears if the EAP-TLS IEEE 802.1X authentication type is selected.*
Secure Credentials	After EAP-TLS is selected and the Validate Certificate is enabled, either: ◆ Select the credential, if listed in the dropdown menu, to validate. ◆ Type the name of the credential if the credential is not listed in the dropdown menu. ***Note:*** *This field appears if EAP-TLS IEEE 802.1X authentication type is selected.*
EAP-TTLS Option	Select a security protocol: ◆ EAP-MSCHAPV2 ◆ MSCHAPV2 ◆ MSCHAP ◆ CHAP ◆ PAP ◆ EAP-MD5 ***Note:*** *This field appears if EAP-TTLS IEEE 802.1X authentication type is selected.*
PEAP Option	Select an option: ◆ EAP-MSCHAPV2 ◆ EAP-MD5 ◆ EAP-TLS ***Note:*** *This field appears if PEAP IEEE 802.1X authentication type is selected.*
FAST Option	Select an option: ◆ MD5 ◆ MSCHAPV2 ◆ GTC ***Note:*** *This field appears if FAST IEEE 802.1X authentication type is selected.*
FAST Provisioning	Select the FAST provisioning option: ◆ Unauthenticated ◆ Authenticated (default) ◆ Both ***Note:*** *This field appears if FAST IEEE 802.1X authentication type and MSCHAPV2 FAST Option is selected.*

Field/Button	Description
Username	Enter a username.
Password	Enter a password. Check the **Show Password** check box to make the password viewable as you enter it in the Password field. ***Note:*** *This field appears if the EAP-TTLS, PEAP, or FAST IEEE 802.1X authentication type is selected.*
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

Notes:

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

To Configure Network Link Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

QoS Statistics and Configuration

QoS (Quality of Service) can be enabled and configured for both the Wireless (wlan0) Network and wired Network (eth0). If enabled, the router will control the flow of outbound traffic according to the user-defined filters. In other words, QoS improves performance by allowing the user to prioritize applications. Filters can be defined to prioritize traffic based on the source or destination network, source or destination port, or the source MAC address. Up to 32 user-defined filters can be added. The following are predefined priority classes:

- Network Control and Internetwork Control are typically used for network control packets such as ICMP and have the highest priorities. Bandwidth allocation is a minimum 5% to network control.
- Voice: Bandwidth allocation is minimum 30%.
- Video: Bandwidth allocation is minimum 20%.
- Critical Applications: Bandwidth allocation is minimum 15%.
- Excellent Effort: Bandwidth allocation is minimum 10%.
- Best Effort: Bandwidth allocation is minimum 10%.
- Background: Bandwidth allocation is minimum 5% and has the lowest priority.

Table 6-19 Wired (eth0) Network QoS Settings shows the network QoS settings that can be configured including adding new filters.

Table 6-19 Wired (eth0) Network QoS Settings

Wired (eth0) Network Settings	Description
State	Click to enable or disable state.
Import filters	Click to enable or disable import filters to import configurations from other interfaces.
Uplink Speed	Enter the maximum uplink speed. Set 0 to set speed to default.
Delete	Click the checkbox to the left of any existing QoS filter to be deleted and click the Submit button.
Filter type	Select the filter type from the drop-down window: ◆ Network ◆ Port
Network	Enter the Network, if the Network filter type is selected.
Ports	Enter the Port, if the Port filter type is selected.
Priority	Select the priority of the filter from the drop-down menu.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View and Configure Wired Network QoS Settings

Using Web Manager

- To view Ethernet (eth0) QoS statistics, click **Network** on the menu and select **Wired Network > QoS**.
- To modify Ethernet (eth0) QoS information, click **Network** on the menu and select **Wired Network > QoS > Configuration**.

Using the CLI

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

Using XML

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

Wired (eth0) Network Failover

The SGX 5150 device gateway provides WAN network failover, in the form of a "dead remote host reachability" mechanism (essentially a ping against a known host). If the remote host is determined to be not reachable, the SGX 5150 gateway will failover to the Wi-Fi interface. If the remote host is determined to be reachable, the gateway will failback to the Ethernet interface.

Table 6-20 Wired (eth0) Network Failover Settings

Wired Network (Failover) Settings	Description
State	Click to enable or disable state.
Failover Interface	Always select wlan0 in the SGX 5150 device gateway.
Hostname	Enter the remote host to test reachability.
Method	Select ICMP or TCP based ping.
Timeout	Indicate the interval to wait for ping response from remote host.
Interval	Indicate the interval in which to test reachability
Failover Threshold	Indicate the allowed number of failed pings – after which the SGX 5150 gateway will failover to the wlan0 interface.
Failback Threshold	Indicate the number of successful pings – after which the SGX 5150 gateway will failback to the Ethernet interface.
Test (button)	Click the **Test** button to test if failover hostname is reachable.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View and Configure Wired Network Failover Settings

Using Web Manager

- To view Ethernet Failover statistics, click **Network** on the menu and select **Wired Network > Failover**.
- To modify Ethernet Failover settings, click **Network** on the menu and select **Wired Network > Failover > Configuration**.

Using the CLI

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

Using XML

- Include in your file: `<configgroup name="network failover" instance="eth0">`

Wireless (wlan0) Network

The wireless network pages are used to configure and view the status of the wireless (wlan0) interface and link on the SGX 5150 gateway. To see the effect of these items after a reboot, view the Status page.

Wireless (wlan0) Network Interface

Table 6-21 displays the wireless interface status and configuration information. The view-only status information is available on the Wireless (wlan0) Network Interface Status page. This same information is configurable on the Wireless (wlan0) Network Interface Configuration page.

Table 6-21 Wireless (wlan0) Interface Configuration

Field/Button	Description
State	Select to enable or disable the interface
Hostname	Enter the hostname for the interface. It must begin with a letter or number, continue with a sequence of letters, numbers, or hyphens, and end with a letter or number. This setting will take effect immediately, but will not register the hostname with a DNS server until the next reboot**.**
Priority	Priority ranges from 0-10. The IP stack will give the interface with the lowest numerical value highest priority and the highest numerical values lowest priority when sending data. This setting only applies when the gateway is not in bridging mode and both interfaces are connected to the same IP subnet.
MTU	When DHCP is enabled, the MTU size is (usually) provided with the IP address. When not provided by the DHCP server, or using a static configuration, this value is used. The MTU size can be from 576 to 1500 bytes, the default being 1500 bytes.
IPv4 State	Select to enable or disable.
DHCP Client	Select to turn **On** or **Off**. At boot up, after the physical link is up, the SGX 5150 unit will attempt to obtain IPv4 settings from a DHCP server and will periodically renew these settings with the server. ***Note:*** *Overrides the configured IPv4 address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the SGX 5150 gateway. Within Web Manager, click* ***Renew*** *to renew the DHCP lease.*
IP Address	Enter the static IPv4 address to use for the interface. You may enter it alone or in CIDR format. ***Note:*** *This setting will be used if Static IP is active (DHCP is Disabled). Changing this value requires you to reboot the SGX 5150 gateway. When DHCP is enabled, the SGX 5150 unit tries to obtain an IPv4 address from a DHCP server. If it cannot, the SGX 5150 unit generates and uses an Auto IP address in the range of 169.254.xxx.xxx, with a network mask of 255.255.0.0.*
Default Gateway	Enter the IPv4 address of the router for this network. ***Note:*** *This setting will be used if Static IP is active (DHCP is* ***Disabled****).*
Domain	Enter the domain name suffix for the interface. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no Domain Suffix was acquired from the server****.***
DHCP Client ID	Enter the ID if the DHCP server requires a DHCP Client ID option. The DHCP server's lease table shows IP addresses and MAC addresses for devices. The lease table shows the client ID, in hexadecimal notation, instead of the SGX 5150 device MAC address.
Primary DNS	Enter the IP address of the primary domain name server ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
Secondary DNS	Enter the IP address of the secondary domain name server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
IPv6 State	Select to enable or disable.

Field/Button	Description
IPv6 DHCP Client	Select to turn **On** or **Off**. At bootup, after the physical link is up, the SGX 5150 unit will attempt to obtain IPv6 settings from a DHCPv6 server and will periodically renew these settings with the server. ◆ **On:** enables the SGX 5150 server to obtain IPv6 setting from a DHCPv6 server upon bootup. ◆ **Off:** enables the SGX 5150 server to obtain IPv4 settings from a DHCP server upon bootup. ***Note:*** *Overrides the configured IP address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the SGX 5150 gateway. Within Web Manager, click Renew to renew the DHCPV6 lease.*
IPv6 Auto Configuration	Select to turn **On** or **Off** IPv6 auto configuration.
IPv6 IP Address	Enter the static IPv6 address to use for the interface. ***Note:*** *This setting is used if Static IPv6 is active (DHCPv6 is Disabled). Changing this value requires a reboot. When DHCPv6 is enabled, the SGX 5150 unit tries to obtain an IPv6 address from a DHCPv6 server. If it cannot, then SGX 5150 unit generates and uses a Link local IPv6 address.*
IPv6 Default Gateway	Enter the default IPv6 default gateway.
IPv6 Domain	Enter the domain name suffix for the interface. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no Domain Suffix was acquired from the server.*
IPv6 Primary DNS	Enter the IP address of the primary Domain Name Server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
IPv6 Secondary DNS	Enter the IP address of the secondary Domain Name Server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View or Configure Wireless Network Interface Settings

Using Web Manager

- To view the wireless (wlan0) network interface status, on the **Network** page, then select **Wireless Network** > **Interface**.
- To configure wireless (wlan0) network interface settings, on the **Network** page, select **Wireless Network** > **Interface** > **Configuration**.

Using the CLI

- To enter the command level: `enable > config > if 2`

Using XML

- Include in your file: `<configgroup name= "interface" instance="wlan0">`

Wireless (wlan0) Network Link

Configuration details are stored in one or more WLAN profiles. See *WLAN Profiles (on page 74)* to view and configure WLAN profiles. You can select and prioritize up to four preconfigured WLAN

profiles for automatic connection to wireless networks. Dynamic profiles, created via quick connect/WPS, have a higher priority over a static profile. Listed dynamic and static profiles can be prioritized with 1 being highest priority through 4 being lowest priority.

Table 6-22 displays the wireless link status and configuration information. The view-only status information is available on the Wireless (wlan0) Network WLAN Link Status page. This same information is configurable on the Wireless (wlan0) Network WLAN Link Configuration page.

Table 6-22 Wireless (wlan0) Link Configuration

Field/Button	Description
Choice 1 Profile **Choice 2 Profile** **Choice 3 Profile** **Choice 4 Profile**	Enter up to four (4) *WLAN Profiles (on page 74)* for automatic connection to wireless networks in order of priority, with **Choice 1 Profile** being highest priority through **Choice 4 Profile** being lowest priority. If a profile in the choice list is deleted, that profile is skipped in the connection attempt.
Antenna Diversity	Enable antenna diversity or select a specific antenna for use.
Debugging Level	Set the verbosity level for printing WLAN link messages to the TLOG (default is **Info**).
WiFi Direct GO Mode	Select to enable or disable. If enabled, WPS issues the credentials when the client device indicates that it wishes to connect with our device. No password is required. Go to *Wi-Fi Protected Setup (on page 72)* to setup WPS.
Band	Select the band from the drop-down menu. This will be the band on which the radio will operate. This global band setting will control both WLAN0 and SoftAP interfaces and override any frequency settings on the SoftAP interface. ***Notes:*** ◆ *To prevent inconsistent channel/band combinations, the user interface will coordinate the 'SoftAP Channel' and 'WLAN Band' settings.* ◆ *Wi-Fi Direct requires that the 2.4 GHz band be available. The UI will prevent the selection of '5GHz Only' when Wi-Fi Direct GO Mode is enabled.*
Scanning Latency	Select the desired **Scanning Latency**: ◆ **Standard** performs a complete unbroken scan of a list of channels. Scanning Channel List accepts list of channels. ◆ **Enhanced Throughput** breaks the scanning into small blocks of channels, reducing the impact on network throughput and improving the availability of the Access Point (AP0) interface (if enabled). ***Warning:*** ***Selecting Enhanced Throughput may greatly increase the time required to establish a connection on the wlan0 interface. The scanning channel list is unavailable when Enhanced Throughput is selected.*** *The **Scanning Channel List** setting only accepts 20 MHz channels (5 GHz band.) If the external access point to which the SGX 5150 STA interface is connecting supports 'wide' channels (40 MHz or above), it is possible that the SGX 5150 gateway may appear to connect on a channel not in the Scanning Channel List. For example, if the external AP is configured for channel 36 with 40 MHz support enabled the SGX 5150 may indicate a connection on channel 38. It has also been observed with the Netgear WNDAP350 AP (configured with 40 MHz channel support) that the SGX 5150 may establish a connection with either of the bonded 20 MHz channels (whether or not it is included in the 'Scanning Channel List'.) For example, if the Netgear WNDAP350 is configured to operate on channel 40 (with 40 MHz support enabled) the SGX 5150 may establish a connection on channel 36.*

Field/Button	Description
Scanning Channel List	Enter the **Scanning Channel List** in the field. This field accepts comma separated integers as list of channels. An empty list is considered as default and all radio supported channels are considered.
Apply (button)	Click the **Apply** button to apply the WLAN settings without saving them to flash memory. If the WLAN settings do not work, reboot the device to restore the original settings. The **Apply** button appears when new settings are entered.
Submit (button)	Click the **Submit** button to update the WLAN settings and save them to flash memory. The **Submit** button appears when new settings are entered.

Smart Roam

Wireless network (wlan0) smart roaming can be enabled and configured on the SGX 5150 gateway.

Table 6-23 Smart Roam Settings

Field/Button	Description
Roaming	Enable or disable Roaming. Disabled by default.
Level	Choose a radio preset: ◆ Low (default) ◆ Medium ◆ High Upon changing any value, the **Level** is changed to Custom.
Scan Interval	Scan interval in seconds. The scan interval is the time between scans looking for a roaming candidate.
RSSI Delta For 2.4 GHz	RSSI 2.4 GHz delta value in dBm. A device with an RSSI delta higher than the current access point is a roaming candidate.
RSSI Delta For 5 GHz	RSSI 5 GHz delta value in dBm. A device with an RSSI delta higher than the current access point is a roaming candidate.
Scan Threshold For 2.4 GHz	The 2.4 GHz RSSI threshold. When the signal drops below the scan threshold, the radio attempts to roam.
Scan Threshold For 5 GHz	The 5 GHz RSSI threshold. When the signal drops below the scan threshold, the radio attempts to roam.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View or Configure Network Link Settings

Using Web Manager

- To view wireless (wlan0) link statistics, on the **Network** page, select **Wireless Network** > **Link**.
- To configure wireless (wlan0) link settings, on the **Network** page, select **Wireless Network** > **Link** > **Configuration**.
- To configure wireless (wlan0) roaming settings, on the **Network** page, select **Wireless Network** > **Link** > **Smart Roam**.

Using the CLI

- To enter the command level: `enable > config > if 2 > link`

Using XML

- Include in your file: `<configgroup name= "interface" instance="wlan0">`

Wireless (wlan0) Network QoS

QoS (Quality of Service) can be enabled and configured for both Wired (eth0) Network and Wireless (wlan0) Network. If enabled, the router will control the flow of outbound traffic according to the user-defined filters. In other words, QoS improves performance by allowing the user to prioritize applications. Filters can be defined to prioritize traffic based on the source or destination network, source or destination port, or the source MAC address. Up to 32 user-defined filters can be added. The following are predefined priority classes:

- Network Control and Internetwork Control are typically used for network control packets such as ICMP and have the highest priorities. Bandwidth allocation is a minimum 5% to each network control.
- Voice: Bandwidth allocation is minimum 30%.
- Video: Bandwidth allocation is minimum 20%.
- Critical Applications: Bandwidth allocation is minimum 15%.
- Excellent Effort: Bandwidth allocation is minimum 10%.
- Best Effort: Bandwidth allocation is minimum 10%.
- Background: Bandwidth allocation is minimum 5% and has the lowest priority. *Table 6-24* shows the network QoS settings that can be configured including adding new filters.

Table 6-24 Wireless (wlan0) Network QoS Settings

Wireless Network (QoS) Settings	Description
State	Click to enable or disable state.
Import filters	Click to enable or disable import filters to import configurations from other interfaces.
Uplink Speed	Enter the maximum uplink speed. Set 0 to set speed to default.

Table 6-25 Adding or Deleting Wireless (wlan0) Network QoS Settings

Adding or Deleting Wireless Network (QoS) Settings	Description
Delete	Click the checkbox to the left of any existing QoS filter to be deleted and click the Submit button.
Filter type	Select the filter type from the drop-down window: ◆ Mac Address ◆ Network ◆ Port
MAC Address	Enter the MAC address, if the MAC Address filter type is selected.

Adding or Deleting Wireless Network (QoS) Settings	Description
Network	Enter the Network, if the Network filter type is selected.
Ports	Enter the Port, if the Port filter type is selected.
Priority	Select the priority of the filter from the drop-down menu.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View or Configure Wireless Network QoS Settings

Using Web Manager

- To view Wireless (wlan0) QoS statistics, click Network on the menu and select **Wireless Network > QoS**.
- To modify Wireless (wlan0) QoS information, click Network on the menu and select **Wireless Network > QoS > Configuration**.

Using the CLI

- To enter the wlan0 QoS command level: `enable > config > if 2 > qos`

Using XML

- Include in your file: `<configgroup name="qos" instance="wlan0">`

Wireless (wlan0) Network Failover

The SGX 5150 device gateway provides wlan0 failover, in the form of a "dead remote host reachability" mechanism (essentially a ping against a known host). If the remote host is determined to be not reachable, the SGX 5150 gateway will failover to the Ethernet interface. If the remote host is determined to be reachable, the gateway will failback to the Wi-Fi interface.

Table 6-26 Wireless (wlan0) Network Failover

Settings	Description
State	Click to enable or disable state.
Failover Interface	Always select eth0 in the SGX 5150 device gateway.
Hostname	Enter the remote host to test reachability.
Method	Select ICMP or TCP based ping.
Timeout	Indicate the interval to wait for ping response from remote host.
Interval	Indicate the interval in which to test reachability
Failover Threshold	Indicate the allowed number of failed pings - after which the SGX 5150 gateway will failover to the wlan0 interface.
Failback Threshold	Indicate the number of successful pings - after which the SGX 5150 gateway will failback to the Ethernet interface.
Test (button)	Click the **Test** button to test if the configured Hostname is reachable.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View or Configure Wireless Network Failover Settings

Using Web Manager

- To view wireless network Failover statistics, click **Network** on the menu and select **Wireless Network > Failover**.
- To modify wireless network Failover settings, click **Network** on the menu and select **Wireless Network > Failover > Configuration**.

Using the CLI

- To enter the wlan0 link command level: `enable > config > if 2 > failover`

Using XML

- Include in your file: `<configgroup name="network failover" instance="wlan0">`

Wired (usb0) Network

The wired (usb0) network pages are described in this section.

Interface (usb0) Status and Configuration

Table 6-27 displays the wired (usb0) interface status and configuration information. The view-only status information is available on the Wired (usb0) Network Interface Status page. This same information is configurable on the Wired (usb0) Network Interface Configuration page.

Table 6-27 Wired (usb0) Network Interface

Field/Button	Description
State	Select to enable or disable the interface
Hostname	Enter the hostname for the interface. It must begin with a letter or number, continue with a sequence of letters, numbers, or hyphens, and end with a letter or number. This setting will take effect immediately, but will not register the hostname with a DNS server until the next reboot**.**
Priority	Priority ranges from 0-10. The IP stack will give the interface with the lowest numerical value highest priority and the highest numerical values lowest priority when sending data. This setting only applies when the SGX 5150 gateway is not in bridging mode and both interfaces are connected to the same IP subnet.
MTU	When DHCP is enabled, the MTU size is (usually) provided with the IP address. When not provided by the DHCP server, or using a static configuration, this value is used. The MTU size can be from 576 to 1500 bytes, the default being 1500 bytes.
IPv4 State	Select to enable or disable.
DHCP Client	Select to turn **On** or **Off**. At boot up, after the physical link is up, the *SGX 5150 unit* will attempt to obtain IPv4 settings from a DHCP server and will periodically renew these settings with the server. ***Note:*** *Overrides the configured IPv4 address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the SGX 5150 gateway. Within Web Manager, click* ***Renew*** *to renew the DHCP lease.*

Field/Button	Description
IP Address	Enter the static IPv4 address to use for the interface. You may enter it alone or in CIDR format. ***Note:*** *This setting will be used if Static IP is active (both DHCP and BOOTP are Disabled). Changing this value requires you to reboot the SGX 5150 gateway. When DHCP is enabled, the SGX 5150 unit tries to obtain an IPv4 address from a DHCP server. If it cannot, the SGX 5150 unit generates and uses an Auto IP address in the range of 169.254.xxx.xxx, with a network mask of 255.255.0.0.*
Default Gateway	Enter the IPv4 address of the router for this network. ***Note:*** *This setting will be used if Static IP is active (DHCPis **Disabled**).*
Domain	Enter the domain name suffix for the interface. ***Note:*** *This setting will be used when either static IP or auto IP is active, or if DHCP is active and no domain suffix was acquired from the server.*
DHCP Client ID	Enter the ID if the DHCP server requires a DHCP client ID option. The DHCP server's lease table shows IP addresses and MAC addresses for devices. The lease table shows the client ID, in hexadecimal notation, instead of the SGX 5150 MAC address.
Primary DNS	Enter the IP address of the primary domain name server (DNS.) ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
Secondary DNS	Enter the IP address of the secondary domain name server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
IPv6 State	Select to enable or disable.
IPv6 DHCP Client	Select to turn **On** or **Off**. At bootup, after the physical link is up, the SGX 5150 unit will attempt to obtain IPv6 settings from a DHCPv6 server and will periodically renew these settings with the server. ◆ **On:** enables the SGX 5150 server to obtain IPv6 setting from a DHCPv6 server upon bootup. ◆ **Off:** enables the SGX 5150 server to obtain IPv4 settings from a DHCP server upon bootup. ***Note:*** *Overrides the configured IP address/mask, gateway, hostname, and domain. Changing this value requires you to reboot the SGX 5150 gateway. Within Web Manager, click Renew to renew the DHCPV6 lease.*
IPv6 Auto Configuration	Select to turn **On** or **Off** IPv6 auto configuration.
IPv6 IP Address	Enter the static IPv6 address to use for the interface. ***Note:*** *This setting is used if Static IPv6 is active (DHCPv6 is Disabled). Changing this value requires a reboot. When DHCPv6 is enabled, the SGX 5150 unit tries to obtain an IPv6 address from a DHCPv6 server. If it cannot, then SGX 5150 unit generates and uses a Link local IPv6 address.*
IPv6 Default Gateway	Enter the default IPv6 default gateway.
IPv6 Domain	Enter the domain name suffix for the interface. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no Domain Suffix was acquired from the server.*
IPv6 Primary DNS	Enter the IP address of the primary domain name server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*

Field/Button	Description
IPv6 Secondary DNS	Enter the IP address of the secondary domain name server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure Network Interface Settings

Using Web Manager

- To view Ethernet (usb0) Interface statistics, on the **Network** page, select **Wired Network (USB)** > **Interface**.
- To configure Ethernet (usb0) interface settings, on the **Network** page, select **Wired Network (USB)** > **Interface** > **Configuration**.

Using the CLI

- To enter the command level: `enable > config > if 3 (config-if:usb0)`

Using XML

- Include in your file: `<configgroup name= "interface" instance="usb0">`

QoS Statistics and Configuration

QoS (Quality of Service) can be enabled and configured for both the Wireless (wlan0) Network and wired Wireless Network (usb0). If enabled, the router will control the flow of outbound traffic according towthe user-defined filters. In other words, QoS improves performance by allowing the user to prioritize applications. Filters can be defined to prioritize traffic based on the source or destination network, source or destination port, or the source MAC address. Up to 32 user-defined filters can be added. The following are predefined priority classes:

- Network Control and Internetwork Control are typically used for network control packets such as ICMP and have the highest priorities. Bandwidth allocation is a minimum 5% to each network control.
- Voice: Bandwidth allocation is minimum 30%.
- Video: Bandwidth allocation is minimum 20%.
- Critical Applications: Bandwidth allocation is minimum 15%.
- Excellent Effort: Bandwidth allocation is minimum 10%.
- Best Effort: Bandwidth allocation is minimum 10%.
- Background: Bandwidth allocation is minimum 5% and has the lowest priority.

Table 6-28 Wired (usb0) Network QoS Settings shows the network QoS settings that can be configured including adding new filters.

Table 6-28 Wired (usb0) Network QoS Settings

Wired (usb0) Network Settings	Description
State	Click to enable or disable state.
Import filters	Click to enable or disable import filters to import configurations from other interfaces.
Uplink Speed	Enter the maximum uplink speed. Set 0 to set speed to default.
Delete	Click the checkbox to the left of any existing QoS filter to be deleted and click the Submit button.
Filter type	Select the filter type from the drop-down window: ◆ Network ◆ Port
Network	Enter the Network, if the Network filter type is selected.
Ports	Enter the Port, if the Port filter type is selected.
Priority	Select the priority of the filter from the drop-down menu.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View and Configure Wired Network (USB) QoS Settings

Using Web Manager

- To view Ethernet (usb0) QoS statistics, click **Network** on the menu and select **Wired Network (USB) > QoS**.
- To modify Ethernet (usb0) QoS information, click **Network** on the menu and select **Wired Network (USB) > QoS > Configuration**.

Using the CLI

- To enter the usb0 QoS command level: `enable > config > if 3 > qos`

Using XML

- Include in your file: `<configgroup name="qos" instance="usb0">`

Wired (usb0) Network Failover

The SGX 5150 device gateway provides a USB network failover, in the form of a "dead remote host reachability" mechanism (essentially a ping against a known host). If the remote host is determined to be not reachable, the SGX 5150 gateway will failover to the Wi-Fi interface. If the remote host is determined to be reachable, the gateway will failback to the USB interface.

Table 6-29 Wired (usb0) Network Failover Settings

Wired (usb0) Network (Failover) Settings	Description
State	Click to enable or disable state.
Failover Interface	Always select eth0 in the SGX 5150 device gateway.
Hostname	Enter the remote host to test reachability.
Method	Select ICMP or TCP based ping.

Wired (usb0) Network (Failover) Settings	Description
Timeout	Indicate the interval to wait for ping response from remote host.
Interval	Indicate the interval in which to test reachability
Failover Threshold	Indicate the allowed number of failed pings – after which the SGX 5150 gateway will failover to the wlan0 interface.
Failback Threshold	Indicate the number of successful pings – after which the SGX 5150 gateway will failback to the Ethernet interface.
Test (button)	Click the **Test** button to test if the configured Hostname is reachable.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View and Configure Wired (USB0) Network Failover Settings

Using Web Manager

- To view USB Failover statistics, click **Network** on the menu and select **Wired Network (USB) > Failover**.
- To modify USB Failover settings, click **Network** on the menu and select **Wired Network (USB) > Failover > Configuration**.

Using the CLI

- To enter the usb0 link command level: `enable > config > if 3 > failover`

Using XML

- Include in your file: `<configgroup name="network failover" instance="usb0">`

Protocol Stack

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

IP Settings

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

Table 6-30 IP Protocol Stack Settings

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

Protocol Stack IP Settings	Description
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure IP Protocol Stack Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

ICMP Settings

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

Table 6-31 ICMP Protocol Stack Settings

Protocol Stack ICMIP Settings	Description
State	The State selection is used to turn on/off processing of ICMP messages. This includes both incoming and outgoing messages. Choose **Enabled** or **Disabled**.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure ICMP Protocol Stack Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

ARP Settings

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

Table 6-32 ARP Protocol Stack Settings

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

To Configure ARP Network Stack Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

VPN

Access VPN statistics and configuration options on this page.

Table 6-33 VPN Settings

VPN Setting	Description
Show details	Click this link to view the VPN log.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.
Configuration	
Name	Enter the name of this VPN connection.
State	Select to enable or disable the VPN connection.
Connection Type	Select connection type in the drop-down menu: ◆ **Host to Host** - VPN tunnel for Local and Remote subnets are fixed. ◆ **Host to Subnet** - VPN tunnel for Remote subnet area is dynamic and Local subnet is fixed.

VPN Setting	Description
IKEv2	Select the IKE version 2 settings to be used. The acceptable values are: ◆ **Permit**: (the default) signifying no IKEv2 should be transmitted, but will be accepted if the other ends initiates to us with IKEv2. ◆ **Never**: signifying no IKEv2 negotiation should be transmitted or accepted. ◆ **Propose**: signifying that the device will permit IKEv2, and also use it as the default to initiate. ◆ **Insist**: signifying that the device will only accept and receive IKEv2 and IKEv1 negotiations will be rejected.
Authentication Mode	Select the authentication mode of IPSec VPN. Pre-shared Key (PSK) is used when there is a single key common to both ends of the VPN. RSA uses RSA digital signatures. XAUTH provides an additional level of authentication by allowing the IPSec gateway to request extended authentication from remote users, thus forcing remote users to respond with their credentials before being allowed access to the VPN.
Mode Configuration	Select to enable or disable extended authentication operation and the settings provided to the client during the configuration exchange.
Type	Select **Tunnel** or **Transport** type from the drop-down menu. Tunnel Mode is used for protecting traffic between different networks, when traffic must pass through an intermediate, untrusted network. Transport Mode is used for end-to-end communications (for example, for communications between a client and a server).
Interface	Select the interface to use to connect to VPN Gateway. ◆ any ◆ eth0 ◆ usb0 ◆ wlan0
Remote Network	
Endpoint	Enter the remote VPN Gateway's IP Address.
Subnet	Enter the subnet behind the VPN Gateway.
ID	Enter the identifier expected to receive from the remote host during Phase 1 negotiation.
Router/Next Hop	Enter the next-hop gateway IP address for the VPN Gateway.
Local Network	
Subnet	Enter the subnet the local devices have access to or can be accessed from the VPN connection.
ID	Enter the identifier sent to the remote host during Phase 1 negotiation.
Router/Next Hop	Enter the next-hop gateway IP address for this connection to the public network.
Key Management	
Perfect Forward Secrecy (PFS)	Select to enable or disable the Perfect Forward Secrecy. Enabling this feature will require IKE to generate a new set of keys in Phase 2 rather than using the same key generated in Phase 1.
Pre-shared Key (PSK)	Enter the Pre-Shared Key used in the IPSec setting between the Local and VPN Gateway.
ISAKMP Phase 1 (IKE)	
Aggressive Mode	Select to enable or disable Aggressive Mode. In Aggressive mode, IKE tries to combine as much information into fewer packets while maintaining security. Aggressive mode is slightly faster but less secure.

VPN Setting	Description
NAT Traversal	Select to enable or disable NAT Traversal. If there is an external NAT device between VPN tunnels, the user must enable NAT Traversal.
Encryption	Select the encryption algorithm in key exchange from the drop-down menu.
Authentication	Select the hash algorithm in key exchange from the drop-down menu.
DH Group	Select the Diffie-Hellman (DH) groups (the Key Exchange group between the Remote and VPN Gateways) from the drop-down menu.
IKE Lifetime	Enter the number of hours for the IKE SA lifetime.
ISAKMP Phase 2 (ESP)	
Encryption	Select the encryption algorithm in data exchange from the drop-down menu.
Authentication	Select the hash algorithm in data exchange from the drop-down menu.
DH Group	Select the Diffie-Hellman (DH) groups (the Key Exchange group between the Remote and VPN Gateways) for Phase 2 from the drop-down menu.
SA Lifetime	Enter the number of hours for the SA lifetime in Phase 2.
Unreachable Host Detection	
Host	Enter the unreachable detection host monitoring the connectivity with the host on the remote network.
Ping Interval	Enter the Ping Interval to monitor connectivity with a host on the remote network.
Max Tries	Enter the number of Max Tries for pinging the host before the VPN tunnel is restarted.

Configuring VPN Settings

You may edit or view VPN settings.

Using Web Manager

- To view or configure VPN settings on the **Network** page, click **VPN**.

Using the CLI

- To enter the VPN level: `enable > configure > vpn1`

Using XML

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

Wi-Fi Protected Setup

Using Wi-Fi® protected setup (WPS), you have the option of connecting the SGX 5150 unit to a router or access point in a single operation instead of manually creating a profile with a network name (SSID), setting up wireless security parameters and updating the choice list. You may setup WPS through pin or push button functionality through Web Manager or through CLI.

Note: *Not all access points support Wi-Fi protected setup pin or Wi-Fi protected setup push button.*

Table 6-34 Wi-Fi Protected Setup

WPS buttons	Description
WPS (PIN)	Click the **WPS (PIN)** button in Web Manager to setup WPS by pin and click **OK** in the confirmation popup which appears. A randomly generated pin will appear on the screen. Enter this pin at the access point and point your browser to the correct IP address.
WPS (PBC)	Click the **WPS (PBC)** button in Web Manager to setup WPS by push button, click **OK** in the confirmation popup which appears, and the credentials are passed to the SGX 5150 unit automatically. Then point your browser to the correct IP address. ***Note:*** *Make sure the WPS PBC is triggered on the Access Point to utilize this option.*
WPS Pushbutton CP	If Enabled, WPS can be initiated via pushbutton CP, which may be accessible to walk-up users.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Initiate WPS

Using Web Manager

- To initiate WPS, on the **Network** page, click **Wi-Fi Protected Setup**.

Using the CLI

- To enter the command level: `enable > config > if 2 > link`

Using XML

- Not applicable.

To Show WPS Status

Using the CLI

- To enter the command level: `enable > config > if 2 > link`

Using XML

- Not applicable.

WLAN Scan/QuickConnect

Going to this page initiates a scan of wireless networks within range of the SGX 5150 unit and allows users to add a WLAN profile after testing it. This list refreshes automatically every 15 seconds. There is also an option to automatically update the scan results every 60 seconds, which is disabled by default. The scan results contain the following prepopulated information about each wireless device: service set identifier (SSID), basic service set identifier (BSSI), channel number (CH), received signal strength indication (RSSI), and Security Suite. You may also run a filtered scan of network names by the first few letters within the name.

Click on any network name for QuickConnect configuration.

Table 6-35 WLAN Scan/Quick Connect Results

WLAN Quick Connect Settings	Description
Network Name (search field)	Enter the first few letters of a network name in the search field before pressing the **Scan** button (next field description below).
Scan "<network SSID>"	Click **Scan** to search for all network names containing the first few letters entered in the **Network Name** search field. Performs a scan for devices within range of the SGX 5150 unit. To limit the scan to devices that are configured with the specified SSID, include the network SSID. To perform a scan for all devices, omit the network SSID. The command syntax requires the opening and closing quotation marks. If you omit the SSID, include the quotation marks, for example, scan "".
Refresh scan results every 60 seconds (check box)	To automatically update the list every 60 seconds, select the checkbox. To stop automatically updating the list, clear the checkbox.
SSID	To display a network configuration profile, click the service set identifier (SSID) of a specific network.
BSSID	The basic service set identifier (BSSID) is a unique 48-bit address that identifies the access point that creates the wireless network.
CH (Channel)	The channel number and frequency (MHz) of a network.
RSSI	A real-time value that indicates the signal strength of the network. Green indicates the strongest, yellow indicates average, and red indicates the weakest signal strength. The received signal strength indication (RSSI) that is reported in scan results is a single sample. To review the signal strength average over time, use the status command. The average is based on the connected AP.
Security Suite	The security suite of a network. For example: WEP, WPA, WPA2, WPS. Although WPS is reported with the security flags, it does not indicate a security setting. WPS indicates that an AP supports WPS.

To View WLAN Link Scan and Status Information

Using Web Manager

- To view the WLAN Link Scan and Status information, on the **Network** page, click **WLAN Scan/Quick Connect**.

Using the CLI

- Not applicable.

Using XML

- Include in your file: `<statusggroup name="wlan scan">`

WLAN Profiles

A WLAN profile defines all of the settings needed to establish a wireless connection. This is true when in infrastructure mode for an access point. A maximum of eight profiles can exist on the SGX 5150 unit at a time. All enabled profiles are active.

The SGX 5150 unit supports dynamic profiles and prioritization of the profiles. Dynamic Profiles are created using WPS or Quick Connect. Profiles are assigned numbers based on priority. For example, dynamic profiles list in reverse order of creation, followed by choice-list profiles, then any remaining profiles.

Create a new profile by entering a name in the text box, then click the Submit button which will appear. The new profile is initially saved with default parameter values.

Note: *WLAN Profiles created by Quick Connect, Quick Setup, or WPS are called dynamic profiles and have a higher priority than user created profiles.*

Note: *The SGX 5150 includes a default WLAN profile named "default_infrastructure_profile" with SSID "Lantronix Initial Infra Network" and security suite set to* ***None****.*

The profiles on the WLAN Profiles page are listed in order of priority. The prioritization scheme is dynamic profiles, user created profiles from WLAN choice list, and then other user created profiles.

Table 6-36 WLAN Profiles

WLAN Profile Settings	Description
Enabled (check box)	Check the checkbox to the right of the WLAN profile listed right to enable the specific profile. Unchecking the enabled checkbox disables the WLAN profile.
Delete (check box)	Check the checkbox to the right of the WLAN profile listed right and click the Submit button which appears, to delete the specific profile.
Name (link to WLAN profile)	Click an existing WLAN profile listed under the Name column to reveal the configuration options as shown in *Table 6-37 Individual WLAN Profile Settings*. Modify configuration options as desired.
Name ("Add a new profile" field)	Enter the name of a new profile and click **Submit** to add it. The profile appears in the WLAN Profiles list.

Configuring WLAN Profile Settings

You can edit, create, or delete a WLAN profile.

Using Web Manager

- To edit, create or delete a WLAN profile, on the **Network** page, click **WLAN Profiles**.

Using the CLI

- To enter the WLAN Profile level: `enable > configure > wlan profiles`

Using XML

- Include in your file:

```
<configgroup name="wlan profile" instance="profile_name">
```

Table 6-37 Individual WLAN Profile Settings

WLAN Profile Settings	Description
Network Name (SSID)	Enter or modify the network name.
State	Click to enable or disable.

WLAN Profile Settings	Description
Suite	Select a security suite configuration: ◆ **None** Select None to not select a security suite. ◆ **WEP** WEP security is available in Infrastructure mode. WEP is a simple and efficient security mode, encrypting the data using the RC4 algorithm. However, WEP has become more vulnerable due to advances in hacking technology. State-of-the-art equipment can find WEP keys in 5 minutes. For stronger security, use WPA, or the stronger WPA2, with AES (CCMP). ◆ **WPA2/WPA Mixed Mode**
Authentication	**If WEP security suite is selected,** select one of these authentication options which appear. ◆ **Shared**: Encryption keys of both parties are compared as a form of authentication. If mismatches occur, no connection establishes. ◆ **Open**: A connection establishes without first checking for matching encryption keys. If keys do not match, however, data becomes garbled and prevents connectivity on the IP level. **If WPA or WPA2/WPA Mixed Mode security suite is selected,** select one of these authentication options which appear: ◆ **PSK:** In pre-shared keying, the same key must be configured both on the SGX 5150 side and on the access point side. ◆ **IEEE 802.1X:** This authentication method communicates with a RADIUS authentication server that is part of the network. The RADIUS server matches the credentials sent by the SGX 5150 unit with an internal database. If IEEE 802.1X is selected under authentication type, select the protocol to use to authenticate the WLAN client.
PMF	Select one of the following options regarding protected management frames (PMF): ◆ Disable ◆ Optional ◆ Required ***Note:*** *This option is available when the WPA2/WPA mixed mode suite and the IEEE 802.1x authentication settings are selected.*
Key Type	Select a **Hex** or **Passphrase** key type after indicating the security suite type.
Key Size	If the WEP security suite is selected, then select **40 bits** or **104 bits** key size in this field.
Passphrase	If Passphrase key type is selected, enter an alphanumeric phrase up to 63 characters in length in this field which becomes available. Spaces and special characters are allowed. Check Show **Password** to show the passphrase entered.
TX Key Index	If WEP security suite and Hex key type have been selected, then select the TX key index from the drop-down menu, which becomes available. ◆ For interoperability with some products that generate four identical keys from a passphrase, this index must be one. ◆ For Keys 1-4, enter one or more encryption keys in hexadecimal format. Enter 10 hexadecimal digits (0-9, a-f) for WEP40 and 26 for WEP104. For security reasons, the configured keys are not shown.

WLAN Profile Settings	Description
IEEE 802.1X	If IEEE 802.1X authentication is selected, choose a particular type: ◆ **LEAP**: type a User Name and Password, then select an Encryption. ◆ **EAP-TLS**: Type a Username. ◆ **EAP-TTLS** ◆ **PEAP:** For PEAP Option, select a security protocol. ◆ **FAST:** If selected, select the Fast Option and Fast Provisioning options.
FAST Option	Select the FAST option from the drop-down menu: ◆ MD5 (default) ◆ MSCHAPV2 ◆ GTC ***Note:*** *This option is available when the WPA2/WPA mixed mode suite and the IEEE 802.1x authentication settings are selected.*
FAST Provisioning	Select the FAST provisioning option from the drop-down menu: ◆ Unauthenticated ◆ Authenticated (default) ◆ Both ***Note:*** *This option is available when the WPA2/WPA mixed mode suite, the FAST IEEE 802.1x authentication, and the MSCHAPV2 FAST option are selected.*
EAP-TTLS Option	Select a security protocol: ◆ EAP-MSCHAPV2 ◆ MSCHAPV2 ◆ MSCHAP ◆ CHAP ◆ PAP ◆ EAP-MD5 ***Note:*** *This option is available when the WPA2/WPA mixed mode suite, the IEEE 802.1x authentication, and EAP-TTLS settings are selected.*
PEAP Option	Select **EAP-MSCHAPV2**, **EAP-MD5** or **EAP-TLS.** ***Note:*** *This option is available when the WPA2/WPA mixed mode suite, the IEEE 802.1x authentication, and PEAP settings are selected.*
Validate Certificate	If EAP-TLS is selected, validate the certificate installed on the SGX 5150 gateway by selecting **Enabled** in the Validate Certificate field which appears. Validates the certificate installed on the SGX 5150 gateway with the one received from the RADIUS server.
Credentials	After EAP-TLS is selected and the Validate Certificate is enabled, either: ◆ Select the credential, if listed in the drop-down menu, to validate. ◆ Type the name of the credential if the credential is not listed in the drop-down menu.
Username	Enter a username.
Password	Enter a password if the LEAP, EAP-TTLS and PEAP option is chosen. Check the **Show Password** check box to make the password viewable as you enter it in the Password field.
Inner Credentials	Provide inner credentials with enterprise authentication when PEAP/TLS is selected. Inner credentials specify the client certificate required for the TLS inner authentication. ***Note:*** *This option is available when the WPA2/WPA Mixed Mode suite, the IEEE 802.1x authentication, PEAP and PEAP EAP-TLS settings are selected.*

WLAN Profile Settings	Description
Advanced Configuration (Link)	Click the **Advanced Configuration** to reveal additional configuration settings.
TX Power Maximum	Enter the **TX Power Maximum** in dBm.
Power Management	Select to enable or disable.
Apply (button)	Click this button after making configuration selections above, to apply but not submit/save your choices.
Test Connection (button)	Click this button to test the connection according to the configuration selections made above, but not to submit/save your choices.
Submit (button)	Click this button to submit and save your configuration choices.

7: Filesystem

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

- Directories can be created, deleted, moved, and renamed. A directory must be empty before it can be deleted.
- Files can be created, deleted, moved, renamed, uploaded via HTTP, and transfered to and from a TFTP server. Newly created files will be empty.
- Some filesystems may contain a `'lost+found'` directory.
- The SGX 5150 XL has 8 GB of internal USB flash storage; this is displayed as `'Internal_Storage'` in the fileystem.

  Note: *The internal storage cannot be unmounted or deleted.*

Table 7-38 File Modification Settings

File Modification Commands	Description
`rm`	Removes the specified file from the file system.
`touch`	Creates the specified file as an empty file.
`cp`	Creates a copy of a file.
`mkdir`	Creates a directory on the file system.
`rmdir`	Removes a directory from the file system.
`format`	Format the file system and remove all data. ***Warning:*** ***Formatting the filesystem will delete all files on it and Internal_Storage (if available).***

Table 7-39 USB Auto Mount Configuration Settings

Configuration Settings	Description
USB Auto Mount	If Enabled, a USB drive connected to a USB port on the device will be automatically mounted and accessible via the filesystem. If Disabled, the USB drive will not be mounted.

File Transfer and Modification

Files can be transferred to and from the SGX 5150 device via the TFTP protocol. This can be useful for saving and restoring XML configuration files. Files can also be uploaded via HTTP.

Table 7-40 File Transfer Settings

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

To View, Transfer, or Modify Filesystem Files

Using Web Manager

- To view current filesystem browser statistics or to format the filesystem, click **Filesystem** in the menu and select **Statistics**.

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

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

Using the CLI

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

Using XML

- Not applicable.

8: Diagnostics

Diagnostic settings for the SGX 5150 unit can be viewed and modified under the Diagnostics tab in the Web Manager user interface. This chapter describes the following diagnostic settings:

- *DNS*
- *Hardware*
- *IP Sockets*
- *Log*
- *Memory*
- *Ping*
- *Processes*
- *Routes*
- *Threads*
- *Traceroute*

DNS

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

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

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

Table 8-41 DNS Settings

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

Accessing the DNS Settings

Using Web Manager

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

Note: *If DNS information is not supplied by DHCP, configure Ethernet (eth0) internet settings according to instructions at* *Wired (eth0) Network (on page 51)* *and configure*

Wireless (wlan0) Network interface settings according to instructions at *Wireless (wlan0) Network (on page 57)*.

Using CLI

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

Using XML

- Not applicable.

Hardware

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

To View Hardware Information

Using Web Manager

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

Using the CLI

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

Using XML

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

IP Sockets

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

To View the List of IP Sockets

Using Web Manager

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

Using the CLI

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

Using XML

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

Log

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

Table 8-42 Log Settings

Diagnostics	Log Description
Output	Select a diagnostic log output type: ◆ **Disable** - Turn off the logging feature. ◆ **Filesystem** - Directs logging to /log.txt. Use **Max Length** to limit the size in Kbytes that the /log.txt file will be allowed to grow to. If this size is exceeded, the file will be reinitialized using the 100 most recent messages. ◆ **Line 1** - Directs logging to the selected serial line. ◆ **USB** - Directs logging to the selected USB port.

To Configure the Diagnostic Log Output

Using Web Manager

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

Using the CLI

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

Using XML

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

Memory

The memory information includes the total and available memory (in bytes).

To View Memory Usage

Using Web Manager

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

Using the CLI

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

Using XML

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

Ping

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

Table 8-43 Ping Configuration

IP Socket	Description
Host	Enter the IP address or host name for the SGX 5150 unit that you want to ping.
Count	Enter the number of ping packets that the SGX 5150 unit attempts to send to the Host. The default number of packets is 3.
Timeout	Enter the time in seconds that the SGX 5150 unit waits for a response from the Host before it times out. The default time is 5 seconds.
Ping (button)	Click this button to submit a ping according to the Host, Count, and Timeout indicated above.

To Ping a Remote Host

Using Web Manager

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

Using the CLI

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

Using XML

- Not applicable.

Processes

The SGX 5150 unit shows all the processes currently running on the system. It shows the process ID (PID), parent process ID (PPID), user, CPU percentage, percentage of total CPU cycles, and process command line information.

To View Process Information

Using Web Manager

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

Using the CLI

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

Using XML

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

Routes

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

Using Web Manager

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

Using CLI

- To enter the command level: `enable > show routes`

Using XML

- Not applicable.

Threads

The SGX 5150 unit threads information shows details of threads in the ltrx_evo task which can be useful for technical experts in debugging.

To View Thread Information

Using Web Manager

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

Using the CLI

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

Using XML

- Not applicable.

Traceroute

You can use traceroute to trace a packet from the SGX 5150 unit to an Internet host. A traceroute shows how many hops the packet requires to reach the host, and how long each hop takes. This information can be helpful to diagnose delays for a web page that loads slowly.

Table 8-44 Traceroute Settings

Traceroute Fields	Description
Host	Enter the IP address or DNS host name of the destination device.
Protocol	Select the protocol that you want to use for the traceroute. ◆ TCP ◆ ICMP ◆ UDP
Traceroute (button)	Click the **Traceroute** button to enter the settings.

To Perform a Traceroute

Using Web Manager

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

Using the CLI

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

Using XML

- Not applicable.

9: Administration

Administrative features for the SGX 5150 device gateway are organized beneath the Administration tab in the Web Manager user interface. This chapter describes the following administrative settings:

- *Actions*
- *Applications*
- *Bluetooth*
- *Bluetooth Serial*
- *CLI*
- *Clock*
- *ConsoleFlow*
- *Discovery*
- *Email*
- *FTP*
- *Gateway*
- *GRE*
- *Host*
- *HTTP*
- *Line*
- *Modbus*
- *RSS*
- *Security*
- *SFTP*
- *SMTP*
- *SNMP*
- *SSH*
- *SSL*
- *Syslog*
- *System*
- *Terminal*
- *Tunnel*
- *USB*
- *User Management*
- *XML*
- *Quick Setup*

Actions

Table 9-45 contains the configuration options for all the alarms and reports listed above.

Table 9-45 Action Settings

Action Settings	Description
Delay	Use Delay to defer alarm processing. Alarm actions will not be executed if the cause is corrected within this time.
Email	Use Email to send an email to configured Email recipients. ◆ If an **Alarm Email** profile number is selected, that email will be sent when the alarm is turned on. The contents of **Alarm Message** will be placed into the email body when an alarm email is sent. If the alarm stays on longer than the Reminder Interval, another alarm email is sent. ◆ If a **Normal Email** profile number is selected, that email will be sent when the alarm is turned off. The contents of **Normal Message** will be placed into the email body when a normal email is sent. If the alarm stays off longer than the Reminder Interval, another normal email is sent.
FTP Put	Use FTP Put to put a file on configured FTP server. Filename will be used to upload to remote FTP server. The IP **Address** or hostname is the FTP server to connect. Port number is port on which FTP server is listening on. Use Protocol to connect to FTP server. FTPS is a SSL encrypted communication channel and SSL Trusted Authorities must be setup with FTP server SSL certificate. Username is used to logon to FTP server. If FTP server does not require authentication, use anonymous. Password is used to logon to FTP server. If FTP server does not require authentication, a common practice is to use user's email address. If the alarm stays on or off longer than the **Reminder Interval**, another FTP Put is performed. In **Sequential Mode**, connections will be attempted starting with number 1 until a connection is successful. In **Simultaneous Mode**, all possible connections will be made.
HTTP Post	Use HTTP Post post to configured HTTP server. The URL appears behind the HTTP server IP address or hostname. E.g. `http://some_http_server/some_url` The IP **Address** or hostname is the HTTP server to connect to. Port number is the port which HTTP server is listening on. Use Protocol to connect to HTTP server. HTTPS is a SSL encrypted communication channel and SSL Trusted Authorities must be setup with HTTP server SSL certificate. Username used to logon to HTTP server if authentication is required. Password used to logon to HTTP server if authentication is required. If the alarm stays on or off longer than the **Reminder Interval**, another HTTP Post is performed. In **Sequential Mode**, connections will be attempted starting with number 1 until a connection is successful. In **Simultaneous Mode**, all possible connections will be made.
SNMP Trap	Use SNMP Trap to send SNMP trap to configured trap destinations. SNMP Trap **State** can be **Enabled** or **Disabled**. The contents of **Alarm Message** are included when an alarm SNMP trap is sent. If the alarm stays on longer than the **Reminder Interval**, another alarm SNMP Trap is sent. The contents of **Normal Message** are included when a normal SNMP trap is sent. If the alarm stays off longer than the Reminder Interval, another normal SNMP Trap is sent.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure Action Settings

Using Web Manager

- To view Action status, on the **Administration** page, click **Action > Status** on the menu.
- To modify Action information, on the **Administration** page, click **Action > Configuration** on the menu and select a specific action from the drop-down menu.

Using the CLI

- To enter the eth0 link state change command level: `enable > config > action > eth0 link state change`
- To enter the wlan0 link state change command level: `enable > config > action > wlan0 link state change`
- To enter the usb0 link state change command level: `enable > config > action > usb0 link state change`
- To enter on scheduled reboot command level: `enable > config > action > on scheduled reboot`

Using XML

- Include in your file: `<configgroup name = "action" instance = "eth0 link state change">`
- Include in your file: `<configgroup name = "action" instance = "wlan0 link state change">`
- Include in your file: `<configgroup name = "action" instance = "usb0 link state change">`
- Include in your file: `<configgroup name = "action" instance = "on scheduled reboot">`

Python

Python™ is a dynamic, object-oriented programming language that can be used for developing a wide range of software applications. The Lantronix SGX 5150 includes the installation of Python interpreter, making it easy to load and run custom Python scripts on your device.

The version of Python programming language installed on the Lantronix SGX 5150 comes with "batteries included" by having the Python language's standard library. In addition, the developer can take advantage of thousands of available third party packages to speed up development.

IDE

Python scripts can be written with any text editor. If using Windows for development, Notepad++ is a powerful choice as this text editor includes traditional IDE features such as syntax highlighting and automatic indentation (http://notepad-plus-plus.org/). Notepad++ also includes the ability to customize through plugins. Some interesting plugins for the development of Python scripts for the Lantronix SGX 5150 platform include the following:

- **PyNPP:** https://github.com/mpcabd/PyNPP
  This plugin allows the user to use keystrokes to launch the open Python script in the local Python interpreter for debugging and testing.

- **NppFTP:** http://sourceforge.net/projects/nppftp/
  This plugin provides a one-click upload of a file to an FTP server. Debugging and testing on the SGX 5150 easier because SGX 5150 products have an FTP server through which to upload files into the file system.

Applications

The SGX 5150 supports the ability to install and uninstall user-defined Python scripts and packages and will include the following:

bin	python	
lib	libpython{version}.so	
	<ltrx python sdk>	
	libpython{version}	"python precompiled scripts
		"python shared libraries

Table 9-46 contains the setting options for configuring, installing, uninstalling and running external applications via Python scripts.

Caution: ***Use extreme caution when installing and running scripts.***

Table 9-46 Script Settings

Script Settings	Description
Reserved Start Port	Enter the Reserved Start Port. The range is between 1024 and 65535.
Reserved Ports	Enter a Reserved Port. The range is between 2 and 32.
Script (Number)	Click the **Run** button to manually execute the script. ***Note:*** *The script is run with configuration saved to the Flash.*
Enabled (checkbox)	Check the **Enabled** checkbox within a particular script to enable it. Uncheck the checkbox to disable the script.
Run on startup (checkbox)	Check the **Run on startup** checkbox within a particular script to have it run upon the start up of the SGX 5150 unit. Uncheck the checkbox to disable automatically running the unit upon startup.
Run on shutdown (checkbox)	Check the **Run on shutdown** checkbox within a particular script to have it run on shutdown of the SGX 5150 unit. Uncheck the checkbox to disable automatically running the script upon shutdown.
Script	Enter the path of the script to run.
Parameter	Enter the script parameters (if any).
Output	Enter output log file (if desired) for the script to redirect output of script to file. If the name of output log contains "%t", it will translate it into time stamp (e.g., script1_%t.log => script1_2007-01-02_19-06-57.log)
Uninstall (button)	Click the **Uninstall** button in a Python package to uninstall it.
Remove All (button)	Click the **Remove All** button to uninstall all Python packages.
Filename (field)	Enter the package file name pathway in the file system and click the **Install** button to install it.

To Configure Application Settings

Using Web Manager

- To configure application scripts, on the **Administration** page, click **Applications** on the menu.

Using the CLI

- To enter the application script change command level: `enable > config > applications`

Using XML

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

Bluetooth

The Bluetooth client allows you to provision the gateway with configuration settings using the mobile gateway provisioning application through a BLE connection. With Bluetooth enabled, you can use your mobile device to connect to the gateway and download and configure settings.

Bluetooth Status and Configuration

View-only status information on the Bluetooth Status page displays the current Bluetooth state, the gateways's MAC address, and current connected devices (if any).

See *Table 9-47* for the Bluetooth settings that can be modified on the Bluetooth Configuration page.

Table 9-47 Bluetooth Configuration

Bluetooth - Configuration Settings	Description
State	Select to enable or disable Bluetooth on the gateway. ◆ **Enable**: Turns Bluetooth on (default) ◆ **Disable**: Turns Bluetooth off
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View and configure Bluetooth settings:

Using Web Manager:

- To view Bluetooth status, on the **Administration** page, click **Bluetooth > Status**.
- To configure Bluetooth settings, on the **Administration** page, click **Bluetooth > Configuration**.

Using the CLI:

- To enter the Bluetooth command level: `enable > config > bluetooth`

Using XML:

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

Bluetooth Serial

Bluetooth Serial allows you to connect to a device using the Bluetooth SPP profile for tunneling or command mode.

Bluetooth Serial Statistics and Configuration

View-only statistics on the Bluetooth Serial Statistics page displays information on data transfered and any errors using Bluetooth Serial.

See *Table 9-48* for the Bluetooth Serial settings that can be modified on the Bluetooth Serial Configuration page.

Table 9-48 Bluetooth Serial Configuration

Bluetooth Serial - Configuration Settings	Description
Name	Enter a name to allow this line to be displayed in the Login Connect Menu. Leave blank to exclude it from the menu.
Interface	This is set to **Bluetooth-RFCOMM** and can't be changed.
State	Select to enable or disable Bluetooth Serial on the gateway. ◆ **Enable**: Turns Bluetooth Serial on (default) ◆ **Disable**: Turns Bluetooth Serial off
Protocol	Select the protocol to use. ◆ **None**: No protocol will be used. ◆ **Tunnel**: Uses tunnel over the Bluetooth Serial connection.
Line Mode	This is set to **Serial Device** and can't be changed.
Gap Timer	Enter the time in milliseconds after the last character is received that the received serial bytes will be forwarded.
Threshold	Enter the number of bytes to be received after which the received characters will be forwarded.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View and configure Bluetooth settings:

Using Web Manager:

- To view Bluetooth Serial statistics, on the **Administration** page, click **Bluetooth Serial > Statistics > Bluetooth 1 > Statistics**.
- To configure Bluetooth Serial settings, on the **Administration** page, click **Bluetooth Serial > Bluetooth 1 > Configuration**.

Using the CLI:

- To enter the Bluetooth Serial command level: `enable > config > bluetooth serial`

Using XML:

- Include in your file: `<configgroup name = "bluetooth serial">`

CLI

The command line interface (CLI) settings allow you to control how users connect to and interact with the command line of the SGX 5150 unit. It is possible to configure access via the Telnet and SSH protocols, in addition to general CLI options.

CLI Status and Configuration

View-only status information on the Command Line Interface Status page displays the current Telnet and SSH server status, uptime, and current connections (if any.)

See *Table 9-49* for the bridge settings that can be modified on the Command Line Interface Configuration page.

Table 9-49 CLI Configuration Settings

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

To View and Configure Basic CLI Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Clock

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

Table 9-50 Clock Settings

Bridge Fields	Description
Method	Select **Manual** or **SNTP** from the drop-down window.
Date	**If Manual method is selected,** enter the date using the **Year**, **Month** and **Day** drop down menus that become available.
Time	**If Manual method is selected,** enter the time using the **Hour**, **Minute (Min)** and **Second (Sec)** drop down menus that become available.
NTP Server	**If SNTP method is selected,** the clock will keep time synchronized with the NTP Server by default. Enter an alternative NTP server if you wish to use an address other than the default.
Time Zone	Select the desired Time Zone from the drop-down menu based on geographic location. The time zones listed are in Universal Time Coordinated (UTC), formerly known as Greenwich Mean Time (GMT). Syslog and other applications may use UTC. The UTC Offset of the form HHMM (H = hour, M = minute) is applied to the UTC time to get the local time. The SGX 5150 gateway will make seasonal time changes required for Daylight Savings Time.

To Specify a Clock-Setting Method

Using Web Manager

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

Using the CLI

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

Using XML

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

ConsoleFlow

The SGX 5150 device comes integrated with the 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 Settings (Line 1, Line 2, USB 1, Bluetooth Serial 1)** - To enable remote management and data access to your application or device attached on the serial line.

Configure ConsoleFlow Client

This page displays the configuration and status for ConsoleFlow client.

Table 9-51 ConsoleFlow Client Configuration

ConsoleFlow Client	Description
State	Click to enable or disable the ConsoleFlow client.
Device ID	Read only. Displays the gateway's Device ID. Device ID may be provisioned through Lantronix Provision Manager. ***Note:*** *Device ID can only be provisioned once. It will persist across resets.*
Device Key	Read only. Shows whether the gateway's Device Key has been configured. Device Key may be configured through the Lantronix Provision Manager.
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	Enable to allow firmware updates to be applied via ConsoleFlow. Enabled by default.
Apply Configuration Updates	Select when to **Apply Configuration Updates** from the dropdown menu: ◆ **Never:** signifying no configuration updates will be applied. ◆ **If unchanged**: signifying configuration updates will only be applied if no changes have been made locally. ◆ **Always:** signifying configuration updates will always apply.
Reboot After Update	Automatically reboot device after firmware or configuration update. ***Note:*** *Setting causes automatic reboot after a firmware update.*
Active Connection	Select the connection instance to use when connecting to ConsoleFlow. The configuration options for both Connection 1 and Connection 2 are below.
Connection 1	Connection 1 settings.
Host	Enter the host name or IP address.
Port	Enter the ConsoleFlow SSL port.
Secure Port	Click to enable or disable the ConsoleFlow client secure port 443.
Validate Certificates	Click to enable or disable the validation of server certificates on ConsoleFlow client.

ConsoleFlow Client	Description
Local Port	Enter the local port for ConsoleFlow connections. When configured, a total of 16 consecutive ports will be reserved.
MQTT State	Enable or disable MQTT.
MQTT Host	Hostname or IP address of MQTT server.
MQTT Port	Enter the port of the ConsoleFlow MQTT server. When configured, a total of 32 consecutive ports will be reserved.
MQTT Security	Enable SSL for MQTT.
MQTT Local Port	Enter the local port of ConsoleFlow MQTT client. When configured, a total of 32 consecutive ports will be reserved.
Use Proxy	Enable or disable the use of a proxy for this connection. Disabled by default.
Proxy Type	Proxy server type. The supported type is SOCKS5.
Proxy Host	Hostname or IP address of the proxy server to be used.
Proxy Port	Port of the proxy server to be used. Default port is **80**.
Proxy Username	Username for the proxy server.
Proxy Password	Password for the proxy server.
Connection 2	Connection 2 settings are identical to Connection 1 settings.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

Configure ConsoleFlow Line

Note: *The following section describes the steps to view and configure ConsoleFlow Line 1 settings; these steps also apply to Line 2, USB 1, and Bluetooth Serial 1 line status and configuration.*

Table 9-52 ConsoleFlow Line

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

To Configure ConsoleFlow

Using Web Manager

- To configure ConsoleFlow Client, on the **Administration** page, click **ConsoleFlow > Client**.
- To configure ConsoleFlow Line 1, on the **Administration** page, click **ConsoleFlow > Line 1**.
- To configure ConsoleFlow Line 2, on the **Administration** page, click **ConsoleFlow > Line 2**.
- To configure ConsoleFlow USB 1, on the **Administration** page, click **ConsoleFlow > USB 1**.
- To configure ConsoleFlow Bluetooth Serial 1, on the **Administration** page, click **ConsoleFlow > Bluetooth Serial 1**.

Using the CLI

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

Using XML

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

Discovery

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

The current statistics and configuration options for device discovery, including UPnP query port, are available for the SGX 5150 unit.

Table 9-53 Discovery Settings

Discovery Settings	Description
Query Port Server State	Select to enable or disable the query port server from responding to autodiscovery messages on port 0x77FE.
UPnP Server State	Select to enable or disable the UPnP server from discovering devices in Windows network places.
UPnP Server Port	Update the UPnP server port. Leaving this field blank will restore the default settings.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure Discovery

Using Web Manager

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

Using the CLI

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

Using XML

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

Email

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

Table 9-54 Email Configuration

Email – Configuration Settings	Description
Send Email (button)	Click **Send Email** after completing the fields below.
From	Click the **Configure SMTP** link to configure SMTP. See *SMTP (on page 118)*.
To	Enter the email address to which the email alerts will be sent. Multiple addresses are separated by semicolon (;). Required field if email is to be sent.
CC	Enter the email address to which the email alerts will be copied. Multiple addresses are separated by semicolon (;).
Reply To	Enter the email address to list in the Reply-To field of the email alert.
Subject	Enter the subject for the email alert. ***Note:*** *Emails sent as a result of an alarm will display the name of the alarm in the subject of the email, overriding the email subject configured in this field.*
Message File	Enter the path of the file to send with the email alert. This file appears within the message body of the email, not as an attachment.
Priority	Select the priority level for the email alert: ◆ Urgent ◆ High ◆ Normal ◆ Low ◆ Very Low

To View, Configure and Send Email

Note: *The following section describes the steps to view and configure Email 1 settings; these steps apply to other emails available for the SGX 5150 gateway.*

Using Web Manager

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

Using the CLI

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

Using XML

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

FTP

The FTP protocol can be used to upload and download user files, and upgrade the SGX 5150 firmware. A configurable option is provided to enable or disable access via this protocol.

Table 9-55 FTP Settings

FTP Settings	Description
State	Select to enable or disable the FTP server: ◆ Enabled (default) ◆ Disabled
Port	Enter the Port to be used by FTP server. Entering a Port overrides the default ftp port. Blank the field to restore the default ftp port.
Data Port	Enter the Data Port where the server initiates a data channel to the client. In active mode, the client starts listening for incoming data connections from the server on port M. It sends the FTP command PORT M to inform the server on which port it is listening. The server then initiates a data channel to the client from its Data Port.
Passive Mode Start Port	Define the port range by entering the **Passive Mode Start Port** and **Passive Mode Port**. In passive mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server, which the client then uses to open a data connection to the server IP address and server port number received. In situations where the client is behind a firewall and unable to accept incoming TCP connections, passive mode may be used.
Passive Mode Ports	
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure FTP Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Gateway

The SGX 5150 IoT device gateway can be configured as a wireless router with DHCP server functionality.

Status

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

◆ To view gateway status: on the **Administration** page, click **Gateway > Status**.

WAN

Table 9-56 WAN Configuration

Gateway Settings	Description
Configuration	
Operating Mode	Select the type of operating mode: ◆ **Disabled**: prevents the SGX 5150 gateway to be used as a gateway; use the gateway normally. ◆ **Gateway**: allows the gateway to be used as a router with NAT. ◆ **Router**: allows the SGX 5150 gateway to be used as a router without NAT.
Firewall	Select to enable or disable firewall: ◆ **Enabled**: enables the SGX 5150 gateway firewall. ◆ **Disabled**: disable the SGX 5150 gateway firewall.
MAC Address filter	Select to enable or disable the MAC address filter.
IP Address filter	Select to enable or disable the IP address filter.
Default IP Address Filter Policy	Select the default policy used when the IP address filter enabled. ◆ **Accept**: Connections from IP addresses not defined in the IP Address filter will be accepted. ◆ **Drop**: Connections from IP addresses not defined in the IP Address filter will be dropped.
WAN Interface	Specify the interface with which the gateway will connect to the WAN: ◆ wlan0: connect to WAN via WLAN (default) ◆ eth0: connect to WAN via Ethernet ◆ usb0: connect to WAN via USB
LAN Interface	Specify the interface that the device will use to connect to the LAN. ***Note:*** *When WAN interface is wlan0, the LAN interfaces are eth0 and usb0. When WAN interface is eth0, the LAN interfaces are usb0 and Access Point. When WAN interface is usb0, the LAN interfaces are eth0 and Access Point.*
Router	
IP Address	Assign a static IP address to the gateway.
IPv6 Address	Assign a static IPv6 address to the gateway.
Primary DNS	Enter the IP address of the primary Domain Name Server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*
Secondary DNS	Enter the IP address of the secondary Domain Name Server. ***Note:*** *This setting will be used when either Static IP or Auto IP is active, or if DHCP is active and no DNS server was acquired from the server.*

MAC Address Filters

Accept or drop traffic from specified MAC addresses using the settings below.

Table 9-57 Adding or Deleting MAC Address Filters

Adding or Deleting MAC Address Filter Settings	Description
Delete	Click the checkbox to the left of any existing mac address filter to be deleted (if any) and click the **Submit** button.
MAC Address	Enter a new mac address to add a new filter.
Action	Select to **Accept** or **Drop** above indicated MAC Address field.
Add (button)	Click the **Add** button to enter new MAC Address filter settings.

IP Address Filters

Accept or drop traffic from specified IP addresses using the settings below.

Table 9-58 Adding or Deleting IP Address Filters

Adding or Deleting IP Address Filter Settings	Description
Delete	Click the checkbox to the left of any existing IP address filter to be deleted (if any) and click the **Submit** button.
IP Address	Enter a new IP address to add a new filter.
Action	Select to **Accept** or **Drop** above indicated IP Address field.
Add (button)	Click the **Add** button to enter new IP Address filter settings.

To Configure Gateway WAN Settings

Using Web Manager

- To view gateway status information, on the **Administration** page, click **Gateway > Status**.
- To modify gateway WAN information, on the **Administration** page, click **Gateway > Configuration > WAN**.

Using the CLI

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

Using XML

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

Port Forwarding

Port forwarding allows remote computers (for example, computers on the Internet) to connect to a specific computer or service within a private local-area network (LAN). Port Forwarding rules apply to inbound traffic and will not work if the SGX 5150 gateway is not reachable or traffic to certain ports is blocked before it reaches the gateway.

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

Table 9-59 Port Forwarding Rules List

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

Table 9-60 Adding a New Port Forwarding Rule

Adding New Port Forwarding Rule Settings	Description
Name	Enter a User Friendly name for the rule (optional)
Ingress IP Address (Optional)	Enter the destination address of the packets. This option can only be used with single ports and not with port range.
Start Port	Enter the starting port number.
End Port	Enter the end port number (optional). If start port and end port are same it assumes a single port. If start port and end port are not the same – it is a port range.
Protocol	Select the protocol for the rule. **TCP**, **UDP**, or **Both**.
IP Address	Enter the target for the port forwarding rule.
Target Port	Indicate the target port. This is the port which the packets are to be forwarded. This options can only be used with single ports and not with port range. If this value is not specified. If this value is not specified, the packets are forwarded to same port or pot range. Optional field.

To Configure Gateway Port Forwarding Settings

Using Web Manager

- To modify gateway port forwarding information, on the **Administration** page, click **Gateway > Configuration > Port Forwarding**.

Using the CLI

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

Using XML

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

Static Routes

Allows the user to add routes to the SGX 5150 gateway routing table.

Table 9-61 Static Route Settings

Static Route Settings	Description
Enabled	Enables the static route
Delete	Deletes the static route
Name	User friendly name for the route. Click on the [Edit] icon to make changes.
Route	Network or Host for the route
Applied	If the route was successfully applied. Routing table updates require a reboot and route needs to be valid as per other device configurables.

Table 9-62 Routing Table

Routing Table Access	Description
Routing Table (Header/Link)	Click this header/link to reveal the current system IPv4 and IPv6 routing tables. Please note that some fields may differ from static route definitions. The following information displays in the **IPv4 routing table**: ◆ Network ◆ Gateway ◆ Mask ◆ Flags ◆ Metric ◆ Interface The following information displays in the **IPv6 routing table**: ◆ Network ◆ NextHop ◆ Flags ◆ Metric ◆ Interface

Table 9-63 Adding a New Static Route

Adding New Static Route Settings	Description
Name	User friendly name for the route
Network	Network or Host for the route

Adding New Static Route Settings	Description
Gateway	Gateway for the route
Interface	Interface for the route
Metric	Priority for the route. Lower metric means higher priority
Add (button)	Click the **Add** button when the new static route fields have been entered.

To Configure Gateway Static Route Settings

Using Web Manager

- To modify gateway static route information, on the **Administration** page, click **Gateway > Configuration > Static Routes**.

Using the CLI

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

Using XML

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

DHCP Server

Allows the user to configure the SGX 5150 gateway as a DHCP server.

Table 9-64 DHCP Settings

DHCP Settings	Description
Configuration	
Lease time	Duration for which lease is initially assigned. Clients must renew after this duration.
DHCP Settings	
State	Enable or Disable the DHCP server for the DHCP settings. ◆ **Enabled**: DHCP server is enabled ◆ **Disabled**: DHCP server is disabled.
DHCP Relay	Enable for the gateway to operate as a DHCP relay agent between the DHCP server on the network and connected Ethernet devices. ◆ **Enabled**: DHCP Relay is enabled. ◆ **Disabled**: DHCP Relay is disabled.
Start IP Address	Start IP Address of address pool.
End IP Address	End IP Address of address pool.
DHCP v6 Settings	
State	Enable or Disable the DHCP server for the DHCPv6 settings. ◆ **Enabled**: DHCP server is enabled ◆ **Disabled**: DHCP server is disabled.
Start IPv6 Address	Start IPv6 Address of address pool

DHCP Settings	Description
End IPv6 Address	End IPv6 Address of address pool

To Configure Gateway DHCP Server Settings

Using Web Manager

- To modify gateway DHCP server or static lease information, on the **Administration** page, click **Gateway > Configuration > DHCP Server**.

Using the CLI

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

Using XML

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

Static Lease Listing

The SGX 5150 gateway also provides the ability to pre-assign specific IP addresses to connected devices using static leases. This would ensure that the connected device (identified by the MAC address) always gets the same IP address even while using DHCP.

Table 9-65 Static Lease Listing

Static Lease List Settings	Description
Delete	Click checkbox beside existing static lease MAC Address/IP Address to delete, if available and if desired.
MAC Address	MAC Address of existing static leases are listed here.
IP Address	Static IP Address of existing static leases are listed here.
IPv6 Address	Static IPv6 Address of existing static leases are listed here.

Table 9-66 Add a Static Lease

Add a Static Lease Settings	Description
MAC Address	Enter the MAC Address of the static lease to be added.
IP Address	Enter static IP address of the static lease to be added.
IPv6 Address	Enter static IPv6 address of the static lease to be added.
Add (button)	Click the **Add** button when the new static lease fields have been entered.

Routing Protocols

The SGX 5150 IoT device gateway allows the configuration of routing protocols. Routing protocols specify how routers communicate with each other, disseminating information that enables the selection of routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a prior knowledge of networks directly attached to it. A routing protocol shares this information among immediate neighbors first, then through the

network. This way, routers gain knowledge of the topology of the network. The SGX 5150 device supports RIP and OSPF protocols.

Table 9-67 Routing Protocol Settings

Routing Settings	Description
RIP	
State	Select to enable or disable the RIP state.
Version	Select how the RIP is to be configured. It can accept **Version 1**, **Version 2**, or **Version 1 and 2**.
Update Interval	Indicate the number of seconds for the Update Interval. Send unsolicited Response message every Update Interval seconds containing the complete routing table to all neighboring RIP routers.
Timeout Interval	Indicate the number of seconds for the Timeout Interval. Upon expiration of the Timeout Interval, the routes are no longer valid, however, they are retained in the routing table for a short time so that neighbors can be notified that the route has been dropped.
GC Interval	Indicate the number of seconds for the GC Interval. Upon expiration of the GC Interval, the routes are finally removed from the routing table.
OSPF	
State	Select to Enable or Disable the OSPF state.
Hello Interval	Indicate the number of seconds for the Hello Interval. Hello packet will be sent every Hello Interval seconds.
Dead Interval	Indicate the number of seconds for the Dead Interval. Sets the time period for which hello packets must not have been seen before neighbors declare the router down.

To Configure Gateway Routing Protocol Settings

Using Web Manager

- To modify gateway protocol settings, on the **Administration** page, click **Gateway > Configuration > Routing Protocol**.

Using the CLI

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

Using XML

- Include in your file: `<configgroup name = "routing protocols">`

Virtual IP

The SGX 5150 IoT device gateway allows the configuration of Virtual IP addresses. Virtual IP is a means to map an externally visible IP address to LAN-side IP addresses. SGX 5150 units will support creating up to three virtual IP address mappings.

Table 9-68 Existing Virtual IP Settings

Virtual IP Settings	Description
Enabled (checkbox)	Uncheck the **Enabled** checkbox adjacent to a virtual IP address (if any listed) to disable it. Keep the checkbox checked to keep the virtual IP address enabled. A virtual IP address is enabled by default.
Delete (checkbox)	Check the **Delete** checkbox adjacent to a virtual IP address (if any listed) to be deleted, clicking the **Submit** button.
Name	Displays the name of the virtual IP address.
IP Address	Displays the virtual IP address to which the LAN IP address is to be mapped.
LAN IP Address	Displays the LAN IP address to which the virtual IP address is to be mapped.

Table 9-69 Add a Virtual IP

Virtual IP Settings	Description
Name	Enter a name of the virtual IP address.
IP Address	Enter the virtual IP address to which the LAN IP address is to be mapped.
LAN IP Address	Enter the LAN IP address to which the virtual IP address is to be mapped.
Add (button)	Click the **Add** button to add a new virtual IP. Newly added static leases will appear under Static Leases (see *Table 9-65 Static Lease Listing*).

To Configure Gateway Virtual IP

Using Web Manager

- To modify gateway DHCP server information, on the **Administration** page, click **Gateway > Configuration > Virtual IP**.

Using the CLI

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

Using XML

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

GRE

GRE tunneling is available on the SGX 5150, providing more capabilities than IP-in-IP tunneling. For example, it supports transporting multicast traffic and IPv6 through a GRE tunnel.

Table 9-70 GRE Settings

GRE Settings	Description
Name	Enter the user-defined name of the GRE tunnel.
State	Select to enable and disable GRE tunnel.
IP Address	Assign a IP address/mask for the GRE tunnel.

GRE Settings	Description
MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit.
Local Network	Select the local network to use the GRE tunnel. Select **vpn 1** to use the VPN network. Select **any** to use any available interface to remote host.
Remote Host	Enter the remote IP address to use for the GRE tunnel.
Remote Network	Enter the remote network to use for the GRE tunnel.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure GRE Settings

Using Web Manager

- To view or configure GRE settings for a specific tunnel, on the **Administration** page, click **GRE**.

Using the CLI

- To enter GRE command level: `enable > gre`

Using XML

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

Host

Table 9-71 Host Settings

Host Settings	Description
Name	Enter a name for the host. This name appears on the Login Connect Menu. To leave a host out of the menu, leave this field blank.
Protocol	Select the protocol to use to connect to the host. Choices are: ◆ Telnet ◆ SSH ***Note:*** *SSH keys must be loaded or created on the SSH page for the SSH protocol to work.*
SSH Username	Appears if you selected SSH as the protocol. Enter a username to select a preconfigured Username/Password/Key (configured on the SSH: Client Users page), or leave it blank to be prompted for a username and password at connect time. ***Note:*** *This configuration option is only available when SSH is selected for Protocol.*
Remote Address	Enter an IP address for the host to which the SGX 5150 gateway will connect.
Remote Port	Enter the port on the host to which the SGX 5150 gateway will connect.

Host Settings	Description
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure Host Settings

Note: *The following section describes the steps to view and configure Host 1 settings; these steps apply to other host instances of the SGX 5150 gateway.*

Using Web Manager

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

Using the CLI

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

Using XML

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

HTTP

Hypertext Transfer Protocol (HTTP) is a request-response standard protocol between clients and servers. HTTP defines how messages are formatted and transmitted. It also defines the actions Web servers and browsers take in response to different commands. HTTP Authentication enables the requirement of user names and passwords for access to the SGX 5150 gateway.

Interface Status, Configuration and Authentication

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

See *Table 9-72* for the HTTP settings that can be modified on the HTTP Configuration page. See *Table 9-73* for the HTTP settings that can be authenticated on the HTTP Authentication page.

Table 9-72 HTTP Configuration

HTTP Settings	Description
State	Select to enable or disable the HTTP server.
Port	Enter the port for the HTTP server to use. The default is **80**.
HTTPS State	Select to enable or disable.
Secure Port	Enter the port for the HTTPS server to use. The default is **443**. The HTTP server only listens on the **HTTPS Port** when an SSL certificate is configured.

HTTP Settings	Description
Secure Protocols	Select to enable or disable the following protocols: ◆ **SSL3** = Secure Sockets Layer version 3 ◆ **TLS1.0** = Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF. ◆ **TLS1.1** = Transport Layer Security version 1.1 ◆ **TLS1.2** = Transport Layer Security version 1.2 The protocols are enabled by default. ***Note:*** *A server certificate and associated private key need to be installed in the **SSL** configuration section to use **HTTPS**.*
Secure Credentials	Specify the name of the set of RSA and/or DSA certificates and keys to be used for the secure connection.
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is **10** seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is **40** KB (this prevents DoS attacks). ***Note:*** *You may need to increase this number in some cases where the browser is sending data aggressively within TCP Windows size limit, when file (including firmware upgrade) is uploaded from webpage.*
Logging State	Select to enable or disable HTTP server logging: ◆ **Enabled** (default) ◆ **Disabled**
Max Log Entries	Set the maximum number of HTTP server log entries. Only the last **Max Log Entries** are cached and viewable.
Log Format	Set the log format string for the HTTP server. Follow these **Log Format** rules: ◆ **%a** - remote IP address (could be a proxy) ◆ **%b** - bytes sent excluding headers ◆ **%B** - bytes sent excluding headers (0 = '-') ◆ **%h** - remote host (same as '%a') ◆ **%{h}i** - header contents from request (h = header string) ◆ **%m** - request method ◆ **%p** - ephemeral local port value used for request ◆ **%q** - query string (prepend with '?' or empty '-') ◆ **%t** - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t') ◆ **%u** - remote user (could be bogus for 401 status) ◆ **%U** - URL path info ◆ **%r** - first line of request (same as '%m %U%q <version>') ◆ **%s** - return status
Authentication Timeout	The timeout period applies if the selected authentication type is either **Digest** or **SSL/Digest**. After this period of inactivity, the client must authenticate again.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To View or Configure HTTP Authentication

Using Web Manager

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

Using the CLI

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

Using XML

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

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

Table 9-73 HTTP Authentication

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

To Configure HTTP Authentication

Using Web Manager

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

Using the CLI

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

Using XML

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

Line

The SGX 5150 units offer 1 or 2 serial ports which use standard RS232 interfaces.

All serial settings such as Baud Rate, Parity, Data Bits, etc, apply to this line.

The line settings allow configuration of the serial line.

Note: *The following section describes the steps to view and configure Line 1 settings; these steps apply to other line instances of the SGX 5150 gateway.*

Line Status and Configuration

View-only status information on the Line 1 - Statistics page displays line statistics including information on bytes, queued bytes, breaks, flow control, parity errors, framing errors, overrun errors, no Rx buffer errors, CTS input, RTS output, DSR input, and DTR output.

See *Table 9-74* for the line settings that can be modified on the Line 1 - Configuration page. See *Table 9-75* for the line settings that can be established on the Line 1 - Command Mode page.

Table 9-74 Line Configuration Settings

Line Settings	Description
Name	Enter a name or short description for the line, if desired. By default, there is no name specified. A name that contains white space must be quoted.
Interface	**Interface** is set to **RS232** and cannot be changed.
State	Select to enable or disable the operational state of the Line. The default is Enabled.
Protocol	Set the operational protocol for the Line. The default is Tunnel. Choices are: ◆ None ◆ Modbus RTU ◆ Modbus ASCII ◆ Tunnel
Baud Rate	Select the desired baud rate from the drop-down menu.
Parity	Select parity from the drop-down menu: **None**, **Even** or **Odd**.
Data Bits	Select data bits from the drop-down menu: **7** or **8**.
Stop Bits	Select **1** or **2** stop bits from the drop-down menu.
Flow Control	Select **None**, **Hardware** or **Software** flow control from the drop-down menu.
Gap Timer	Set the gap timer delay to set the number of milliseconds to pass from the last character received before the driver forwards the received serial bytes. By default, the delay is four character periods at the current baud rate (minimum 1 msec). Gap timer range is 1 to 5000 milliseconds (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.
Early Initialization	Select to enable or disable early initialization. Enabling this option initializes the serial port in the early stages of bootup (around 5 seconds of power on). As a result, data received on this serial port is buffered and transmitted to the network side.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

Table 9-75 Line Command Mode Setting

Line Command Mode Settings	Description
Mode	Set the Command Mode state of the Line. When in Command Mode, a CLI session operates exclusively on the Line. Choices are: ◆ Always ◆ Use Serial String ◆ Disabled ***Note:*** *In order to enable Command Mode on the Line, Tunneling on the Line must be Disabled (both Connect and Accept modes). Also, custom baud rates are not supported in Command Mode.*
Wait Time	Enter the amount of time to wait during boot time for the Serial String. This timer starts right after the Signon Message has been sent on the Serial Line and applies only if mode is "Use Serial String". ***Note:*** *This field becomes available when Use Serial String is selected for Mode.*
Serial String	Enter the Text or Binary string of bytes that must be read on the Serial Line during boot time in order to enable Command Mode. It may contain a time element to specify a required delay in milliseconds x, formed as {x}. Applies only if mode is "Use Serial String". It may contain a binary character(s) of the form [x]. For example, use decimal [12] or hex [0xc]. ***Note:*** *This field becomes available when Use Serial String is selected for Mode.*
Echo Serial String	Select Enable or Disable for Echo Serial String. Applies only if mode is "Use Serial String". Select enable to echo received characters backed out on the line while looking for the serial string. ***Note:*** *This field becomes available when Use Serial String is selected for Mode.*
Signon Message	Enter the string of bytes to be sent to the Serial Line during boot time. It may contain a binary character(s) of the form [x]. For example, use decimal [12] or hex [0xc]. Click the **Submit** button after entering the signon message. ***Note:*** *The **Submit** button will only appear if the Mode is not disabled.*

To View and Configure Line Configuration and Command Mode

Note: *The steps to view and configure Line 1 settings provided in this section are the same for viewing and configuring Line 2.*

Using Web Manager

- To view line 1 statistics, on the **Administration** page, click **Line > Line 1 > Statistics**.
- To configure line 1, on the **Administration** page, click **Line > Line 1 > Configuration**.
- To configure line 1 command mode on the **Administration** page, click **Line > Line 1 > Command Mode**.

Using the CLI

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

Using XML

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

Modbus

The SGX 5150 IoT device gateway operates as a master device that connects to slave devices. The Modbus ASCII/RTU based serial slave devices can be connected via the Ethernet through an existing Modbus TCP/IP network. Any device having access to a given Modbus implementation will be able to perform full range of operations that the implementation supports. Modbus/TCP uses a reserved TCP port of 502 and includes a single byte function code (1=255) preceded by a 6 byte header:

Table 9-76 Byte Header of Modbus Application Protocol

Transaction ID (2 bytes)	Identification of request/response transaction - copied by slave
Protocol ID (2 bytes)	0 - Modbus protocol
Length (2 bytes)	Number of following bytes includes the unit identifier
Address (1 byte)	Identification of remove slave

Serial Transmission Mode

SGX 5150 IoT device gateways can be set up to communicate on standard Modbus networks using either RTU or ASCII. Users select the desired mode and serial port communication parameters (baud rate, parity mode, etc) when in the line configuration options.

Table 9-77 Modbus Transmission Modes

RTU	ASCII
◆ Address: 8 bits (0 to 247 decimal, 0 is used for broadcast) ◆ Function: 8 bits (1 to 255, 0 is not valid) ◆ Data: N X 8 bits (N=0 to 252 bytes) ◆ CRC Check: 16 bits	◆ Address: 2 CHARS ◆ Function: 2 CHARS ◆ Data: N CHARS (N=0 to 252 CHARS) ◆ LRC Check: 2 CHARS

The Modbus web pages allow you to check Modbus status and make configuration changes.

Modbus Statistics

This read-only web page displays the current connection status of the Modbus servers listening on the TCP ports. When a connection is active, the remote client information is displayed as well as the number of PDUs that have been sent and received. Additionally, a **Kill** link will be present which can be used to kill the connection.

Modbus Configuration

This web page shows the current negotiated Modbus settings and allows configuration changes.

Table 9-78 Modbus Configuration

Modbus Configuration Settings	Description
TCP Server State	Select **On** or **Off**. If **On**, the Modbus server is active on TCP 502.
Additional TCP Server Port	Enter the Additional TCP Server Port, if any. ***Note:*** *If present, is used in addition to TCP port 502.*
Response Timeout	Enter the number of milliseconds to wait for a response on the serial side. The SGX 5150 gateway returns exception code 11 to the network master controller if the slave serial device fails to reply within this time out.
RSS Trace Input	Enable or disable the **RSS Trace Input** by clicking **On** or **Off**.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

Note: *The serial line protocol must also be configured for Modbus, in addition to configuring the Modbus server. See* *Line (on page 112)* *and* *Tunnel (on page 132)* *for details.*

To View and Configure the Modbus Server

Using Web Manager

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

Using the CLI

- To enter the Modbus command level: `enable > configure > modbus`

Using XML

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

RSS

An RDF Site Summary (RSS) syndication feed is served by the HTTP Server. This feed contains up-to-date information regarding the configuration changes that occur on the SGX 5150 gateway.

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

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

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

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

Table 9-79 RSS

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

To Configure RSS Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

Security

The SGX 5150 supports a security mode that complies with the FIPS 140-2 standard. FIPS (Federal Information Processing Standard) 140-2 is a security standard developed by the United States federal government that defines rules, regulations, and standards for the use of encryption and cryptographic services. The National Institute of Standards and Technology (NIST) maintains the documents related to FIPS at: http://csrc.nist.gov/publications/PubsFIPS.html.

The FIPS 140-2 standard is available at: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf.

FIPS 140-2 defines four security levels, Level 1 through Level 4. The SGX 5150 is FIPS certified at Level 1. The console manager is FIPS certified at Level 1. FIPS 140-2 compliance requires a defined cryptographic boundary around the cryptographic module on a device. In FIPS mode, the console manager allows only FIPS-approved cryptographic algorithms to be used, and weak algorithms (such as MD5 and DES) are disabled.

To enable FIPS mode, the **Administration -> Security -> FIPS 140-2 Mode** flag needs to be **Enabled** and the SGX 5150 unit rebooted. Each time a FIPS application is started, it will perform a power up self test to verify the integrity of the unit's cryptographic module. If there are any issues with the integrity of the cryptographic module, the application will terminate and an error will be logged in the system log.

For FIPS 140-2 to be enabled:

- Telnet service must be disabled.
- FTP service must be disabled.
- HTTP Secure Credentials must be selected.
- HTTP Authentication Type must be set to Basic.

- A Trusted Authority certificate for the RADIUS server must be configured in order for authentication to succeed.
- VPN must be disabled.
- Modbus must be disabled.
- Line Command Mode must be disabled.
- Syslog must be disabled.
- USB Command Mode must be disabled.
- Tunnel Accept Mode Protocol cannot be TCP or Telnet.
- Tunnel Connect Mode Host Protocol cannot be TCP, Telnet, UDP, or UDP AES.
- Enabled WLAN profiles must use the WPA2/WPA Mixed Mode security suite, or they must be disabled.
- Enabled WLAN profiles must use EAP-TLS/PEAP-EAP-TLS/EAP-TTLS-PAP IEEE 802.1X authentication, or they must be disabled.

If any non-FIPS functionality is enabled, a series of error messages will appear. Follow the error messages to disable all of the functionalities.

To Configure Security Settings

Using Web Manager

- To view and enable/disable security settings, on the **Administration** page, click **Security**.

Using the CLI

- To enter the security command level: `enable > configure > security`

Using XML

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

SFTP

The Secure File Transfer Protocol (SFTP) protocol can be used to control secure file transfers via the SSH port. The SFTP server uses the same port as SSH.

To enable SFTP access, the **Administration -> SFTP -> SFTP State** flag needs to be **Enabled**.

Note: *SSH state must be Enabled to enable SFTP.*

To Configure SFTP Settings

Using Web Manager

- To view and enable/disable security settings, on the **Administration** page, click **SFTP**.

Using the CLI

- To enter the security command level: `enable > configure > sftp`

Using XML

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

SMTP

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

Table 9-80 SMTP Settings

SMTP Settings	Description
From Address	Enter the From Address here. This is an email address and is required. If you wish to direct oubtound email messages through a mail server, put your client email address here.
Server Address	Enter the Server Address to direct outbound email messages through a mail server.
Server Port	Enter the SMTP server port number. The default is 25
Username	Enter a Username to direct outbound email messages through a mail server.
Password	Enter a Password to direct outbound email messages through a mail server.
Overriding Domain	Enter the domain name to override the current domain name in EHLO (Extended Hello).
Local Port	Enter the local port for the SMTP protocol. The local port is the source port for the SMTP client.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure SMTP Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

SNMP

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

Table 9-81 SNMP Settings

SNMP Settings	Description
SNMP Agent	
State	Select to enable or disable the SNMP agent state.
Port	Set the port of the SNMP agent.
Version	Select the SNMP version used by the SNMP agent.
Read Community	Specify the read community used by the agent (defaults to public community).
Write Community	Specify the write community used by the agent (defaults to private community).
System MIB	
System Contact	Specify the system contact.
System Name	Update the system name, as necessary. The default system name is SGX5150.
System Description	Update the system description, as necessary. The default system information includes the manufacturer name, model name, version and the serial number of the SGX 5150 gateway.
System Location	Specify a system location for the SNMP setting.
MIB	
Lantronix MIB File	Click the Lantronix MIB file name to save and load it into the MIB browser and trap receiver. This is the base MIB file for Lantronix products. Load or compile this file first.
MIB File	Click the MIB file name to save and load it into the MIB browser and trap receiver. This is the product specific MIB file. Load or compile this after the Lantronix MIB File.
SNMP Traps	
Primary Destination	Enter the Primary Destination. ***Note:*** *SNMP Traps fields become available when SNMP Agent State is enabled.*
Primary Destination Port	Enter the Primary Destination port. ***Note:*** *SNMP Traps fields become available when SNMP Agent State is enabled.*
Secondary Destination	Enter the Secondary Destination. ***Note:*** *SNMP Traps fields become available when SNMP Agent State is enabled.*
Secondary Destination Port	Enter the Secondary Destination port. ***Note:*** *SNMP Traps fields become available when SNMP Agent State is enabled.*

To Configure SNMP Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

SSH

The SSH Server Host Keys are used by all applications that play the role of an SSH Server during Tunneling in Accept Mode. These keys can be created elsewhere and uploaded to the SGX 5150 gateway or automatically generated on the gateway.

Configuration is required when the SGX 5150 device is either (1) the SSH server or (2) an SSH client. The SSH server is used by the CLI (Command Mode) and for tunneling in Accept Mode. The SSH client is for tunneling in Connect Mode.

To configure the SGX 5150 as an SSH server, there are two requirements:

- **Defined Host Keys:** both private and public keys are required. These keys are used for the Diffie-Hellman key exchange (used for the underlying encryption protocol).
- **Defined Users**: these users are permitted to connect to the SGX 5150 SSH server.

SSH Server: Host Keys

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

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

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

Table 9-82 SSH Server Host Keys

SSH Settings	Description
Private Key	Click the **Choose File...** button to navigate to the existing private key you want to upload. In Web Manager, you can also browse to the private key to be uploaded. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Public Key	Click the **Choose File...** button to navigate to the existing public key you want to upload. In Web Manager, you can also browse to the public key to be uploaded.
Submit (button)	Click the **Submit** button after changes are made in the above Upload Keys fields.
Key Type	Select a key type to use for the new key: ◆ RSA ◆ DSA
Bit Size	Select a bit length for the new key: ◆ 512 ◆ 768 ◆ 1024 ◆ 2048 ◆ 4096
Submit (button)	Click the **Submit** button after changes are made in the above Create New Keys fields.

Note: *SSH Keys from other programs may be converted to the required SGX 5150 format. Use Open SSH to perform the conversion.*

SSH Server: Authorized Users

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

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

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

Table 9-83 SSH Server Authorized Users

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

SSH Client: Known Hosts

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

Table 9-84 SSH Client Known Hosts

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

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

SSH Client: Users

The SSH Client Users are used by all applications that play the role of an SSH Client during Tunneling in Connect Mode. To configure the SGX 5150 as an SSH client, an SSH client user must be both configured and also exist on the remote SSH server.

At the very least, a Password or Key Pair must be configured for a user. The keys for public key authentication can be created elsewhere and uploaded to the SGX 5150 gateway or automatically generated on the gateway.

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

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

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

Table 9-85 SSH Client Users

SSH Settings	Description
Username	Enter the name that the SGX 5150 gateway uses to connect to an SSH server.
Password	Enter the password associated with the username.
Remote Command	Enter the command that can be executed remotely. Default is shell, which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.
Private Key	Click the **Choose File...** button to browse to the existing private key you want to upload by clicking the **Choose File** button. In Web Manager, you can also browse to the private key to be uploaded. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Public Key	Click the **Choose File...** button to browse to the existing public key you want to upload by clicking the **Choose File** button. In Web Manager, you can also browse to the public key to be uploaded.
Key Type	Select a key type for the key: ◆ RSA ◆ DSA
Add/Edit (button)	Click the **Add/Edit** button after changes are made in the above SSH Server: Users fields.

Table 9-86 Create New Keys

SSH Setting	Description
Username	Enter the **Username** for the new key.
Key Type	Select a key type for the new key: ◆ RSA ◆ DSA

SSH Setting	Description
Bit Size	Select the bit length of the new key: ◆ 512 ◆ 768 ◆ 1024 ◆ 2048 ◆ 4096 Using a larger bit size takes more time to generate the key. Approximate times are: ◆ 1 second for a 512 bit RSA key ◆ 1 second for a 768 bit RSA key ◆ 1 second for a 1024 bit RSA key ◆ 2 seconds for a 512 bit DSA key ◆ 2 seconds for a 768 bit DSA key ◆ 20 seconds for a 1024 bit DSA key ***Note:*** *Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 2048 bits long.*
Submit (button)	Click the **Submit** button after changes are made in the above Create New Keys fields.

To Configure SSH Settings

Using Web Manager

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

Using the CLI

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

Using XML

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

SSL

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

SSL certificates identify the SGX 5150 unit to peers and are used with some methods of wireless authentication. Provide a name at upload time to identify certificates on the SGX 5150 unit.

You can upload Certificate and Private key combinations, obtained from an external Certificate Authority (CA), to the SGX 5150 unit. The SGX 5150 unit can also generate self-signed certificates with associated private keys.

Credentials

The SGX 5150 unit 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 SGX 5150 unit. Once you create your credentials, then configure them with the desired certificates.

To Create a New Credential

Using Web Manager

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

Using the CLI

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

Using XML

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

To Delete a Credential

Using Web Manager

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

Using CLI

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

Using XML

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

Table 9-87 SSL Credential - Upload Certificate

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

New Key Type	Select the key type being uploaded: ◆ PEM ◆ Encrypted PEM ◆ PKCS12
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

Table 9-88 SSL Credential - Create New Self-Signed Certificate

Field	Description
Country (2 Letter code)	Enter the 2 letter code for the country where the organization is located. This is a two-letter ISO code (e.g., “US” for the United States).
State/Province	Enter the state or province where the organization is located.
Locality (City)	Enter the city where the organization is located.
Organization	Enter the organization name to which the SGX 5150 unit belongs.
Organization Unit	Enter the organization unit which specifies the department or organization to which the SGX 5150 unit belongs.
Common Name	Enter a network name for the SGX 5150 unit 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 SGX 5150 unit 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 SGX 5150 unit 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 from the drop-down menu.
ECDSA Curve	Select **256**, **384**, or **521** bit.

To Configure an SSL Credential to Use an Uploaded Certificate

1. In the Web Manager, click the **Administration** tab.
2. Click **SSL**.
3. Click **Credentials**.
4. Under the **View or Edit** heading, click the credential that you want to modify to access the information page for that credential.
5. To upload a **New Certificate** to assign to the credential, click **Browse...** beside **New Certificate**, locate the valid certificate, then double-click the file to select it.
6. Identify the **New Certificate Type** selected.
   - If you select SSL authority, RSA, or DSA certificates, select **PEM** or **PKCS7**.
   - If the Web Manager determines that the certificate is an Authority Certificate type, the New Certificate Type field updates to **PKCS12** automatically. For PKCS12 certificates, enter a password.

   Note: *Ensure that the certificate is formatted properly with a valid open and close tag. Also ensure that the Private Key is associated to the selected certificate and that it is formatted properly with a valid open and close tag.*

7. To locate the associated valid **New Private Key** for this certificate, click **Browse...** to browse to and select the file.
8. Select the **New Key Type** from the drop-down menu.
9. Click **Submit**.

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

1. In the Web Manager, click the **Administration** tab.
2. Click **SSL**.
3. Click **Credentials**.
4. Under **View or Edit,** click the credential you wish to modify to access the information page for that credential.
5. Enter the details for a new self-signed certificate for this credential. Reference *Table 9-88 SSL Credential - Create New Self-Signed Certificate on page 125*.
6. Click **Submit**. The process to create a self-signed certificate can take up to 30 seconds, depending on the length of the key.

Trusted Authorities

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

Table 9-89 SSL Trusted Authority

Trusted Authorities Settings	Description
Authority	Click the **Browse...** 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.
New Certificate Type	Select the certificate type through the drop-down window. This field may automatically update, depending upon extension of the certificate entered.
Delete All	To delete all existing certificate authorities as listed, click the **Delete ALL** button.
Delete	To delete an existing certificate authority, click the **Delete** button beside the specific authority listed under **Current Certificate Authorities**.

To Upload an Authority Certificate

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

To upload a trusted authority certificate:

1. In the Web Manager, click the **Administration** tab.
2. Click **SSL**.
3. Click **Trusted Authorities.**

4. Click **Browse...** to browse to and select an authority certificate.
5. Select the **New Certificate Type** from the drop-down window:
   - If you select SSL authority, RSA, or DSA certificates, select **PEM** or **PKCS7**.
   - If the Web Manager determines that the certificate is an authority certificate type, the field updates to **PKCS12** automatically. For PKCS12 certificates, type a **Password**.

Notes:

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

6. Click **Submit**.

CSR (Certificate Signing Request)

The SGX 5150 unit uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the SGX 5150 unit has to expose its identity to a client using a cryptographic certificate. Upon leaving the factory this certificate and the underlying secret key is the same for all SGX 5150 units and will not match the network configuration where it is installed. The certificate's underlying secret key is also used for securing the SSL handshake. Leaving the default certificate unmodified is all right in most circumstances and is necessary only if the network facility is vulnerable to man-in-the-middle attack.

It is possible to generate and install a new base64 encoded x.509 certificate that is unique for a particular SGX 5150 unit. The SGX 5150 unit is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA).

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

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

Table 9-90 SSL CSR (Certificate Signing Request)

Field	Description
Country (2 Letter code)	Enter the two-letter ISO code (e.g., US for the United States) for the country where the organization is located.
State/Province	Enter the state or province where the organization is located.
Locality (City)	Enter the city where the organization is located.
Organization	Enter the organization name to which the SGX 5150 unit belongs.
Organization Unit	Enter the department within the organization to which the SGX 5150 unit belongs.

Field	Description
Common Name	Enter the network name of the SGX 5150 unit once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the SGX 5150 unit 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 SGX 5150 unit is accessed using HTTPS.
Type	Select **RSA** or **ECDSA**.
Key length	Select the key length: **2048** or **4096**.
ECDSA Curve	Select **256**, **384**, or **521** bit.

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

Syslog

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

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

To Configure Syslog Settings

Using Web Manager

1. In the Web Manager, click the **Administration** tab.
2. Click **Syslog**.
3. To enable Syslog, for **State**, select **Enabled**.
4. For **Host**, type the IP address of the remote server that stores the logs.
5. For **Remote Port**, enter the port number for the remote host that supports logging services. The default port number is 514.
6. For **Local Port**, enter the local port to use for Syslog.
7. For **Severity Log Level**, click the arrow to select the minimum level message type that you want the system to log.
8. Click **Submit**.

Using CLI

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

Using XML

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

System

The SGX 5150 settings allow for reboot, restoring factory defaults, uploading new firmware and updating a system's reboot schedule, short name, and long name.

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

Table 9-91 System Settings

System Settings	Description
State	Select to enable or disable the reboot schedule. ***Warning:*** ***Use extreme caution when using scheduled reboots. The SGX 5150 gateway will automatically reboot as scheduled. Any configuration changes not saved to flash memory will be lost. CLI/WEB sessions and network traffic will be interrupted. To avoid frequent reboots, device will not be rebooted if it was started or configured less than 30 minutes from the current date/time.***
Schedule	Select the reboot schedule interval: **Daily** or **Interval**
Time (24 hour)	Set the time to reboot by selecting the **Hour** and **Min** (Minute) in the drop-down menus. ***Note:*** *This configuration option appears when the **Daily** schedule is selected.*
Interval	Enter the interval number in the field. Then select the type of interval from the drop-down menu: ◆ Hours ◆ Days ◆ Weeks ◆ Months ***Note:*** *This configuration option appears when the **Interval** schedule is selected.*
Submit (button)	Click the **Submit** button after settings are made in the above Reboot Schedule fields.
Reboot Device	Click the **Reboot** button to reboot the SGX 5150 gateway. When rebooted, your browser should be refreshed and redirected to the main status page after 30 seconds. ***Note:*** *The redirect will not work as expected if the IP Address of the SGX 5150 gateway changes after reboot.*
Restore Factory Defaults	Click the **Factory Defaults** button to restore the SGX 5150 gateway to the original factory settings. All configuration will be lost. The SGX 5150 unit automatically reboots upon setting back to the defaults. After setting the configuration back to the factory defaults, the gateway will automatically be rebooted.

System Settings	Description
Upload New Firmware	Click **Choose File** to browse to and select the firmware file. If Secure Boot is enabled, only authorized software is allowed to run on the SGX 5150 gateway. Secure Boot requires that the firmware is signed by Lantronix or the authorized OEM. To check if Secure Boot is enabled, click **Status** in the header and check the status of Secure Boot under Device. Uploading new firmware writes the new firmware file to firmware.rom on the SGX 5150 gateway. The gateway automatically reboots upon the installation of new firmware. See the section *FTP on page 99*. ***Caution:*** ***Do not to power off or reset the SGX 5150 gateway while uploading new firmware. Once the upload has completed and the new firmware has been verified and flashed to memory, the SGX 5150 gateway will automatically be rebooted.***
Standalone Firmware Installer	Click **Reboot to Standalone Firmware Installer** to reboot the SGX 5150 gateway to a standalone firmware installer mode. When the SGX 5150 gateway is rebooted, your browser should be refreshed and redirected to the firmware installer page after 30 seconds. Upload and install new device firmware from that page.
Short Name	Enter a short name for the system name. A maximum of 32 characters are allowed.
Long Name	Enter a long name for the system name. A maximum of 64 characters are allowed.

To access System settings:

Using Web Manager

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

Using the CLI

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

Using XML

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

Terminal

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

Table 9-92 Terminal on Network and Line Settings

Terminal on Network and Line Settings	Description
Terminal Type	Enter text to describe the type of terminal. The text will be sent to a host via IAC. ***Note:*** *IAC means, "interpret as command." It is a way to send commands over the network such as* **send break** *or* **start echoing**. *IAC is only supported in Telnet.*
Login Connect Menu	Select the interface to display when the user logs in. Choices are: ◆ **Enabled** = shows the Login Connect Menu. ◆ **Disabled** = shows the CLI (default)
Exit Connect Menu	Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are: ◆ **Enabled** = a choice allows the user to exit to the CLI. ◆ **Disabled** = there is no exit to the CLI (default)
Send Break	Enter the Send Break control character received from the network on its way to a serial line which would cause the line output to be forced inactive. Example setting: `<Ctrl> Y` Blank the field to set to `<None>`. ***Note:*** *This field is not available for terminal network configuration.*
Break Duration	Specify the length of the spacing condition placed on the line when a break is sent. ***Note:*** *This field is not available for terminal network configuration.*
Echo	Select whether to enable echo: ◆ **Enabled** ◆ **Disabled** ***Note:*** *Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable* ***Echo*** *if your terminal echoes, in which case you will see double of each character typed. Default is enabled.*

To Configure the Terminal Network Connection

Using Web Manager

◆ To configure the Terminal on Network, click **Administration** in the header and select **Terminal > Network**.

Using the CLI

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

Using XML

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

To Configure the Terminal Line or USB Connection

Note: *The following section describes the steps to view and configure terminal line 1 settings; these steps apply to terminal line 2 and terminal line 3 of the SGX 5150 gateway.*

Using Web Manager

- To configure a particular Terminal Line, click **Administration** in the header and select **Terminal > Line 1**.
- To configure the Terminal USB, click **Administration** in the header and select **Terminal > USB 1**.

Using the CLI

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

Using XML

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

Tunnel

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

Note: *The following section describes the steps to view and configure Tunnel 1 settings; these steps apply to other tunnel instances of the SGX 5150 gateway.*

Tunnel Statistics

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

To View Tunnel Statistics

Using Web Manager

- To view statistics for a specific tunnel, on the **Administration** page, click **Tunnel** > **Tunnel 1 > Statistics**.

Using the CLI

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

Using XML

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

Serial Settings

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

Table 9-93 Tunnel Serial Settings

Terminal Serial Settings	Description
Line Settings	Line Settings information here is display only. Go to the section, *To Configure the Terminal Line or USB Connection* to modify these settings.
Protocol	Protocol information here is display only. Go to the section, *To Configure the Terminal Line or USB Connection* to modify these settings.
DTR	Select the conditions in which the Data Terminal Ready (DTR) control signal on the serial line are asserted. Choices are: ◆ **Unasserted** ◆ **TruPort** = the DTR is asserted whenever either a connect or an accept mode tunnel connection is active with the Telnet Protocol RFC2217 saying that the remote DSR is asserted. ◆ **Asserted while connected** = the DTR is asserted whenever either a connect or an accept mode tunnel connection is active. ◆ **Continuously asserted**

To Configure Tunnel Serial Settings

Using Web Manager

- To configure the Serial Settings for a specific tunnel, on the **Administration** page, click **Tunnel** > **Tunnel 1 > Serial Settings**.

Using the CLI

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

Using XML

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

Packing Mode

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

Table 9-94 Tunnel Packing Mode Settings

Tunnel Packing Mode Settings	Description
Mode	Configure the Tunnel Packing Mode. Choices are: ◆ **Disable** = Data not packed. ◆ **Timeout** = data sent after timeout occurs. ◆ **Send Character** = data sent when the Send Character is read on the Serial Line.
Threshold	Set the threshold (byte count). If the received serial data reaches this threshold, then the data will be sent on the network. Valid range is 100 to 1450 bytes. Default is 512. ***Note:*** *This configuration option appears when Timeout mode or Send Character mode is selected.*

Tunnel Packing Mode Settings (continued)	Description
Timeout	Set the timeout value, in milliseconds, after the first character is received on the serial line, before data is sent on the network. Valid range is 1 to 30000 milliseconds. Default is 1000. This setting becomes available when the Timeout mode is selected. ***Note:*** *This configuration option appears when Timeout mode is selected.*
Send Character	Enter Control Characters in any of the following forms: ◆ `<control>J` ◆ `0xA` (hexadecimal) ◆ `\10` (decimal) If used, the Send Character is a single printable character or a control character that, when read on the Serial Line, forces the queued data to be sent on the network immediately. ***Note:*** *This configuration option appears when Send Character mode is selected.*
Trailing Character	Enter Control Characters in any of the following forms: ◆ `<control>J` ◆ `0xA` (hexadecimal) ◆ `\10` (decimal). If used, the Trailing Character is a single printable character or a control character that is injected into the outgoing data stream right after the Send Character. Disable the Trailing Character by blanking the field (setting it to <None>). ***Note:*** *This configuration option appears when Send Character mode is selected.*

To Configure Tunnel Packing Mode Settings

Using Web Manager

- To configure the Packing Mode for a specific tunnel, on the **Administration** page, click **Tunnel > Tunnel 1 > Packing Mode**.

Using the CLI

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

Using XML

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

Accept Mode

In Accept Mode, the SGX 5150 listens (waits) for incoming connections from the network. A remote node on the network initiates the connection. The configurable local port is the port the remote device connects to for this connection.There is no remote port or address. Supported serial lines and associated local port numbers progress sequentially in matching value. For instance, the default local port is 10001 for serial line 1 and the default local port for serial line 2 is 10002, and so on for the number of serial lines supported. Serial data can still be received while waiting for a network connection, keeping in mind serial data buffer limitations.

Table 9-95 Tunnel Accept Mode Settings

Tunnel Accept Mode Settings	Description
Mode	Set the method used to start a tunnel in Accept mode. Choices are: ◆ **Disable** = do not accept an incoming connection. ◆ **Always** = accept an incoming connection (*default*). ◆ **Any Character** = start waiting for an incoming connection when any character is read on the serial line. ◆ **Start Character** = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. ◆ **Modem Control Asserted** = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made. ◆ **Modem Emulation** = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.
Local Port	Set the port number for use as the network local port. The default local port number for each supported serial line number progresses sequentially in equal value so that Tunnel X: 1000X. For example: ◆ Tunnel 1: 10001 ◆ Tunnel 2: 10002
Protocol	Select the protocol type for use with Accept Mode: ◆ SSH ◆ SSL ◆ TCP (default protocol) ◆ TCP AES ◆ Telnet
Tunnel Buffer State	Enable or disable the buffering of tunnel data when the connection is lost or not established. Default is disabled.
Tunnel Buffer Size	Specify the size, in MB, of the tunnel buffer. The maximum size is 2 MB for devices with 64 MB of RAM and 8 MB for devices with 256 MB of RAM. The default tunnel buffer size is 1 MB. A buffer of under 4 MB across all tunnels is recommended.
TCP Keep Alive	Enter the time, in milliseconds, the SGX 5150 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.

Tunnel Accept Mode Settings (continued)	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 (in Binary mode): `AB[255,0xFF]C[[D]` Results in a string containing binary values where the dots appear: `AB··C[D]` **Directives** ◆ `%i` local IP address ◆ `%m` MAC address ◆ `%n` network interface name ◆ `%p` local port ◆ `%s` serial number ◆ `%%` %
Flush Serial	Set whether the serial line data buffer is flushed upon a new network connection. 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 networkare sent on into the Serial Line. Any buffered characters are sent first.
Password	Enter a password. This password can be up to 31 characters in length and must contain only alphanumeric characters and punctuation. When set, clients must send the correct password string to the unit within 30 seconds from opening network connection in order to enable data transmission. The password sent to the unit must be terminated with one of the following: ◆ 0A (Line Feed) ◆ 00 (Null) ◆ 0D 0A (Carriage Return/Line Feed) ◆ 0D 00 (Carriage Return/Null) If, **Prompt for Password** is set to **Enabled** and a password is provided, the user will be prompted for the password upon connection.
Email on Connect	Select an email profile number to which an email notification will be sent upon the establishment of an accept mode tunnel.
Email on Disconnect	Select an email profile number to which an email notification will be sent upon the disconnection of an accept mode tunnel.

Tunnel Accept Mode Settings (continued)	Description
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure Tunnel Accept Mode Settings

Using Web Manager

- To configure the Accept Mode for a specific tunnel, on the **Administration** page, click **Tunnel > Tunnel 1 > Accept Mode**.

Using the CLI

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

Using XML

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

Connect Mode

In Connect Mode, the SGX 5150 continues to attempt an outgoing connection on the network, until established (based on which connection method is selected in the configuration described in *Table 9-96*). 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 SGX 5150 will not make a connection unless it can resolve the address. For Connect Mode using UDP, the SGX 5150 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. Telnet protocol is not supported in Tunnels on USB interfaces. The TCP keepalive time is the time in which probes are periodically sent to the other end of the connection. This ensures the other side is still connected.*

Table 9-96 Tunnel Connect Mode Settings

Tunnel Connect Mode Settings	Description
Mode	Set the method to be used to attempt a connection to a remote host or device. Choices are: ◆ **Disable** = an outgoing connection is never attempted. (*default*) ◆ **Always** = a connection is attempted until one is made. If the connection gets disconnected, the SGX 5150 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. ◆ **Modem Control Asserted** = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made. ◆ **Modem Emulation** = a connection is attempted when triggered by modem emulation AT commands.

Tunnel Connect Mode Settings (continued)	Description
Local Port	Enter an alternative Local Port. The Local Port is set to <Random> by default but can be overridden. Blank the field to restore the default.
Host 1	Click on the displayed information to expand it for editing. Complete the Host fields that appear according to *Table 9-97*. If <None> is displayed, clicking it will allow you to configure a new host. At least one Host is required to enable Connect Mode as this information is necessary to connect to that host. Once you start to edit Host 1, a box for Host 2 will show up. Editing Host 2 will cause a Host 3 box to appear. Up to 32 hosts are available.
Reconnect Timer	Set the value of the reconnect timeout (in milliseconds) for outgoing connections established by the SGX 5150 gateway. Valid range is 1 to 65535 milliseconds. Default is 15000.
Flush Serial Data	Set whether the serial Line data buffer is flushed upon a new network connection. Choices are: ◆ **Enabled** = serial data buffer is flushed on network connection ◆ **Disabled** = serial data buffer is not flushed on network connection (*default*)
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ◆ **Enabled** = If Enabled, incoming characters from the Serial Line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the Serial Line if hardware or software flow control is configured. ◆ **Disabled** = this is the default setting; incoming characters from the Serial Line are sent on into the network. Any buffered characters are sent first.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: ◆ **Enabled** = If Enabled, incoming characters from the network will not be forwarded to the Serial Line. Instead, they will be buffered and will eventually flow off the network side. ◆ **Disabled** = this is the default setting; incoming characters from the network are sent on into the Serial Line. Any buffered characters are sent first.
Email on Connect	Select an email profile number to which an email notification will be sent upon the establishment of an accept mode tunnel.
Email of Disconnect	Select an email profile number to which an email notification will be sent upon the disconnection of an accept mode tunnel.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

Table 9-97 Host Settings

Host Field	Description
Configuration Details (to the right of a Host)	Click on **<None>** if the host is not yet configured, or the configured details to the right of a Host (Instance) to open up Host settings fields for that host. The next numerical instance of the host will become available as you complete fields for a particular host.
Address	Enter the address for the remote host connection. Either a DNS address or an IP address maybe provided.
Port	Designate the TCP or UDP port on the remote host for connection.

Host Field	Description
Protocol	Select the desired security protocol. SSH is recommended for circumstances with high security concerns. When using SSH, both the SSH server host keys and the SSH server authorized users must be configured.
SSH Username	Enter a Username. This configuration field becomes available when the SSH Protocol is selected.
Secure Protocols	Select secure protocols to enable. This configuration field becomes available when the SSL protocol is selected. ◆ SSL3 ◆ TLS1.0 ◆ TLS1.1 ◆ TLS1.2
Credentials	Select an existing credential from the drop-down list. This configuration field becomes available when the SSL protocol is selected. Credentials can be created, viewed or edited at the *SSL* > *Credentials* page.
Validate Certificate	Select to enable or disable. This configuration field becomes available when the SSL protocol is selected.
Tunnel Buffer State	Enable or disable the buffering of tunnel data when the connection is lost or not established. Default is disabled. Connect Mode tunnel buffering will occur after the initial connection has been established and then the host loses its network connectivity or the network is interrupted.
Tunnel Buffer Size	Specify the size, in MB, of the tunnel buffer. The maximum size is 2 MB for devices with 64 MB of RAM and 8 MB for devices with 256 MB of RAM. The default tunnel buffer size is 1 MB. A buffer of under 4 MB across all tunnels is recommended.
TCP Keep Alive	Enter the time, in milliseconds, the SGX 5150 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 and select **Text** or **Hexadecimal** to indicate format. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
AES Decrypt Key	Enter the AES Decrypt Key and select **Text** or **Hexadecimal** to indicate format. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
Initial Send	Enter the Initial Send character and select either **Text** or **Binary** format. This configuration field becomes available when the SSH, TCP, UDP, or UDP AES protocol is selected.

Notes:

- *If the keep alive time expires, the user timeout is expired, and there are probes in flight, the connection will be reset. For this reason, it is recommended that if keep alive is used in conjunction with the user timeout, the keep alive timeouts be larger than the user timeout. If it is smaller, what will typically be seen is that the initial probe will be sent, then at the interval where the next probe would normally be sent, the connection will be reset, with no additional probes sent. Also note that in these cases: if the keep alive timer is significantly smaller than the user timeout, probes will continue to be sent for an unreachable host until the user timeout expires.*
- *If there is data in flight when the TCP retransmission timeout kicks in, the user timeout is checked as a limiting condition only when the timer expirations would normally be checked during RTO handling. In other words, the user timeout will not be an exact limit; in practice, it will always take somewhat longer for the connection to be closed. The longer the user timeout is, the more likely it will expire between exponentially slower retransmissions, and the connection will not experience an error until the next retransmission timeout is checked. Also note that the user timeout expiration during retransmission returns an error to the application; it does not automatically reset the connection as happens with keep alive timeout. It is up to the application (e.g., tunneling) to close the connection (this happens almost immediately with tunneling).*

To Configure Tunnel Connect Mode Settings

Using Web Manager

- To configure the Connect Mode for a specific tunnel, on the **Administration** page, click **Tunnel > Tunnel 1 > Connect Mode**.

Using the CLI

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

Using XML

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

Connecting Multiple Hosts

If more than one host is configured, a **Host Mode** option appears. Host Mode controls how multiple hosts will be accessed. For the SGX 5150, the Connect Mode supports up to 32 hosts. Hosts may be accessed sequentially or simultaneously:

- **Sequential** – Sequential host lists establish a prioritized list of tunnels. The host specified as Host 1 will be attempted first. If that fails, it will proceed to Host 2, 3, etc, in the order they are specified. When a connection drops, the cycle starts again with Host 1 and proceeds in order. Establishing the host order is accomplished with host list promotion (see *Host List Promotion on page 141*). 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 SGX 5150 gateway can support a maximum of 64 total aggregate connections.

Host List Promotion

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

To promote a specific Host:

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

Disconnect Mode

Specifies the optional conditions for disconnecting any Accept Mode or Connect Mode connection that may be established. If any of these conditions are selected but do not occur and the network disconnects to the SGX 5150 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. The gateway can support a maximum of 64 total aggregate connections.

Table 9-98 Tunnel Disconnect Mode Settings

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

To Configure Tunnel Disconnect Mode Settings

Using Web Manager

- To configure the Disconnect Mode for a specific tunnel, on the **Administration** page, click **Tunnel > Tunnel 1 > Disconnect Mode**.

Using the CLI

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

Using XML

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

Modem Emulation

Some older equipment is designed to attach to a serial port and dial into a network with a modem. This equipment uses AT commands to control the connection. For compatibility with these older devices on modern networks, the SGX 5150 mimics the behavior of the modem.

Table 9-99 Tunnel Modem Emulation Settings

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

To Configure Tunnel Modem Emulation Settings

Using Web Manager

◆ To configure the Modem Emulation for a specific tunnel, on the **Administration** page, click **Tunnel > Tunnel 1 > Modem Emulation**.

Using the CLI

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

Using XML

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

USB

USB statistics can be viewed and USB settings and command mode may be configured on these USB pages.

USB Statistics

This page displays the current status and various statistics for the USB Line.

To View USB Statistics

Using Web Manager

- To view usb statistics, on the **Administration** page, click **USB > Statistics**.

Using the CLI

- To enter the usb command level: `enable > usb <number>`

Using XML

- Include in your file: `<configgroup name="usb line" instance="3">`

USB Configuration

This page displays the current configuration of the USB Line. Changing any of the fields takes effect immediately. Further configuration is available at Wired Network (USB) for 'Ethernet Device' mode.

Table 9-100 USB Configuration

USB Settings	Description
Name	Enter the **Name** of the USB line. Named lines appear in the 'Login Connect Menu', if enabled. Set it blank to leave it out of the menu.
Interface	**Interface** is set to **USB-CDC-ACM** and cannot be changed.
State	Select to enable or disable the **State**.
Protocol	Select type of **Protocol** from the drop-down menu: **Tunnel** or **None**.
Line Mode	Select the USB port mode from the drop-down menu. The USB port can be configured in one of the following: **Ethernet Device, Serial Device**, or **Host**. Host mode supports connecting Mass Storage and Serial devices.
Gap Timer	Indicate the gap time in milliseconds. The driver forwards received serial bytes after the **Gap Timer** delay from the last character received. By default, the delay is four character periods at the current baud rate (minimum 1 ms).
Threshold	Enter the threshold in bytes. The driver will forward received characters after threshold bytes have been received.

USB Settings	Description
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure USB Settings

Using Web Manager

- To configure usb settings, on the **Administration** page, click **USB > Configuration**.

Using the CLI

- To enter the usb command level: `enable > usb`

Using XML

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

USB Command Mode

Table 9-101 USB Command Mode

USB Command Mode Settings	Description
Mode	When Command Mode is enabled, the Command Line Interface (CLI) is attached to the USB Line. Command Mode can be enabled in a number of ways: ◆ The **Always** choice immediately enables Command Mode for the USB Line. ◆ The **Use Serial String** choice enables Command Mode when the Serial String is read on the USB Line during boot time. ◆ **Disabled**
Wait Time	Enter the **Wait Time** in milliseconds. The specified time defines the amount of time to wait during boot time for the Serial String. This timer starts right after the Signon Message has been sent on the USB Line.
Serial String	Enter the **Serial String**. The Serial String is a string of bytes that must be read on the USB Line during boot time in order to enable Command Mode. It may contain a time element to specify a required delay in milliseconds x, formed as {x}.
Echo Serial String	Select to enable or disable.
Signon Message	Enter the Signon Message, which is a string of bytes that is sent on the USB Line during boot time. Place a binary character into either the Serial String or the Signon Message using `[x]`. For example, use decimal `[12]` or hex `[0xc]`.
Submit (button)	Click the **Submit** button to enter the settings. The **Submit** button appears when new settings are entered.

To Configure USB Command Mode

Using Web Manager

- To configure usb command mode, on the **Administration** page, click **USB > Command Mode**.

Using the CLI

- To enter the usb command level: `enable > usb`

Using XML

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

User Management

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

Table 9-102 Administrator Settings

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

Administrator Settings	Description
Username	View and modify the Administrator **Username** as desired. The default Username is `Admin`.
Password	Modify the Administrator **Password** as desired. The default Password is the last 8 characters of the Device ID (for devices manufactured after January 1, 2020) or `PASS` (for all older units).
Submit	Click **Submit** to submit changes to the **Username** and/or **Password**. The **Submit** button appears when either or both Username and Password are modified.

Table 9-103 Current Users List

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

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

Table 9-104 New User Settings

Create new user login, password and roles here. Admin-created users can be deleted or altered in the Current Users list (*Table 9-103*). Up to 8 user accounts can be created to access the SGX 5150 gateway.

New User Settings	Description
Username	Enter the **Username** of the new user. Must be between 4 and 15 characters.
Password	Enter the **Password** of the new user. Must be between 4 and 15 characters.

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

Table 9-105 Current Roles List

The system-defined default roles that come with the SGX 5150 gateway along with any Admin-created user roles are listed here. Admin-created custom roles can be deleted or altered.

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

Table 9-106 New Role Settings

Create a custom role here. Admin-created custom roles can be deleted or altered in the Current Roles list (*Table 9-105*). Up to 8 custom roles can be created.

New Role Settings	Description
Name	Enter the name of a new role to be created.
Actions	Check the **Actions** that the new role will have access to, if any: ◆ Device Reboot ◆ Factory Reset ◆ Firmware Upgrade

New Role Settings	Description
Configuration Groups	Check the Configuration Groups the new role will have access to configuring, if any: ◆ Access Point ◆ Action ◆ Applications ◆ ARP ◆ Bluetooth ◆ Bluetooth Line ◆ Bluetooth spp master ◆ Bluetooth spp slave ◆ Bridge ◆ CLI ◆ Clock ◆ ConsoleFlow ◆ ConsoleFlow Line ◆ CP Functions ◆ Device ◆ DHCP Server ◆ Diagnostics ◆ Discovery ◆ Email ◆ Wired Network ◆ Filesystem ◆ FTP Server ◆ Gateway ◆ GRE ◆ Host ◆ HTTP Authentication ◆ HTTP ◆ ICMP ◆ Input Filters ◆ Interface ◆ IP ◆ IP filters ◆ Line ◆ Modbus ◆ Network Failover ◆ QoS ◆ Reboot Schedule ◆ Routing Protocols ◆ RSS ◆ Security ◆ Serial Command Mode ◆ SFTP Server ◆ Smart Roam ◆ SMTP ◆ SNMP ◆ SSH ◆ SSH client ◆ SSH server ◆ SSL ◆ Syslog ◆ Telnet ◆ Terminal ◆ Tunnel Accept ◆ Tunnel Connect ◆ Tunnel Disconnect ◆ Tunnel Modem ◆ Tunnel Packing ◆ Tunnel Serial ◆ USB Line ◆ User Management ◆ Virtual IP ◆ VPN ◆ WLAN Profile ◆ Wireless Network
Add	Click **Add** to submit the new role. Click **OK** in the confirmation window which appears to add the role.

To Configure User Management

Using Web Manager

- To configure usb command mode, on the **Administration** page, click **User Management.**

Using the CLI

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

Using XML

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

XML

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

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

The exported file can be modified and imported to update the configuration on this SGX 5150 gateway or another.

XML records can also be exported to browser window or to a download link on the SGX 5150 gateway.

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

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

To Export Configuration

By default, all settings groups are checked.

Using Web Manager

1. In the Web Manager, click the **Administration** tab.
2. Click **XML**.
3. Click **Export Configuration**.
4. Select where to send exported status information:
   - **Export to browser** sends the information into a separate web window which appears.
   - **Export to local file** sends information into a new locally saved file. A file name must be specified in field provided if this option is selected.
5. Select **Download (from link)** to download this content as a file, or click **Export to browser** to open a web browser with this content.
6. To include descriptive comments in the XML file, check **Comments**.
7. For **Lines to Export**, check the lines and/or the network that you want to export to the XML configuration file.
   - Clicking the **Clear All** button will uncheck all checkboxes.
   - Clicking the **Select All** button will check all checkboxes.
8. Click the desired **Groups to Export**. Several checkboxes are available.
   - Clicking the **Clear All** button will uncheck all checkboxes.
   - Clicking the **Select All but Networking** button will check all checkboxes except `Interface:etho, Bridge:br0 and Interface:wlan0.`

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

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

Using the CLI

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

Using XML

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

To Export Status

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

Using Web Manager

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

Notes:

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

7. Click **Export**.

Using the CLI

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

Using XML

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

To Import Configuration

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

Using Web Manager

1. In the Web Manager, click the **Administration** tab.
2. Click **XML**.
3. Click **Import Configuration**.
4. Select where to import configuration information:
   - **Configuration from External file** picks up all the settings from the external file. For this option, click **Choose File...** to locate and select the XML configuration file that you wish to import. The name of the file will appear in the Web Manager screen. Click **Import**.

- **Configuration from Filesystem** picks up settings from the selected Groups, Lines and Instances. Make selections in form which appears (see *Table 9-107*) and click **Import**.
- **Line(s) from single line Settings on the Filesystem** copies lines settings from an the input file containing only one Line instance to all of the selected Lines. Make selections in form which appears (see *Table 9-107*) and click **Import**.
- **Import configuration from (entire) external XCR file** allows you to browse to an external XCR file. For this option, click **Choose File... t**o locate and select the XCR file you wish to import. The name of the file will appear in Web manager screen. Click **Import**.

Using the CLI

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

Using XML

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

Table 9-107 Configuration from Filesystem

Setting	Description
Filename	Enter the name of the file on the SGX 5150 unit (local to its filesystem) that contains XCR data.
Lines to Import	Select filter instances to be imported in the line, serial, tunnel and terminal groups. This affects both Whole Groups to Import and Text List selections. Click **Clear All** to clear all checkmarks, or **Select All** to check all checkmarks.
Whole Groups to Import	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group. Click **Clear All** to clear all checkmarks, or **Select All but Networking** to check all checkmarks except Networking.
Text List	Enter the string to import specific instances of a group. The textual format of this string is: `<g>:<i>;<g>:<i>;...` Each group name <g> is followed by a colon and the instance value <i> and each <g>:<i> value is separated by a semi-colon. If a group has no instance then only the group name <g> should be specified.
Import (button)	Click the **Import** button when the Configuration from Filesystem fields are completed above.

Table 9-108 Line(s) from single line Settings on the Filesystem

Setting	Description
Filename	Enter the name of the file on the SGX 5150 unit (local to its filesystem) that contains XCR data.
Lines to Import	Select filter instances to be imported in the line, serial, tunnel and terminal groups. This affects both Whole Groups to Import and Text List selections. Click **Clear All** to clear all checkmarks, or **Select All** to check all checkmarks.
Whole Groups to Import	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group. Click **Clear All** to clear all checkmarks, or **Select All but Networking** to check all checkmarks except Networking.

Import (button)	Click the **Import** button when the Line(s) from single line Settings on the Filesystem fields are completed above.

Quick Setup

Quick Setup provides a place to configure all basic settings in one place. You may access Quick Setup through the Administration menu or whenever you reset your system to factory defaults.

Note: *The SGX 5150 IoT Device Gateway Quick Start Guide provides for instructions on accessing Web Manager via SoftAP (go to* www.lantronix.com/support/documentation*).*

To Utilize Quick Setup

Using Web Manager

1. In the Web Manager, click the **Administration** tab.
2. Click **Quick Setup**.
3. Click **OK** in the verification window which appears.
4. Update the Quick Setup information below:

Table 9-109 Administrator Settings

Setting	Description
Username	View and modify the Administrator username. The default username is **admin**.
Password	Modify the Administrator password as desired. The default password is the last 8 characters of the Device ID (for units manufactured after January 1, 2020), or **PASS** for older units. Check the **Show Password** check box to make the password viewable as you enter it in the Password field.

Table 9-110 Bridge 1(br0) Configuration

Setting	Description
State	Select to enable or disable the state
Bridging Mode	Select **Host**, **Network**, or **Static Network**.
Transparent Mode	Select to enable or disable the transparent mode.
Network Access for Gateway	Select to enable or disable network access for the gateway. This can only be enabled if Transparent Mode is **Enabled**.
Ethernet Interface	Select the desired interface: eth0 or usb0
Bridging MAC Address	Enter the bridging MAC address
Bridging IP Address	Enter the bridging IP address
Bridging IPv6 Address	Enter the bridging IPv6 address

Setting	Description
Auto Detect IPv4 Address	Check the radio button to enable it. If checked, the SGX 5150 gateway will attempt to learn the IP Address by using the source or destination IP address of packets arriving on the Ethernet interface. ***Warning:*** ***Running processes may be impacted while the SGX 5150 gateway monitors Ethernet traffic to determine the wired host IP address.***
Initial Scan Interval	Enter the **Initial Scan Interval** in seconds.
Scan Interval	Enter the **Scan Interval** in seconds.

Table 9-111 Wi-Fi Protected Setup

Setting	Description
WPS (PBC)	Click this button for push button connect.
WPS (PIN)	Click this button for pin hole connect.

Table 9-112 Current Configuration

Setting	Description
Network Name (SSID)	View existing network name/SSID, if any.
State	Select to enable or disable the state
IPv4 State	Select to enable or disable the state
DHCP Client	Select to turn on or off
IPv6 State	Select to enable or disable the state
IPv6 DHCP Client	Select to turn on or off
IPv6 Auto Configuration	Select to turn on or off

Table 9-113 Available Networks

Setting	Description
Refresh scan results every 60 seconds	Check this checkbox and click **Scan** to scan available networks every 60 seconds. Scroll through list of available networks listed, as desired.
Show entries (dropdown menu)	Select the number of entries to show on the page at a time.
Search (field)	Enter characters within the name of an SSID in the Search field to limit scan results to SSIDs with characters typed.
Previous 1 2 3 4 5 6 Next	Click to navigate among multiple pages of WLAN link scan results.

5. Click **Clear** at any time to clear all fields of choices made (if any). The **Clear** button will only appear when changes have been made to fields above.
6. Click **Manual Setup** to return to the Status page where you may make changes directly in the configuration pages accessible through the **Network**, **Diagnostic** and **Administration** tabs.
7. Click **Submit** to submit configuration choices on the Quick Setup page.

Using the CLI

- Not applicable.

Using XML

- Not applicable.

10: Developing Applications Using Yocto SDK

This chapter is intended for developers.

Using Lantronix PremierWave BSP Yocto Project

Summary

These instructions explain how to use PremierWave BSP Yocto to create a ROM image for the SGX 5150 that will include your own applications/configuration.

This is based on Yocto Jethro.

Prerequisites

Development is done on a PC running Linux OS natively. These instructions have been validated on Ubuntu 16.04. Install the necessary packages using the following commands:

```
sudo apt-get install gawk wget git-core diffstat unzip textinfo gcc-
      multilib \ build-essential chrpath socat libsdl1.2-dev xterm
sudo apt-get install lzop
```

Build the ROM Image and SDK

Navigate to the folder in which you cloned the repo and build the ROM image and SDK using the following commands:

```
cd yocto_premierwave/sources
git clone -b jethro git://git.yoctoproject.org/poky.git
git clone -b jethro git://git.openembedded.org/meta-openembedded.git
cd ..
./customer_set_target.sh sgx5150
source sources/poky/oe-init-build-env build
bitbake ltrx-customer-image
```

The step "`bitbake ltrx-customer-image`" builds the target ROM image ("SGX5150_.rom" in "build/tmp/deploy/images/sgx5150/"). The initial build takes about 1 hour. Further builds after modifying your application are much faster because only changes are processed.

```
bitbake ltrx-customer-image -c populate_sdk
```

The step "`bitbake ltrx-customer-image -c populate_sdk`" builds the SDK, "poky-glibc-x86_64-ltrx-customer-image-armv5e-toolchain-2.0.3.sh" (together with two other manifest files) under the folder "build/tmp/deploy/sdk/". This build takes about another 30 minutes.

Install SDK

Go to the folder containing the built SDK and install it using the following command:

```
./poky-glibc-x86_64-ltrx-customer-image-armv5e-toolchain-2.0.3.sh
```

Confirm you want to proceed by entering "`Y`".

Use SDK to Build/Test Your Application

1. In your application source folder, run the SDK environment script as shown below. Note the actual script path is determined during the SDK installation in the above step.

```
. /opt/poky/2.0.3/environment-setup-armv5e-poky-linux-gnueabi
echo $CC
```

2. Build your application as a standalone executable as shown below.

```
$CC your-app.c -o your-app
```

3. Load the ROM file built above to the target. (See *Upload/Program Firmware into Gateway* for details).
4. Copy (scp/ftp) the application executable file to the target using the user **root** with the password **root**.
5. Login the device using the user **root** and the password **root**. Run/test the application executable.

Add/Update Your Application into the ROM Image

Once the application is working, you can build your application into the ROM image. The GIT folder structure is as follows:

```
yocto_premierwave
├── build
│   ├── conf
│   │   ├── bblayers.conf
│   │   └── local.conf
│   └── tmp
│       ├── deploy
│       └── log
├── examples
│   └── ...
├── README.md
└── sources
    ├── meta-application
    │   ├── conf
    │   │   └── layer.conf
    │   ├── recipes-application
    │   │   └── **helloworld**
    │   │       ├── files
    │   │       │   ├── COPYING.MIT
    │   │       │   └── helloworld.c
    │   │       └── helloworld.bb
    │   └── recipes-bsp
    │       └── images
    │           └── **ltrx-customer-image.bbappend**
    ├── meta-lantronix
    │   ├── classes
    │   ├── conf
    │   ├── COPYING.MIT
    │   ├── README
    │   ├── recipes-bsp
    │   ├── ...
```

As shown above, “helloworld” is provided as an example application. Create a folder in “recipes-application” for your application, put the recipe and code in the folder you created, and then add your application to “ltrx-customer-image.bbappend” located in “recipes-bsp/images/”.

After changes are made, rebuild the ROM image as follows. The built ROM image will contain your application. This build is quick because it only processes the changes.

```
bitbake ltrx-customer-image -c cleanall
bitbake ltrx-customer-image
```

Upload/Program Firmware into Gateway

Flash this like any normal SGX 5150 ROM image.

Examples

Code examples using Lantronix APIs are located in the folder "examples/".

"**ltrx-customer-image.bbappend**" located in "sources/meta-application/recipes-bsp/images/" provides instructions to:

- change root password
- disable root login
- extend /etc/inittab to start an application during bootup

Secure Boot

Secure Boot ensures that only digitally-signed software is run on the SGX 5150. If you plan to release custom firmware, you must prepare the SGX 5150 for OEM Secure Boot using the process below.

Note: *Preparing the SGX 5150 to use custom firmware requires the use of the serial port on the SGX 5150. SGX 5150 models that do not have a serial port are unable to use custom firmware.*

Firmware Filenames

The following files are used in the process of preparing the SGX 5150 for Secure Boot. The version number may be different.

- SGX5150_<version>.rom - Application firmware
- at9g252_mfgtestldr_<version>.rom - MFG loader
- at9g252_recovldr_<version>.rom - Recovery loader

Preparing the SGX 5150 for OEM Secure Boot

1. Create an OEM public-private key pair using the following command:

```
openssl ecparam -name secp256r1 -genkey -out oem-priv.pem
openssl ec -in oem-priv.pem -pubout -out oem-pub.pem
```

2. Use the request form to submit the public key to Lantronix for signature. Lantronix returns the signed public key as a .rom file that is named similarly to optional_rsa_key_pub.signed.rom.
3. Sign the application firmware with the OEM private key.

```
ltrx-signimage -f oem-priv.pem SGX5150_<version>.signed.rom
      SGX5150_<version>.oem.signed.rom
```

4. Launch the MFG loader (at9g252_mfgtestldr_<version>.signed.rom) by connecting to the device over serial using a terminal emulator such as TeraTerm and sending the following command until the G prompt appears:

```
!SL
```

5. Send the MFG loader file (at9g252_mfgtestldr_<version>.signed.rom). In TeraTerm, this is done by clicking **File** > **Send File**.
6. Install the Lantronix-signed OEM key (oem-pub.signed.rom).

```
flash download serial
```

7. Lock the OEM key.crypto lock-key oem-key
8. Download the OEM-signed application firmware (SGX5150_<version>.oem.signed.rom).

```
flash download serial
```

9. Reboot.

Note: *You will need to use the OEM-signed MFG loader, recovery loader, and application firmware once the OEM key has been configured on the device.*

10. Sign the MFG test loader with the OEM private key.

```
ltrx-signimage -f oem-priv.pem at9g252_mfgtestldr_<version>.signed.rom
      at9g252_mfgtestldr_<version>.oem.signed.rom
```

11. Sign the Recovery Loader with the OEM private key.

```
ltrx-signimage -f oem-priv.pem at9g252_recovldr_<version>.signed.rom
      at9g252_recovldr_<version>.oem.signed.rom
```

Releasing Custom Firmware

Once Secure Boot is enabled on the gateway, all custom firmware must be signed with the OEM private key using the ltrx-signimage application. This is done each time you release a firmware rom.

```
ltrx-signimage -f ltrx-priv.pem SGX5150_<version>.signed.rom
      SGX5150_<version>.oem.signed.rom
```

After following the procedure above to prepare the SGX 5150 for OEM Secure Boot, no additional steps with the device are required when releasing new firmware.

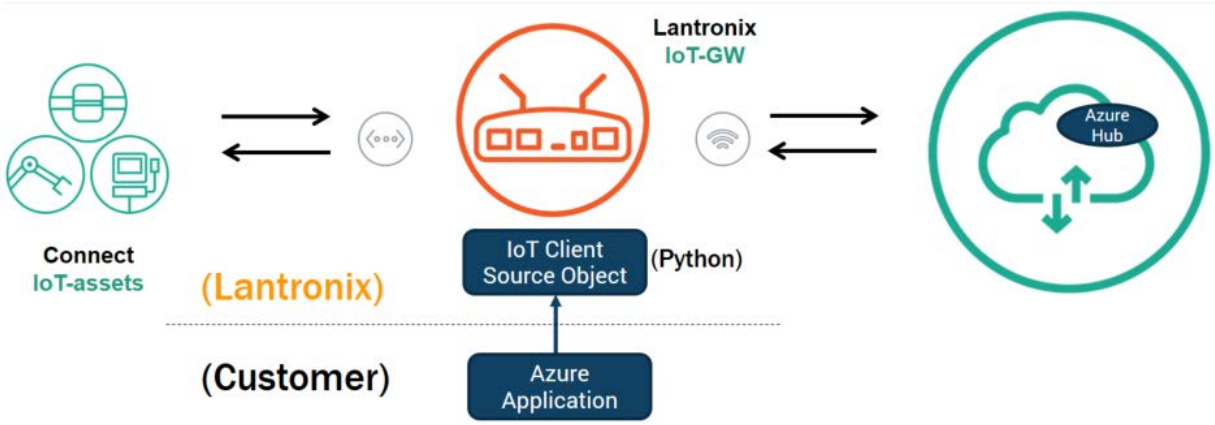
Note: *For next steps and additional information, visit the Yocto Project website at https://www.yoctoproject.org/ and the Lantronix GitHub site at https://github.com/lantronix/.*

Integration with Microsoft Azure

The SGX 5150 is compatible with Microsoft Azure. The gateway uses Yocto Linux, which can run the Azure IoT SDK.

Environment Setup for Microsoft Azure

Figure 10-16 Environment Setup for Microsoft Azure



Python libraries are integrated into SGX 5150 software to support the Azure IoT SDK. This is represented above as “IoT Client Source Object.” Your Azure application must be built on top of the SGX 5150 software. After connecting IoT devices to the SGX 5150, the SGX 5150 can then be connected to Azure Hub.

To set up the SGX 5150 with Microsoft Azure:

1. Include Azure IoT SDK support. In the file sources/meta-applications/recipes-bsp/images/ltrx-customer-image.bbappend, include **IMAGE_INSTALL += “azure-iot-sdk”**.
2. Configure Azure IoT Hub.
3. Register your IoT device(s).
4. Build and deploy Azure IoT SDK on the SGX 5150.

For more information, visit https://github.com/Azure/azure-iot-device-ecosystem/blob/master/iotcertification/templates/template-linux-python.md#PrepareDevice.

Using Lantronix Beacon Scanner

Lantronix Beacon Scanner is an application that scans and displays information on Bluetooth devices that broadcast Apple iBeacon, EddyStone UID Beacon, EddyStone URL Beacon, and EddyStone TLM Beacon. Lantronix Beacon Scanner can be built using the SDK and run from the shell via SSH.

Installing Lantronix Beacon Scanner

1. Build the application, located at “yocto_premierwave/examples/beacon/”, using Yocto SDK.

```
$CC -Wno-poison-system-directories -Wno-return-local-addr
      ltrx_beacon_scanner.c -o example_ltrx_beacon -I/usr/include/glib-
      2.0/ -I/usr/lib/x86_64-linux-gnu/glib-2.0/include/ -I/usr/lib/
      x86_64-linux-gnu/dbus-1.0/include/ -I/usr/include/dbus-1.0/ -
      lltrx-beacon -lglib-2.0 -ldbus-1 -lreadline
```

2. Copy the application executable “example_ltrx_beacon” to the device. This can be done using the Filesystem tab of Web Manager or via scp. If uploading via Web Manager, do not upload it into a subdirectory. If using scp, you must use root credentials (by default the username is “root” and password is “root”) and upload to the /ltrx_user/ directory.

```
scp example_ltrx_beacon root@xxx.xxx.xxx.xxx:/ltrx_user/
```

Using Lantronix Beacon Scanner

To run Lantronix Beacon Scanner, connect to the SGX 5150 via SSH and run the application using the command `ltrx_beacon_scanner`.

1. Connect using SSH using root credentials (by default the username is “root” and password is “root”).

```
ssh root@xxx.xxx.xxx.xxx
```

2. Change to the /ltrx_user/ directory.

```
cd /ltrx_user
```

3. Change the permissions of the example_ltrx_beacon application to executable if this is your first time using Lantronix Beacon Scanner.

```
chmod 777 example_ltrx_beacon
```

4. Run the application.

```
./example_ltrx_beacon
```

The following table describes the commands that can be used in Lantronix Beacon Scanner.

Table 10-114 Lantronix Beacon Scanner commands

Command	Description
devices	This lists all devices (beacons) that were found with the scan command.
info [dev]	This displays information about the specified device.
list	This lists the available controllers, which will be the Bluetooth controller of the PremierWave 2050.
quit	This quits the Lantronix Beacon Scanner.
remove <dev>	This removes a scanned device from the list.

Command	Description
scan <on/off>	This starts or stops scanning for beacons.
select <ctrl>	This selects the default controller. There is only one Bluetooth controller in the PremierWave 2050.
show [ctrl]	This displays information on the Bluetooth controller.
version	This displays the version of the application.

The source file can be found at https://github.com/Lantronix/yocto_premierwave/tree/master/examples/beacon.

A: Lantronix Technical Support

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

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

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

B: Compliance

(According to ISO/IEC Guide and EN 45014)

Manufacturer's Name & Address:

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

Product Name Model:

SGX 5150 IoT Device Gateway

Conforms to the following standards or other normative documents:

Safety

- UL 60950-1, 2nd Edition, 2014-10-14 (Information Technology Equipment - Safety - Part 1: General Requirements)
- CSA C22.2 No. 60950-1-07, 2nd Edition, 2014-10 (Information Technology Equipment - Safety - Part 1: General Requirements)
- CB Scheme IEC 60950-1:2005 (Second Edition); Am1:2009 + Am2:2013
- VCCI

Emissions

- CFR Title 47 FCC Part 15, Subpart B, Class B Emissions
- EN55022: 2010, Class B Emissions
- EN55032: 2012 + AC: 2013, Class B Emissions
- CISPR 32: 2012 Class B Emissions
- CISPR 22: 2009, Class B Emissions
- VCCI V-3: 2015.04

Immunity

- EN55024: 2010
- EN610000-4-2: 2009
- EN61000-4-3: 2006 + A1: 2008 + A2: 2010
- EN61000-4-4: 2004
- EN61000-4-5: 2005
- EN61000-4-6: 2009
- EN61000-4-8: 2010
- EN61000-4-11: 2004
- CISPR 16-1-4: 2008
- ICES-0003 Issue 6

Figure B-1 SGX 5150 Suppliers Declaration of Conformity

LANTRONIX®

SUPPLIERS DECLARATION OF CONFORMITY

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

Product Type:	Wireless IoT Gateway
Product Family:	SGX 5150 Series
Rated:	9-30Vdc, or 5Vdc from USB, or PoE powered, 5.5W maximum
Intended use:	Commercial installations, indoor use

North America

Safety:

- UL 60950-1 (2nd Ed., 2014-10-14)
- CAN/CSA C22.2 No. 60950-1-07 (2nd Ed., 2014-10)

Emissions:

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

European Union

Safety: Low Voltage Directive (2014/35/EC)

- EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011 + A2: 2013
- CB Scheme IEC 60950-1:2005 (2nd Edition) + Am1:2009 + Am2:2013

Emissions: EMC Directive (2014/30/EU)

- EN 55032: 2012 + AC: 2013, Class B
- EN 55022: 2010, Class B

Immunity: EMC Directive (2014/30/EU)

- EN 55024: 2010
- EN 610000-4-2: 2009
- EN 61000-4-3: 2006 + A1: 2008 + A2: 2010
- EN 61000-4-4: 2004
- EN 61000-4-5: 2005
- EN 61000-4-6: 2009
- EN 61000-4-8: 2010
- EN 61000-4-11: 2004
- ETSI EN 301 489-17 V3.1.1 (2016-11)
- ETSI EN 301 489-1 V2.1.1 (2016-11)

Other Countries

- **Australia**
  - CISPR 32: 2012, Class B Emissions
- **Japan**
  - VCCI 32: 2016, Class B Emissions
  - VCCI V-3: 2015.04, Class B Emissions

Wi-Fi Transmitter IDs for the Internal Wireless Module

- **USA FCC ID:** R68PW2050
- **Canada IC ID:** 3867A-PW2050
- **Mexico:** RCPLAPW15-2109
- **Japan ID:** 201-152843

Wi-Fi Transmitter ID for SGX 5150

- **China CMIIT ID:** 2016AP9148

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

Signature: Daryl R. Miller Date: 8-17-18

Name: Daryl R. Miller Title: VP of Engineering

CERT-00103 rev H

Product Name Model:

SGX 5150 MD Wireless IoT Gateway for Medical Devices

Conforms to the following standards or other normative documents:

Medical Safety

- EN 60601-1:2006/ AC:2010/ A1:2013 (Medical electrical equipment -- Part 1: General requirements for basic safety and essential performance)
- ANSI/AAMI ES60601-1: 2005/C1:2009/A2:2010 (Medical electrical equipment -- Part 1: General requirements for basic safety and essential performance)
- CAN/CSA-C22.2 NO. 60601-1-08 (Medical electrical equipment -- Part 1: General requirements for basic safety and essential performance)

Non-Medical Safety

- UL 60950-1, 2nd Edition, 2014-10-14 (Information Technology Equipment - Safety - Part 1: General Requirements)
- CSA C22.2 No. 60950-1-07, 2nd Edition, 2014-10 (Information Technology Equipment - Safety - Part 1: General Requirements)
- CB Scheme IEC 60950-1:2005 (Second Edition) + Am1:2009 + Am2:2013

Emissions

- CISPR 11:2009, class B

Immunity

- EN / IEC 60601-1-2: 2014
- EN 61000-3-2: 2014
- EN 61000-3-3: 2013
- EN / IEC 61000-4-2: 2008
- EN / IEC 61000-4-3: 2006 + A1: 2007 + A2: 2010
- EN / IEC 61000-4-4: 2012
- EN / IEC 61000-4-5: 2005
- EN / IEC 61000-4-6: 2013
- EN / IEC 61000-4-8: 2009, 2010
- EN / IEC 61000-4-11: 2004

Figure B-2 SGX 5150 MD Suppliers Declaration of Conformity

LANTRONIX®

SUPPLIERS DECLARATION OF CONFORMITY

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

Product Type:	Medical Wireless IoT Gateway
Product Family:	SGX 5150 MD
Rated:	12Vdc, 5.5W maximum
Intended use:	Commercial installations, indoor use

North America

Medical Safety:

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

Non-Medical Safety:

- UL 60950-1, 2nd Edition, 2014-10-14
- CAN/CSA C22.2 No. 60950-1-07, 2nd Edition, 2014-10

Emissions:

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

European Union

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

- EN 60601-1:2006/ AC:2010/ A1:2013

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

- EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
- CB Scheme IEC 60950-1:2005 (2nd Edition) + Am1:2009 + Am2:2013

Emissions: Directives (93/42/EEC) and (2014/53/EU)

- IEC/EN 60601-1-2: 2014
- EN 55032: 2012, Class B
- EN 61000-3-2: 2014
- EN 61000-3-3: 2013

Immunity: Directives (93/42/EEC) and (2014/53/EU)

- IEC/EN 60601-1-2: 2014
- EN 55024: 2010
- IEC/EN 610000-4-2: 2008
- IEC/EN 61000-4-3: 2006 + A1: 2008 + A2: 2010
- IEC/EN 61000-4-4: 2012
- IEC/EN 61000-4-5: 2005
- IEC/EN 61000-4-6: 2013
- IEC/EN 61000-4-8: 2009, 2010
- IEC/EN 61000-4-11: 2004
- ETSI EN 301 489-17 V3.1.1 (2016-11)
- ETSI EN 301 489-1 V2.1.1 (2016-11)

Other Countries

- **Australia**
  - CISPR 11: 2009, Class B Emissions
  - CISPR 32: 2015, Class B Emissions
- **Japan**
  - VCCI 32: 2016, Class B Emissions

Wi-Fi Transmitter IDs for the Internal Wireless Module

- **USA FCC ID:** R68PW2050
- **Canada IC ID:** 3867A-PW2050

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

Signature: Dale R. Miller Date: 8-17-18

Name: Daryl R. Miller Title: VP of Engineering

Figure B-3 EU Declaration of Conformity

LANTRONIX

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

EU DECLARATION OF CONFORMITY

This declaration of conformity is issued under the sole responsibility of the manufacturer.

Object of the declaration			
Product Information	Product Name: SGX 5150		
	Model	SW Version (Radio FW)	HW Version
	SGX 5150	6.37.42.9	A11 (or later)

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

- References to the relevant harmonised standards used or references to the technical specifications in relation to which conformity is declared

Radio Equipment Directive 2014/53/EU
EN 300 328 V2.1.1
EN 301 489-1 V2.1.1
EN 301 489-17 V3.1.1
EN 301 893-1 V2.1.1
EN 62311:2008
EN 60950-1:2006 + A1:2010 +A12:2011 +A2:2013

The notified body, TUV SUD BABT, performed a conformity assessment of the technical construction file and issued certificate _BABT-RED000452 i02.01__.

Signature: Daryl R. Miller **Date:** 8-29-17

Name: Daryl R. Miller

Title: VP of Engineering, Lantronix, Inc.

Table B-1 EU Declaration of Conformity

cs Česky [Czech]	Lantronix tímto prohlašuje, že tento SGX 5150 IoT device gateway je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice RED 2014/53/EU.
da Dansk [Danish]	Undertegnede Lantronix erklærer herved, at følgende udstyr SGX 5150 IoT device gateway overholder de væsentlige krav og øvrige relevante krav i direktiv RED 2014/53/EU.
de Deutsch [German]	Hiermit erklärt Lantronix, dass sich das Gerät SGX 5150 IoT device gateway in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie RED 2014/53/EU.
et Eesti [Estonian]	Käesolevaga kinnitab Lantronix seadme SGX 5150 IoT device gateway vastavust direktiivi RED 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, Lantronix, declares that this SGX 5150 IoT device gateway is in compliance with the essential requirements and other relevant provisions of Directive RED 2014/53/EU.
es Español [Spanish]	Por medio de la presente Lantronix declara que el SGX 5150 IoT device gateway cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva RED 2014/53/EU.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Lantronix ΔΗΛΩΝΕΙ ΟΤΙ SGX 5150 IoT device gateway ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ RED 2014/53/EU.
fr Français [French]	Par la présente Lantronix déclare que l'appareil SGX 5150 IoT device gateway est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive RED 2014/53/EU.
it Italiano [Italian]	Con la presente Lantronix dichiara che questo SGX 5150 IoT device gateway è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva RED 2014/53/EU.
Latviski [Latvian]	Ar šo Lantronix deklarē, ka SGX 5150 IoT device gateway atbilst Direktīvas RED 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo Lantronix deklaruoja, kad šis SGX 5150 IoT device gateway atitinka esminius reikalavimus ir kitas RED 2014/53/EU Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart Lantronix dat het toestel SGX 5150 IoT device gateway in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn RED 2014/53/EU.
mt Malti [Maltese]	Hawnhekk, Lantronix, jiddikjara li dan SGX 5150 IoT device gateway jikkonforma malħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva RED 2014/53/EU.
hu Magyar [Hungarian]	Alulírott, Lantronix nyilatkozom, hogy a SGX 5150 IoT device gateway megfelel a vonatkozó alapvetõ követelményeknek és az RED 2014/53/EU irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym Lantronix oświadcza, że SGX 5150 IoT device gateway jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy RED 2014/53/EU.
pt Português [Portuguese]	Lantronix declara que este SGX 5150 IoT device gateway está conforme com os requisitos essenciais e outras disposições da Directiva RED 2014/53/EU.
sl Slovensko [Slovenian]	Lantronix izjavlja, da je ta SGX 5150 IoT device gateway v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive RED 2014/53/EU.
Slovensky [Slovak]	Lantronix týmto vyhlasuje, že SGX 5150 IoT device gateway spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice RED 2014/53/EU.

fi Suomi [Finnish]	Lantronix vakuuttaa täten että SGX 5150 IoT device gateway tyyppinen laite on direktiivin RED 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar Lantronix att denna SGX 5150 IoT device gateway står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv RED 2014/53/EU.

Table B-1 Country Transmitter IDs

Country	Specification
USA FCC ID	R68PW2050
Canada IC ID	3867A-PW2050
Japan ID	201-152843
China SRRC	CMITT ID: 2016AP9148

Table B-2 SGX 5150 Module RF Output Power

Characteristics		Type	Criteria	Unit
RF Average Output Power, 802.11b (2.412 to 2.472 Ghz)	1 Mbps	16	± 2	dBm
	11 Mbps	16	± 2	dBm
RF Average Output Power, 802.11g (2.412 to 2.472 Ghz)	6 Mbps	14	± 2	dBm
	54 Mbps	14	± 2	dBm
RF Average Output Power, 802.11n (2.412 to 2.472 Ghz)	MCS0	13	± 2	dBm
	MCS7	13	± 2	dBm
RF Average Output Power, 802.11a (5.18 to 5.825 Ghz)	6 Mbps	14	± 2	dBm
	54 Mbps	14	± 2	dBm
RF Average Output Power, 802.11n (5.18 to 5.825 Ghz)	MCS0	13	± 2	dBm
	MCS7	13	± 2	dBm
RF Average Output Power, 802.11ac (5.18 to 5.825 Ghz)	MCS8	13	± 2	dBm
	MCS9	11	± 2	dBm
RF output power max, Bluetooth, basic rate (2.402-2.480Ghz)		9.7		dBm
RF output power max, Bluetooth, LE (2.402-2.480Ghz)		9.2		dBm

Manufacturer's Contact:

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

SGX 5150 Regulatory Domains

Table B-3 20 MHz Channels

	Frequency	Channel	USA/Canada (U/US parts)	European Union E/ES parts)	Japan (J/JS parts)
2.4 GHz Band	2412	**1**	Yes	Yes	Yes
	2417	**2**	Yes	Yes	Yes
	2422	**3**	Yes	Yes	Yes
	2427	**4**	Yes	Yes	Yes
	2432	**5**	Yes	Yes	Yes
	2437	**6**	Yes	Yes	Yes
	2442	**7**	Yes	Yes	Yes
	2447	**8**	Yes	Yes	Yes
	2452	**9**	Yes	Yes	Yes
	2457	**10**	Yes	Yes	Yes
	2462	**11**	Yes	Yes	Yes
	2467	**12**	-	Yes	Yes
	2472	**13**	-	Yes	Yes
	2484	**14**	-	-	Yes
5 GHz Band	5180	**36**	Yes	Yes	Yes
	5200	**40**	Yes	Yes	Yes
	5220	**44**	Yes	Yes	Yes
	5240	**48**	Yes	Yes	Yes
	5260	**52**	Yes	Yes	Yes
	5280	**56**	Yes	Yes	Yes
	5300	**60**	Yes	Yes	Yes
	5320	**64**	Yes	Yes	Yes
	5500	**100**	Yes	Yes	-
	5520	**104**	Yes	Yes	-
	5540	**108**	Yes	Yes	-
	5560	**112**	Yes	Yes	-
	5580	**116**	Yes	Yes	-
	5600	**120**	-	Yes	-
	5620	**124**	-	Yes	-
	5640	**128**	-	Yes	-
	5660	**132**	Yes	Yes	-
	5680	**136**	Yes	Yes	-
	5700	**140**	Yes	Yes	-
	5720	**144**	Yes	-	-
	5745	**149**	Yes	-	-
	5765	**153**	Yes	-	-
	5785	**157**	Yes	-	-
	5805	**161**	Yes	-	-
	5825	**165**	Yes	-	-

Table B-4 40 MHz Channels

	Frequency	Channel	USA/Canada (U/US part #)	European Union E/ES part #)	Japan (J/JS parts)
5 GHz Band	5190	**38**	Yes	Yes	Yes
	5230	**46**	Yes	Yes	Yes
	5270	**54**	Yes	Yes	Yes
	5310	**62**	Yes	Yes	Yes
	5510	**102**	Yes	Yes	-
	5550	**110**	Yes	Yes	-
	5590	**118**	N/A	Yes	-
	5630	**126**	N/A	Yes	-
	5670	**134**	Yes	Yes	-
	5755	**151**	Yes	-	-
	5795	**159**	Yes	-	-

Table B-5 80 MHz Channels

	Frequency	Channel	USA/Canada (U/US parts)	European Union E/ES parts)	Japan (J/JS parts)
5 GHz Band	5210	**42**	Yes	Yes	Yes
	5290	**58**	Yes	Yes	Yes
	5530	**106**	Yes	Yes	-
	5610	**122**	-	Yes	-
	5690	**138**	Yes	Yes	-
	5775	**155**	Yes	-	-

Notes:

1. *Models are only for use in their respective regions. Part numbers ending in U/US for US/ Canada, E/ES for European Union, J/JS for Japan. For other countries, user should confirm channel compatibility. SGX 5150 has not been certified in all countries.*
2. *Frequencies from 5150 MHz to 5250 MHz for indoor use only.*
3. *The unit supports 20 MHz bandwidth channels for 2.4 GHz channels.*
4. *The unit supports 20, 40, 80 MHz bandwidth channels for 5 GHz channels where appropriate.*
5. *Region code modifications are not available to the end user.*
6. *SoftAP mode defaults to channel 1. If the unit is connected as a client to an external AP the SoftAP channel follows the external AP. The SoftAP channel is not user configurable.*
7. *In SoftAP mode, the product will not initiate any connection or active scan in 5GHz DFS bands and will only follow external AP or master device to use a channel.*

RoHS, REACH and WEEE Compliance Statement

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