GridTime™ 3000 Installation Manual

Overview

The GridTime™ 3000 is a rack-mountable precision time server for digital substation applications. Its timing protocols and ports are enabled through license bundles (For a full list of all license bundles, see Licenses), allowing for different functionality to be enabled as requirements change.

The GridTime 3000 has an extensive collection of different ports, including:

- Ten Ethernet ports (two RJ-45, eight SFP) on its front panel for Network Time Protocol (NTP) and Precision Time Protocol (PTP) time synchronization
- Fifteen ports on its back panel for input of IRIG-B, and output of a range of legacy time and frequency signals
- An antenna connector on its back panel to utilize a GNSS reference

The GridTime 3000 is designed for use in synchronizing industrial control and Supervisory Control and Data Acquisition (SCADA) equipments. It can provide time synchronization to many different devices simultaneously, such as Phasor Measurement Units (PMUs), Protection Relays, Remote Telemetry Units (RTUs), and other Intelligent Electronic Devices (IEDs) used in electrical substations and industrial control installations.

The GridTime 3000 is designed for harsh electromagnetic environments as all its ports are electrically isolated. This allows output wiring to feed out to operating areas in different earth potential zones without compromising the site earthing security. The isolation also protects the device from high-voltage spikes...

Table of Contents

1. How to Use this Manual

This chapter describes the format, layout, and purpose of this manual.

1.1 Purpose of this Manual

Welcome to the GridTime 3000 GNSS Time Server.

This document helps you use the GridTime 3000 to reliably deliver high-accuracy time to your end devices.

The GridTime 3000 Installation Manual contains everything you need to know for unpacking, installing, using, maintaining, and troubleshooting the Microchip GridTime 3000 GNSS Time Server.

1.2 Who Should Read This Manual

This section describes who should read this manual and what chapters they should read.

Overview is written for general readers who want information about the product. Subsequent sections contain technical information about the product and also describe the installation, maintenance, and configuration instructions or details primarily intended for qualified maintenance personnel. This manual is designed for the following categories of users:

- Systems Engineers – Overview provides an introduction to the GridTime 3000 GNSS Time Server. Cross-references in this chapter direct you to detailed system information in other chapters as appropriate.
- Installation Engineers – Chapters Installation through Operating provide detailed information and procedures to ensure proper installation, operation, configuration, and testing of the GridTime 3000.
- Maintenance Engineers –Maintenance and Troubleshooting chapters and the appendices provide preventive and corrective maintenance guidelines, as well as procedures for diagnosing and troubleshooting fault indications and alarms.

1.3 Conventions Used in This Manual

This section describes the conventions used in the GridTime 3000 Installation Manual.

This manual uses the following conventions:

- Acronyms and Abbreviations- Terms are spelled out the first time they appear in text. Thereafter, only the acronym or abbreviation is used.
- Revision Control- The title page lists the printing date and versions of the product this manual describes.
- Wording Conventions- This manual uses the typographical conventions described in the table below.

Table 1-1. Examples of Wording Conventions

Appearance of text	Example	Meaning
First letter initialized	GridTime 3000 Installation Manual	The title of a document or section.
All capital letters	ADMIN	An operating mode, alarm state, status, or chassis label.
Bold and italicized.	Microchip ***does not*** recommend...	A word or term given special emphasis.

1.4 Warnings, Cautions, Tips, and Notes

This section describes how warnings, cautions, tips and notes are used in the GridTime 3000 Installation Manual.

Warnings, Cautions, Tips, and Notes attract attention to essential or critical information in this guide. The types of information used in this guide are as follows:

Important: All important information use this symbol. The information icon contain installation, operation, or maintenance procedures, practices, conditions, or statements, that provide important information for successful operation of the device.

DANGER To avoid serious personal injury or death, *do not* disregard warnings. All warnings use this symbol. Warnings are installation, operation, or maintenance procedures, practices, or statements, that if not strictly observed, may result in serious personal injury or even death.

CAUTION To avoid personal injury, *do not* disregard cautions. All cautions use this symbol. Cautions are installation, operation, or maintenance procedures, practices, conditions, or statements, that if not strictly observed, may result in damage to, or destruction of, the equipment. Cautions are also used to indicate a long-term health hazard.

Tip: All tips use this symbol. Tips indicate manufacturer-tested methods or known functionality. Tips contain installation, operation, or maintenance procedures, practices, conditions, or statements, that provide important information for optimum performance results.

Note: All notes appear like this. Notes contain installation, operation, or maintenance procedures, practices, conditions, or statements, that alert you to important information, which may make your task easier or increase your understanding.

1.5 Related Documents and Information

See your Microchip representative or sales office (nzp-allsales@microchip.com) for a complete list of available documentation.

1.6 Where to Find Answers to Product and Document Questions

For additional information about the products described in this guide, contact your regional sales representative or nzp-allsales@microchip.com.

For assistance with a GridTime 3000 installation issue or to arrange a return, contact nzp-support@microchip.com.

For more information, see www.microchip.com/support.

2. Key Benefits

This section provides an overview of the key features of GridTime 3000 GNSS Time Server.

2.1 Flexibility

With much of the power industry undergoing a digital migration, many utilities are transitioning from legacy time code distribution to Ethernet-based time distribution. Consequently, time distribution requirements are evolving.

This is why the GridTime 3000 is designed with a licensable hardware model, where licenses are loaded onto the device to enable specific ports and functionality.

This way, if the time distribution needs change and a legacy timing bus system is replaced with an Ethernet time distribution system or a hybrid system, licenses can be purchased to enable the Ethernet timing functionality on the GridTime 3000, instead of purchasing an entirely new time server.

2.2 Redundancy

As the power industry involves mission-critical applications, it is essential to ensure that the equipment remains operational in the event of a system failure. This is why having redundant backup systems in place is crucial for bolstering resiliency against failures.

For this reason, the GridTime 3000 includes multiple features, and expansion options for adding additional redundancy. These include:

- Parallel Redundancy Protocol (PRP) support on all Ethernet ports
- Dual firmware images - the device stores a primary firmware image and a backup image. If the primary image cannot be booted, the backup image is booted instead, which becomes the new primary image
- A dual oscillator expansion option. This offers resiliency in the event of an oscillator failure. See Hardware Options.
- A dual band GNSS receiver. This provides resilience towards GNSS disruptions.

2.3 Reliability

To meet the needs of the power industry, the GridTime 3000 is equipped with features for ensuring robust and reliable operation in the field.

These include:

- Isolated electrical inputs and outputs. This offers protection in the event of surges or large voltage transients.
- Field-replaceable power supplies and power supply fuses. See Power Supply Replacement and Power Supply Fuse Replacement.
- High temperature range tolerance on internal components: -10 ℃ ambient to ≥ +55 ℃ (14 °F to 149 °F).
- Alarms (Alarms) and detailed internal logging systems that allow users to easily self diagnose and remedy issues that appear in the field.

2.4 Time and Frequency Signals

This section describes the timing and frequency signals the GridTime 3000 GNSS Time Server can output, or use as a time source for synchronization.

The GridTime 3000 sends and receives a variety of modern and legacy time signals for time and frequency synchronization and syntonization.

The GridTime 3000 can output the following time and frequency signals:

- Unmodulated IRIG-B signals:
  - IRIG-B004 with AFNOR or C37.118.1 extensions
  - IRIG-B005 with AFNOR or C37.118.1 extensions
  - IRIG-B006
  - IRIG-B007
- Amplitude modulated IRIG-B (AM IRIG-B) signals:
  - IRIG-B124 with AFNOR or C37.118.1 extensions
  - IRIG-B125 with AFNOR or C37.118.1 extensions
  - IRIG-B126
  - IRIG-B127
- Modified Manchester modulated IRIG-B signals:
  - IRIG-B224 with AFNOR or C37.118.1 extensions
  - IRIG-B225 with AFNOR or C37.118.1 extensions
  - IRIG-B226
  - IRIG-B227
- Simulated DCF77 receiver output signal
- Custom pulse train signal (Programmable Pulse):
  - Custom frequency — 1 pulse per day to 250 pulses per second
  - Custom phase offset — none through to 1 pulse period (second, minute, hour and so on), configurable to the millisecond
  - Custom Duration — none through to 1 pulse period (second, minute, hour and so on), configurable to the millisecond
- Output of ITU-T G.703 signals:
  - T1/J1 interface at 1.544 kbits/s - G.703 section 7
  - E1 interface at 2.048 kbits/s - G.703 section 11
  - 2.048 MHz fixed frequency sine and square wave - G.703 section 15
  - 1.544 MHz fixed frequency sine and square wave - Also follows G.703 section 15
  - 10 MHz fixed frequency sine and square wave - G.703 section 20
- Output of time strings over a serial RS422 or RS232 connection (See Time String Specifications for string content definitions):
  - NGTS string
  - IRIG J-1x string
  - String A-String H serial strings
  - NMEA ZDA string
  - NMEA RMC string
- PTP timeTransmitter mode support:
  - IEEE® 1588-2008 E2E Default Profile timeTransmitter
  - IEEE 1588-2008 P2P Default Profile timeTransmitter
  - IEEE C37.238-2011 Power Profile timeTransmitter
  - IEEE C37.238-2017 Power Profile timeTransmitter
  - IEC/IEEE 61850-9-3 Power Utility Profile timeTransmitter
  - ITU-T G.8275.1 Telecom Profile

   – ITU-T G.8265.1 Telecom Profile
- NTP server support:
   – NTP v1, v2, v3, and v4 server support

The GridTime 3000 can receive multiple time signals at once, but will only synchronize to one signal at a time. The device follows its configured time source hierarchy when deciding which source to use for synchronization.

- **GNSS**

  GNSS time synchronization is supported and is recommended for use as the primary reference source for the device. Any of the following GNSS can be used simultaneously:
   – GPS and QZSS
   – GLONASS
   – Galileo
   – BeiDou
- **IRIG-B**

  IRIG-B synchronization is supported through either of the IRIG In ports. The following signal formats can be used:
   – 0-5V TTL DCLS IRIG-B004 signals with C37.118.1 extensions
   – 0-5V TTL DCLS IRIG-B005 signals with C37.118.1 extensions
- **PTP**

  Depending on configuration, PTP ports could be either; forced PTP timeReceiver or can automatically enter timeReceiver mode after synchronization loss. The following PTP profiles can be used:
   – IEEE 1588-2008 E2E Default Profile timeReceiver
   – IEEE 1588-2008 P2P Default Profile timeReceiver
   – IEEE C37.238-2011 Power Profile timeReceiver
   – IEEE C37.238-2017 Power Profile timeReceiver
   – IEC/IEEE 61850-9-3 Power Utility Profile timeReceiver
   – ITU-T G.8275.1 Telecom Profile
   – ITU-T G.8265.1 Telecom Profile
- **Simple Network Time Protocol (SNTP) client support**
   – SNTP v1, v2, v3, and v4 client support

2.5 IEC 62439-3:2016 Parallel Redundancy Protocol (PRP)

This section describes the functionality of PRP on the GridTime 3000 GNSS Time Server.

The GridTime 3000 supports PTP over Parallel Redundancy Protocol (PRP) on all of its Ethernet timing ports. This allows a PTP timeReceiver or timeTransmitter to be identically duplicated across two Ethernet ports on the device as a single redundant interface. The GridTime 3000 can be configured to operate PRP over Ethernet timing ports 1 and 2, Ethernet timing ports 3 and 4, Ethernet timing ports 5 and 6, Ethernet timing ports 7 and 8, and Ethernet timing ports 9 and 10.

Note: This feature requires a PRP license to activate, and the Ethernet timing ports used must also be activated through licenses.

Note: At no time does the GridTime 3000 operates as an Ethernet router, switch, or hub.

2.6 Event Monitoring

This section describes the supported methods for monitoring the GridTime 3000 GNSS Time Server's operational events.

2.6.1 Notifications

The GridTime 3000 generates a notification when a state change occurs, such as 'out of sync' to 'in sync', or a system variable crosses a threshold. This could include the satellite count dropping below the minimum allowable satellites threshold.

Syslog notifications, SNMP notifications, or both can be configured to be sent from the admin Ethernet port to a list of user-defined IP addresses.

2.6.2 Internal Logging

The GridTime 3000 internally logs key operational events as they occur. The logs can be extracted using the CMT. For more information, see the Provisioning Logs section.

2.6.3 Alarms

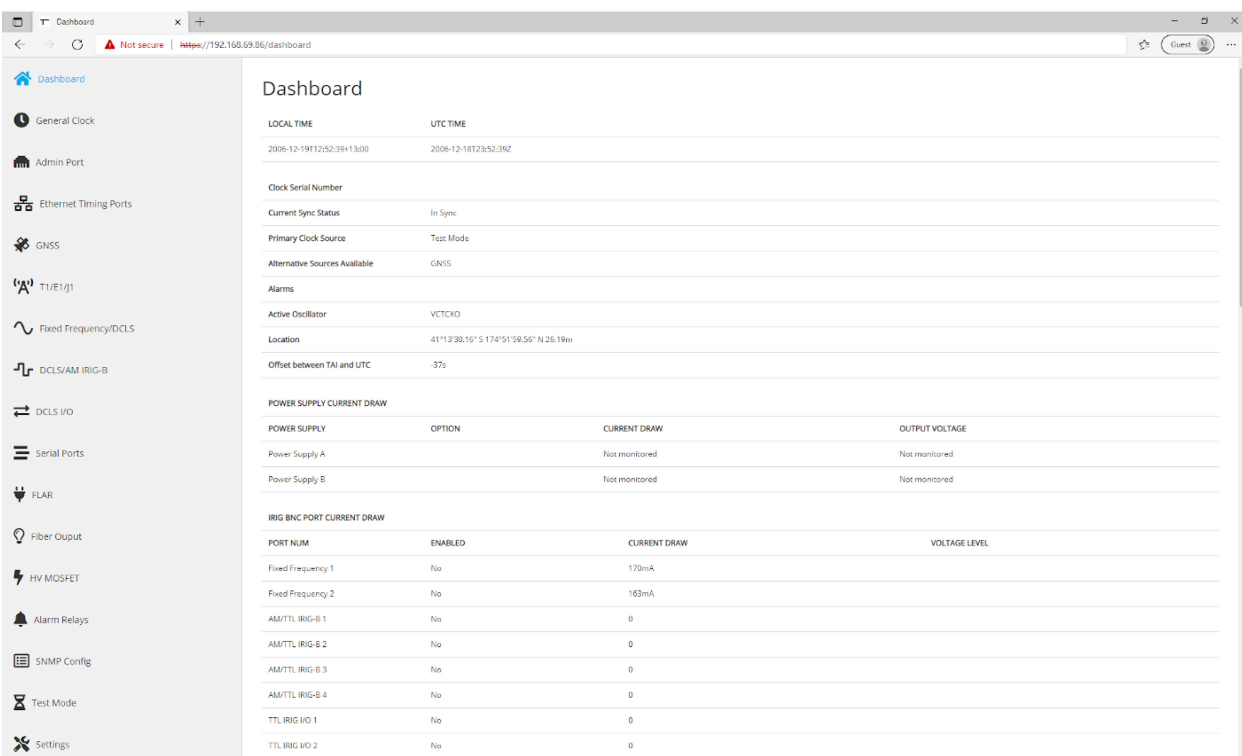
When an event that risks the operation of the device occurs, an alarm and notification is generated. The methods for monitoring alarms, and guidance on clearing alarms as they occur are described in Alarms.

2.7 Device Management

This section describes the device management features the GridTime™ 3000 GNSS Time Server supports.

For device configuration and system monitoring, the GridTime 3000 hosts its own web browser accessible configuration tool called the Clock Management Tool (CMT).

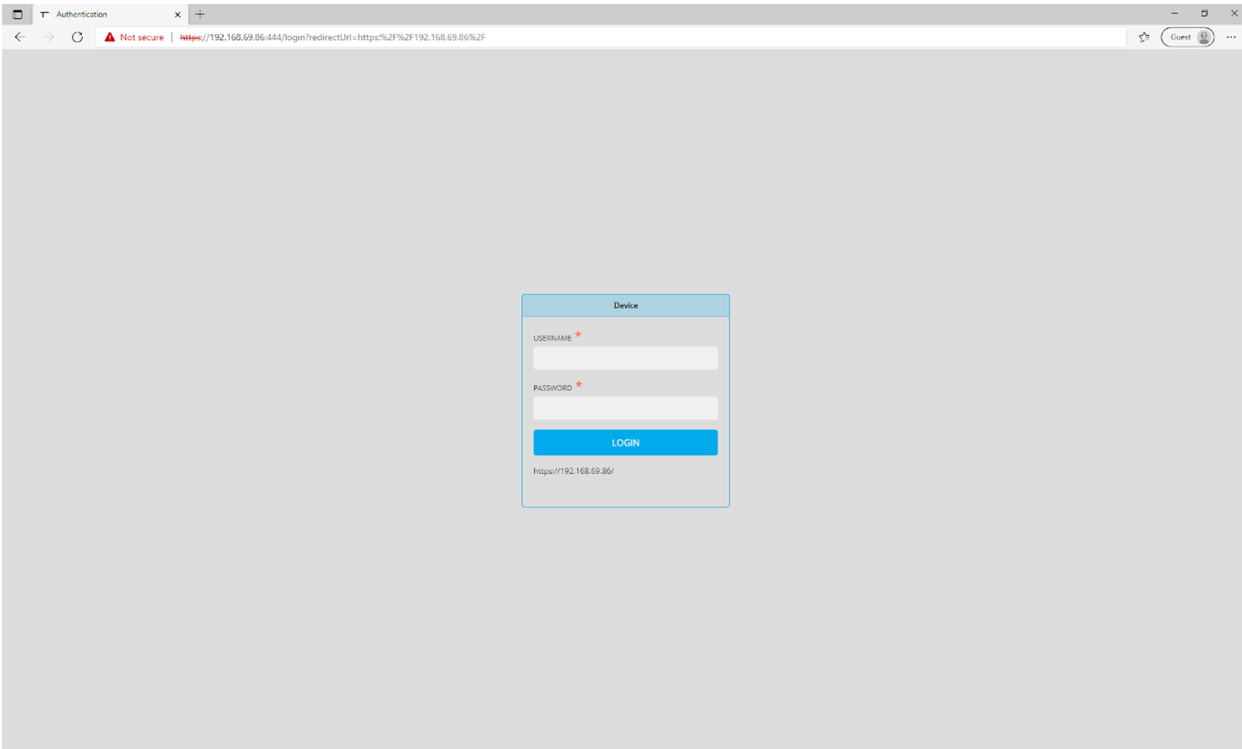
Figure 2-1. CMT Dashboard



The CMT can be accessed by establishing a connection to the device's administrator (admin) USB-C® port or its administrator (admin) Ethernet port. This process is described in Establishing a Connection to the GridTime 3000. Once a connection has been established, an admin port IP address can be typed into a web browser on your PC, and the login screen for the CMT will appear.

The active IP addresses of both admin ports are displayed on the device's LCD.

Figure 2-2. CMT Login Screen



2.8 Security

This section describes the key security features of GridTime 3000.

The GridTime 3000's Clock Management Tool (CMT) is password protected, and supports multiple user logins with administrator controlled levels of access.

It also has additional security built into the upgrade procedure with RSA signatures and RSA/AES encryption and hardware-based assurance and validation modules. These features help in preventing the upload of malicious or corrupted firmware images.

The GridTime 3000 also supports Industry standard RSA based security on its Clock Management Tool (CMT), AES/SHA on Simple Network Management Protocol (SNMPv3), as well as MD5 hashed Network Time Protocol (NTP).

2.8.1 User Security Model

This section describes the User Security Model (USM) used by the GridTime 3000.

The GridTime 3000 features a USM that is split into users and roles. A user is an individual login and represents one person, a role is a group in which a user may be placed in. Each role has it's own set of admin-configured permissions and dictates what configuration settings each user can read or write to.

With the GridTime 3000 USM, each role may have multiple users assigned to it.

Note: Both Clock Management Tool (CMT) and SNMPv3 users can be assigned to a role and will have the permission set of that role enforced.

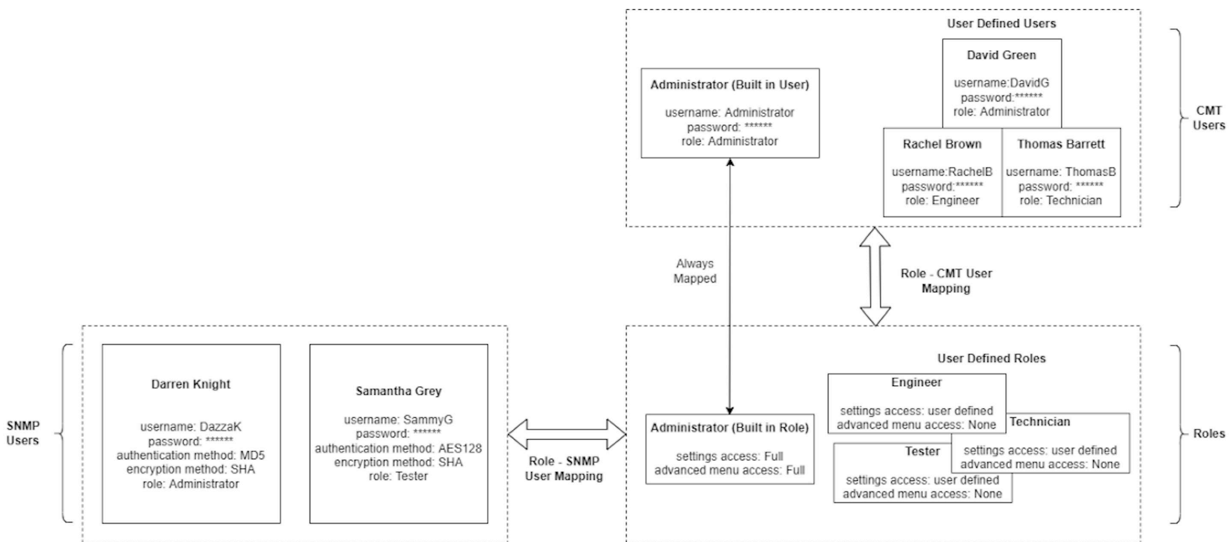
There is always an administrator role defined, this role allows full read and write access to all settings and access to all CMT menus. The administrator role permissions cannot be viewed or edited. Additional roles with variable permission sets can be generated by the administrator user. Only the administrator role allows access to the advanced CMT menus, and the CMT authorization module where CMT user login settings are modified.

In addition to the administrator role, there is always an administrator user defined in the CMT, which is always mapped to the administrator role. Additional CMT users can be generated in the CMT authorization module by the administrator role. See Provisioning Users - Local Users

SNMP users have to be defined by the CMT user, and in addition to basic login details (username + password), the authentication and encryption method has to be defined. SNMP users are used by the SNMPv3 USM.

The following diagram shows a representation of the GridTime 3000 USM.

Figure 2-3. Example: GridTime 3000 USM



3. Physical Overview

This section gives a physical overview of the GridTime 3000 GNSS Time Server. This includes an overview of key device features including:

- Timing ports
- Device management ports
- Alarm and Sync LEDs
- Liquid Crystal Display (LCD)
- Power ports
- Case

The device has a 19-inch rack mount case and features ten 1 Gbps capable Ethernet ports on its front panel, with an array of legacy timing and frequency ports on its back panel.

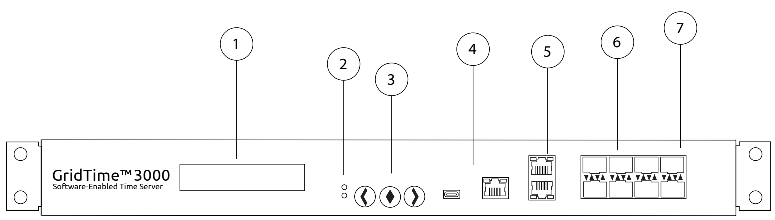
3.1 Front Panel

This section describes the functionality on the GridTime 3000 GNSS Time Server's front panel.

The GridTime 3000 front panel features the following:

- LCD
- Alarm and Sync LEDs
- LCD navigation buttons
- USB-C® Admin and RJ-45 Admin ports
- Ethernet ports

Figure 3-1. GridTime 3000 Front Panel Features



1. LCD
2. Alarm and Sync LEDs
3. LCD Navigation Buttons
4. USB-C Admin and RJ45 Admin Ports
5. Ethernet Ports 1-2: RJ45 Ports (x2)
6. Ethernet Ports 3-8: SFP Ports (x6)
7. Ethernet Ports 9-10: SFP+ Ports (x2)

The following table provides a description of each of the features.

Table 3-1. Front Panel Feature Description

Feature Number	Feature	Description
1	LCD	• Shows the device's current time and other system observables • Information such as active alarms, synchronization state, firmware version, and the current UTC offset are displayed • Information is organized by type on different LCD tabs, which are accessed with the front panel buttons. The contents of each tab is described in LCD Tabs.
2.1	Alarm LED	• Flashes red when one or more alarms are active • Off if no alarms are active • Active alarms are listed on the LCD Alarm Status tab
2.2	Sync LED	• Solid green when device is synchronized to a time source - 'in sync' state • Flashes green when in 'holdover' state, or 'out of sync' state
3	LCD Navigation Buttons	• The left and right buttons are used to scroll through the LCD tabs. • If the center button is pressed, the LCD will display its main tab. If held, it will load the clock power screen, where the device can be safely shutdown or rebooted.
4.1	USB-C Admin Port	• Can be connected to the following with a USB cable to perform device management: – A PC's USB host port – A tablet's USB host port • Supports USB 2.0 • Cannot be used to charge a device • Cannot be connected to a USB to Ethernet network adapter
4.2	RJ-45 Admin Port	• Can be connected to the following over an Ethernet network to perform device management: – PC Ethernet port • SNMP and Syslog notifications can be configured to be sent from the port to a list of user-defined IP addresses • Left LED (ACT LED) flashes green as traffic passes through • Right LED (LNK LED) shows link speed: – Green if 1 Gbps – Orange if 100 Mbps – Off if 10 Mbps • Cannot be used for timing

...........continued

Feature Number	Feature	Description
5	RJ-45 Ports	• Can be used with an SFP for NTP and PTP synchronization at speeds of up to 1 Gbps • Left LED (enabled LED) illuminates if the port has been enabled • Right LED (ACT LED): – Illuminates orange when an active link is established with the port – Blinks as traffic passes through the port • Cannot be used for configuration
6	SFP Ports	• Can be used with an SFP for NTP and PTP synchronization at speeds of up to 1 Gbps • Left LED that points at the port (enabled LED) illuminates if the port has been enabled • Right LED that points at the port (ACT LED): – Illuminates orange when an active link is established with the port – Blinks as traffic passes through the port • Cannot be used for configuration
7	SFP+ Ports	• Can be used with an SFP for NTP and PTP synchronization at speeds of up to 10 Gbps • Left LED that points at the port (enabled LED) illuminates if the port has been enabled • Right LED that points at the port (ACT LED): – Illuminates orange when an active link is established with the port – Blinks as traffic passes through the port

3.1.1 LCD Tabs

This section summarizes the information on each of the GridTime 3000 GNSS Time Server's LCD tabs.

Table 3-2. LCD Tab Information

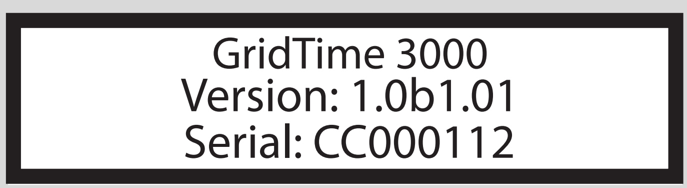
<table>
<tr><th>Name</th><th>Display</th></tr>
<tr><td>Startup display sequence</td><td>
Figure 3-2. Startup Screen 1-GT3K Logo Text

Figure 3-3. Startup Screen 2-GT3K Logo Text and Startup Counter

Each number maps to a specific boot stage in the firmware. Inform Microchip Support if the startup freezes on a particular number.

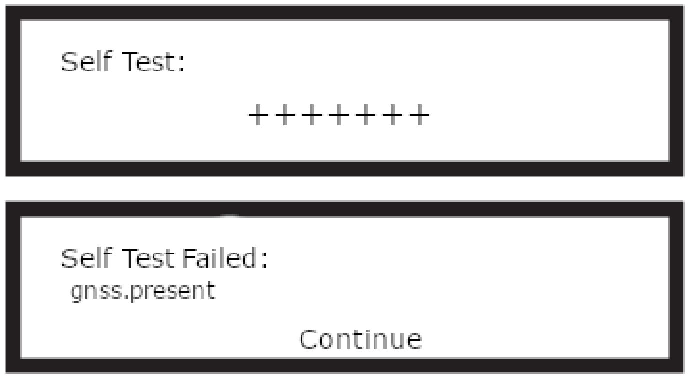
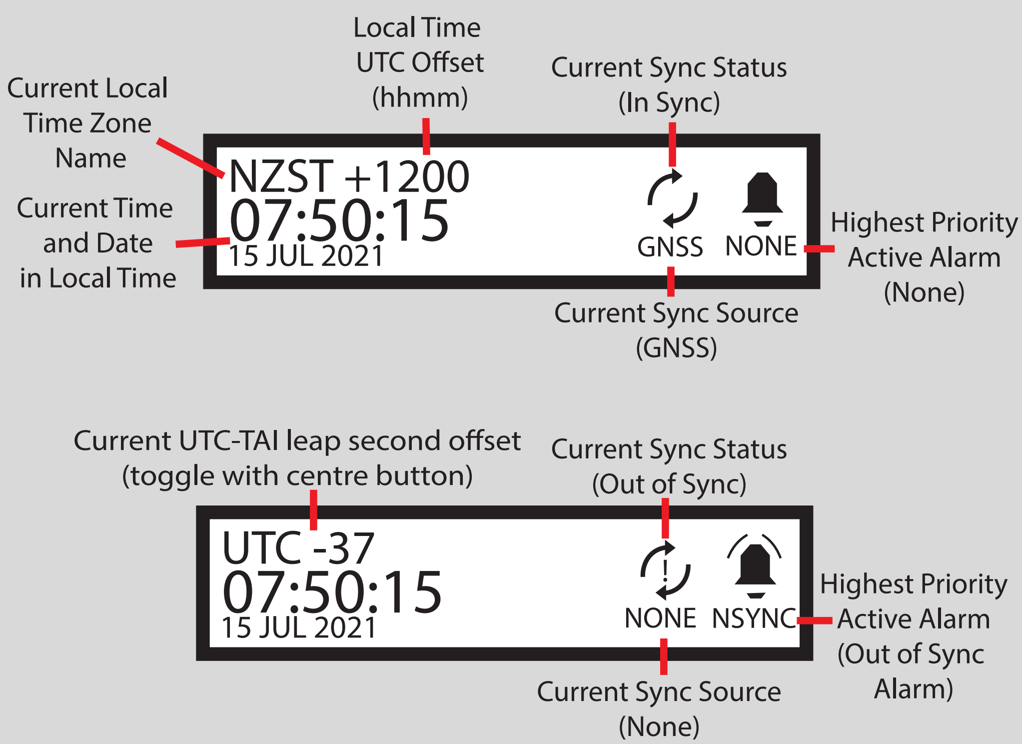
Figure 3-4. Startup Screen 3-GridTime 3000 Logo Text

Figure 3-5. Startup Screen 4-Device Information

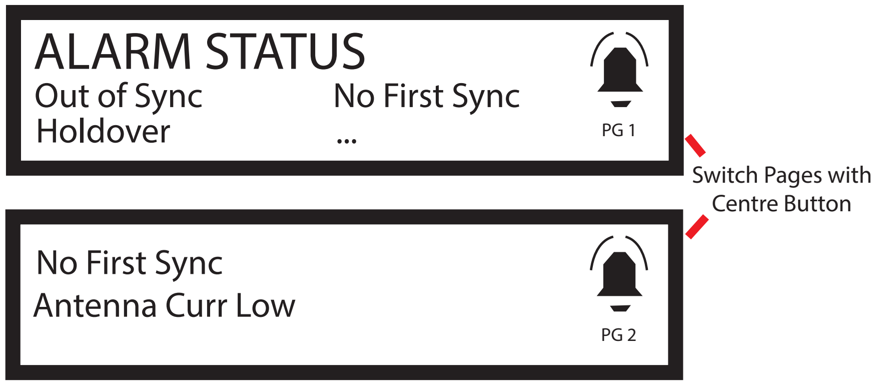
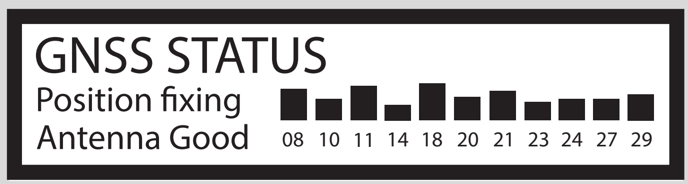


</td></tr>
</table>

...........continued

Name	Display
	Figure 3-6. Startup Screen 5-Self Test  On startup, the GridTime 3000 performs a self test to ensure all subsystems are detected. Each passing test is indicated with a "+" . If one of the tests fail, the cause of the failure is shown on the LCD. If this occurs, attempt to power cycle the device. If the test failure persists, contact technical support (Contacting Technical Support) with the listed cause of failure .
Main display tab	**Figure 3-7.** Main Display Screen  The main display shows the local time and date, the current sync status and sync source, and the alarm status.

...........continued

Name	Display
Alarm Status Tab	**Figure 3-8.** Alarm Status  Shows all currently active alarms.
GNSS Status Tab	**Figure 3-9.** GNSS Status  Shows the current GNSS status, the antenna state, and the first 10 satellites being used for time synchronization ordered by ID. A bar chart shows the signal strength of each satellite.
Clock Information Tab	**Figure 3-10.** Clock Information  Shows the serial number, the firmware version and the IP address of the administration port. **Note:** The front panel Clock Information page displays the IPv4 address of the first connected Management port with an assigned IPv4 address. The Admin port is prioritized, followed by the Timing ports.

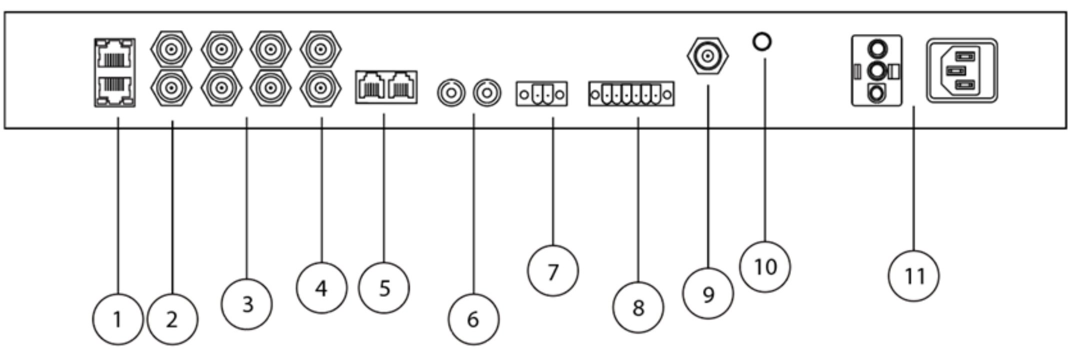
...........continued

Name	Display
Clock Power Tab	**Figure 3-11.** Clock Power  Accessed by holding the middle front panel button when on any other tab. Press the left button to restart the device, the right button to shut down, or the middle button to return to the main tab. **Note:** The shutdown is a software shutdown only, and will not switch off power to the device or its internal components.

3.2 Back Panel

This section describes the functionality on the GridTime 3000 GNSS Time Server's back panel.

Figure 3-12. GridTime 3000 Back Panel Features



1. RJ48C T1/E1/J1 ports (x2)
2. BNC Ports 1-2 -Fixed frequency/TTL ports (x2)
3. BNC ports 3-6 -AM IRIG/TTL ports (x4)
4. BNC ports 7-8 -IRIG in/TTL out ports (x2)
5. RJ12 RS232 and RS422 serial string output ports (x1 of each)
6. ST optical fiber output port (x2)
7. HV MOSFET port — (x1)
8. Form-C Alarm Relay Ports — (x2)
9. TNC GNSS antenna port (x1)
10. Earth Stud
11. Power supply port(s) (up to x2)

Table 3-3. Back Panel Feature Description

Feature Number	Feature	Description
1	T1/E1/J1 Ports	• RJ48C receptacle • Can be configured as a T1/J1 output interface at 1.544 kbits/s - ITU-T G.703 section 7 • Can be configured as an E1 output interface at 2.048 kbits/s - ITU-T G.703 section 11
2	Fixed frequency/TTL ports	• Female BNC Connector • Can output 2.048 MHz fixed frequency sine or square waves - ITU-T G.703 section 15 • Can output 1.544 MHz fixed frequency sine or square waves - follows ITU-T G.703 section 15 • Can output 10 MHz fixed frequency sine or square waves - ITU-T G.703 section 20 • Can output standard GridTime 3000 Pulse output signals[1] over copper
3	AM IRIG/TTL ports	• Female BNC Connector • Can output 1kHz amplitude modulated IRIG-B, with a 3:1 ratio. • Can output standard GridTime Pulse output signals[1] over copper
4	IRIG in/TTL out ports	• Female BNC Connector • Can receive a 0-5V TTL DCLS IRIG-B signal with C37.118-2011 extensions as a synchronization source • Can output standard GridTime Pulse output signals[1] over copper
5.1	RS232 Serial String port	• RJ12 receptacle • Can output serial time strings at RS232 levels
5.2	RS422 Serial String port	• RJ12 receptacle • Can output serial time strings at RS422 levels
6	ST optical fiber ports	• Female ST optical connector • Can transmit all standard GridTime pulse output signals[1] over fiber
7	HV MOSFET	• Two pin male phoenix connector • with an external voltage supply connected, can output all standard GridTime pulse signals[1] at that supply voltage

...........continued		
Feature Number	**Feature**	**Description**
8	Alarm relay ports	• 6 pin male phoenix connector (3 pins per port) • Form-C relay contacts. Each port has: – Normally Closed (NC) contact – Common (C) contact – Normally Open (NO) contact • Specific alarms can be mapped to each port in the CMT — see Alarms. Port enters alarm state if any mapped alarm activates.
9	GNSS antenna port	• Female TNC connector • Can be connected to a suitable GNSS antenna installation to provide a GNSS reference for the device. See Installing the GNSS Antenna. • Outputs 5V (80 mA max) to power a connected GNSS antenna
10	Earth stud	• Earthing point for device. • Connect to earth to provide a safe electrical discharge path. Ground Connections
11	Power supply port(s)	Device can be ordered with a single power supply, or two power supplies for redundancy. Two power supply options are available for selection: • Low voltage option: – Supports DC Only – Range: 24 Vdc-120 Vdc • High voltage option: – Supports AC or DC – AC Range: 100 Vac-240 Vac – DC Range: 120 Vdc-250 Vdc
1 - Standard GridTime 3000 pulse output signals include: • Unmodulated IRIG-B • Amplitude modulated IRIG-B • Modified Manchester modulated IRIG-B • Simulated DCF77 receiver output • Custom pulse signals		

3.3 Hardware Options

This section gives an overview of the GridTime™ 3000 GNSS Time Server's base hardware, and hardware expansion options.

3.3.1 Power Supply

This section describes the GridTime 3000's power supply options.

The GridTime 3000 can be ordered with a single power supply, or two power supplies for redundancy.

Two different power supply types can be ordered — low voltage or high voltage.

The voltage ranges for the two supplies are as shown in the following table.

Table 3-4. Voltage Ratings For Two Power Supplies

Power Supply	AC/DC Support	Ratings
Low voltage	DC support only	24 Vdc-120 Vdc 2.92 A-580 mA
High voltage	AC and DC support	**DC**: 120 Vdc-250 Vdc 590-280 mA **AC**: 100 Vac-240 Vac 700-292 mA 50-60 Hz Only

The voltage ranges are also marked on the product label on the chassis. Operating the device outside of these ratings may cause permanent hardware damage, Microchip assumes no liability for any damage resulting from operating the device outside its operational voltage ratings.

3.3.2 Oscillator

This section describes the GridTime 3000's oscillator options.

The GridTime 3000's base oscillator configuration includes a VCTCXO (Voltage Controlled, Temperature Compensated Crystal Oscillator) .

Additionally, the GridTime 3000 can be ordered with either a VCOCXO (Voltage Controlled, Oven Controlled Crystal Oscillator) or Rubidium oscillator as well. A dual oscillator configuration offers superior redundancy and holdover compared to the VCTCXO only. The expansion oscillators — Rubidium and VCOCXO, are high stability oscillators, and will revert to the VCTCXO oscillator in the event that something goes wrong.

3.4 Case Overview

This section gives an overview of the GridTime 3000's case.

The GridTime 3000 case has a 1U 1.75 inch (44.45 mm) height, a 19 inch (482 mm) width, and a length of 12.97 inch (329.4 mm).

The dimensions of the GridTime 3000 case are outlined in the following figures.

Figure 3-13. GridTime 3000 Case Dimensions - Front

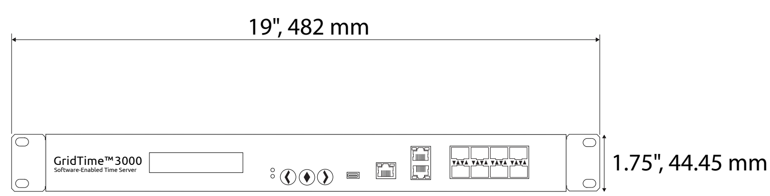
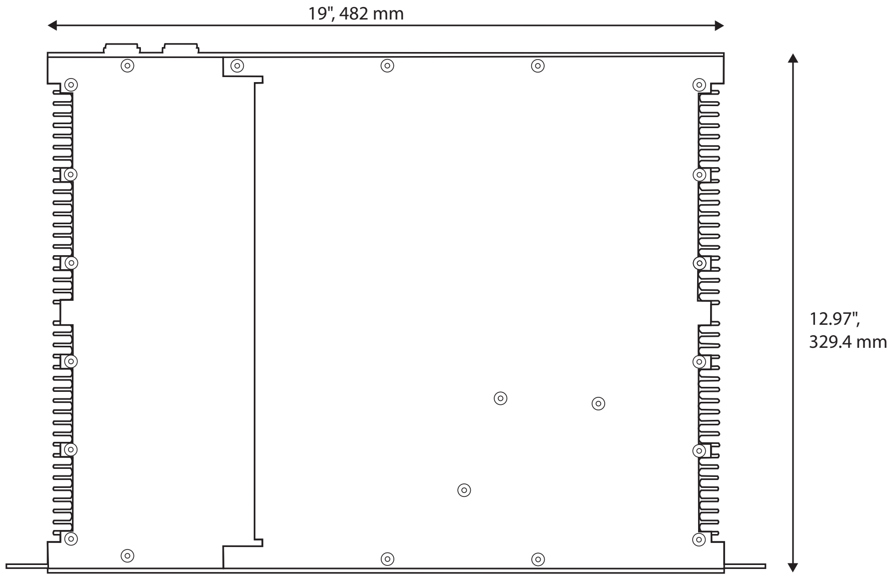


Figure 3-14. GridTime 3000 Case Dimensions - Top



The case lid is comprised of two segments — the main compartment, and the power supply bay.

- The main compartment must never be opened, or else it will induce a breach in warranty.
- Once all power supply(s) have been switched off, the power supply bay may be opened by a qualified user to replace a failed power supply in the device, or to replace a blown power supply fuse. Instructions on how to do both of these can be found in Power Supply Fuse Replacement and Power Supply Replacement.

The side of the GridTime 3000 case features fins for passive heat dissipation.

CAUTION Take care when handling the sides of the case, as the heat sink fins can be uncomfortable to hold.

4. Licenses

This section gives an overview of the licenses that can be purchased with the GridTime 3000 GNSS Time Server, and describes the features activated by each bundle.

The licenses that are purchasable with the GridTime 3000, as well as the features activated by each license, are described in the following table.

For licenses that enable all timing protocols on a group of ports, see Table 3-1 and Table 3-3 for a description of the protocols supported on each port.

Table 4-1. GridTime 3000 Licenses

License Name	Activated Features
Front Panel Features	
Ethernet Copper	Activates 1x RJ-45 Ethernet ports (up to x2 available). **Note:** An additional NTP or PTP license needs to be purchased to use NTP or PTP on ports.
Ethernet SFP (Copper or Fiber)	Activates 1x SFP or SFP+ Ethernet ports for use at 10/100/1000 Mbps communication speeds (up to 6x SFP and 2x SFP+ available). **Note:** An additional NTP or PTP license needs to be purchased to use NTP or PTP on ports.
10GB License	Activates 10 Gbps communication speed on Ethernet timing ports 9 and 10. **Note:** An additional NTP or PTP license needs to be purchased to use NTP or PTP on ports.
PTP	Enables PTP TimeReceiver and TimeTransmitter on all activated Ethernet ports. Enables all PTP profiles. For a list of all supported PTP profiles, see Time and Frequency Signals.
NTP/SNTP	Enables NTP broadcast, multicast, and unicast server mode on all activated Ethernet ports, as well as SNTP multicast, broadcast, and unicast client.
PRP	Enables PRP on all activated Ethernet ports. See IEC 62439-3:2016 Parallel Redundancy Protocol (PRP)
Security	Enables the use of external RADIUS and LDAP authentication servers to authenticate users attempting to gain access to the Clock Management Tool through the Administration ports.
Back Panel Features	
T1/E1 and Fixed Frequency	Activates T1/E1/J1 ports (x2), and ITU G.703 square/sine wave output on Fixed Frequency/TTL BNC ports (x2)
BNC Outputs	Activates BNC ports and their supported I/O signals (x8) (apart from G.703 signals on Fixed Freq/TTL ports)
Fiber Pulse	Activates ST fiber ports and their supported pulse outputs (x2)
Serial Ports	Activates the RS232 serial port and the RS422 serial port, along with their supported time strings
HV MOSFET	Activates HV MOSFET port and its supported pulse outputs.

Note: Downgrading GridTime 3000 Clock firmware from 1.1 to 1.0 may result in total license loss.

Workaround:

1. **Saved License Key:** If the customer has saved a copy of their clock's license key, they can re-apply the saved license key after the downgrade.
2. **Support Assistance**: If no license key has been saved, customers should contact Support for re-issuance of the license key.

5. Alarms

This section describes the GridTime 3000 GNSS Time Server alarms, how they can be monitored, and what corrective action is required when they occur.

The GridTime 3000 generates an alarm when an event that causes a risk to the operation of the device occurs. Some alarms are expected in isolated occurrences due to signal quality fluctuations. These alarms only show an installation problem when they become recurring. Recurring means the alarm does any of the following:

- Never clears
- Triggers and clears repeatedly for an extended period
- Appears again when the unit is power cycled

Some alarms may indicate that maintenance needs to be performed on the device or installation, and/or may require technical support to be contacted. See Contacting Technical Support.

- Low satellites alarm: Not enough usable GNSS satellites detected. If recurring, it requires the antenna installation to be modified.
- Power supply alarm: A power supply has failed. Contact Technical Support.

For a detailed description of the trigger and clearance conditions for each of the GridTime 3000 alarms, see Alarm Monitoring.

5.1 Alarm Monitoring

This section describes the various alarm monitoring methods used with the GridTime 3000. All active alarms are listed on the alarms tab of the device's LCD and on the dashboard of its Clock Management Tool (CMT) in priority order. The highest priority alarm is also abbreviated and displayed under the alarm icon on the main screen of the device's LCD. See Table 2-2 LCD Tab Information

If notifications are configured, the alarms cause SNMP or Syslog notifications to be sent from the admin Ethernet port to a list of user-defined IP addresses. A notification is sent when an alarm is triggered or cleared. All alarms map to a unique notification, but not all notifications map to an alarm, as some notifications simply describe the standard operational events:

- Antenna current high event: Generates alarm, and trigger and clearance notifications
- First sync achieved event: Does not generate alarms, only a trigger notification

The device includes two alarm relay ports, consisting of two 3-pin phoenix form C alarm relay contacts. Each alarm relay port includes a normally closed (NC) contact, a common (C) contact, and a normally open contact (NO). Each alarm relay port can have any alarms enabled for it through configuration. If any of the alarms enabled on an alarm relay port become active, the port goes from the non-alarm state to the alarm state. The alarm state contact impedances are as follows:

- The impedance between the NC an C contacts becomes under 40Ω
- The impedance between the NO and C contacts becomes open circuit

When all the mapped alarms clear, the port goes to the non-alarm state again. The non-alarm state contact impedances are as follows:

- The impedance between the NC and C contacts becomes open circuit
- The impedance between the NO and C contacts becomes under 40Ω

6. Installation

This chapter describes the installation procedures for the GridTime 3000.

6.1 Getting Started

Before you begin installing the GridTime 3000 GNSS Time Server, review the information in this section. If you encounter any difficulties during the installation process, or require additional technical information, contact Microchip FTS Services and Support. For contact details, see Contacting Technical Support.

6.1.1 Security Considerations for Installations

This section describes some of the security considerations to be made when installing the GridTime 3000. The following security considerations should be made when installing the GridTime 3000:

- Equipment is intended for installation in a Restricted Access Area / Les matériels sont destinés à être installés dans des EMPLACEMENTS À ACCÈS RESTREINT
- The GridTime 3000 should be installed where only certified personnel are allowed access.
- The GridTime 3000's Ethernet service ports should be installed with cyber security best practices in mind.

6.1.2 Site Survey

This section outlines the site surveying process that is recommended prior to installing the GridTime 3000.

The GridTime 3000 is intended to be installed in the following locations:

- Dry indoor locations
- Isolated control rooms with few electromagnetic interference (EMI) sources
- Far from switchyards

Before you begin installation, perform the following pre-installation site checks:

- Determine the device location.
- Ensure the appropriate power source is available nearby.
- Ensure that the equipment rack is properly grounded.
- Survey the GNSS antenna installation location.
  - Ensure that the sky is mostly clear of obstacles, and that few electromagnetic interference (EMI) sources are nearby (within a few meters) including other antennas. If the location is prone to lightning strikes, ensure high reaching metallic objects such as lightning rods are nearby to discharge lightning strikes.

The GridTime 3000 is designed to be mounted in a 19-inch (480 mm) rack. It occupies 1.75 in (4.5 cm, 1 RU) of vertical rack space, and has a depth of 11.93 in (303 mm).

Rack mounting tabs are provided with the device, which provide rack mounting holes once they are slid into the slots at both ends of the GridTime 3000's front panel.

The dimensions of the GridTime 3000 case are outlined in the following figures.

Figure 6-1. GridTime 3000 Case Dimensions - Front

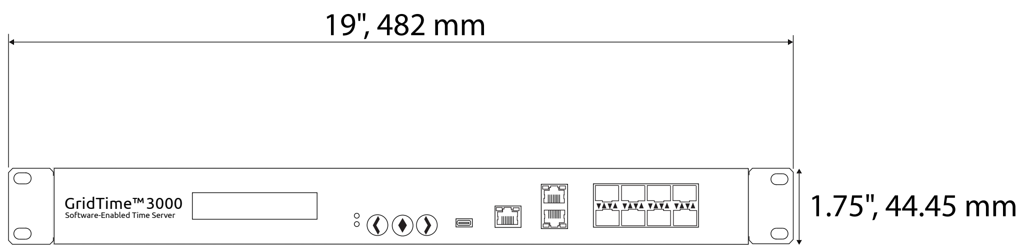
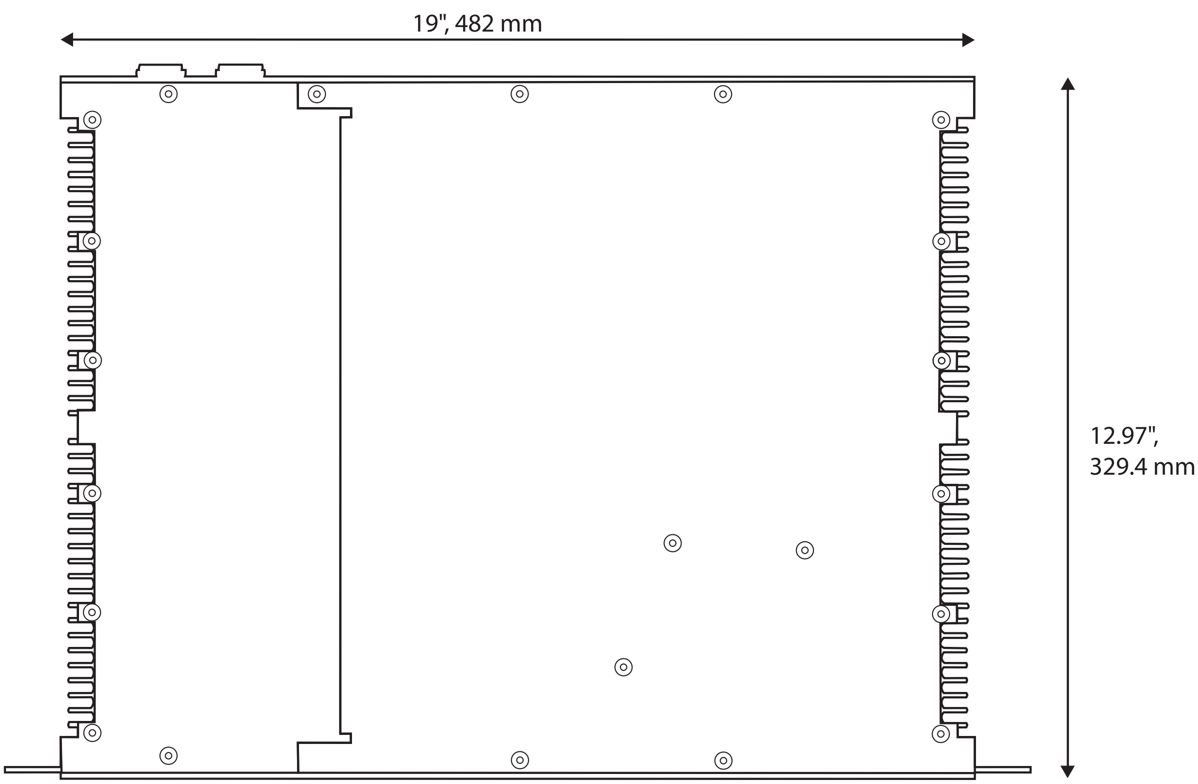


Figure 6-2. GridTime 3000 Case Dimensions - Top



6.1.2.1 Environmental Requirements

This section outlines the environmental requirements for the site installation of GridTime 3000.

To prevent the unit from malfunctioning or interfering with other equipment, install and operate the unit according to the following guidelines:

- Operating temperature: –10 °C to 55 °C (14°F to 131°F)
- Operating Humidity: 90% to 100% RH maximum, non-condensing
- Use only shielded cable for all signal wiring, including I/O, clocks and Ethernet. Ground the shields appropriately at both ends (Making Ground and Power Connections).
- Secure all cable screws to their corresponding connectors.

Important: To avoid interference, you must consider the electromagnetic compatibility (EMC) of nearby equipments when you install the GridTime 3000. Electromagnetic interference can adversely affect the operation of nearby equipment.

6.1.3 Installation Tools and Equipment

This section summarises the equipment and tools required to install the GridTime 3000.

Installation Equipment:

- The GridTime 3000 unit
- Standard tool kit. Useful equipment to include: screwdrivers, spanners, Hexagonal (Allen) keys, wirecutters.
- Cable ties, waxed string or acceptable cable clamps
- 1 mm^2 / 18 AWG (minimum) stranded wire at 300 volt insulation for -48 VDC
- 1 mm^2 / 16 AWG wire to connect grounding lug to permanent earth ground
- Two UL listed Ring Lugs for grounding connections
- Crimping tool to crimp a ring lug to the earth stud — recommended
- Shielded cabling of the appropriate impedance required by the specific signal type for signal wiring (including GPS, and Ethernet)
- Mating connectors for terminating signal wiring
- ESD wrist strap — recommended
- Fasteners for mounting the device to your rack
- Cables and connectors for interfacing with relevant timing ports
- Tools for assembling cables if cables are not already available and fitted with required connectors - wire strippers, crimping tools etc.
- Multi-meter or Voltmeter for verifying continuity in ground connections to the GridTime 3000's chassis.
- PC with a SNMP Management Information Base (MIB) browser, or a supported web browser installed.

Provisioning Equipment:

- Device for performing configuration:
  - A device with a recent version of Google Chrome, Microsoft Edge, or Mozilla Firefox installed.

> **Tip:**
> The following browser versions have been tested:
>
> Google Chrome 97.04692.99 (Offical Build 64-bit) , 98.0.4758.102(Offical Build 64-bit), 99.0.4844.51(Offical Build 64-bit)
>
> Microsoft Edge 99.0.1150.39 (Official build) (64-bit)
>
> Mozilla Firefox 98.0.1 (64-bit)

- If using the USB-C Admin port for configuration:
  - Cable for forming a direct connection between the GridTime 3000's USB-C port, and the USB port on your configuration device.

  - For example, use a USB-C to USB-C cable if your device has a USB-C port, or a USB-C to USB-A cable if your device has a USB-A port.
  - Must be USB 2.0.
- If using the RJ-45 Admin port for configuration:
  - RJ-45 Ethernet cables
    (two needed if going through a DHCP capable switch)
  - Preferred: DHCP server for assigning IP address to RJ-45 Admin port. Without this, you will need to wait for the port to receive a link local IP address (~50 s), and you will have to assign a subnet link local static IP address to the port on your configuration device.

    Tip: Additionally, it is also suitable to connect to the RJ-45 Admin port through an existing Ethernet network with a DHCP server present.

  - If your configuration device has no Ethernet port: A RJ-45 Ethernet to USB adapter can be used to connect the Ethernet cable to a USB port on your device.

6.2 Installation Checklist

This section gives a summary of the key installation steps for the GridTime 3000.

Refer to the followings installation checklist when setting up the device to ensure all the required steps are completed.

- Review all safety documentation and procedures
- Unpack the unit and accessories — Unpacking the Unit
- Install the device in the rack — Rack Mounting the GridTime 3000
- Install an antenna system — Installing the GNSS Antenna
- Connect all signal cables and connectors — Signal Connections
- Connect safety ground, then power connections — Making Ground and Power Connections
- Power the device — Powering the GridTime 3000
- Configure the device using the CMT or SNMP — Clock Management Tool (CMT), Simple Network Management Protocol (SNMP)

6.3 Unpacking the Unit

This section describes how to unpack the GridTime 3000 and its accessories from the box it was shipped in.

When unpacking the device, perform the following steps:

1. Inspect the box for damage before opening. If the box has sustained damage, take photos of the damage immediately and check the packed items for damage.
2. Remove each item from the packaging. Check the package for small items including adapters and antennas.
3. Visually inspect each item for damage. If any item is damaged, take photos of the damage immediately and contact technical support. See Contacting Technical Support.
4. Check each item on the purchase order to confirm the correct items were shipped and received.
5. Validate that the product code matches with what has been ordered

If the items have sustained physical damage or if an item is missing, please contact support. See Contacting Technical Support.

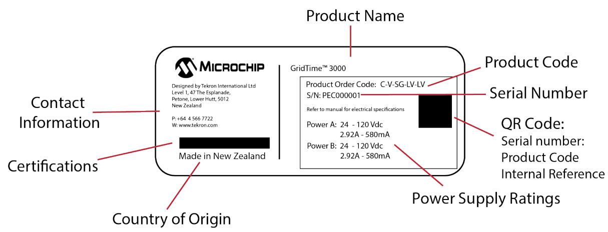
Note: Licenses ordered at the time of manufacture are installed on the device and a paper copy of the license is not provided.

6.3.1 Product Label

This section describes the information on the GridTime 3000 product label, and where the label can be found on the device.

The product label is located on the top lid directly above the SFP ports. For a description of information on the label, see the following figure.

Figure 6-3. Product Label



6.4 Rack Mounting the GridTime 3000

This section describes the process for rack mounting the GridTime 3000.

The GridTime 3000 has been designed to be installed in a 19-inch rack. It is 1U (1.75 Inch) high and has two rack mounting tabs at the front to provide rack mounting holes.

1. Insert the GridTime 3000 so the LCD is facing out of the rack. This will place the mounting fins at the front of the rack.
2. Ensure access to the back of the unit is possible to wire up the device.
3. Fix the unit to the rack using four #10-32 (M6) screws.

Note: Rack mounting screws are not provided.

Note: The device will heat up and cause the surrounding devices to heat up as well. Forced air flow is not required for the unit to operate throughout its rated temperature range. However, any reduction in temperature will improve the long-term reliability of all the equipment in the rack space.

6.5 Making Ground and Power Connections

This section describes how to establish safe ground and power connections to each of the GridTime 3000's ports.

6.5.1 Ground Connections

This section describes how to establish safe grounding connections to the GridTime 3000.

Frame ground connections are made using the M4 Grounding Terminal Studs, which are marked with the universal ground symbol, as shown in Universal Ground Symbol. These studs are located in the middle of the back panel (above the ST Fiber ports) for the GridTime 3000 GridTime 3000 Ground connection.

Figure 6-4. GridTime 3000 Ground Connection

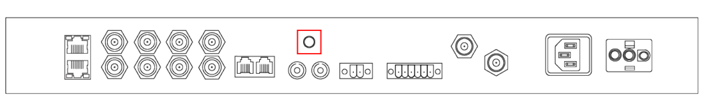
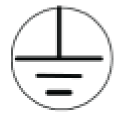


Figure 6-5. Universal Ground Symbol



After installing the GridTime 3000 into the rack, connect the chassis to the proper grounding zone or master ground bar per local building codes for grounding.

Run a 16 AWG (1.5 mm^2) green/yellow-striped insulated wire from the GridTime 3000 grounding lug to the earth ground on the rack. All bare grounding connection points to the GridTime 3000 shall be cleaned and coated with an anti-oxidant solution before connections are made.

Tip: **Recommendation**: Although there are a number of methods for connecting the equipment to earth ground, Microchip recommends running a cable of the shortest possible length from the ground lug to earth ground

---

1. Crimp the customer-supplied UL listed 18 AWG Ring Lug to one end of the 16 AWG wire. Connect the ring lug to the ground terminal on the left side of the front panel using the supplied M4 Kept machine nut, tightening to a torque value of 30 in-lbs, (3,4 Nm). The surface of the GridTime 3000 earth grounding terminal must be clean of contaminants and oxidation.
2. Crimp the appropriate customer-supplied UL listed 18 AWG Ring Lug to the other end of the 1.5 mm^2 / 16 AWG green/yellow-striped wire. Remove the paint and sand the area around the screw hole to ensure the proper conductivity. Coat the connection with an electrically conductive antioxidant compound such as Kopr-shield spray. Connect this Ring Lug to the rack with appropriate customer supplied screws and external star lock washers, tightening to a torque value of 53.45 in-lbs, (6 Nm).
3. Using a digital voltmeter, measure between the ground and chassis and verify the resistance between them.

6.5.2 Power Connections

This section describes how to establish safe power connections to the GridTime 3000.

The GridTime 3000 can be fitted with one or two power supplies. With a single supply configuration, it will have a power supply connected to its P1A port. With a dual supply configuration, it will have one power supply connected to its P1A and one connected to its P1B ports.

There are two power supplies that the GridTime 3000 can be ordered with — a low voltage supply or a high voltage supply.

The power supply bay in GridTime 3000 has a separate lid to allow in-field power supply maintenance to be performed. See Power Supply Fuse Replacement and Power Supply Replacement.

DANGER The following ports must have the power removed before opening the power supply bay:

- P1A (Power Supply)
- P1B (Power Supply)
- Alarm Relay 1 and 2
- HV MOSFET output

Important: The power input connector requires an external over current protection rated to twice the expected maximum operating current.

DANGER Exposed terminals present the risk of electrocution. Ensure all wires are covered.

CAUTION In case of fire or electric shock, cut-off power at the circuit breaker

6.5.2.1 Installation Best Practices

This section describes the installation best practices that should be used when wiring up power connections for the GridTime 3000.

- A circuit breaker rated at twice the maximum expected operating current must be installed between the GridTime 3000 device and the supply.
- For maximum redundancy:
  - Each power supply should be fed by independent Uninterruptible Power Supply (UPS) sources.
  - A separate circuit breaker should be used for each supply.
- Equipment must be installed according to applicable local wiring codes and standards.

6.5.2.2 Power Supply Ratings

This section outlines the ratings of the GridTime 3000 power supplies.

Operating the device outside of these ratings may cause permanent hardware damage, Microchip assumes no liability for any damage resulting from operating the device outside its operational ratings.

The voltage and current ranges for the two supplies are as follows. The ranges are marked on the product label on the chassis.

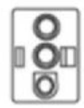
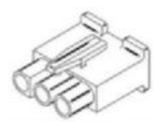
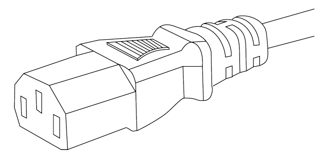
Table 6-1. Power Supply Voltage and Current Range

Power Supply	Ratings
Low voltage	**(DC Only)** 24 Vdc -120 Vdc 2.92 A - 580 mA
High voltage	**DC Ratings** 120 Vdc - 250 Vdc 590 mA - 280 mA **AC Ratings** 100 Vac - 240 Vac 700 mA - 292 mA

6.5.2.3 Connectors

This section describes the connectors used with the GridTime 3000's power supplies.

Table 6-2. Power Supply Connectors

Power Supply	Low Voltage	High Voltage
Connector Image		
Connector Type	AMP Universal MATE-N-LOK	IEC 320-C14
Mating Connector	Molex HCS-125 	
Mating Connector Crimps	Molex 0018121222	Not Applicable
Crimp tool	Molex 638191100	Not Applicable

Instructions for crimping the low voltage DC connector can be found in the Crimping the DC Connector section.

Instructions for crimping the high voltage AC/DC connector can be found in the Crimping the AC Connector section.

6.5.2.4 Fuses

This section describes the fuses supplied with the GridTime 3000.

The fuses for the power supplies are located on the power supply circuit boards. Each supply has two fuses; one larger fuse on the input to the power supply module and one on the output of the module.

Important: This port may be connected to supply voltages up to 250V DC and/or 230V AC if it is a high voltage (HV) PSU.

DANGER The following ports must have the power removed before proceeding:

- P1A (Power Supply)
- P1B (Power Supply)
- Alarm Relay 1 and 2
- HV MOSFET output

DANGER Exposed terminals present the risk of electrocution. Ensure all wires are covered.

Table 6-3. Fuse Rating

Power Supply	Low Voltage	High Voltage
Input Fuse Rating	250V 10A Slow Blow	150 Vdc 4A Slow Blow
Input Fuse Model	Cylindrical 5 mm x 20 mm	Cylindrical 5 mm x 20 mm
Suggested Part	Littelfuse 0218010.MXP	Littelfuse 0239003.MXP
Output Fuse Rating	125V 10A Fast Blow	125V 10A Fast Blow
Output Fuse Model	Nano 2.69 mm x 6.1 mm	Nano 2.69 mm x 6.1 mm
Suggested Part	Littelfuse 0451010.NRL	Littelfuse 0451010.NRL

For instructions on how to replace the fuse in a GridTime 3000 product, please see the instructions in Replacing a fuse.

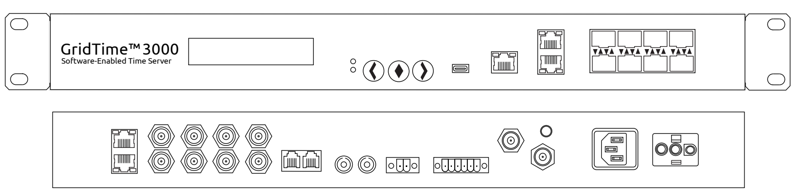
6.6 Signal Connections

This section describes how to make a reliable connection between each of the GridTime 3000's ports and an end device. This includes:

- a summary of what each port is for — more detailed descriptions are in the Physical Overview section
- equipment installation recommendations for each port
- how to configure high performance timing connections between applicable ports and your end device
- how to optimize each connection's reliability
- how to safely connect and disconnect a connector on each port

The GridTime 3000 has a wide array of ports for receiving and delivering time signals, and two ports for device management.

Figure 6-6. GridTime 3000 Ports



6.6.1 Admin Port Connections

This section describes how to make connections to the GridTime 3000's administration ports.

The GridTime 3000 features two ports for device management:

- the admin Ethernet port
- the admin USB-C port

Either port can be used for:

- device configuration
- monitoring system observables, such as the device's current time

The IP addresses currently used by the Admin Ethernet and Admin USB-C ports are displayed on the clock info tab of the GridTime 3000’s LCD (see LCD Tab Information). These addresses are used to access the web configuration interfaces, and for performing device management over SNMP.

6.6.1.1 Admin Ethernet Port

This section describes how to connect to the GridTime 3000's admin Ethernet port.

The admin Ethernet port is a standard 10/100/1000BASE-T RJ-45 receptacle intended for connection to a personal computer (PC) over a direct copper Ethernet link, or through a switched Ethernet network.

Link Negotiation Checks:

- DHCP Server (Optional): By default, the admin Ethernet port is configured to use DHCP addressing. First connection to the port should therefore be made through a switched network with a DHCP server present. If no DHCP server is available, a direct link can be used, but the user will have to wait for the port to fall back to a link local IP address (~50 seconds of wait time).
- Link Speed Auto-negotiation Support: The admin Ethernet port uses auto-negotiation to establish link speed, so the switch or PC port it is connected to should also support auto-negotiation.

To make a connection, ensure the following:

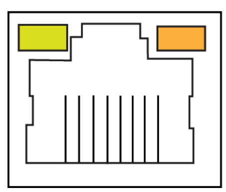
- A copper Ethernet cable terminated with an RJ-45 plug
- Your network adapters are compatible with 10/100/1000BASE-T operation

A straight-through or crossover cable can be used as the port is Auto MDI-X.

To connect the cable to the port:

1. Place one hand on the GridTime 3000 to ensure it does not move.
2. Use the other hand to gently slide the cable’s RJ-45 plug into the port. Ensure the orientation of the plug aligns with the port.
3. Connect the other end of the cable to a switch or a PC’s Ethernet port.

Figure 6-7. A Linked Ethernet Port



If the link is successfully established:

- the right-side LED (LNK LED) will illuminate to a constant green or orange or will stay off depending on the link speed. green = 1Gbps, orange = 100Mbps, off = 10Mbps.
- The left-side LED (ACT LED) will flash green as Ethernet traffic passes through the port.

6.6.1.2 Admin USB-C Port

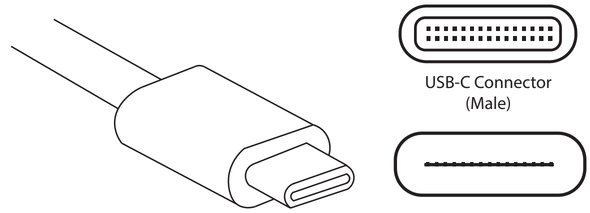
This section describes how to connect to the GridTime 3000's Admin USB-C Port.

The admin USB-C port is a USB-C 2.0 device port, intended for direct connection to:

- a personal computer (PC)
- a tablet with a web browser

The port must be connected to another device port. It cannot be a host port.

Figure 6-8. Connecting the Admin USB-C Port



To form a direct connection:

- If the end device has a USB-C port, use a male USB-C to male USB-C cable
- If the end device has a USB-A port, use a male USB-C to male USB-A cable

Ensure the cable is USB 2.0 or greater so that it supports the required link speeds.

To connect the cable to the port:

1. If it is not rack mounted, place one hand on the GridTime 3000 to ensure it does not move.
2. Slide the cable's USB-C connector gently into the port. The orientation of the connector does not matter as USB-C connectors are rotationally symmetrical.
3. Do the same for the other end of the cable at the end device.

The GridTime 3000 appears as a virtual Ethernet port on the end device if the link is successfully established.

6.6.2 Synchronization and Timing Connections

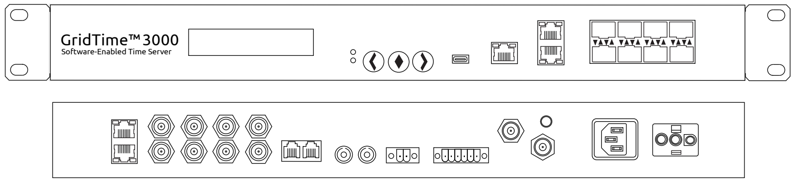
This section explains how to configure all synchronization and timing port connections on the GridTime 3000 GNSS Time Server.

The GridTime 3000 features ten network timing ports on its front panel, all of which can allow the device to act as a PTP or NTP time source to other devices, or to synchronize to an external PTP or NTP time source as a timeReceiver/client.

The GridTime 3000 features the following ports on its back panel:

- Two RJ-48C T1/E1/J1 time signal output ports
- Eight BNC ports that can output user-defined pulses, simulated DCF77 receiver timecodes, DLCS and Modified Manchester IRIG-B (the standard GridTime 3000 pulse outputs). The fixed frequency/TTL BNC ports can also output fixed frequency waveforms, and the AM IRIG/TTL BNC ports can also output AM IRIG. The IRIG In/TTL Out BNC ports can also receive an IRIG-B signal, allowing IRIG to be used as a device time source.
- Two RJ-12 serial string output ports
- Two optical fiber output ports that can output the standard GridTime 3000 pulse outputs
- A high voltage MOSFET switch, that can also be used with an external voltage source to output the standard GridTime 3000 pulse outputs

Figure 6-9. Synchronization and Timing Port Connections



6.6.2.1 Ethernet Ports - RJ-45, SFP, and SFP+ Ports

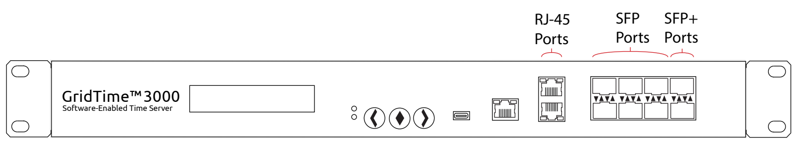
This section describes how to form a connection to the GridTime 3000's Ethernet ports.

The GridTime 3000 features ten ports for NTP and PTP time synchronization over a packet-switched network:

- Two 10/100/1000BASE-T RJ-45 ports — ETH01 and ETH02
- Six 1 Gbps Ethernet small form factor pluggable (SFP) ports — ETH03-ETH08
- Two 10 Gbps Ethernet SFP+ ports — ETH09 and ETH10

These are collectively labeled the 'ETH' ports, as seen on the front panel decal.

Figure 6-10. GridTime 3000 Ethernet Ports



6.6.2.1.1 Network Architecture Recommendations

This section provides some general architecture recommendations when using the GridTime 3000 to deliver time over Ethernet.

- Take note of all the network hops between the time server port and your end devices
- Optimize your architecture to reduce network hops, this improves timing accuracy. A star topology is recommended over a ring or single bus topology for this reason.
- Use boundary clocks if long transmission distances and multiple network hops are needed. This helps to reduce jitter and signal instability that can accumulate with multiple hops through switches.

6.6.2.1.2 ETH01 and ETH02 (RJ-45)

This section describes how to connect to Eth1 or Eth2 on the GridTime 3000.

The RJ-45 ports are standard 10/100/1000BASE-T RJ-45 receptacles.

Cabling recommendations:

- Use a copper Ethernet cable terminated with a RJ-45 plug.
- Follow the cable manufacturer's recommendations.
- Ensure that the cable supports your link speed requirements.

Network device recommendations:

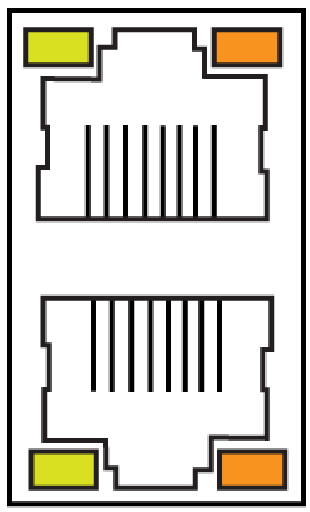
- Ensure all relevant network ports can auto-negotiate link speed, and are capable of at least one of the following:
  - 10BASE-T transmission

  - 100BASE-T transmission
  - 1000BASE-T transmission
- Use PTP aware network switches if you plan to use PTP, as this greatly improves the timing accuracy.

Connecting a cable into a RJ-45 port:

- If not rack-mounted, place one hand on the GridTime 3000 to ensure it does not move.
- Gently slide the cable's RJ-45 plug into the port. Ensure the orientation of the plug aligns with the orientation of the port.
- Connect the other end of the cable into the relevant port in your network.
- Ensure the port is enabled in software. Once enabled, check it's left-hand LED when directly facing the front-panel (enabled LED), is illuminated solid green.
- The right LED (ACT LED) will flash orange as traffic passes through if the cable's network link has successfully been established.

Figure 6-11. RJ-45 Port



Removing a cable from a RJ-45 port:

- If not rack-mounted, place one hand on the GridTime 3000 to ensure it does not move.
- Press down on the flap on cable's the RJ-45 plug with the other hand.
- Slide the RJ-45 plug out of the port gently.

6.6.2.1.3 Eth3- Eth10 (SFP and SFP+ Ports)

This section describes how to connect to Eth3-Eth10 on the GridTime 3000.

The SFP ports support direct attach cables (DAC cables), optical and copper SFP transceivers, and up to 1G transmission speeds. The SFP+ ports support direct attach cables, optical and copper SFP transceivers, and up to 10G transmission speeds.

Only the direct attach cables and SFP transceivers in Recommended SFP transceivers are officially recommended and supported for use with the GridTime 3000. Other cables and SFP transceivers can be used, but they may cause the device to be unable to meet its timing performance ratings. Assistance from Microchip support in debugging issues related to unsupported SFPs cannot be guaranteed. Contact Microchip technical support for the most up to date list of supported direct attach cables and SFP transceivers.

Table 6-4. Supported SFP Transceivers

Brand	Model Number
Finisar	FTLF1217P2BTL
ROBOfiber	SFP-5000-RJ45
FS	SFP-100FX-31
FS	SFP-FB-GE-T
FS	SFP-10GSR-85
FS	SFP-10GLR-31
FS	SFPP-PC03
Bel	SFP-1GBT-06
Cisco	GLC-FE-100FX-RGD
Cisco	GLC-T-RGD
OptixCom/OptoIC	SFP-1250LX-AT2K

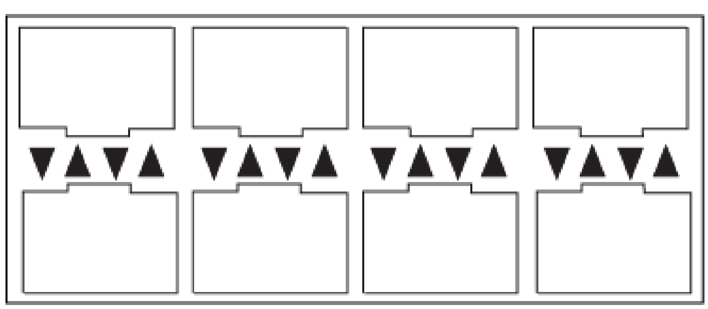
SFP and Cable Recommendations:

- Ensure your cables and SFPs support the link speeds you are using.
- Follow manufacturer recommendations for correct use of cables and SFP transceivers.
- If SFP+ ports are going to run at 10G speeds, use suitable Direct Attach Copper (DAC) cables or fiber SFP transceivers. Do not use copper SFP transceivers as these may create thermal issues.

Network device recommendations:

- Ensure all relevant network ports can auto-negotiate link speed.
- Ensure all network switches in the path support the timing protocol (NTP or PTP) you plan to use.
- For SFP Ports, ensure all relevant network ports support one of the following:
  - 10BASE-T transmission
  - 100BASE-T transmission
  - 1000BASE-T transmission
- For SFP+ Ports, ensure all relevant network ports support one of the following:
  - 10BASE-T transmission
  - 100BASE-T transmission
  - 1000BASE-T transmission
  - 10G BASE-T transmission

Figure 6-12. SFP Port



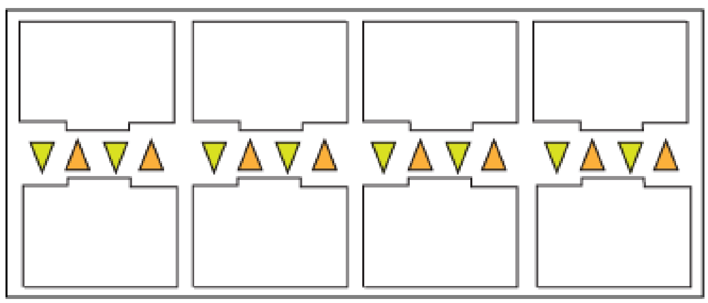
Connecting a cable into a SFP port:

1. For copper and fiber SFP transceivers:
   - Remove any rubber protection from inside the SFP’s bore(s).

- Ensure the SFP's clasp is closed.
- If not rack-mounted, place one hand on the GridTime 3000 to ensure it does not move.
- Align the SFP with the receptacle. The SFP's product label should be face up for the top row of ports, and face down for the bottom row of ports.
- Slide gently slide the SFP into the port. If the orientation is correct it will click into place, if it is incorrect it will be stopped short and will not click into place.
- Plug the cable into the SFP, align its flap(s) with the SFP bore(s).

2. For DAC Cables:
   - If not rack-mounted, place one hand on the GridTime 3000 to ensure it does not move.
   - Align the cable's SFP plug with the receptacle. Its product label should be face up for the top row of ports, and face down for the bottom row of ports
   - Slide gently the cable into the port, if the orientation is correct it will click into place, if it is incorrect it will be stopped short and will not click into place.
3. Plug the other end of the cable into the relevant port in your network.
4. Ensure the port is enabled in software. Once enabled, the left-most LED that points at the port when directly facing the front-panel (enabled LED), goes solid green.
5. The right-most LED that point at the port (ACT LED) flashes orange as traffic passes through if the cable's network link has successfully been established.

Figure 6-13. Cable Connected SFP Port



Removing a cable from a SFP port:

1. If not rack-mounted, place one hand on the GridTime 3000 to ensure it does not move.
2. For Copper and Fiber SFP Transceivers:
   - Press down on the clip of the cable plugged into SFP.
   - Gently pull the cable out of the SFP.
   - To remove the SFP as well, rotate its bail latch so it is at 90 degrees to the SFP.
   - Gently pull out the SFP by its clasp, maintaining the 90-degree angle.
3. For DAC cables:
   - Gently pull out the cable by pulling on its tag.

6.6.2.2 T1/E1/J1 Ports

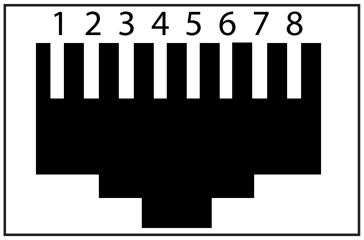
This section describes how to connect to the T1/E1/J1 ports on the GridTime 3000.

The GridTime 3000 features two RJ-48C ports as shown in GridTime 3000 Front Panel Features. The ports can be configured to output a T1, E1, or J1 signal. Both ports will always output the same signal type.

A detailed explanation of the pinout for the RJ-48C ports is given in the following table.

Table 6-5. RJ-48C Pinout

Figure 6-14. RJ-48C Pinout Diagram



Pin	Signal
1	End of line termination (120Ω to pin 2)
2	End of line termination, with pin 1
3	GND
4	TX Ring -
5	TX Tip +
6	Not Connected
7	Not Connected
8	Not Connected

Connecting a cable into a RJ-48Cport:

- If not rack-mounted, place one hand on the GridTime 3000 to ensure it does not move.
- Gently slide the cable's RJ-48C plug into the port. Ensure the orientation of the plug aligns with the orientation of the port.
- Connect the other end of the cable into the relevant port in your network.

Removing a cable from a RJ-48C port:

- If not rack-mounted, place one hand on the GridTime 3000 to ensure it does not move.
- Press down on the flaps on the cable's RJ-48C plug.
- Gently slide the cable out of the port.

6.6.2.3 BNC Ports

This section describes how to form a connection to the GridTime 3000's BNC ports.

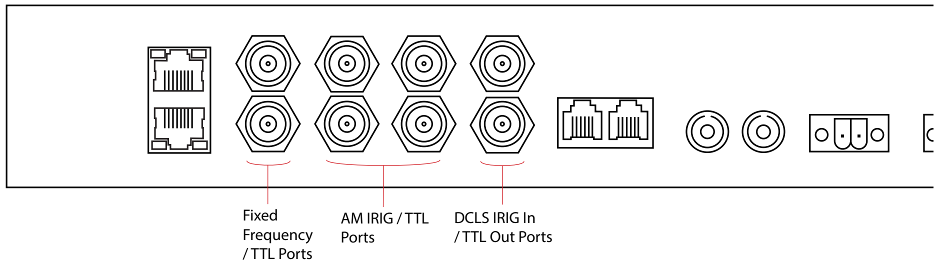
The GridTime 3000 features eight BNC ports (Ports 3-10). Each port can output the standard GridTime 3000 pulse output signals:

- DCLS IRIG-B
- Modified Manchester IRIG-B
- Square wave pulses with a configurable frequency, duration, and phase offset (user-defined pulses)
- DCF77 simulated receiver time signal (DCF77)

The BNC ports are split into three subgroups, each with a unique additional functionality:

- the first two BNC ports (Ports 3 and 4) can also output fixed frequency sinusoidal or square wave signals
- the second four BNC ports (Ports 5-8) can also output AM-IRIG B
- the final two BNC ports (Ports 9 and 10) can also receive a 0-5 V TTL DCLS IRIG-B signal with C37.118.1 extensions as a timing reference input.

Figure 6-15. BNC ports



6.6.2.3.1 Cable Recommendations

This section describes how to select a cable to use with the GridTime 3000 BNC ports.

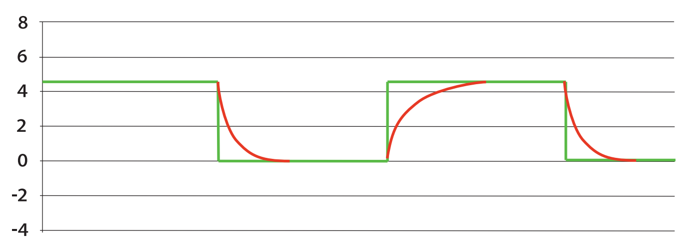
Cable Type — Shielded Twisted Pair (STP) or Coaxial

Either Coaxial or shielded twisted pair (STP) cables can be used with the BNC ports if they have been terminated with a female BNC connector.

STP cable use is recommended over Coaxial cable, as Coaxial cable introduces more line capacitance than STP. Capacitance reduces the cable lengths that can be used before excessive signal loss occurs.

The effects of a high line capacitance can round the edges of TTL signals, which can reduce time accuracy, and in extreme cases can cause end devices to falsely trigger rising or falling edges, preventing the device from reliably decoding signals.

Figure 6-16. Signal Rounding Caused By the High Capacitance of a Coaxial Cable



Cable Frequency Rating

The frequency rating of the cable used should exceed the highest frequency content of the output signal.

- For AM-IRIG this is 1 kHz
- For fixed frequency sine waves, it is the configured fixed frequency (1.544, 2.048, or 10MHz)
- For fixed frequency square waves and TTL signals, this will be far higher due to the harmonics introduced by the sharp edges (~1 MHz).

6.6.2.3.2 Output Circuitry Recommendations

This section describes the installation best practices for output circuity connected to the GridTime 3000's BNC ports.

Topology Recommendations

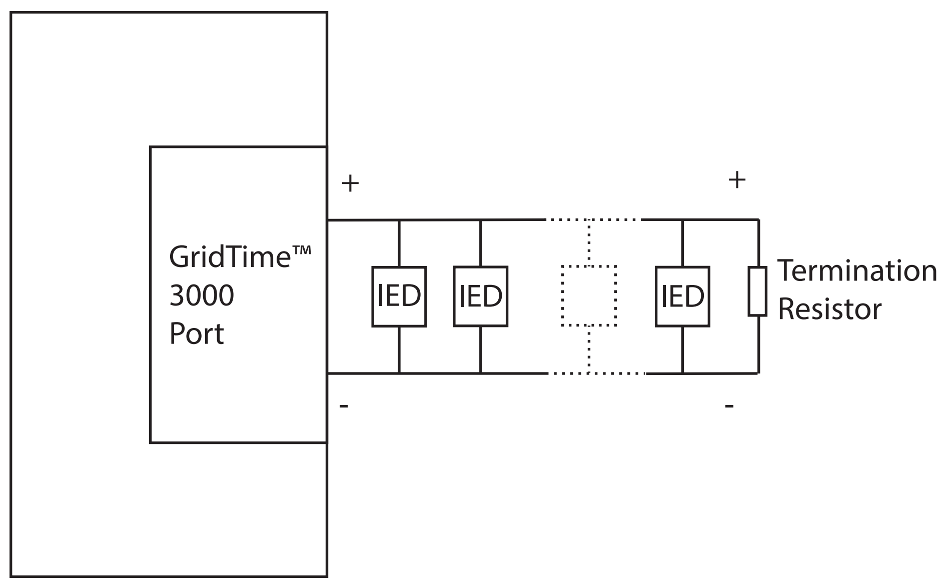
- Connecting a Single End Device to a port:
  If the connection from the BNC port needs to go to only a single device, make a direct connection between the BNC port and the port of the end device, and put a termination resistor in parallel

with the cable. Ensure that the cable and the end device input meet the recommendations mentioned in the Cable Recommendations section.

- Connecting Multiple End Devices to a port:
  If multiple end devices need to be connected to a single BNC port, connect the end devices in parallel along a single bus, with a termination resistor also in parallel. To determine how many devices can be used on the bus and the wire length restrictions on the bus, see the Cable Recommendations section.

  The circuitry should use a multi-dropping topology, not a star topology.

Figure 6-17. Circuitry Topology



Termination Resistor Selection

- **TTL Signals**
  When outputting TTL signals:
  – DCLS or Modified Manchester IRIG-B
  – User-defined pulses
  – DCF77

  It is recommended that a single termination resistor is used to dampen signal overshoot and reflections that result from the sharp edges of the signal. The termination resistor must meet the following requirements:
  – Resistance of the termination resistor should be approximately the same as the characteristic impedance of the bus cable, which should be in the cable's datasheet.
  – Should have a sufficient power rating. Use the Power = Voltage^2/Resistance to calculate the maximum power dissipation required, with 5V as the Voltage term (all TTL signals from the ports are 0-5V), and the resistance value of the resistor as the Resistance term.
- **AM-IRIG**
  When outputting AM IRIG-B signals, it is recommended that a termination resistor is used to ensure that the end devices receive the correct voltage levels.

  $R_{term} = (((R_s \times V_{req})/(V_{out} - V_{req})) - 1/R_l)^{-1}$

If R_{term} comes out negative, the bus is overloaded. See the Cable Recommendations section.

- **Fixed Frequency**

  Loading and Cable Length Recommendations: The BNC ports are rated to supply 150 mA of current, more current than this will trigger a high current alarm. Ensure the combined maximum current draw of all devices does not exceed 150 mA. The maximum expected current draw of each end device can be added to calculate the combined maximum current draw.

Earth Cables

- For STP, earth shield in a way that avoids earth loops.
- Limit bending of cables
- Do not bend the installation cables beyond their rated bend radius. Cables should gradually bend around corners where possible. Bending cables beyond their rated bend radius can alter their impedance and permanently damage the cable.
- Run cables far away from interference sources. Cables should be run far away from potential interference sources such as radio frequency (RF) emitters. The distance required is dependent on the strength of the interference source.

Connecting a cable to a BNC port:

- Align the slots on the cable's connector with the bumps on either side of the BNC port.
- If not rack mounted, use one hand to hold the GridTime 3000 in place.
- Gently slide the cable's connector over the port.
- Gently twist the cable's connector clockwise to fasten it in place, ensure the bumps on the BNC port are fully pushed down into the cable's connector slots.

Removing a cable from a BNC port:

- If not rack mounted, use one hand to hold the GridTime 3000 in place.
- Gently twist the cable's BNC connector counterclockwise to release it.
- Gently slide the cable out of the port.

6.6.2.4 RJ-12 Serial String Ports

This section describes how to form a connection to the GridTime 3000's RJ-12 ports.

The GridTime 3000 features two RJ-12 serial string output ports:

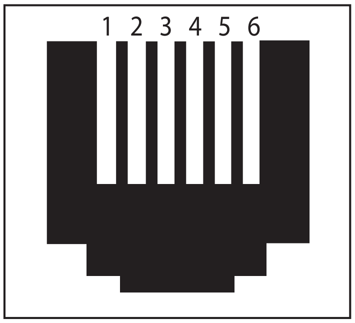
- the RS-422 port — uses RS-422 transmission (Port 11)
- the RS-232 port — uses RS-232 transmission (Port 12)

Each port can be configured to output its own ASCII time code string from a list of supported strings. For a complete list of these strings, see Time String Specifications.

The ports are standard RJ-12 receptacles.

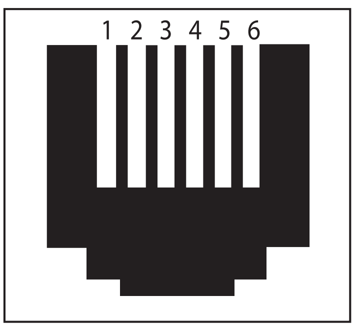
The pinout of the RS-232 port is given in the following table.

Table 6-6. RS-232 Port Pinout

	Pin	Signal
Figure 6-18. RS-232 Port Pinout 	1	0V
	2	Clock Receive
	3	0V
	4	Clock Transmit
	5	Clock CTS
	6	Clock RTS

The pinout of the RS-422 port is given in the following table.

Table 6-7. RS-422 Port Pinout

	Pin	Signal
Figure 6-19. RS-422 Port Pinout 	1	Not Connected
	2	Isolated 0V*
	3	Clock Transmit -ve
	4	Clock Transmit +ve
	5	Isolated 0V*
	6	Not Connected
*Isolated 0V is not connected to Chassis earth.		

An RJ-12 to male DB9 cable accessory is optionally sold with the GridTime 3000, which can be used to interface the RJ-12 ports with a female DB9 connector.

The DB9 pin mappings when the cable is plugged into the device's RS-422 and RS-232 ports are given in tables RJ-12 to DB9 cable pin mapping when plugged into RS-422 port and RJ-12 to DB9 cable pin mapping when plugged into RS-232 port.

Table 6-8. RJ-12 to DB9 Cable Pin Mapping When Plugged Into RS-232 Port

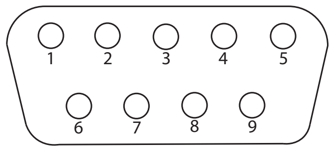
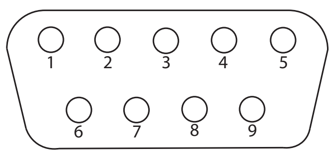
	Pin	Description
	1	Not Connected
	2	Clock Transmit
	3	Clock Receive
	4	Not Connected
	5	0V
	6	0V
	7	Clock CTS
	8	Clock RTS
	9	Not Connected

Table 6-9. RJ-12 to DB9 Cable Pin Mapping When Plugged Into RS-422 Port

	Pin	Description
	1	Not Connected
	2	Clock Transmit +ve
	3	0V
	4	Not Connected
	5	Not Connected
	6	Clock Transmit -ve
	7	0V
	8	Not Connected
	9	Not Connected

Connecting a cable into a RJ-12 port:

1. If not rack mounted, place one hand on the GridTime 3000 to ensure it does not move.
2. Gently slide the cable's RJ-12 plug into the port. Ensure the orientation of the plug aligns with the orientation of the port.
3. Plug the other end of the cable into the relevant port in your network, ensure the orientation is correct.

Removing a cable from a RJ-12 port:

1. If not rack mounted, place one hand on the GridTime 3000 to ensure it does not move.
2. Press down on the flaps on the cable's RJ-12 plug.
3. Gently slide the cable out of the port.

Note: Serial String Outputs RS232 and RS422 are output only and will not accept a serial string input.

6.6.2.5 TX Fiber Ports

This section describes how to connect to the GridTime 3000's TX Fiber ports.

The GridTime 3000 features two optical fiber transmitters (Port 13 and 14) for the output of IRIG-B, DCF-77, and custom pulse signals, as shown in.

To connect to the TX Fiber ports, the link must:

- be optical
- use a multimode fiber cable with a straight-tip (ST) connector
- use a cable with one of the following core structures:
  - 50/125 µm plastic optical fiber (POF)

  - 62.5/125 µm POF
  - 100/140 µm POF
  - 200 µm hard-clad silica (HCS)
- use a transmission wavelength of λ = 820 nm
- not force the cable to exceed its bend radius
- have a length that allows sufficient power to be delivered to the receiver of the end device

Cable Length

The allowable cable length is dependent on:

- the environmental temperature
- the core structure of the cable
- the termination quality of the cable's connector
- the sensitivity of the receiver on the end device
- the optical power delivered into the cable.

The optical power delivered into a cable by the device's transmitter is as follows:

Table 6-10. Optical Power Delivered

Core Structure	50/125 µm POF	62.5/125 µm POF	100/140 µm POF	200 µm HCS
Typical Optical Power	−15.8 dBm	−12 dBm	−8.5 dBm	−4.5 dBm
Worst Case Optical Power	−19.8 dBm	−16 dBm	−12.5 dBm	−8.5 dBm

Assuming the worst case temperature conditions, and that the fiber cable has a high-quality polished termination, an upper boundary for the cable length can be calculated using the worst-case optical power from the preceding table, and:

- the cable's attenuation figure (check its datasheet)
- the receiver sensitivity (check its datasheet)

Length (km) = (Worst Case Optical Power (dBm) – Receiver Sensitivity (dBm))/(Cable Attenuation Figure (dB/km))

If you are using:

- a 62.5/125 µm POF cable with a high-quality polished termination
- a typical 62.5/125 µm cable attenuation figure of 4 dB/km
- a Microchip Isolated Timing Repeater (ITR) as the end device, which has a receiver sensitivity of −24 dBm

then, the upper bound for the cable length would be:

Length = ((-16 dBm) – (-24 dBm))/(4 dB/km) = 2 km

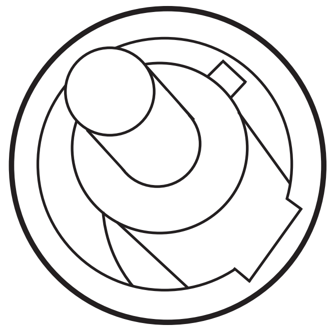
In this scenario, the cable length should not significantly exceed 2 km. Ensuring the environmental temperature is always roughly 25 °C allows for more cable length.

A repeater such as the Microchip ITR can be used if the cable runs greatly exceed the length boundary required.

Connecting a cable into a ST Fiber port:

1. If present, twist the device's black plastic cap on the fiber port counterclockwise so it is no longer locked in by its notches, then gently pull it off the port
2. Rotate the outer part of the cable's ST connector so that the outer notch is at 90 degrees to the inner notch

Figure 6-20. ST Fiber Port



3. Line up the ST connector so that the port's inner notch is in line with the topmost notch on the TX fiber port.
4. If not rack mounted, place one hand on the GridTime 3000 to ensure it does not move.
5. Gently slide the ST port into the TX fiber port until it hits the end.
6. Push the outer part of the ST connector down the tracks and twist it clockwise so it locks in place.
7. Connect the other end of the cable into the relevant port on your end device, follow a similar process to plug in the connector.

Removing a cable from a ST Fiber port:

1. If not rack mounted, place one hand on the GridTime 3000 to ensure it does not move.
2. Push in the cable's ST connector and twist it counterclockwise to release the connector.
3. Gently slide the cable out of the port.

6.6.2.6 HV MOSFET Port

This section describes how to connect to the GridTime 3000's HV MOSFET port.

The GridTime 3000 features a power MOSFET Switch port for the output of IRIG-B, DCF77, and user-defined pulse TTL timing signals at custom amplitudes (HV MOSFET Port).

The port allows timing signals to be outputted at custom amplitudes up to ±250V to suit the end device input requirements. If a 0-5V TTL signal is sufficient for your end device(s), the BNC port(s) should be used instead of the HV MOSFET port.

An external DC supply that provides sufficient voltage for the end device input logic levels must be used with this port. This can be the same supply used to power the GridTime 3000 if it is being DC powered.

The switching voltage and current ratings are provided in HV MOSFET Port Specifications.

Table 6-11. HV MOSFET Port Specifications

Ratings	Connector
Allows switching of 250V at 100 mA maximum.	2-pin

Cable Recommendations

- Use a cable terminated with a 2-pin phoenix connector
- Ensure the cable is rated for the current expected to run through it

Tip: To meet IEC 61850-3 standards, this port should be installed with a shielded cable. The shield should be connected to earth at both ends.

Wiring Recommendations

- As the port is only a switch, an external power supply must provide the switching voltage. The port does not provide its own voltage.
  - conventional current flow must be into the “+” terminal and out of the “-” terminal. Incorrect polarity will cause the output state to always be low.
- Use a circuit breaker with twice the rated current to protect the port and the connected end device.

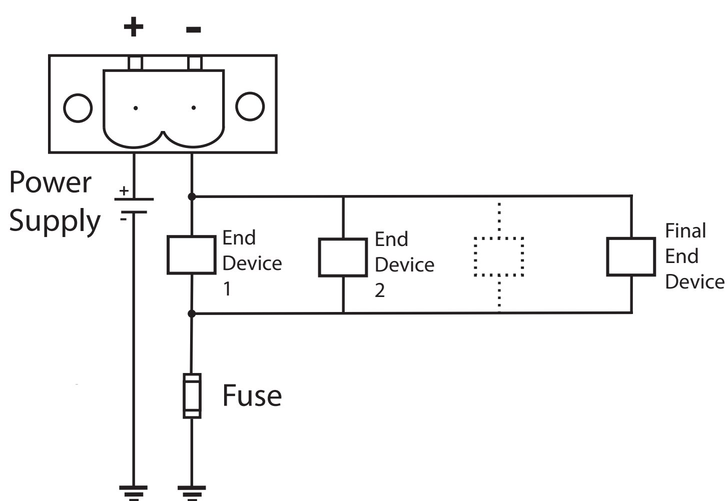
Single End Device

- The end device should also be connected in series with the port, power supply, and circuit breaker.
- An inline resistor should also be included in series if the end device does not load the circuit with the current it requires. Use $R = V_{required}/I_{required}$ to determine its resistance.

Multiple End Devices

- The end devices should be multi-dropped into a bus. The device bus should be connected in series with the port, power supply and circuit breaker.
- An inline resistor should also be included in series if the end devices do not load the circuit with the current they require. Use $R = V_{required}/I_{required}$ to determine its resistance.

Figure 6-21. HV MOSFET Port Suggested Circuitry Configuration



CAUTION In case of fire or electric shock, cut-off power at circuit breaker

Output isolation (from chassis and I/O) is still maintained when the HV MOSFET is enabled. This simplifies the external load/supply arrangements, particularly when operating with positive-earth systems.

6.6.2.7 Antenna Port

This section describes how to connect to the GridTime 3000's GNSS Antenna port.

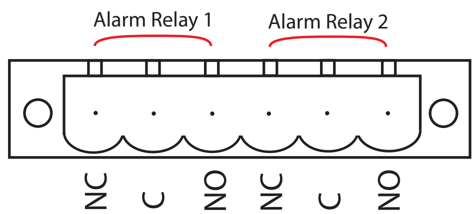
To connect to the antenna port, refer to Installing the GNSS Antenna.

6.6.3 Alarm Relay Connections

This section describes how to wire up and monitor the GridTime 3000's alarm relay ports.

The GridTime 3000 includes two alarm relay ports on its back panel, consisting of two 3-pin phoenix form C alarm relay contacts. Each alarm relay port includes a normally closed (NC) contact, a common (C) contact, and a normally open contact (NO).

Figure 6-22. Alarm Relay Ports



Contact Impedances

Each alarm relay port can have any of the supported alarms enabled through configuration. If any alarms enabled on an alarm relay port become active, the port goes from the non-alarm state to the alarm state. It returns to the non-alarm state once all enabled alarms are cleared.

When in the alarm state:

- The impedance between the NC and C contacts is less than 40Ω
- The impedance between the NO and C contacts is open circuit

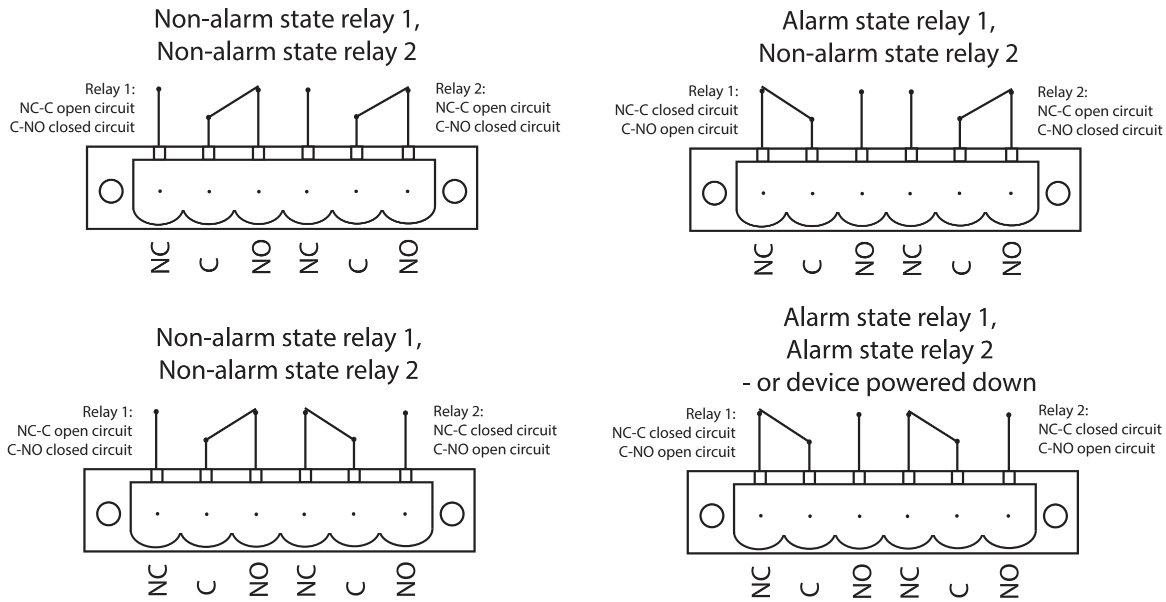
When in the non-alarm state:

- The impedance between the NC and C contacts is open circuit
- The impedance between the NO and C contacts is less than 40Ω

When the GridTime 3000 is powered down:

- Same impedances between contacts as the alarm state
- The impedance between the NC and C contacts is less than 40Ω
- The impedance between the NO and C contacts is open circuit

Figure 6-23. Alarm Relay Port States



Cable Recommendations

- Use a cable terminated with a six-pin phoenix connector with locking screws.
- Ensure the cable is rated for expected current from the end device.

Connection Recommendations:

- Use an in-line resistor or load which draws a safe current amount. This will ensure excessive current is not drawn when a pair of contacts is in the low impedance state.
- Use a circuit breaker with twice the rated current to protect the relay port and the connected end device.
- Apply an external source of power to monitor whether current is passing through the relay.
- For a normally closed alarm configuration, plug the cable's 2 pin connector into the NC and C contacts.
- For a normally open alarm configuration, plug the cable's 2 pin connector into the NO and C contacts.

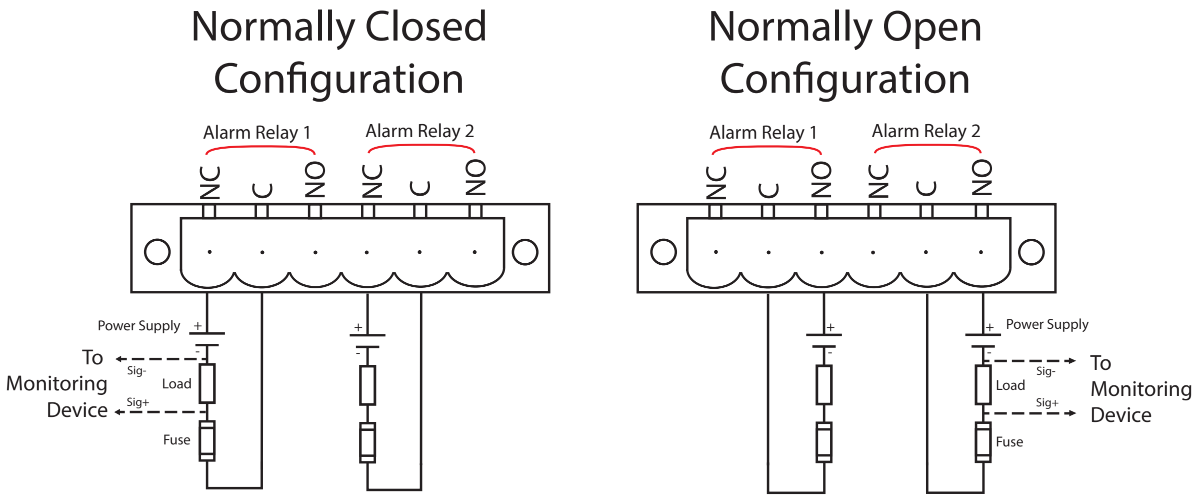
CAUTION In case of fire or electric shock, cut-off power at circuit breaker

---

Equivalent Circuit Diagrams

Connect the alarm relay and the external components for a normally closed or normally open configuration as per the equivalent circuit diagrams in Alarm Relay Recommended Circuit Configuration.

Figure 6-24. Alarm Relay Recommended Circuit Configuration



Note: The diagrams above are equivalent circuits of what is recommended, the external components shown may be present internally in the end monitoring device.

Connecting a cable into the alarm relay:

- Align the 6-pin phoenix connector with the port contacts.
- If not rack mounted, hold the GridTime 3000 in place with one hand.
- Gently slide the connector into the port until it cannot be pushed any further.

Removing a cable from the alarm relay:

- If not rack mounted, hold the GridTime 3000 in place with one hand.
- Gently slide the connector out of the port.

6.7 Installing the GNSS Antenna

This section describes:

- GNSS constellations and signals the GridTime 3000 supports
- how to reliably install an antenna with the GridTime 3000
- how to design your antenna system
- how to connect your antenna cable

The GridTime 3000 features one TNC port which allows for synchronization to time from global navigation satellite systems (GNSSs). This port is named the ‘antenna port’ and is labeled ‘ANT 1’ on the device’s decal.

A GNSS antenna can be connected to the antenna port through a radio frequency (RF) cable terminated with a TNC connector. A 50 ohm coaxial cable is recommended.

Unless configured to do otherwise, the device's default settings will always treat GNSS as its highest priority time source for synchronization even if other time source(s) are also available (NTP, PTP, or IRIG-B).

Four GNSS constellations are supported, and a different upper and lower baseband signal can be received from each. This is shown in Baseband Signals of Supported GNSS Constellations.

Table 6-12. Baseband Signals of Supported GNSS Constellations

GNSS	Lower Baseband Signal	Upper Baseband Signal
GPS/QZSS	L2C (1227.600 MHz)	L1C/A (1575.420 MHz)
GLONASS	L2OF (1246 MHz + k*437.5 kHz, k= -7, ..., 5, 6)	L1OF (1602 MHz + k*562.5 kHz, k= -7, ..., 5, 6)
Galileo	E5b (1207.140 MHz)	E1-B/C (1575.420 MHz)
BeiDou	B2I (1207.140 MHz)	B1I (1561.098 MHz)

Any number of the supported GNSSs can simultaneously be used for time synchronization. Either their upper signal, or simultaneously their upper and lower signals can be used for synchronization.

It is best to utilize as many GNSSs and GNSS basebands as possible. This can improve accuracy, make jamming and spoofing more difficult, and removes vulnerability to a malfunction or deliberate denial of a particular GNSS system.

When synchronized to one or more GNSS signals, the device's Clock Management Tool and LCD dashboards will show 'GNSS' as the current time source See Table 2-2 LCD Tab Information.

6.7.1 Microchip Antenna Kit versus Custom Equipment Installations

This section describes the differences between custom GNSS and antenna equipment and the Microchip antenna kit.

The GNSS receiver inside the device is highly sensitive and supports a wide range of antenna and lead-in cable combinations. However, the Microchip antenna kits are recommended in preference to other equipment, and support cannot be guaranteed if equipment issues result from custom equipment choices. The Microchip antenna kits have been tested with the GridTime 3000 and are proven to give good GNSS performance.

The Microchip antenna kits offer a range of cable lengths and protection levels. They are electrically compatible with the device's antenna port and are compatible with all supported GNSS input signals.

If custom equipment is chosen, read the next three sections on custom antenna installation recommendations, otherwise, skip to the All installations sections.

6.7.2 Custom Installation - Antenna Port Input Requirements

This section describes the input requirements that must be met by a custom antenna installation.

Custom antenna installations must meet the antenna port input specifications in Antenna Port Input Specifications.

Table 6-13. Antenna Port Input Specifications

Parameter	Specification
Signal Type	Must support at least one of the following: GNSS L1C/A, L2C, L1OF, L2OF, E1B/C, E5b, B1I, or B2I
Gain	Between 15 dB and 30 dB of gain including gain of antenna and loss of cable and inline components
Frequency	Must support frequency bands used by the desired signal types
Impedance	50 ohms
Coupling	DC-center pin provides power to GNSS antenna or inline amplifier
Output voltage to antenna	5 Vdc
Output current to antenna	80 mA maximum
Connector type	Female TNC connector
Decal label	ANT1

6.7.3 Custom Installation - Antenna Recommendations

This section provides key recommendations when selecting an antenna for a custom antenna installation with the GridTime 3000.

The following recommendations should be considered when selecting an antenna for a custom antenna installation:

- Select an amplified active antenna with integral low-noise amplifer (LNA) to ensure good performance under nominal signal reception.
- Select a dual-band antenna that is compatible with at least one of the supported GNSS constellations.
- Use an active antenna that can be powered with less than 5V and under 80 mA, accounting for cable and in-line component losses.

6.7.4 Custom Installation - Cable recommendations

This section provides key recommendations when selecting an antenna cable for a custom antenna installation with the GridTime 3000.

The following recommendations should be considered when selecting an antenna cable for a custom installation:

- Select a cable with shielding against radio frequency (RF) interference
- Select a cable that is compatible with your antenna
- Ensure the cable is terminated with a TNC connector – you may need to terminate the cable yourself
- Use a low-loss 50 Ω coaxial cable

6.7.5 All Installations - Connection Recommendations

This section provides key recommendations on how to safely connect an antenna cable to the GridTime 3000.

- Safe cable grounding techniques should be used on the RF cable.
- A lightning arrestor should be installed in-line with the antenna cable to protect the device from lightning strikes
- The GNSS cables should only be connected once the device's chassis is properly earth grounded
- Follow local building electrical codes for grounding the device's chassis

DANGER To avoid serious personal injury or death, use extreme caution when installing the antenna near, under, or around high voltage lines.

6.7.6 All Installations - Antenna Placement Recommendations

This section provides recommendations on positioning the GNSS antenna in your installation for optimum timing performance.

- Mount the antenna outside, preferably on the roof with an unobstructed view of the sky
- Do not mount the antenna near a wall or other obstruction that may impact the sky view.
- Do not mount the antenna near other RF emitters such as satellite dishes or WiFi routers
- Mount the antenna well above roads or parking lots.
- For a multi-antenna installation, place antennas at least one meter apart from one another.

To achieve the highest level of accuracy it is recommended the antenna is provided with an RF gain between 15 to 35 dB and positioned in an area with an unobstructed view of the sky and in a low multipath environment. If the antenna is not placed in the correct environment and these conditions are not met, the device may require a longer GNSS acquisition window or will prevent the GNSS input from being used.

6.7.7 All Installations - Delay Compensation

This section describes how to compensate for the signal propagation delay through an antenna installation.

Ensure that the cable delay on the device is set to compensate for the total propagation delay through the antenna and cable, and any lightning arrestors or in-line amplifiers in the installation. Time synchronization to GNSSs will be inaccurate by the value of the propagation delay error if left uncompensated.

See Provisioning GNSS for the delay values of the Microchip supplied antenna accessories, and further guidance on setting up the delay compensation value.

6.8 Powering the GridTime 3000

This section describes how to power up the GridTime™ 3000 GNSS Time Server once all signal connections have been established.

The GridTime 3000 does not have a power switch; the device will power up as soon as power is applied to its P1A port or P1B port. Power application monitoring and switching must be done externally to the device.

6.8.1 Powering Up

This section summarizes the key power up steps for the GridTime 3000.

1. If the power supply to the device is controlled by a switch, check the switch is in the off position.
2. Connect a power supply cable to the device’s P1A power port, and to its P1B power port if it has a dual power supply configuration
3. Turn on the supply to the unit if the supply is switch controlled.

6.8.1.1 Normal Power Up Indicators

This section describes the key indicators that should be observable after a successful power up of the GridTime 3000.

Once power has successfully been applied to the GridTime 3000, its LCD backlight will illuminate blue, and its start-up sequence will begin. Refer to Table 2-2-1 Start Up LCD Tab Information

A counter will appear on the LCD which shows the progression of the start-up sequence. Refer to Table 2-2-2 Start Up LCD Tab Information

Once the start-up sequence has finished, the LCD’s dashboard screen will load up. Refer to Table 2-2-3 Start Up LCD Tab Information

If the power up sequence is successful, the following front panel indicators can be observed.

Table 6-14. Normal Power Up Indicators

Indicator	Expected Behavior	Conditions
ALM LED	Will initially flash red to indicate that alarms are active. The following alarms will be active at start-up until cleared: • Out of sync alarm • Low sats alarm • GNSS no Fix alarm • No First sync alarm	**Flashing Red** — at least one alarm is active **Off** — no alarms are active
ADMIN Ethernet port	If a cable is connected, LNK LED will give link speed color, and ACT LED will flash as traffic passes through if the port has a live Ethernet link connected	**LNK LED (Right)** — off for 10Mbps link, orange for 100 Mbps link, green for 1 Gbps link, off for no active link **ACT LED (Left)** — sold orange and flashes with traffic, off for no active link
ETH1-ETH10 ports	Enabled LEDs will go green if port is enabled, and the ACT LED will flash as traffic passes through if the port has a live Ethernet link connected	**Enabled LED** – green when port is enabled, off if disabled **ACT LED** – sold orange and flashes with traffic, off for no active link
SYN LED	Will initially flash green to indicate that the device has not gained synchronization to a time source yet	**Flashing Green** – device is not synchronized to a time source **Solid Green** – device is synchronized to a time source

6.8.2 Powering Down

This section describes how to safely power down the GridTime™ 3000.

It is recommended that the GridTime™ 3000 is shutdown prior to removing power. To perform a shutdown:

1. Hold down the center button on the front panel until the clock power screen appears. Refer to Table 2-2 Clock Power Tab Information
2. Once the screen appears, press the right-hand button when facing the front panel directly to perform a shutdown.
3. Wait ~20 seconds for the LCD to go completely blue to validate that the shutdown is complete, it will remain backlit while the unit is still powered.

Once the unit has fully shut down:

- If the power supply is switch controlled, switch off power to the device.
- Gently slide the power supply cable out of P1A, and P1B if the unit has dual supplies.
  - IEC cables can be directly pulled out.
  - DC connectors will need to be unclipped and then pulled out.

7. Clock Management Tool (CMT)

This chapter describes the GridTime 3000's Clock Management Tool (CMT).

The CMT is a web browser management interface that is used to configure and monitor the GridTime 3000.

Once a a USB-C Admin or Admin Ethernet connection has been established with the GridTime 3000 — see Establishing a Connection to the GridTime 3000, the CMT can be accessed by entering the IP address of the admin port into a web browser. Refer to Table 2-2 Clock Information tab

8. Simple Network Management Protocol (SNMP)

This chapter describes how SNMP can be used with the GridTime 3000.

The Simple Network Management Protocol (SNMP) is an application layer protocol that allows you to manage network devices. SNMP is based on a client-server query-response mode that requires an Ethernet connection. A manager application (software installed on a computer) is the client generating the queries, and an agent (GridTime 3000 software) is the server generating responses.

The GridTime 3000 supports SNMPv1, SNMPv2c, and SNMPv3. SNMPv3 provides additional security features not previously available in SNMPv2c. In addition to SNMPv2c functions, SNMPv3 allows user and trap-user levels that are based on authentication and privacy settings. The authentication algorithm is either HMAC-SHA-1-96 or MD5, with a 20-character key. The privacy settings are based on either the CBC-DES or AES encryption standard, with a 16-character key. All keys are uppercase.

The GridTime 3000 sends SNMP notifications into the network from its Admin Ethernet ports if notifications are configured. If SNMP read/write privileges are enabled, it can also be used to monitor and configure GridTime 3000 variables.

Note: SNMP is an optional feature for the GridTime 3000 that must be enabled to function. See Provisioning SNMP Settings for details.

8.1 GridTime 3000 Management Information Base (MIB)

This section describes the GridTime 3000 MIB.

A Management Information Base (MIB) is a database of managed objects, their object identifiers, and variables.

The GridTime 3000 has its own MIB, which can be downloaded from my.microsemi.com as a text file. This MIB describes all of the GridTime 3000's settings and system observables.

With the use of a MIB browser, the GridTime 3000 MIB can be used to monitor status and configure variables. With the GridTime 3000, an SNMP network manager can be set up to monitor the status of the GridTime 3000.

Other MIBs can also be used to monitor the GridTime 3000's status and configure its variables, these are described in the following section.

8.2 Public MIB Support

This section describes the public MIBs the GridTime 3000 supports.

The GridTime 3000 supports the following MIBs for configuration and monitoring system observables:

- RFC 1213 MIB - Management Information Base for Network Management of TCP/IP-based internets

9. Provisioning

This chapter describes how to provision the GridTime 3000. This should be followed after the GridTime 3000 is installed (Installation) and the connections (Signal Connections) are established.

9.1 Establishing a Connection to the GridTime 3000

This section describes how to establish a connection to the GridTime 3000.

To provision the GridTime 3000, a connection must be established between a PC and the GridTime 3000's admin USB-C or admin Ethernet port.

For step-by-step guidance on this, see Admin Port Connections.

For guidance on how to access and log into the GridTime 3000's Clock Management Tool (CMT) see the following section.

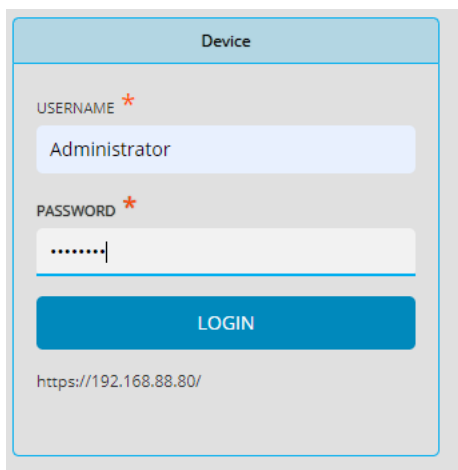
9.2 Logging In and Out

This section describes how to log in and out of the GridTime 3000's CMT.

1. To open the CMT, type the IP address of a connected admin port into the address bar of a web browser on a connected PC. The CMT login screen appears.
   If a connection is not already established between a PC and one of the GridTime 3000's admin ports, establish the connection (see Establishing a Connection to the GridTime 3000).

   Note: The current IP address of the administration ports can be viewed on the front LCD.
2. In the CMT login screen, enter the login username and password for the GridTime 3000 unit and click **LOGIN**.

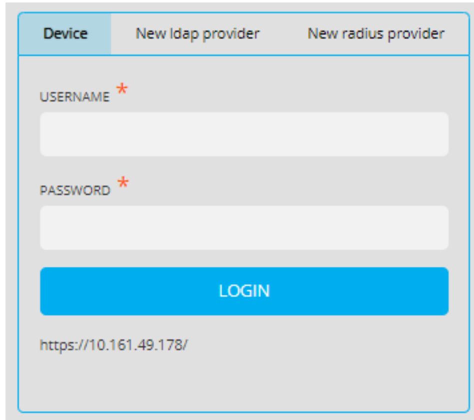
Figure 9-1. CMT Login Screen



Note: If the GridTime 3000 has not previously been set up with a password, the login screen instructs you to choose an Administrator password for the unit. After this has been done, you can login using the login window above.

Note: If the GridTime 3000 has been configured to use RADIUS and/or LDAP, you will first have to select the relevant authentication provider before being able to log in using one of these methods.

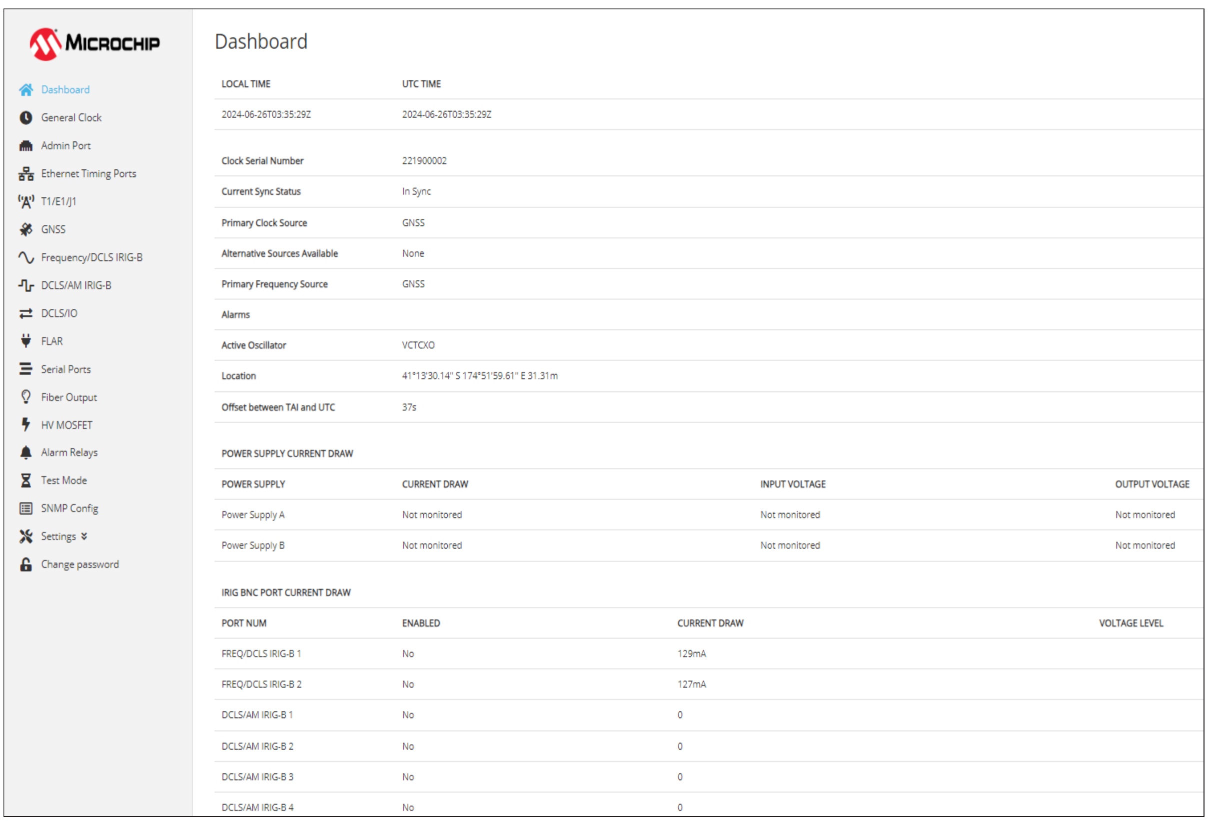
Figure 9-2. CMT Login Screen - RADIUS/LDAP Authentication



Upon successful login, the CMT dashboard screen appears indicating that you have logged into the GridTime 3000 CMT.

The entire CMT screen is divided into two sections; the left and the middle navigation panes. The left navigation pane lists all the settings available in the CMT, and the middle navigation pane displays the options available for a particular setting that the user selects on the left navigation pane.

Figure 9-3. CMT Dashboard



3. To log out of the CMT, scroll to the bottom of the page, and on the left navigation pane, click **Logout** with the door icon.

This takes you back to the CMT login screen Figure 9-1.

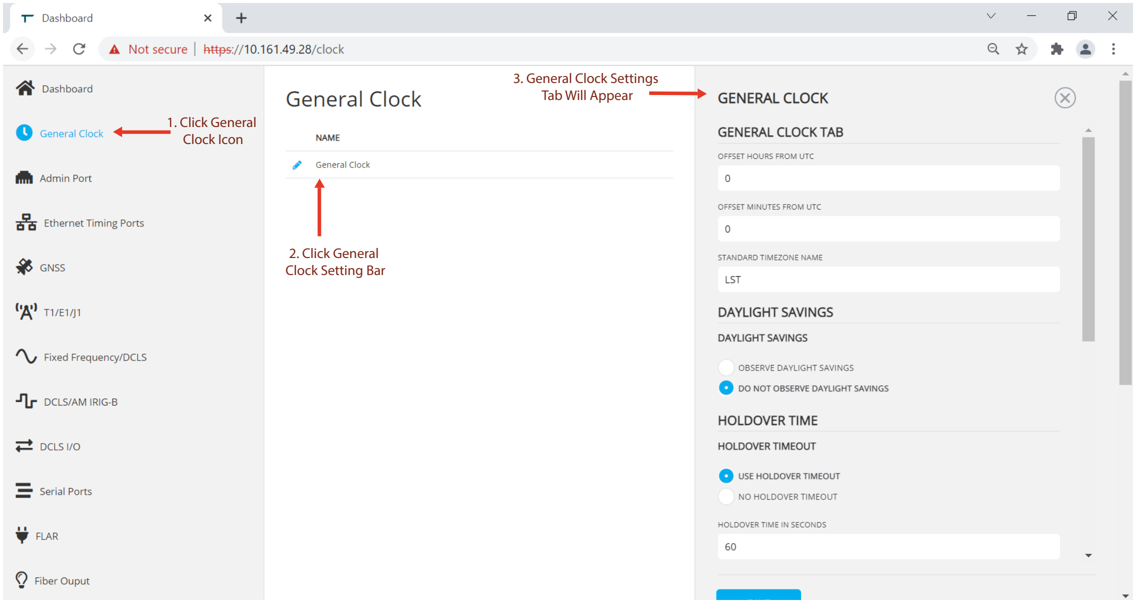
9.3 Provisioning the General Clock Settings

This section describes how to provision the general clock settings for GridTime 3000.

The general clock settings are used to configure the time zone offset and daylight savings behavior, the holdover entry and exit behavior, and the sync source selection behavior.

1. **Navigate to General Clock Window**
   To navigate to the general clock window, on the left navigation pane, click **General Clock**, and then the general clock settings bar in the center of the screen. The **GENERAL SETTINGS** window appears on the right pane.

Figure 9-4. Clock Management Tool - General Clock Tab



2. **Setup Local Time Zone**
   Using the offset hours from UTC, offset minutes from UTC, and the standard time zone name settings, configure your local standard time offset from UTC in hours and minutes, and the name of your local timezone.

   Figure 9-5. General Clock Tab

   The offset in hours can be configured in the range of -12 to 14 hours, and the offset in minutes can be configured in the range of 0 to 59 minutes. The standard timezone name can be configured as any ASCII string, but only the first five characters will be displayed on the LCD and used in messages.

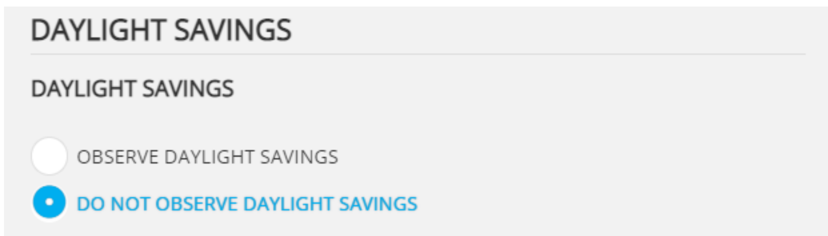
   Note: This step is for configuring the standard timezone offsets only. If your region observes daylight savings, daylight savings offsets are configured in step 3.

Important:
Regional time zone UTC offsets and daylight savings offsets are not automatically detected by the GridTime 3000, and must be manually entered by a user. Updates to the UTC offset or daylight savings in the region of use must also be actively monitored and maintained by a user.

For up-to-date information on regional UTC offsets and daylight savings offsets, visit www.timeanddate.com/time/change/ .

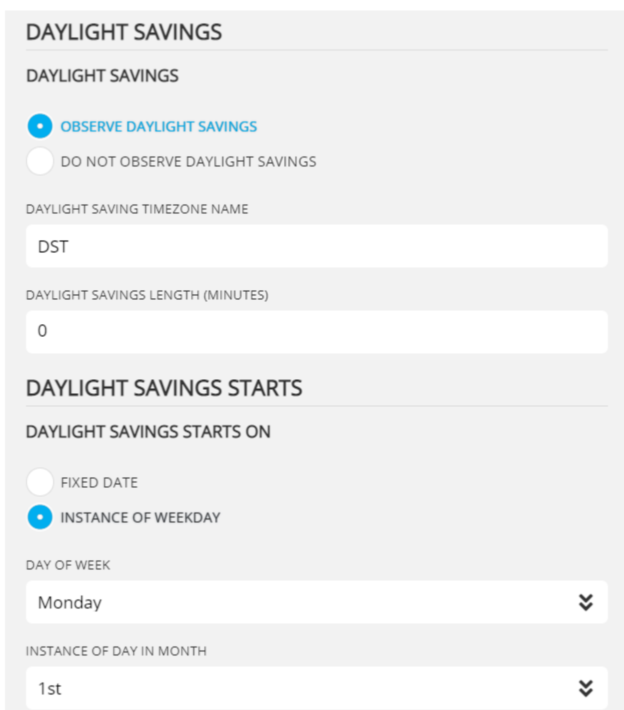
3. **Setup Daylight Savings**
   If your region does not observe daylight savings, under **DAYLIGHT SAVINGS** section, select the **DO NOT OBSERVE DAYLIGHT SAVINGS** radio button. This hides all other daylight savings settings.

Figure 9-6. DAYLIGHT SAVINGS



If your region does observe daylight savings, under **DAYLIGHT SAVINGS** section, select the **OBSERVE DAYLIGHT SAVINGS** radio button. This shows all the additional daylight savings that need to be configured.

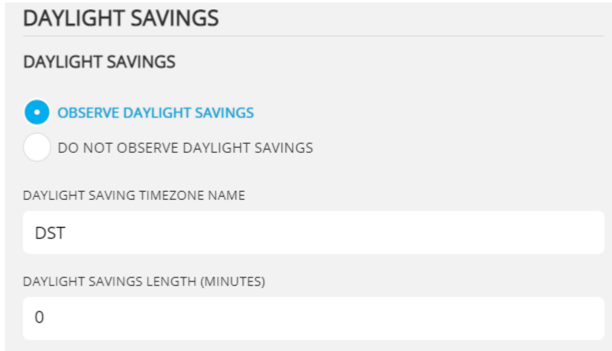
Figure 9-7. DAYLIGHT SAVINGS - ADDITIONAL SETTINGS



a. **Setup Daylight Savings Time Zone**

Using the daylight savings timezone name and daylight savings length settings, configure the name of your daylight savings timezone, and your regional daylight savings time jump in minutes.

Figure 9-8. Setup Daylight Savings Timezone

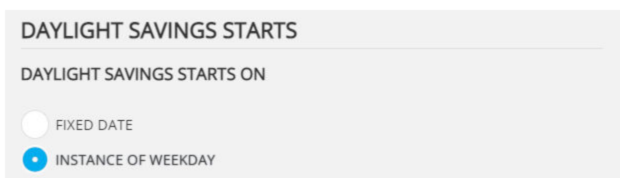


The daylight savings timezone name can be any ASCII string, but only the first five characters will be displayed on the LCD or used in messages. The daylight savings length can be any jump value from 0 to 3600 minutes (60 hours). If the daylight savings length is set to 0, then the clock will behave as though it is not observing daylight savings.

b. **Setup Daylight Savings Start**

If your regional daylight savings jump begins on a specific instance of a weekday, under the **DAYLIGHT SAVINGS STARTS** section, select the **INSTANCE OF WEEKDAY** radio button, and go to step 3.2.1. If your daylight savings time jump begins on a fixed date, select the **FIXED DATE** radio button, and go to step 3.2.2.

Figure 9-9. Daylight Savings Start Settings

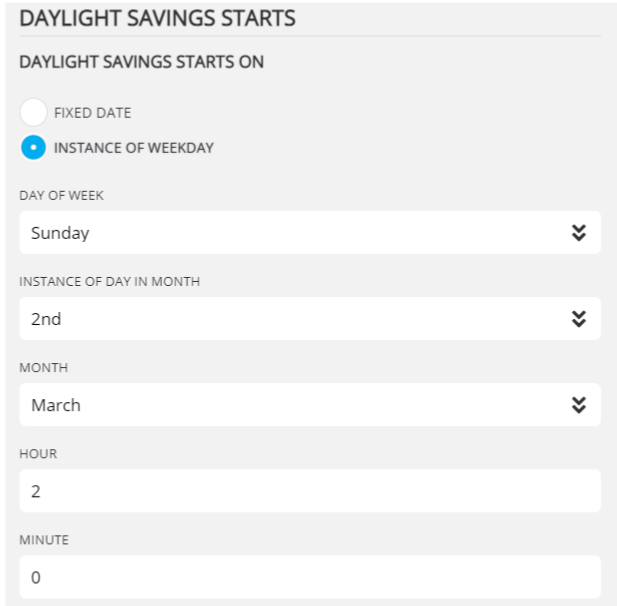


i. **Setup Daylight Savings Start Instance of Weekday**

When using the daylight savings starts on the instance of weekday option, configure the **DAY OF WEEK**, **INSTANCE OF DAY IN MONTH**, and the **MONTH** the daylight savings jump occurs, and the time of the day when the jump occurs in hours and minutes from midnight.

For example, if the GridTime 3000 is installed in Denver, Colorado, where the daylight savings currently begins on the 2nd Sunday of March at 2.00 am, you would configure the following settings.

Figure 9-10. Daylight Savings Start -Instance of Weekday Settings Example



ii. **Setup Daylight Savings Start Fixed Date**

When using the daylight savings start on fixed date option, configure the **MONTH** and **DAY** the daylight savings jump occurs, and the time of the day when the jump occurs in hours and minutes from midnight.

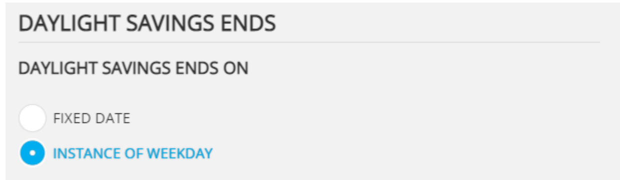
For example, if a region's daylight savings begins on the 13th of April at 3.00 am, you would use the following settings.

Figure 9-11. Daylight Savings Start -Fixed Date Settings Example

c. **Setup Daylight Savings End**

If your regional daylight savings time ends on a specific instance of a weekday, under the **DAYLIGHT SAVINGS ENDS ON** section, select the **INSTANCE OF WEEKDAY** radio button and go to step 3.3.1. If your daylight savings time ends on a fixed date, select **FIXED DATE** and go to step 3.3.2.

Figure 9-12. Daylight Savings End Settings

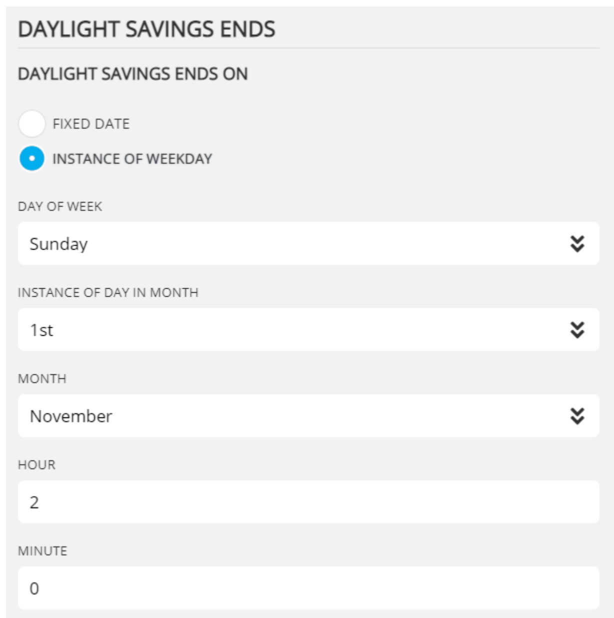


i. **Setup Daylight Savings Ends Instance of Weekday**

When using the daylight savings ends on instance of weekday option, configure the **DAY OF WEEK** and **INSTANCE OF DAY IN MONTH** the daylight savings time ends, and the time of the day when this occurs in hours and minutes from midnight.

For example, if the GridTime 3000 is installed in Denver, Colorado, where the daylight savings currently ends on the 1st Sunday of November at 2.00 am, you would configure the following settings.

Figure 9-13. Daylight Savings End-Instance of Weekday Settings Example



ii. **Setup Daylight Savings Ends Fixed Date**

When using the daylight savings ends on fixed date option, configure the **MONTH** and **DAY** when the end of daylight savings occurs, and the time of day when it occurs in hours and minutes from midnight.

For example, if a region's daylight savings ends on the 18th of December at 3.30 pm, you would use the following settings.

Figure 9-14. Daylight Savings End-Fixed Date Settings Example

4. **Setup Holdover Timeout**

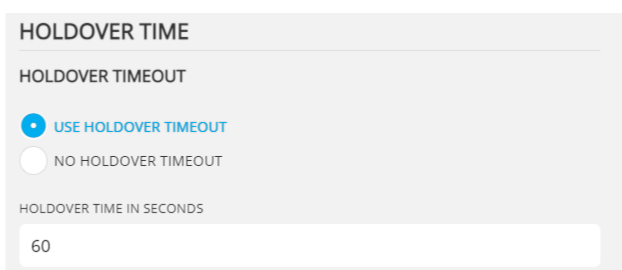
   Use the holdover time settings under the **HOLDOVER TIME** section to configure the maximum time in seconds the GridTime 3000 remains in the holdover state after losing all of its sync sources before entering the out-of-sync state. When in the holdover state, the GridTime 3000 relies on its internal oscillator in free run mode as a time reference. The accuracy of the oscillator time reference slowly degrades as the oscillator drifts. This slow decline in accuracy during holdover is tracked by the accuracy reported in the GridTime 3000's outputs. If a rubidium or Oven Controlled Crystal Oscillator (OCXO) expansion is fitted in the GridTime 3000, the oscillator time drifts slower than the time drift of the base Voltage Controlled, Temperature Compensated Crystal Oscillator (VCTCXO) that is fitted.

   Once the holdover time has expired, the GridTime 3000's time is considered too inaccurate to be usable and the GridTime 3000 enters the out-of-sync state. In this state, the GridTime 3000 still relies on its oscillator as a reference, but will trigger the out-of-sync alarm and triggers the indication of out-of-sync on outputs that have a specific out of sync indicator, such as PTP clockClass.

   The GridTime 3000 can re-synchronize to a sync source if it becomes available when in the holdover or out-of-sync states, which makes it reenter the in-sync state.

   To use holdover timeout, select the **USE HOLDOVER TIMEOUT** radio button. You can then enter the time you want the GridTime 3000 to remain in holdover after losing its sync sources, in the **HOLDOVER TIME IN SECONDS** text box.

   Figure 9-15. Holdover Time Settings

   If you do not want to put a time limit on the GridTime 3000's time in holdover, select the **NO HOLDOVER TIMEOUT** radio button.

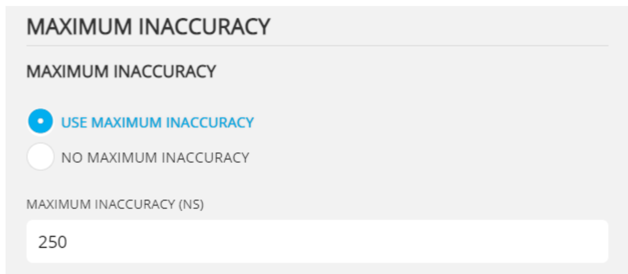
5. **Setup Maximum Inaccuracy**

The maximum inaccuracy setting is similar to the holdover timeout setting, except that instead of limiting the GridTime 3000's time in holdover, it sets up an inaccuracy threshold instead. This means that when the GridTime 3000 loses all of its synchronization sources and enters the holdover state, it will exit the holdover state and enter the out of sync state once the reported inaccuracy of its oscillator derived time reaches the user-defined inaccuracy threshold.

This setting can be used simultaneously with the holdover timeout setting, the GridTime 3000 will just transition from 'holdover' to 'out of sync' when either holdover timeout occurs or the maximum inaccuracy threshold is reached — whichever occurs first.

To set up a maximum inaccuracy threshold, select the **USE MAXIMUM INACCURACY** radio button. You must then enter the maximum inaccuracy threshold in nanoseconds in the **MAXIMUM INACCURACY (NS)** text box.

Figure 9-16. Maximum Inaccuracy Settings



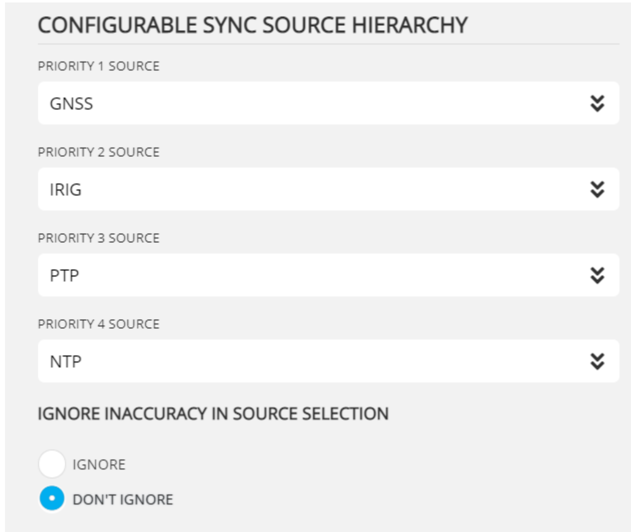
Important:
Once the GridTime 3000 enters the 'out of sync' state, it will trigger the out of sync alarm and will trigger the indication of out of sync on outputs that have a specific out of sync indicator, such as PTP clockClass. Other devices will be unlikely to synchronize to the GridTime 3000 when it is in this state, so if you are setting up holdover timeout or a maximum inaccuracy threshold, ensure you have other backup time sources for critical systems in your installation, or that your devices have their own holdover during an extended sync dropout.

If you need the GridTime 3000 to act as an indefinite time source during a GNSS dropout, disable holdover timeout and the maximum inaccuracy threshold and it will stay permanently in the 'holdover' state when all synchronization sources are lost until it regains a sync source and reenters the 'in sync' state.

6. **Setup the Sync Source Hierarchy**
   By default, when the GridTime 3000 has multiple sync sources available, it selects the most accurate sync source and synchronizes to this. If one or more sync sources are reporting the same accuracy, it applies the sync source hierarchy and synchronizes to the highest priority source available. This is the behavior when **IGNORE INACCURACY IN SOURCE SELECTION** is set to **DON'T IGNORE**, which is the default setting.

   If **IGNORE INACCURACY IN SOURCE SELECTION** is set to **IGNORE**, GridTime 3000 ignores the reported accuracy of all of the available sync sources and simply synchronizes to the highest priority source as per the sync source hierarchy.

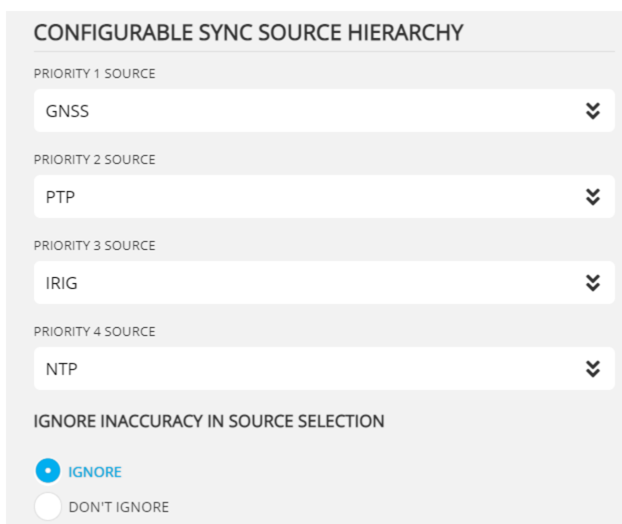
Figure 9-17. Sync Source Hierarchy Settings



Note: Microchip recommends leaving the configurable sync source hierarchy settings as their defaults unless you have a specific reason to modify the hierarchy and sync source selection behavior.

For example, if you have PTP and IRIG available as sync sources but the IRIG is falsely reporting an artificially high accuracy, you may set **IGNORE INACCURACY IN SOURCE SELECTION** to **IGNORE**, and configure PTP as the higher priority sync source as shown in the following image.
Note: The **IGNORE INACCURACY IN SOURCE SELECTION** will only apply to the reported inaccuracy, and will not change if the reported inaccuracy is reporting differently to the observed inaccuracy.

Figure 9-18. Ignore Inaccuracy in Source Selection Example



Note: For the device to change from the current sync source to an alternate sync source with a higher priority, the relative time between each of the sync sources must be less than one microsecond, otherwise the alternate sync source will be ignored.

7. **Save Settings**
   To write the settings to GridTime 3000, click **SAVE**

A **Saved!** notification appears on the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-19. Successful Save Notification

9.4 Provisioning the Admin Ethernet Port

This section describes how to provision the Admin Ethernet port for GridTime 3000.

The Admin Ethernet port settings are used to configure the IP addressing behavior and related settings for the GridTime 3000's Admin Ethernet port.

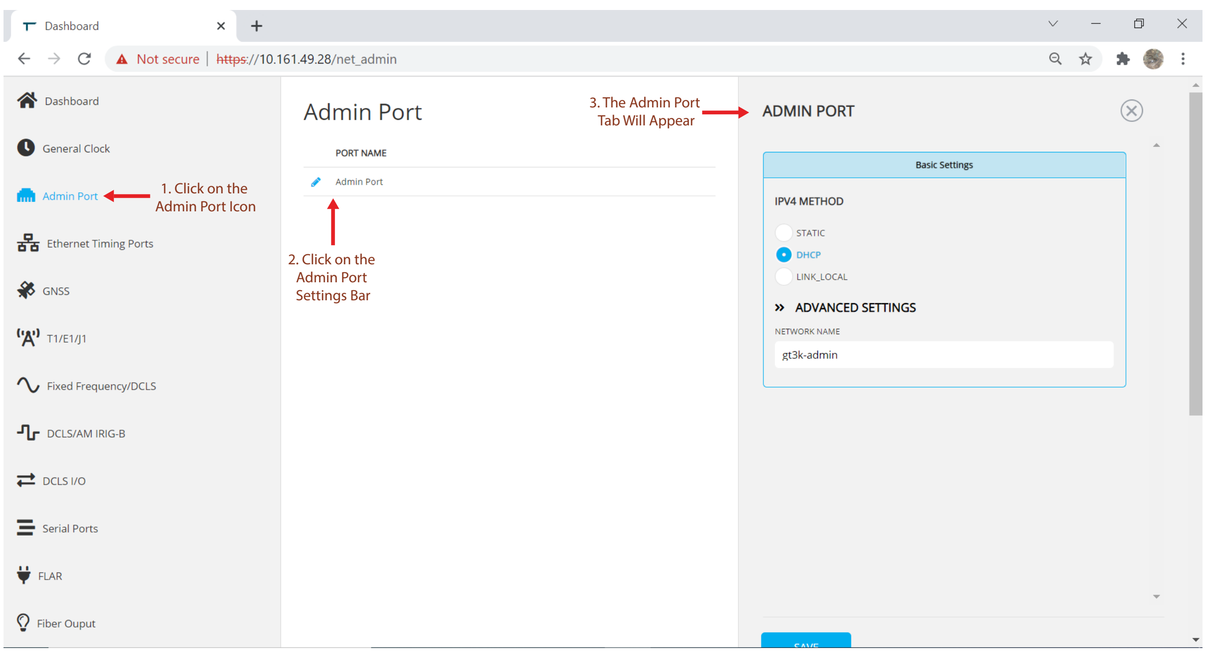
By default, the Admin Ethernet port is configured to use DHCP addressing, with a hostname of **gt3k-admin**.

All Admin Ethernet port settings can be modified, but do not necessarily need to be modified while provisioning the GridTime 3000. For example, if a DHCP server will not be available when operating the GridTime 3000 in the future, the addressing mode should be changed to static and a static address should be configured, but otherwise it should be left as DHCP (the default setting).

1. **Navigate to Admin Port Configuration Window**

   To navigate to the Admin Ethernet Port configuration window, on the left navigation pane, click **Admin Port**, and then click the **Admin Port** settings bar in the center of the screen. This opens the **ADMIN PORT** pane on the right.

   Figure 9-20. Admin Port Configuration



2. **Addressing Mode**

   Follow the instructions in one of the following three sections depending on whether you want to set up the port with a static, link local, or DHCP IP addressing mode:

   - Static IP Address
   - DHCP IP Address
   - Link Local IP Address

Note: The TCP port number 8080 is 'open' on the administrator port. This port number is used by the Microchip 'upgrade and log retrieval' tool and requires a valid username and password to be entered before traffic is allowed through the port.
The Microchip 'upgrade and log retrieval' tool is available on request in the event that an upgrade using the Clock Management Tool is unsuccessful.

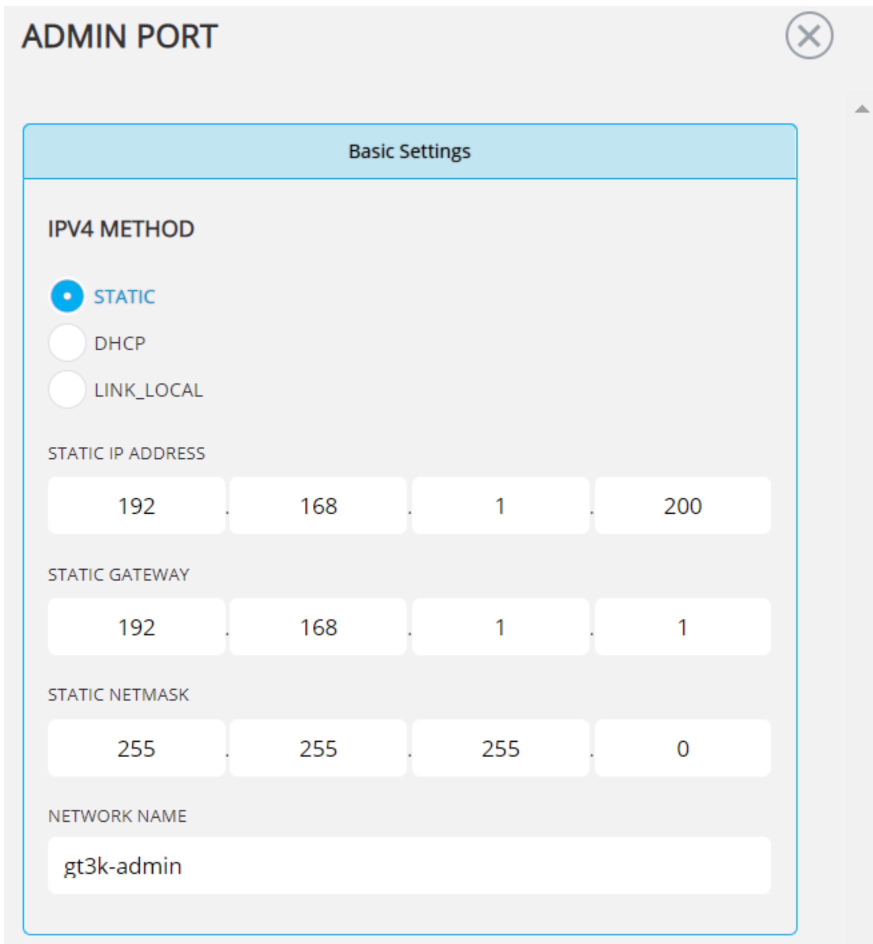
Note: Simultaneous configuration of multiple Carbon units through the USB-C admin port can cause unpredictable behavior because they use the same default IP address. It is recommended to configure one unit at a time for reliability.

9.4.1 Static IP Address

This section describes how to provision the Admin Ethernet Port with a static IP Address.

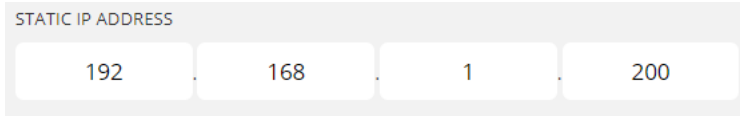
1. **Set IP Addressing Mode to Static**
   Under the **ADMIN PORT** pane on the right, under the **IPv4 Method** section, select the **STATIC** radio button. This expands the static IP addressing settings.

   Figure 9-21. Static IP Address Setting

2. **Set the Static IP Address**
   By default, the static IP address is 192.168.1.200. To change this address, enter a different valid IP address in the subnet your configuration PC is using.

Figure 9-22. Default Static IP Address

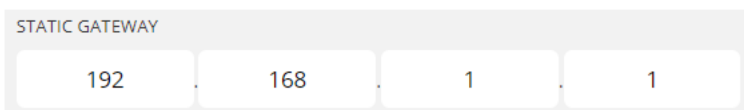


Important:
Make sure that the IP address you choose is in subnet with your PC prior to saving the settings. If you are accessing the CMT through the Admin Ethernet port, once the address is set, you will have to log back into the CMT using the new address as your URL. If the new address is out of subnet with your PC's port, you will not be able to access the CMT through the Admin Ethernet port until you change your PC's IP address to be in subnet.

If this happens by mistake, you can also use the Admin USB-C port to log back into the CMT and change the IP address of the Admin Ethernet port to an in subnet address.

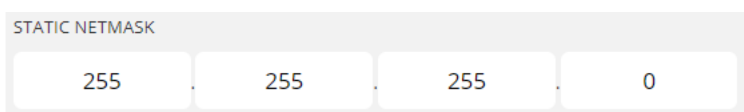
3. **Set Gateway**
   By default, the gateway address is set to 192.168.1.1. If a gateway is present in your network, modify the static gateway setting to your gateway address. If no gateway is present, configure the static gateway address as 0.0.0.0.

Figure 9-23. Default Static Gateway Address



4. **Set Netmask**
   By default, the netmask is set to 255.255.255.0. If your network requires a different netmask, modify the static netmask setting as required. By combining the netmask and static IP address you have configured, you can validate that your network and host addresses are correct for your network.

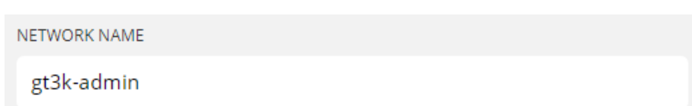
Figure 9-24. Default Static Netmask



5. **Set Network Name**
   To modify the network name (if required), type the new name in the **NETWORK NAME** text box. This field will set the hostname of the port.

   By default, the network name is **gt3k-admin**.

Figure 9-25. Default Network Name



6. **Save Settings**
   To write the settings to GridTime 3000, click **SAVE**.

A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

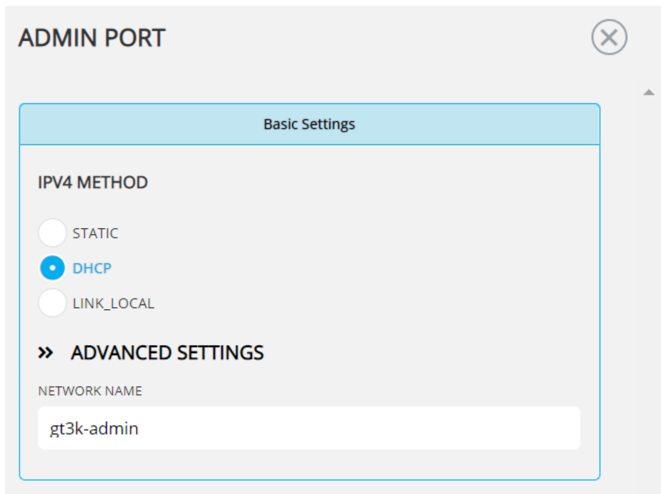
Figure 9-26. Successful Save Notification

9.4.2 DHCP IP Address

This section describes how to provision the Admin Ethernet Port with a DHCP IP Address.

1. **Set IP Addressing Mode to DHCP**
   By default, the IP addressing mode of the Admin Ethernet port is set to DHCP. If set to another mode, to set it back to DHCP, under the **ADMIN PORT > Basic Settings > IPv4 Method** section, select the **DHCP** radio button.

   Figure 9-27. DHCP Address Setting

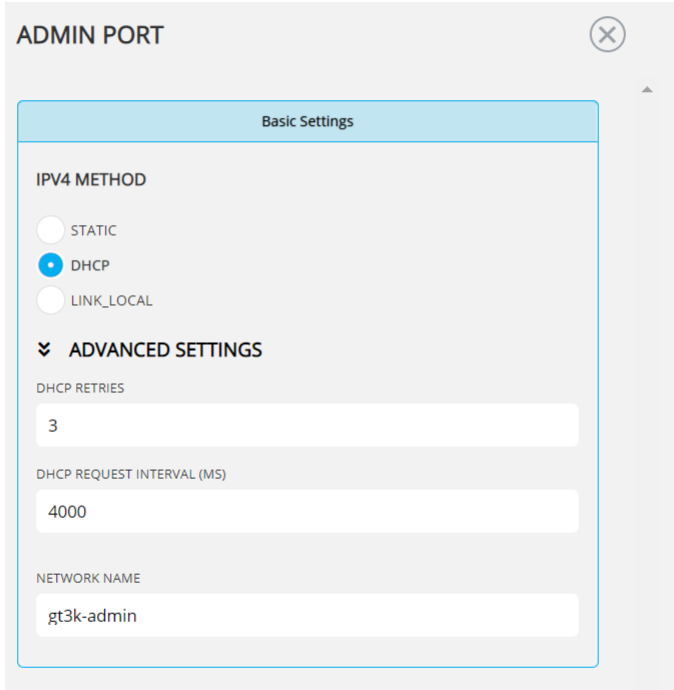
   Important:
   Make sure that prior to saving with the addressing mode changed to DHCP, you either have a DHCP server available or a PC Ethernet port that can be set to a static link local IP address in subnet with the Admin Ethernet Port's address. As soon as the addressing mode has been saved as DHCP, the Admin Ethernet port will attempt to get a new IP address from a DHCP server, and if this fails, it will fall back to a link local address.

   If you are accessing the CMT through the Admin Ethernet port, any time the IP address of the port changes, you will have to log back into the CMT using the new address as your URL. If the new address is out of subnet with your PC's port, you will be unable to access the CMT through the Admin Ethernet port until you change your PC's IP address to be in subnet.

   If this happens by mistake, you can also use the Admin USB-C port to log back into the CMT and change the IP address of the Admin Ethernet port to an in subnet address.

2. **Advanced Settings**
   Click **>> ADVANCED SETTINGS** to reveal the advanced port settings. These settings should not be modified in most cases.

Figure 9-28. DHCP Advanced Settings



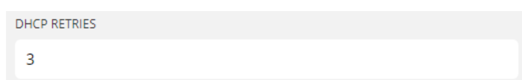
a. **DHCP Retries**

To gain an IP address over DHCP, the port sends DHCP discovery messages into the network expecting a DHCP server to respond. If it sees no response after the first message, it will send another discovery message — this is known as a DHCP retry.

The DHCP Retries setting determines how many DHCP retries the port will make before falling back to a link local IP Address.

To modify the number of DHCP retries the port will make, enter the new number in the **DHCP RETRIES** text box, the default value is 3.

Figure 9-29. DHCP Retry Setting



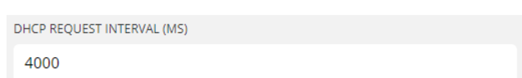
b. **DHCP Request Interval**

The DHCP Request Interval sets the base time between DHCP discover attempts in milliseconds. The time between DHCP discover messages is multiplied by two between the first message and the second (first DHCP retry), then the time is multiplied by two again for the following message and so on up to a limit of 64 seconds.

If a different base interval is required, enter the interval in the **DHCP REQUEST INTERVAL (MS)** text box.

The default DHCP Request Interval is 4000 ms (4 seconds).

Figure 9-30. DHCP Request Interval Settings



3. **Set Network Name**

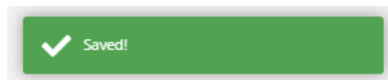
To enter a unique hostname (if required) for the admin Ethernet port, type the name in the **NETWORK NAME** text box. This field will set the hostname of the port.

By default, the hostname is **gt3k-admin**.

Figure 9-31. Default Network Name

4. **Save Settings**
   To write the settings to GridTime 3000, click **SAVE**. A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-32. Successful Save Notification

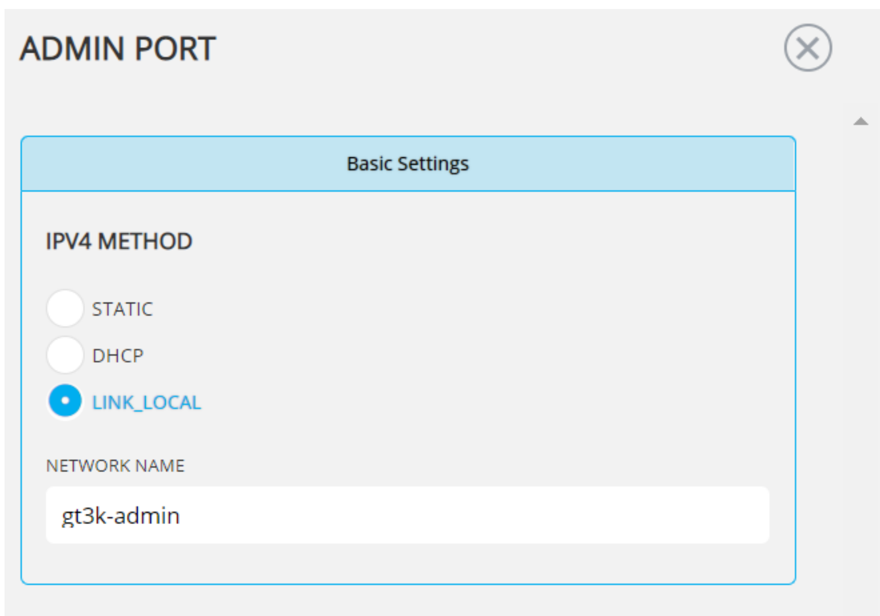


9.4.3 Link Local IP Address

This section describes how to provision the Admin Ethernet Port with a Link Local IP Address.

1. **Set IP Addressing Mode to Link Local**
   Under the **ADMIN PORT > Basic Settings > IPv4 Method** section, select the **LINK_LOCAL** radio button.

Figure 9-33. Link Local Address Setting



Important:
Make sure that prior to setting the port to a link local addressing mode that you have a PC Ethernet port that can be set to a static link local IP address in subnet with the Admin Ethernet Port's address. As soon as the addressing mode has been saved as link local, the Admin Ethernet port will receive a new a link local address.

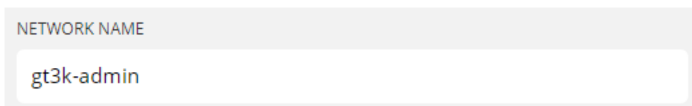
If you are accessing the CMT through the Admin Ethernet port, any time the IP address of the port changes you will have to log back into the CMT using the new address as your URL. If the new address is out of subnet with your PC's port, you will be unable to access the CMT through the Admin Ethernet port until you change your PC's IP address to be in subnet.

If this happens by mistake, you can also use the Admin USB-C port to log back into the CMT and change the IP address of the Admin Ethernet port to an in subnet address.

2. **Set Network Name**
   To modify the network name (if required), type the new name in the **NETWORK NAME** text box. This field will set the hostname of the port.

   By default, the network name is **gt3k-admin**.

Figure 9-34. Default Network Name



3. **Save Settings**
   To write the settings to GridTime 3000, click **SAVE**.

   A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-35. Successful Save Notification

9.5 Provisioning the Ethernet Ports

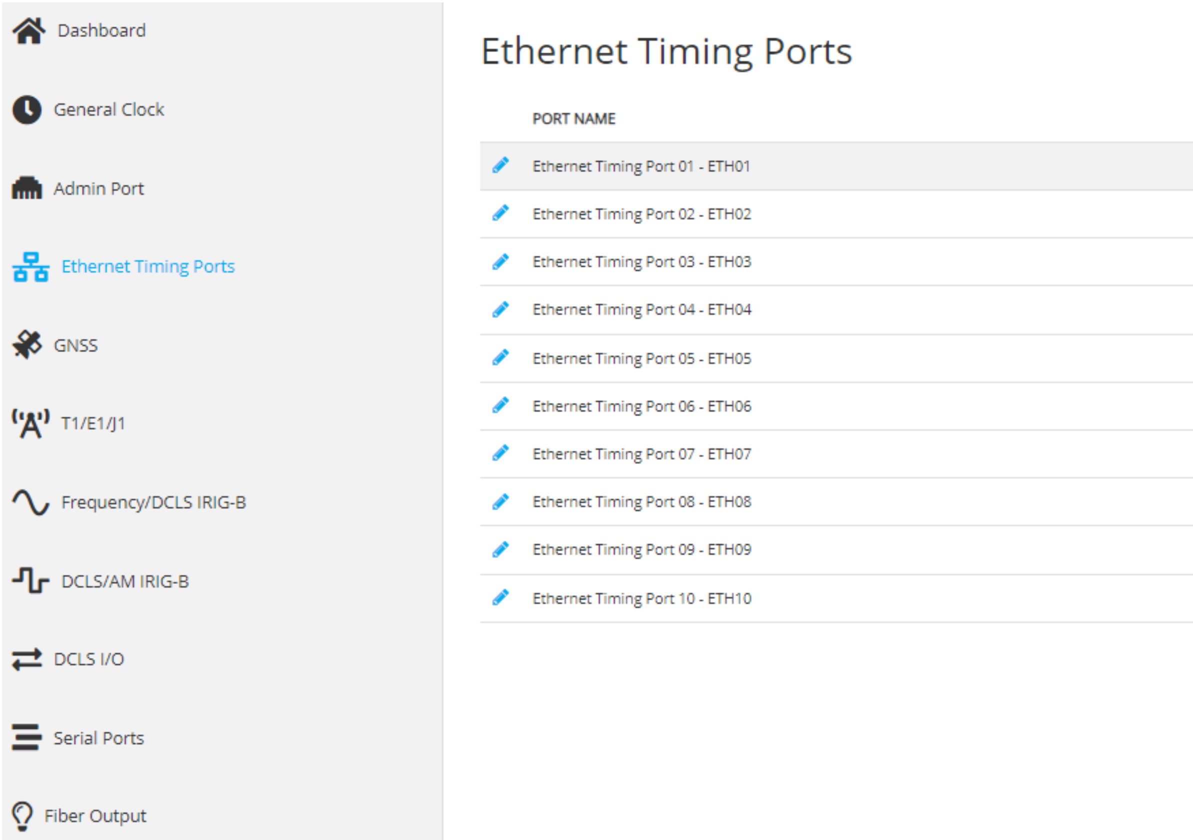
This section describes how to provision the Ethernet ports of GridTime 3000.

The Ethernet ports on GridTime 3000 can be configured as Network Time Protocol (NTP) clients and servers, and Precision Time Protocol (PTP) timeReceivers and timeTransmitters. PTP can also be run over two ports simultaneously as a Parallel Redundancy Protocol (PRP) pair.

Prior to configuring the NTP or PTP settings, basic port network settings should be set up according to the following steps:

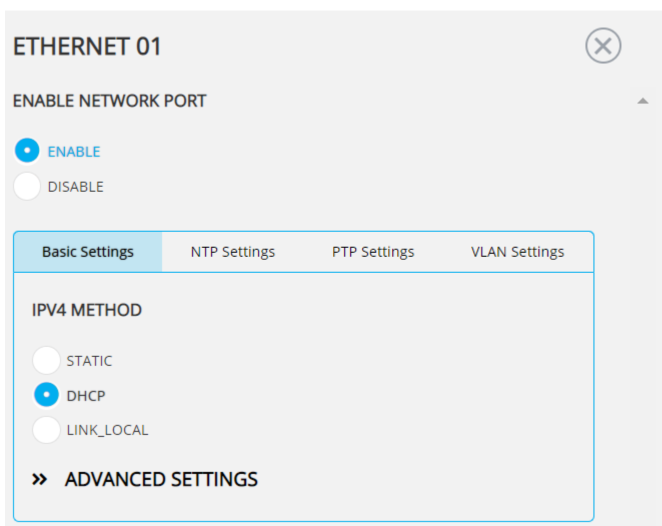
1. **Navigate to Ethernet Port Configuration Window**
   To navigate to the Ethernet port configuration window, on the left navigation pane, click **Ethernet Timing Ports**, and then click the settings bar corresponding to the port. The settings for the corresponding port is displayed on the right pane.

Figure 9-36. Ethernet Timing Ports



2. **Enable Port**
   To enable a port, select the **ENABLE** radio button. This brings up the relevant port settings.

Figure 9-37. Ethernet Timing Port Settings



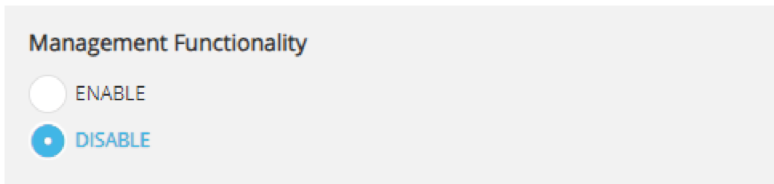
3. **Set up the Addressing Mode**
   Follow the instructions in one of the following three sections depending on whether you want to set up the port with a static, DHCP, or link local IP Addressing mode:
   – Static IP Address

- DHCP IP Address
- Link Local IP Address

4. **Enable Management Functionality**
By enabling the management functionality, all timing ports can provide access to the Configuration Management Tool (CMT) and Simple Network Management Protocol (SNMP) while continuing to provide timing services on the same port. Additionally, these ports can route SNMP and SYSLOG notifications.

Note: All management-capable ports, including Admin and USB ports, must have unique IPv4 addresses. The system is designed to prevent configurations that would allow duplicate addresses.

Figure 9-38. Enable Management Functionality



Note: Management functionality settings are disabled by default.

PRP and VLANs
- To provision PRP on the port, see Provisioning PRP.
- To provision VLAN use on the port, see Provisioning VLAN Settings.

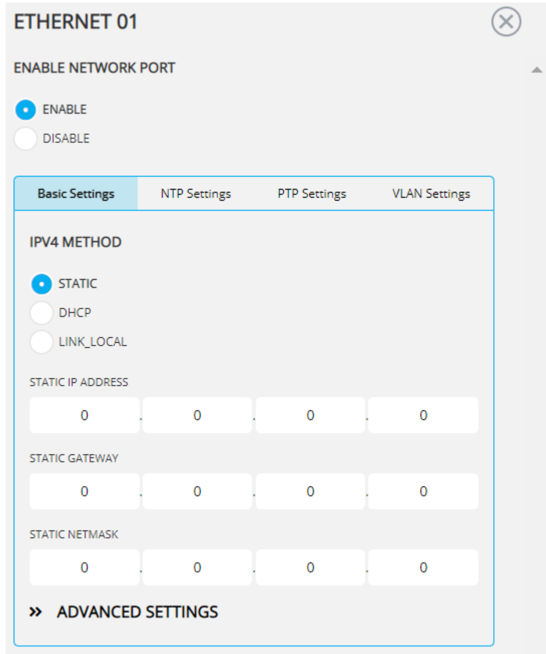
5. **PTP and NTP**
- To provision PTP on the port, see Provisioning PTP.
- To provision NTP on the port, see Provisioning NTP.

9.5.1 Static IP Address

This section describes how to provision an Ethernet port with a static IP Address.

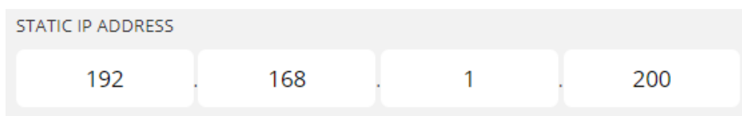
1. **Select Static for IPv4 Method**
Under the **Basic Settings** tab, in the **IPV4 METHOD** section, select the **STATIC** radio button, causing the static IP addressing settings to appear.

Figure 9-39. Static IPv4 Settings



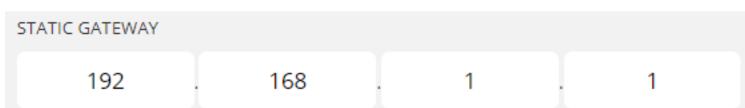
2. **Set IP Address**
   Enter a different valid IP address in the subnet your configuration PC is using.

Figure 9-40. Static IP–Address Setting



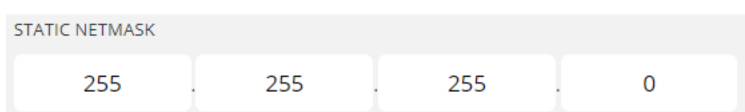
3. **Set Gateway**
   If a gateway is present in your network, enter the address of your gateway. If no gateway is present the static gateway address can be configured as 0.0.0.0.

Figure 9-41. Static IP–Gateway Settings



4. **Set Netmask**
   Enter the netmask used by your network. By combining the netmask and static IP address you have configured, validate that your network and host addresses are correct for your network.

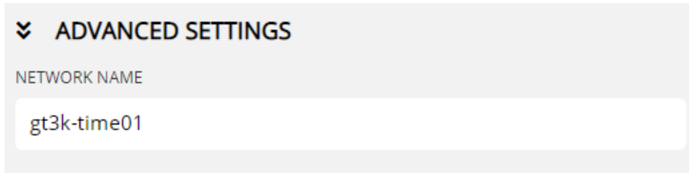
Figure 9-42. Static IP–Netmask Settings



5. **Advanced Settings**
   If required, the network name can be modified. To do this, click the **ADVANCED SETTINGS** drop down and in the **NETWORK NAME** text box, type the new name. This field sets the hostname of the port.

By default, the network name is 'gt3k-time[port number]'.

Figure 9-43. Network Name Settings

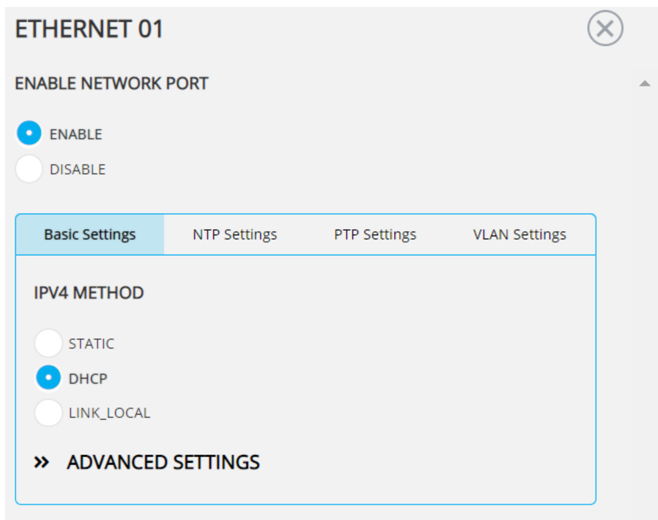


9.5.2 DHCP IP Address

This section describes how to provision an Ethernet port with a DHCP IP Address.

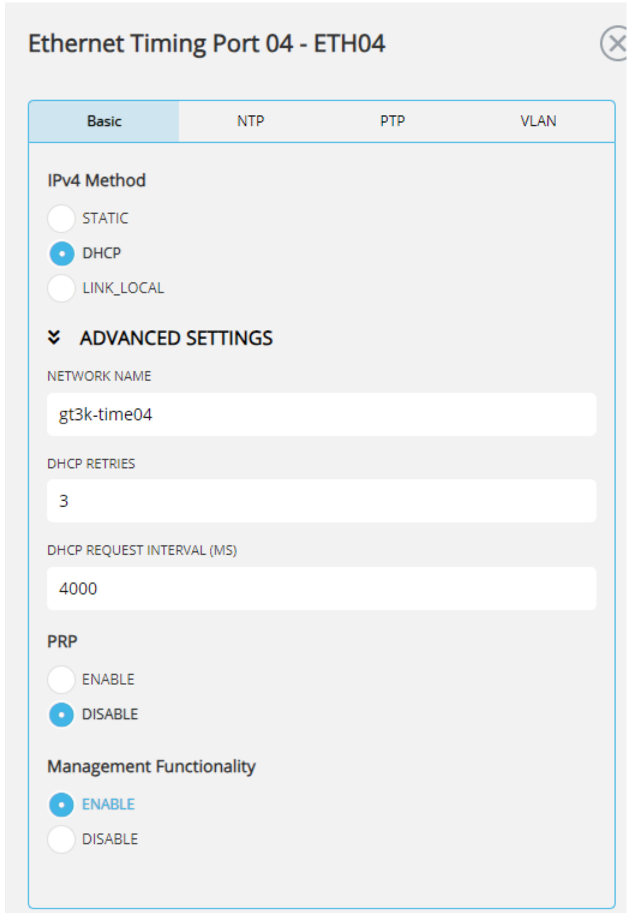
1. **Select DHCP for IPv4 Method**
   Under the **Basic Settings** tab, in the **IPV4 METHOD** section, select the **DHCP** radio button. This should be selected by default.

   Figure 9-44. DHCP Settings



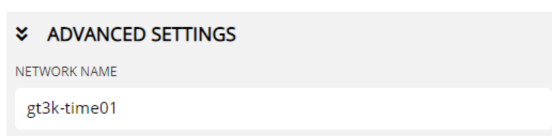
2. **Advanced Settings**
   To reveal the advanced port settings, click the **ADVANCED SETTINGS** drop down.

Figure 9-45. Advanced Settings



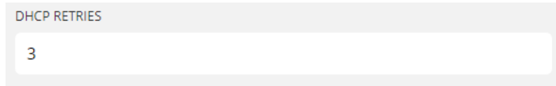
a. **Network Name**
   If required, the network name can be modified. To do this, in the **NETWORK NAME** text box, type the new name. This field sets the hostname of the port.
   By default, the network name is 'gt3k-time[port number]'.

Figure 9-46. DHCP–Network Name Settings



b. **DHCP Retries**
   To gain an IP address over DHCP, the port sends DHCP discovery messages into the network expecting a DHCP server to respond. If there is no response after the first message, it sends another discovery message — this is known as a DHCP retry.
   The DHCP retries setting determines how many DHCP retries the port makes before falling back to a link local IP Address.
   To modify the number of DHCP retries the port will make, in the **DHCP RETRIES** text box, enter the new number. The default value is 3.

Figure 9-47. DHCP Retry Setting



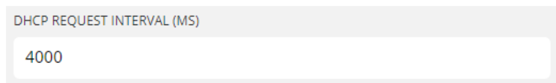
c. **DHCP Request Interval**

The DHCP Request Interval sets the base time between DHCP discover attempts in milliseconds. The time between DHCP discover messages is multiplied by two between the first message and the second (first DHCP retry), then the time is multiplied by two again for the following message, and so on up to a limit of 64 seconds.

If a different base interval is required, in the **DHCP REQUEST INTERVAL (MS)** text box, enter the interval.

The default DHCP Request Interval is 4000 ms (4 seconds).

Figure 9-48. DHCP Request Interval Settings



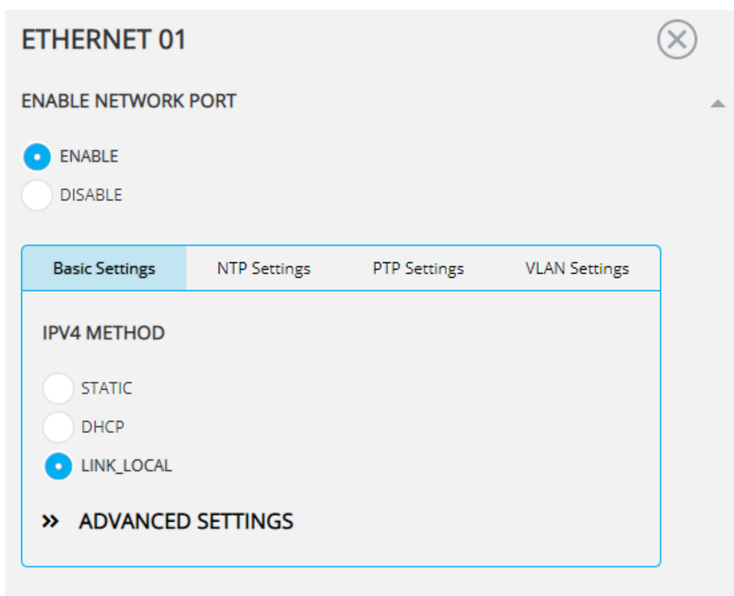
9.5.3 Link Local IP Address

This section describes how to provision an Ethernet port with a link local IP Address.

1. **Select Link Local for IPv4 Method**

   Under the **Basic Setting**s Settings tab, in the **IPV4 METHOD** section, select the **LINK_LOCAL** radio button, causing the static IP addressing settings to appear.

Figure 9-49. Link Local IPV4 Settings

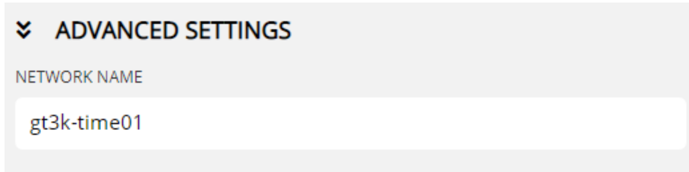


2. **Network Name**

   If required, the network name can be modified. To do this, click the **ADVANCED SETTINGS** drop down and in the **NETWORK NAME** text box, type the new name. This field sets the hostname of the port.

   The default network name will be 'gt3k-time[port number]'.

Figure 9-50. Network Name Settings

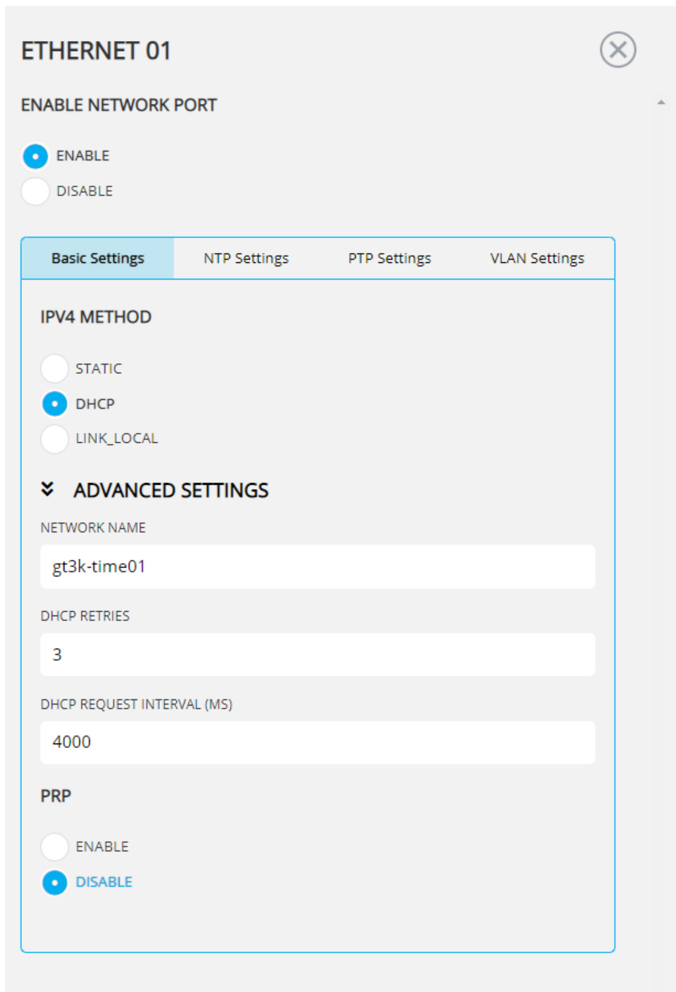


9.5.4 Provisioning PRP

This section describes how to provision PRP on a GridTime 3000 Ethernet Port.

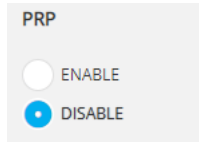
1. **Reveal Advanced Settings**
   To reveal the advanced port settings, click the **ADVANCED SETTINGS** drop down.

Figure 9-51. Advanced Settings



2. **Enable PRP**
   Select **ENABLE** from the PRP radio buttons.

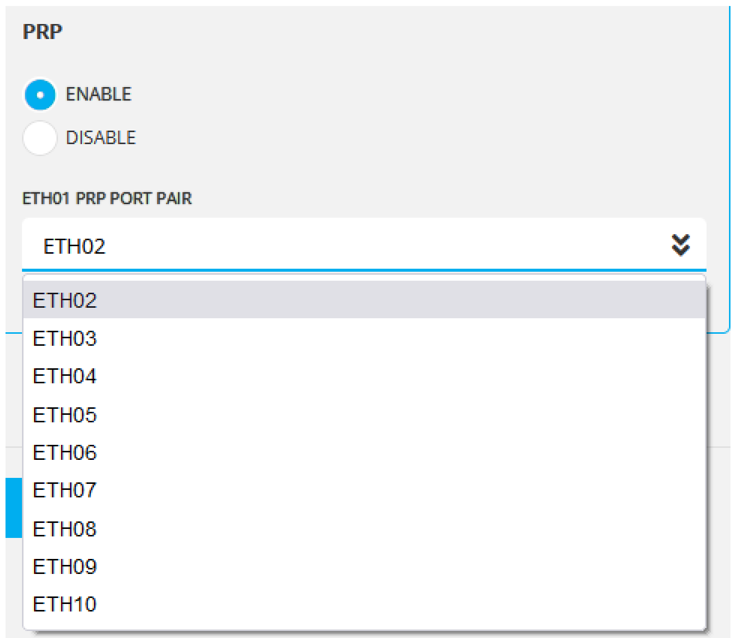
Figure 9-52. PRP Enable/Disable



This makes the current port you are configuring a PRP LAN A port. All PTP traffic coming from this port is duplicated on the port you select as the PRP LAN B port.

3. **Select PRP LAN B Port**
   To configure a port to be the PRP LAN B port, from the **PRP PORT PAIR** drop down, select the port name that you intend to set as PRP LAN B port.

Figure 9-53. Selecting the PRP LAN B Port



Tip: Although the GridTime 3000 allows any pair of ports to be configured as PRP LAN A and PRP LAN B, this is not recommended by Microchip Technology or by IEC-62439-3:2016. PRP LAN A should be either immediately above PRP LAN B, or directly to the left of PRP LAN B.

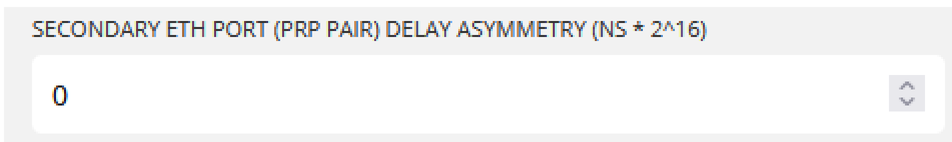
Note: Once you have selected a port as the PRP LAN B port, no configuration is required on the PRP LAN B port you have selected. All settings you have configured on the PRP LAN A port will automatically be used on the PRP LAN B port, and all previously configured settings on the PRP LAN B port will be ignored, although they are still accessible and modifiable.

Note: The PRP LAN B port will be marked with a warning as shown.

Figure 9-54. Warning on PRP LAN B Setting

Note: Configure Port B PTP Delay Asymmetry (if applicable)
If the delay asymmetry of the PRP Port B is known and the user is configuring PRP to use PTP, the delay asymmetry can be entered under the **PTP** tab of Eth 01, in the **SECONDARY ETH PORT (PRP PAIR) DELAY ASYMMETRY (NS * 2^16)** text box as shown in the following figure.

Figure 9-55. Secondary Ethernet Port Delay Asymmetry



4. **Save Settings**
   To write the settings to the GridTime 3000, click SAVE.

A **Saved!** notification appears in the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

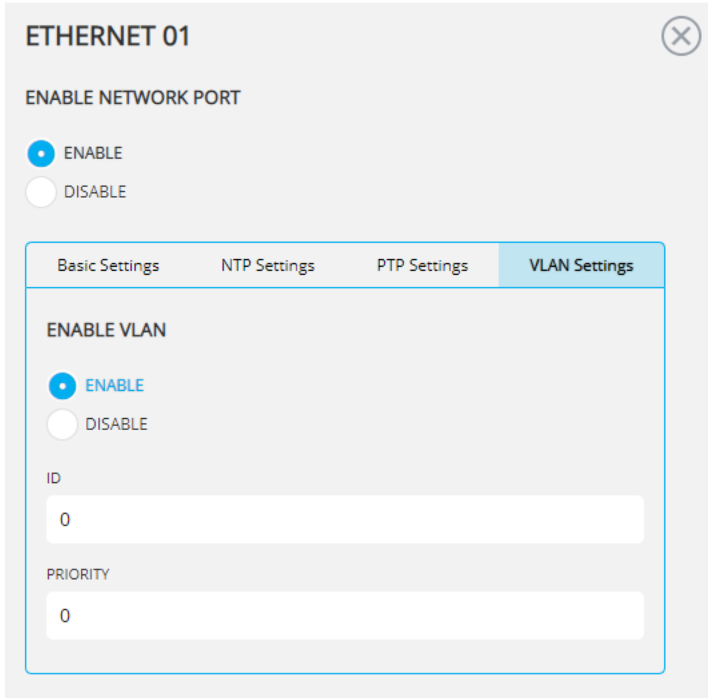
Figure 9-56. Successful Save Notification

9.5.5 Provisioning VLAN Settings

This section describes how to provision VLAN use on a GridTime 3000 Ethernet Port.

1. **Enable VLAN Tagging**
   To enable VLAN tagging, navigate to the port's **VLAN Settings** tab and from the **ENABLE VLAN** radio buttons, select **ENABLE**.

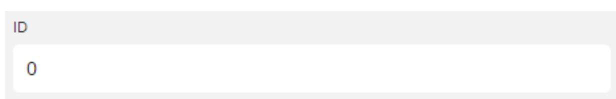
Figure 9-57. Enable VLAN Settings



Once enabled, VLAN tags are applied to all outgoing traffic from the port including NTP and PTP.

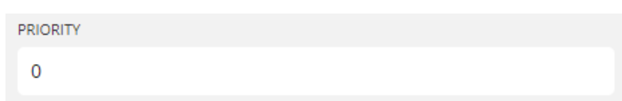
2. **Set VLAN ID**
   In the **ID** text box, type the VLAN ID of your network. VLAN IDs in the range of 0-4094 are supported and a VLAN ID of 0 will disable VLAN tagging.

Figure 9-58. VLAN ID Setting



3. **Set VLAN Priority**
   Type the priority you want to be included in the VLAN tags on outgoing traffic into the **PRIORITY** text box. Priority values in the range of 0-7 are supported.

Figure 9-59. VLAN Priority Setting



4. **Save Settings**.

   To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-60. Successful Save Notification

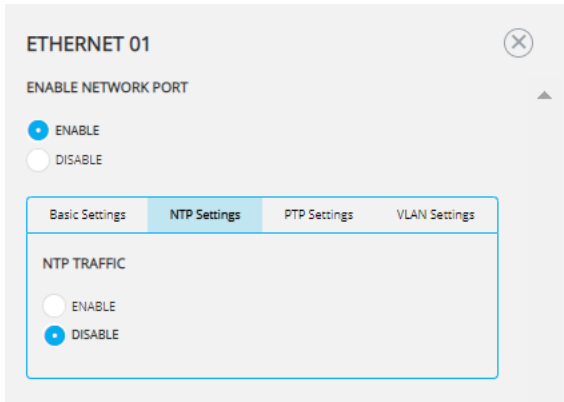
9.5.6 Provisioning NTP

This port describes how to setup a GridTime 3000 Ethernet port as an NTP server or client.

Note: Both an NTP Server/Client and PTP timeTransmitter/timeReceiver can be simultaneously set up on a GridTime 3000 Ethernet Port.

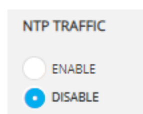
1. **Navigate to NTP Sub Tab**
   To navigate to the PTP sub tab, in the port's configuration window, click the **NTP Settings** tab.

   Figure 9-61. NTP Settings

2. **Enable NTP Traffic**
   From the **NTP TRAFFIC** radio buttons, select **ENABLE**.

   Figure 9-62. Enable NTP Traffic

   This reveals the NTP settings for the port.
3. Follow the instructions in one of these following sections for the next steps:
   – NTP Client
   – Listening Server
   – Broadcast Server
   – Multicast Server
   – Broadcast and Multicast Server

   The supported NTP modes are NTP Client, Listening Server, Broadcast Server, Multicast Server, and Broadcast and Multicast Server.

   The NTP Client can poll a server for the time, and can also sync to NTP broadcasts and multicasts it receives.

   A Listening NTP server is quiet until it receives a client request, and to which it responds to with the appropriate timestamps upon reception.

   The other server modes behave the same as the listening server when requests are received, but also sends NTP multicasts and broadcasts into the network at user-defined intervals.

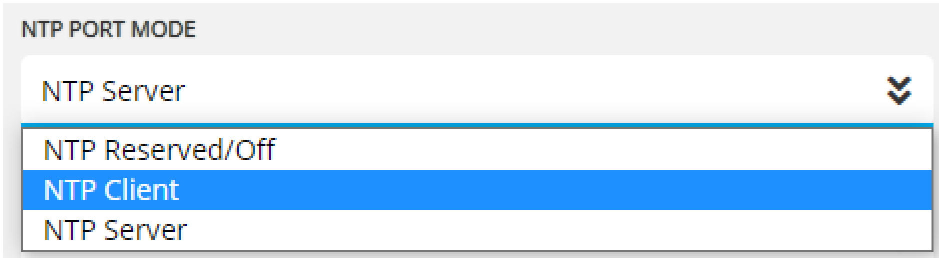
9.5.6.1 NTP Client

This section describes how to provision an NTP client.

1. **Select NTP Client for NTP Port Mode**

From the **NTP PORT MODE** drop-down list, select **NTP Client**.

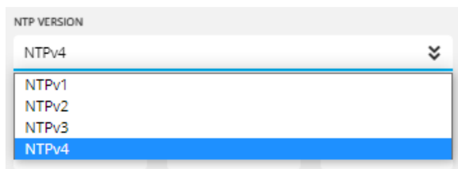
Figure 9-63. NTP Port Mode Settings



This will reveal additional SNTP client related settings.

2. **Select NTP Version**
   From the **NTP VERSION** drop-down list, select the NTP version to be used by the NTP client. By default, this is set to **NTPv4**.

   Figure 9-64. NTP Version Settings

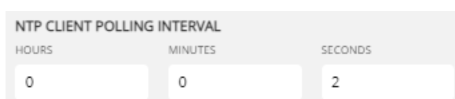


3. **Enter Client Polling Interval**
   Enter the NTP client's polling interval in the **NTP CLIENT POLLING INTERVAL** time boxes.

   This interval determines how frequently the NTP client sends unicast NTP requests to the NTP Server IP Address specified by the **NTP SERVER IP ADDRESS** setting.

   The supported range for this setting is 0-24 hours. By default it is set to 2 seconds.

   Figure 9-65. Client Polling Interval Settings



Note: NTP client to server polling is unicast so relies on the NTP client port's IP address being in the same subnet as the NTP server's IP address. Review the network settings of the port under configuration to ensure this is the case.

Tip: If the NTP client should not poll an NTP server and instead synchronize only to broadcast/multicast from an NTP server, this setting should be configured as '0' in all fields, meaning that the port will never send unicast requests to a server.

4. **Accept or Decline Broadcast Messages**
   Select whether the NTP client will accept or ignore broadcast messages from an NTP server using the **CLIENT BROADCAST MESSAGES** radio buttons.

   If **ACCEPT** is selected, the NTP client synchronizes to broadcast the messages it receives, if DECLINE is selected, broadcasts are ignored.

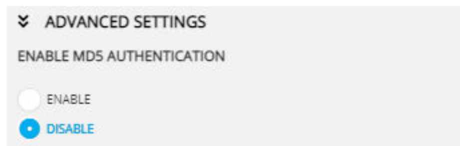
Figure 9-66. Accept/Decline Broadcast Messages

5. **Enter NTP Server IP Address**
   Enter the IP address of the NTP server that unicast NTP requests will be sent to.

   Figure 9-67. IP Address Setting

6. **Advanced Settings**
   Click the **ADVANCED SETTINGS** drop-down list to reveal the advanced NTP settings.

   Figure 9-68. Advanced NTP Settings

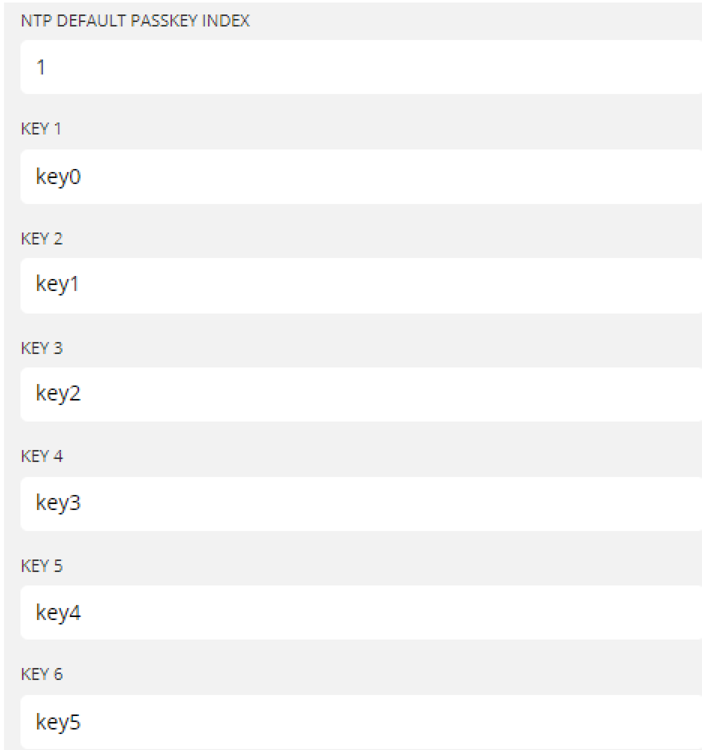


7. **Enable MD5 Authentication**
   If the NTP server on the network is using MD5 authenticated NTP communication, select the **ENABLE** radio button under the **ENABLE MD5 AUTHENTICATION** section. This reveals the MD5 Authentication Key text boxes and authenticates the incoming NTP packets.

   To set the hash key, change one or more of the KEY text boxes, and change the **NTP DEFAULT PASSKEY INDEX** to the index of the key you have changed.

   In the following example setting, **NTP DEFAULT PASSKEY INDEX** is set to 1 and will enable the use of **key0** as the hash key.

Figure 9-69. MD5 Authentication Key Settings



8. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE.**
   A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

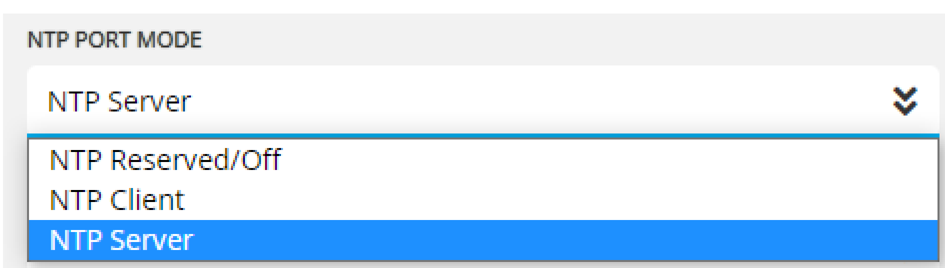
Figure 9-70. Successful Save Notification

9.5.6.2 Listening Server

This section describes how to provision a listening NTP server.

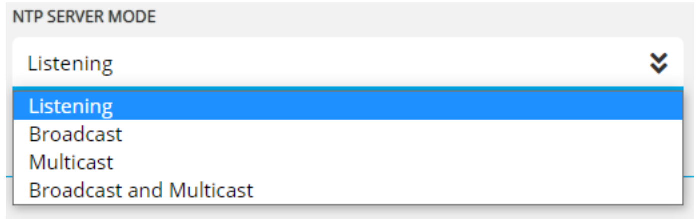
1. **Select NTP Server for the NTP Port Mode**
   From the **NTP PORT MODE** drop-down list, select **NTP Server**.

Figure 9-71. NTP Port Mode Settings



2. **Select Listening Server for the NTP Server Mode**
   From the **NTP SERVER MODE** drop-down list, select **Listening**.

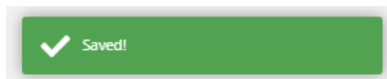
Figure 9-72. NTP Server Mode Settings



3. Ensure that the port's IP address is in the same subnet as the NTP clients that will be making NTP requests to the server.
4. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE.**

   A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-73. Successful Save Notification

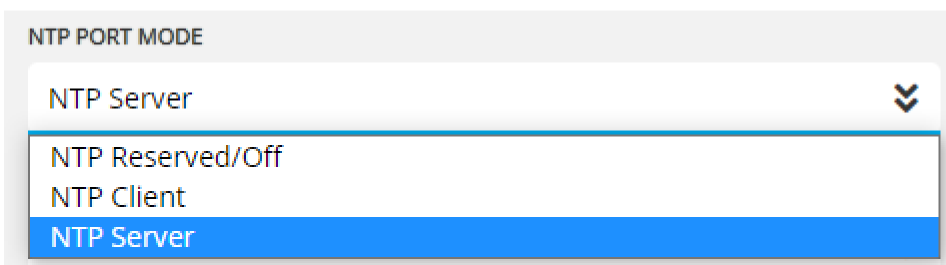


9.5.6.3 Broadcast Server

This section describes how to provision a broadcast NTP Server

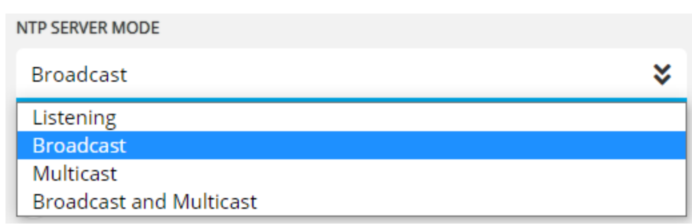
1. **Select NTP Server for the NTP Port Mode**
   From the **NTP PORT MODE** drop-down list, select **NTP Server**.

Figure 9-74. NTP Port Mode Settings



2. **Select Broadcast for the NTP Server Mode**
   From the **NTP SERVER MODE** drop-down list, select **Broadcast**.

Figure 9-75. NTP Server Mode Settings

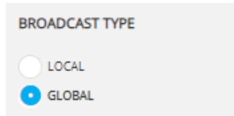


3. **Local or Global Broadcasts**
   Choose whether broadcasts are local or global from the **BROADCAST TYPE** radio buttons. The setting changes between using the global broadcast address or a local broadcast address. The global broadcast address is 255.255.255.255, while the local broadcast address depends on the network settings.

For example, if the port's IP is 192.168.1.1 and the netmask is 255.255.255.0, then the local broadcast address will be 192.168.1.255.

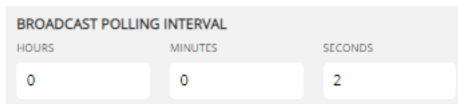
By default, the broadcast type is set to **GLOBAL**.

Figure 9-76. Broadcast Type Setting



4. **Enter Broadcast Interval**
   Enter the broadcast interval into the **BROADCAST POLLING INTERVAL** time boxes. This setting determines how frequently the port sends the broadcast NTP messages into the network. The supported interval range is 0-24 hours, the default setting is 2 seconds.

Figure 9-77. Client Polling Interval Settings



5. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE.**

   A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

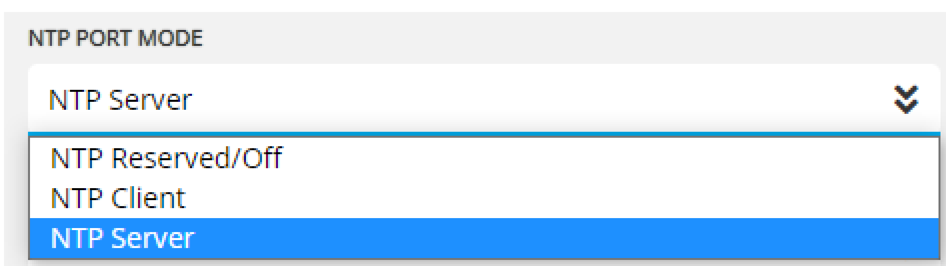
Figure 9-78. Successful Save Notification

9.5.6.4 Multicast Server

This section describes how to provision a multicast NTP server.

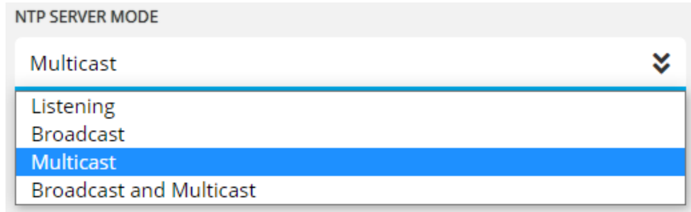
1. **Select NTP Server for NTP Port Mode**
   From the **NTP PORT MODE** drop-down list, select **NTP Server**.

Figure 9-79. NTP Port Mode Settings



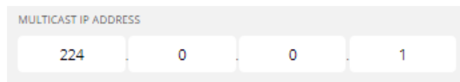
2. **Select Multicast Server for NTP Server Mode**
   From the **NTP SERVER MODE** drop-down list, select **Multicast**.

Figure 9-80. NTP Server Mode Settings



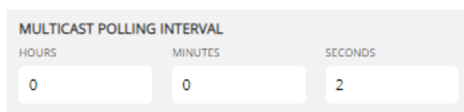
3. **Enter Multicast IP Address**
   Enter the IP Address for the port to send multicasts NTP messages to. If the entered address is within the reserved multicast address range (224.0.0.0–239.255.255.255), the message will also use a multicast destination MAC address, otherwise it will use the broadcast MAC address.

Figure 9-81. Multicast IP Address Setting



4. **Enter Multicast Interval**
   Enter the broadcast interval into the **MULTICAST POLLING INTERVAL** time boxes. This setting determines how frequently the port sends multicast NTP messages into the network. The supported interval range is 0-24 hours, the default setting is 2 seconds.

Figure 9-82. Multicast Polling Interval Setting



5. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE.**

   A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

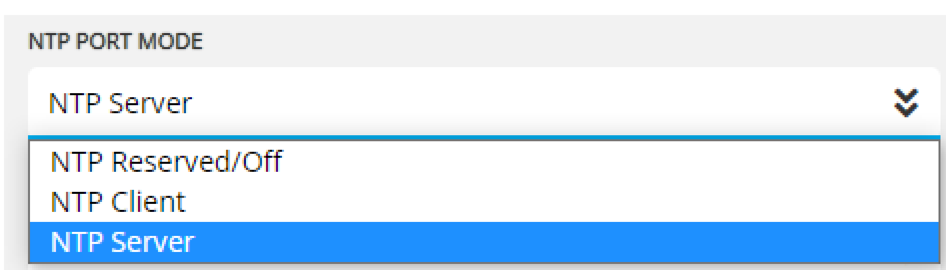
Figure 9-83. Successful Save Notification

9.5.6.5 Broadcast and Multicast Server

This section describes how to provision a broadcast and multicast NTP server.

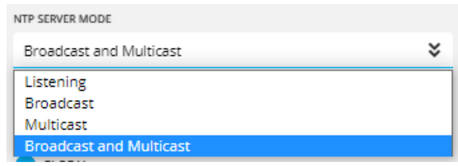
1. **Select NTP Server for NTP Port Mode**
   From the **NTP PORT MODE** drop-down list, select **NTP Server**.

Figure 9-84. NTP Port Mode Settings



2. **Select Broadcast and Multicast Server for NTP Server Mode**
   From the **NTP SERVER MODE** drop-down list, select **Broadcast and Multicast**.

   Figure 9-85. NTP Server Mode Settings

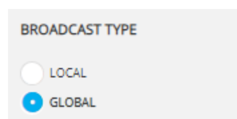
   

   This reveals additional SNTP client related settings.
3. **Local or Global Broadcasts**
   Choose whether broadcasts are local or global from the **BROADCAST TYPE** radio buttons. The setting changes between using the global broadcast address or a local broadcast address. The global broadcast address is 255.255.255.255, while the local broadcast address depends on the network settings.

   For example, if the port's IP is 192.168.1.1 and the netmask is 255.255.255.0, then the local broadcast address will be 192.168.1.255.

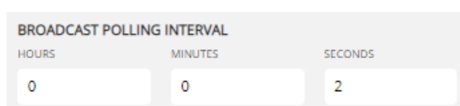
   By default, the broadcast type is set to **GLOBAL**.

   Figure 9-86. Broadcast Type Setting

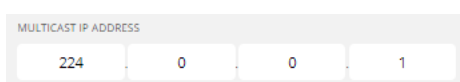
4. **Enter Broadcast Interval**
   Enter the broadcast interval into the **BROADCAST POLLING INTERVAL** time boxes. This setting determines how frequently the port sends the broadcast NTP messages into the network. The supported interval range is 0-24 hours, the default setting is 2 seconds.

   Figure 9-87. Broadcast Polling Interval Settings

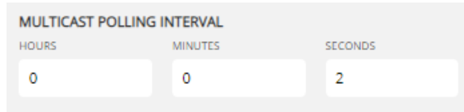
5. **Enter Multicast IP Address**
   Enter the IP Address for the port to send multicasts NTP messages to. If the entered address is within the reserved multicast address range (224.0.0.0–239.255.255.255), the message will also use a multicast destination MAC address, otherwise it will use the broadcast MAC address.

   Figure 9-88. Multicast IP Address Setting

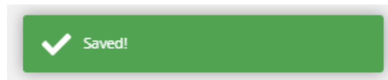
6. **Enter Multicast Interval**
   Enter the broadcast interval into the **MULTICAST POLLING INTERVAL** time boxes. This setting determines how frequently the port sends multicast NTP messages into the network. The supported interval range is 0-24 hours, the default setting is 2 seconds.

Figure 9-89. Multicast Polling Interval Setting



7. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE.**
   A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-90. Successful Save Notification



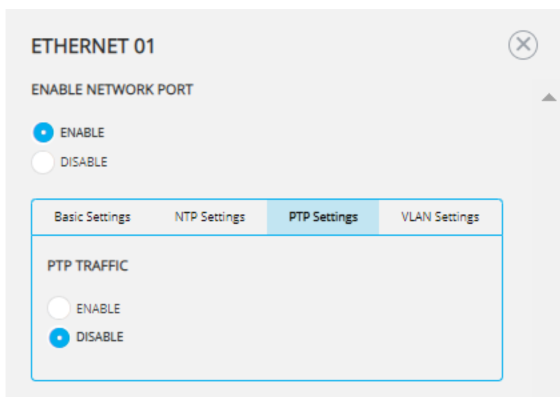
9.5.7 Provisioning PTP

This section describes how to provision PTP on the GridTime 3000.

Note: Both an NTP server/client and PTP timeTransmitter/timeReceiver can be simultaneously set up on a GridTime 3000 Ethernet Port.

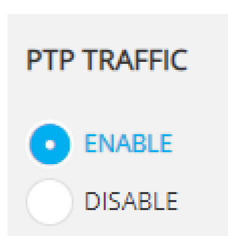
1. **Navigate to PTP Sub Tab**
   To navigate to the PTP sub tab. in the port's configuration window, click the **PTP Settings** tab.

Figure 9-91. PTP Settings



2. **Enable PTP Traffic**
   From the **PTP TRAFFIC** radio buttons, select **ENABLE**.

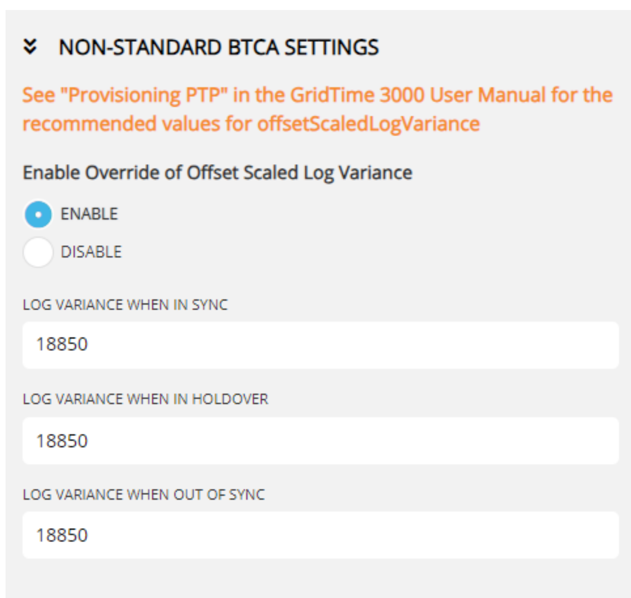
Figure 9-92. Enable PTP Traffic



This reveals the PTP settings for the port.

3. Follow the instructions in one of the following sections for guidance on provisioning each PTP profile:
   – Peer to Peer Default Profile
   – End to End Default Profile
   – C37.238-2011 Power Profile
   – C37.238-2017 Power Profile
   – 61850-9-3 Power Utility Profile
   – G.8275.1 Telecom Profile
   – G.8265.1 Telecom Profile
4. **Custom offsetScaledLogVariance**
   The Offset Scaled Log Variance is a value within a PTP packet to indicate the stability of a given clock. It is also used as the fifth determining factor of the Best TimeTransmitter Clock Algorithm (BTCA)
   If the installation requires the customization of the offsetScaledLogVariance value to manipulate the BTCA, follow these instructions:
   a. Scroll down and click the **NON-STANDARD BTCA SETTINGS** drop down.
   b. Under the **Enable Override of Offset Scaled Log Variance** radio buttons, select **ENABLE**.
   c. Modify the offsetScaledLogVariance value for when it is in sync, in holdover, and out of sync, in the respective text boxes.

Figure 9-93. Setting the Offset Scaled Log Variance



Note: These fields should only be edited by a user familiar with how the offsetScaledLogVariance values are used. Modifying these values changes how the BTCA operates and may impact downstream devices. It is recommended to keep the default value of 18850, if unsure.

Note: By allowing this to change, Microchip Technology Inc. assumes no liability for the malperformance of any device as a result of changing this setting.

The following table lists the recommended offsetScaledLogVariance values.

Table 9-1. OffsetScaledLogVariance Recommended Values

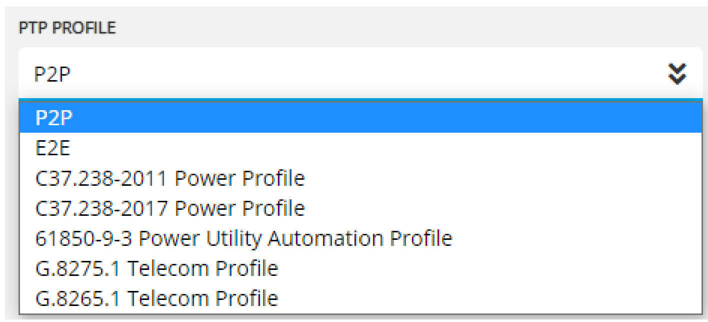
Case	Value	Hex
Best Case (Unrealistic)	0	0000
Recommended	18850	49A2
NTS 03-G+	20061	4E5D
Worst Case/Not Calculated	65535	FFFF

9.5.7.1 Peer to Peer Default Profile

This section describes how to provision a GridTime 3000 with the Peer to Peer Default Profile.

1. **Select Peer to Peer Default Profile**
   From the **PTP PROFILE** drop-down list, select **P2P** .

Figure 9-94. Selecting the P2P Profile



2. Follow the instructions in one of the following sections depending on your desired PTP Clock Mode:
   – Peer to Peer Default Profile Auto Mode
   – Peer to Peer Default Profile TimeTransmitter Only Mode
   – Peer to Peer Default Profile TimeReceiver Only Mode

PTP Clock Mode Descriptions

Auto mode allows the port to operate either in the TimeTransmitter or TimeReceiver state depending on whether the GridTime 3000 is in sync or not. When the GridTime 3000 is in sync or in holdover, the port will be in the TimeTransmitter or passive TimeTransmitter state; when the GridTime 3000 is out of sync, the port will be in the TimeReceiver state unless it is the only time TimeTransmitter on the network.

In TimeTransmitter only mode, the port will always either be in the TimeTransmitter or passive TimeTransmitter state depending on whether it has won the Best TimeTransmitter Clock Algorithm (BTCA) or not.

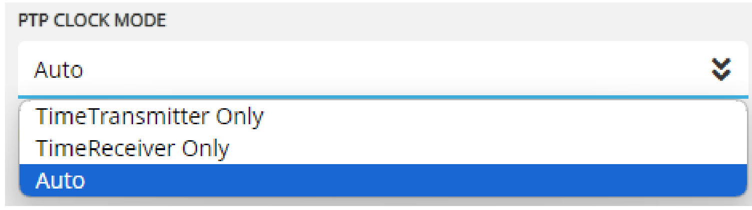
In TimeReceiver only mode, the port will always be in the client or listening state depending on whether or not there is a PTP TimeTransmitter available to sync to.

9.5.7.1.1 Peer to Peer Default Profile Auto Mode

This section describes how to provision a PTP Peer to Peer Default Profile Auto Mode Clock.

1. **Select Auto for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **Auto**.

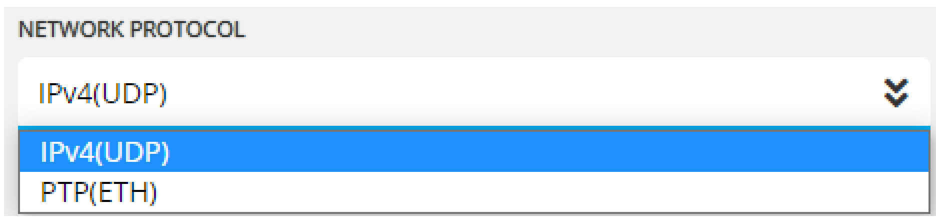
Figure 9-95. PTP Clock Mode Settings



2. **Select Network Protocol**
   From the **NETWORK PROTOCOL** drop-down list, select the network protocol that the PTP will operate on.

   The Network protocol should be consistent across the network subnet. The supported options are IPv4 (layer 4) and PTP over Ethernet (layer 2). By default, the network protocol is set to **IPv4 (UDP)**.

   Figure 9-96. Network Protocol Settings

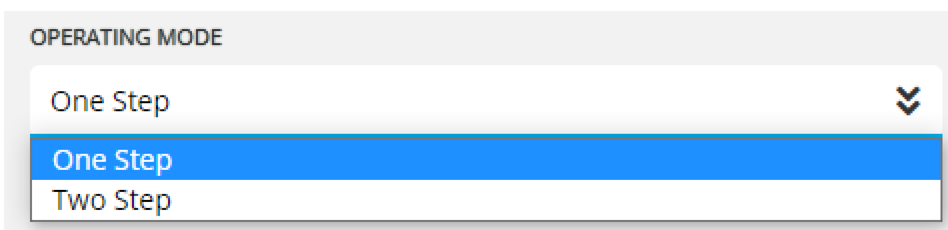
   

   Note: IPv4 is the most common PTP Network Protocol.

3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

   Figure 9-97. Setting the Operating Mode

   Note: Select **Two Step** if the Operating Mode is unknown.

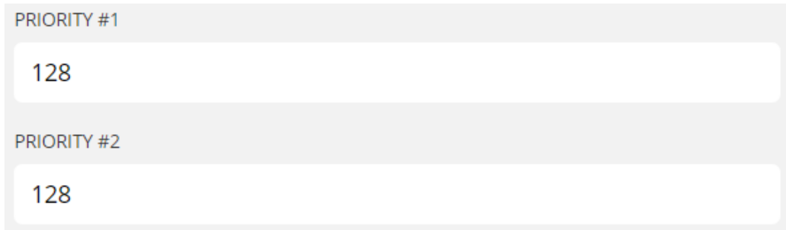
4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to **P2P**, which will set the delay mechanism to peer to peer as defined in IEEE 1588v2-2008.

5. **Configure Priority 1 and Priority 2 Fields**
   Modify the **PRIORITY #1** and **PRIORITY #2** fields if required, otherwise it is recommended to retain the default values.

   These parameters modify the automatic selection of TimeTransmitter clocks in PTP networks. Lower values mean that the unit will be preferred against other TimeTransmitter capable clocks during the selection process. The priority 1 value is used to manually select which TimeTransmitter capable clock will become the grandmaster and will be used in preference over other selection criteria including clock accuracy, so should be modified very carefully. The priority 2 value is treated as the least important criteria, providing greater selection control between otherwise-equal clocks

For both priority fields, the input range is 0 to 255, where 0 is the highest priority. The default setting is 128.

Figure 9-98. Setting the TimeTransmitter Clock Priority

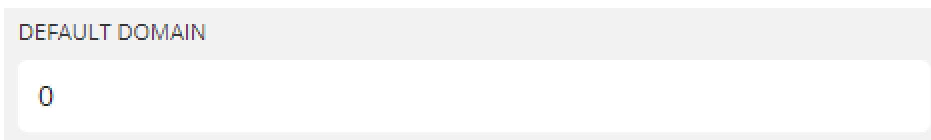


6. **Configure Default Domain**

   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with domain '0'. Changing the domain causes only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

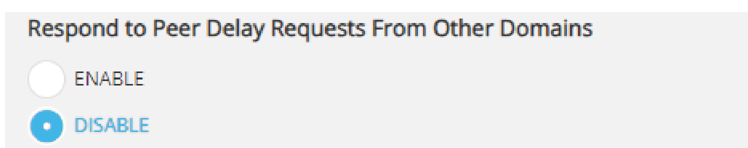
Figure 9-99. Default Domain Settings



7. **Respond to Peer Delay Requests From Other Domains**

   If enabled, the port responds to peer delay requests regardless of the domain identifier in the request packet. The peer delay responses include the same domain identifier as the incoming request.

Figure 9-100. Enable/Disable Peer Delay Request Responses



Note: Respond to Peer Delay Requests from other domains settings are disabled by default.

8. **Configure Delay Asymmetry**

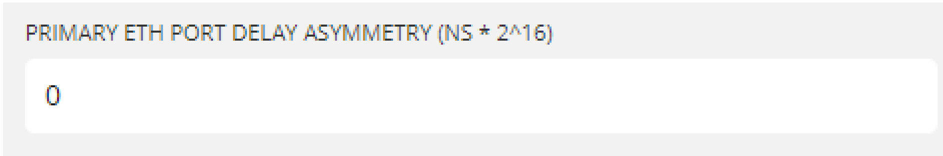
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.

   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces the PTP time accuracy.

   Delay asymmetry is calculated by the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the error caused by delay in asymmetry in the PTP delay calculation mechanism.

If the delay asymmetry is known, entering it manually allows it to be compensated for, and improves time accuracy. The input range is 3.2768e+14 ns×$2^{\wedge 16}$ to −3.2768e+14 ns×$2^{\wedge 16}$ (-5 to 5 seconds).

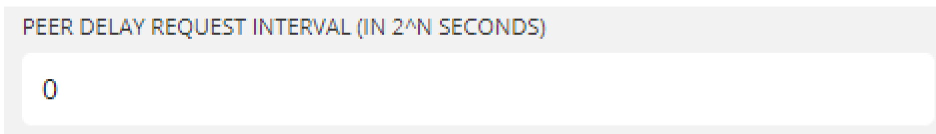
Figure 9-101. Setting the Delay Asymmetry



9. **Configure Peer Delay Request Interval**
   The Peer Delay Request interval specifies the time interval between successive Peer Delay Request messages being sent to other PTP devices on the network. This option only appears when a profile that uses the Peer-to-Peer delay mechanism is selected.

   By default, this is set to 0 in $2^{\wedge n}$ seconds, or 1 second. The supported range is 0-5 in $2^{\wedge n}$ seconds, or 1-32 seconds.

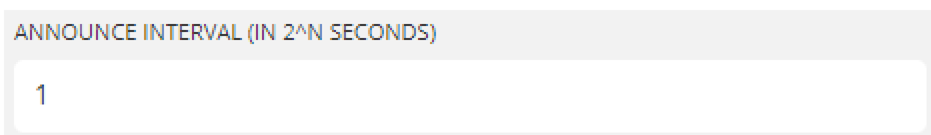
Figure 9-102. Setting the Peer Delay Request Interval



10. **Configure Announce Interval**
    The Announce interval specifies the time interval between successive Announce messages being sent to other PTP devices on the network.

    By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is 0-4 in $2^{\wedge n}$ seconds, or 1-16 seconds.

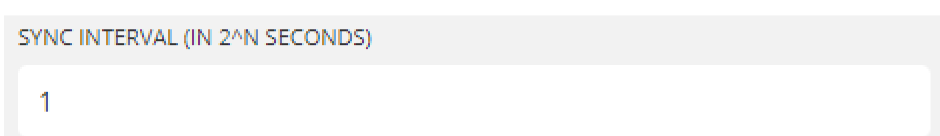
Figure 9-103. Setting the Announce Interval



11. **Announce Receipt Timeout**
    By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
12. **Configure Sync Interval**
    The Sync interval specifies the time interval between successive Sync messages being sent to other PTP devices on the network. This option only appears when the PTP clock is TimeTransmitter capable.

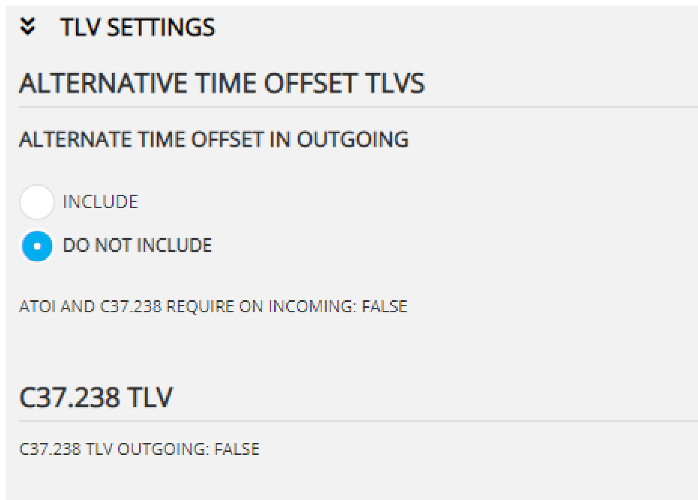
    By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is -1 to 1 in $2^{\wedge n}$ seconds, or 0.5 to 2 seconds.

Figure 9-104. Setting the Sync Interval



13. **BTCA**
    By default, **BTCA** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008
14. **Clock Class Rules**
    By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
15. **Configure TLV Settings > Alternate Time Offset In Outgoing**
    In the E2E and P2P default profiles, there is an option to either include or exclude Alternative Time Offset TLVs (ATOI TLVs) in outgoing PTP messages by using the **TLV SETTINGS > ALTERNATE TIME OFFSET IN OUTGOING** setting.

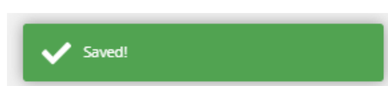
Figure 9-105. TLV Settings



16. **TLV Settings > ATOI and C37.238 Require on incoming**
    By default, the **ATOI AND C37.238 REQUIRE ON INCOMING** setting is set to **FALSE**.
17. **TLV Settings > C37.238 TLV Outgoing**
    By default, the **C37.238 TLV OUTGOING** is set to **FALSE**, preventing the C37.238 TLV from being sent on outgoing packets.
18. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-106. Successful Save Notification

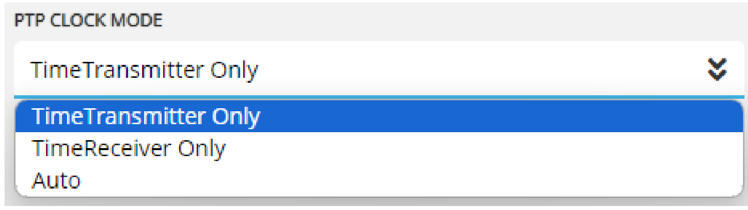


9.5.7.1.2 Peer to Peer Default Profile TimeTransmitter Only Mode

This section describes how to provision a PTP Peer to Peer Default Profile TimeTransmitter Only Mode Clock.

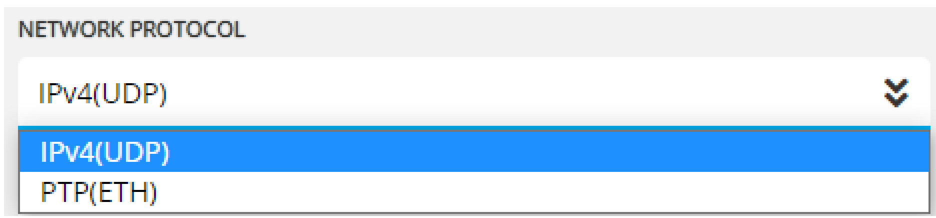
1. **Select TimeTransmitter Only for PTP Clock Mode**
   From the **PTP Clock Mode** drop-down list, select **TimeTransmitter Only**.

Figure 9-107. PTP Clock Mode Settings



2. **Select Network Protocol**
   From the **NETWORK PROTOCOL** drop-down list, select the network protocol that the PTP will operate on.
   The Network protocol should be consistent across the network subnet. The supported options are IPv4 (layer 4) and PTP over Ethernet (layer 2). By default the network protocol is set to **IPv4(UDP)**.

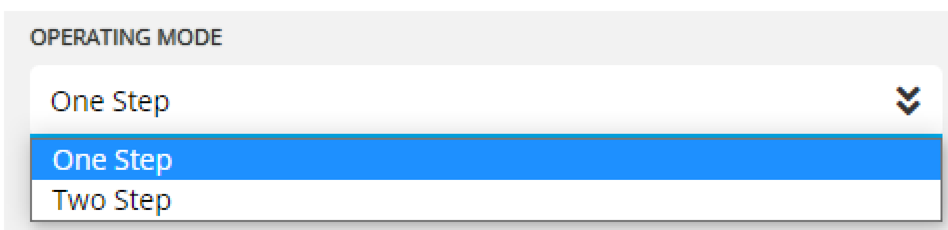
Figure 9-108. Network Protocol Settings



Note: IPv4 is the most common PTP Network Protocol.

3. **Select Operating Mode**
   From the OPERATING MODE drop-down list, select the operating mode for the PTP network .
   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-109. Setting the Operating Mode



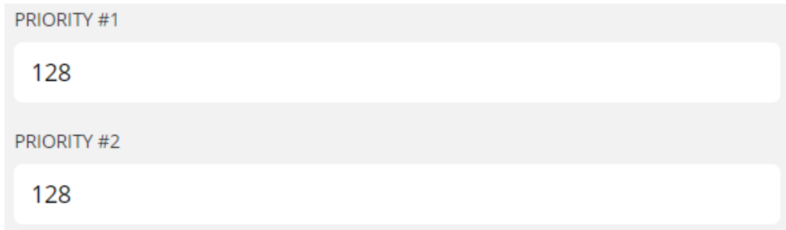
Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to **P2P**, which will set the delay mechanism to peer to peer as defined in IEEE 1588v2-2008.
5. **Configure Priority 1 and Priority 2 Fields**
   Modify the **PRIORITY #1** and **PRIORITY #2** fields if required, otherwise it is recommended to retain the default values.
   These parameters modify the automatic selection of TimeTransmitter clocks in PTP networks. Lower values mean that the unit will be preferred against other TimeTransmitter capable clocks during the selection process. The priority 1 value is used to manually select which TimeTransmitter capable clock will become the grandmaster and will be used in preference over other selection criteria including clock accuracy , so should be modified very carefully. The

priority 2 value is treated as the least important criteria, providing greater selection control between otherwise-equal clocks.

For both priority fields, the input range is 0 to 255, where 0 is the highest priority. The default setting is 128.

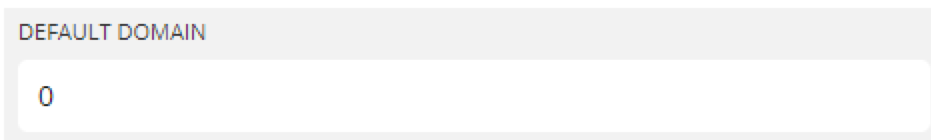
Figure 9-110. Setting the TimeTransmitter Clock Priority



6. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with domain '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

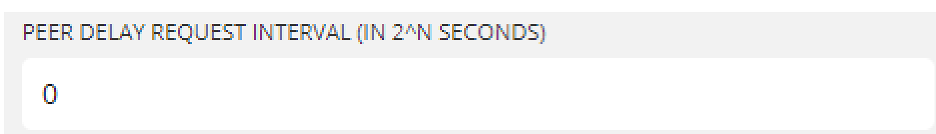
Figure 9-111. Default Domain Settings



7. **Configure Peer Delay Request Interval**
   The Peer Delay Request interval specifies the time interval between successive Peer Delay Request messages being sent to other PTP devices on the network. This option only appears when a profile that uses the Peer-to-Peer delay mechanism is selected.

   By default, this is set to 0 in $2^{\wedge n}$ seconds, or 1 second. The supported range is 0-5 in $2^{\wedge n}$ seconds, or 1-32 seconds.

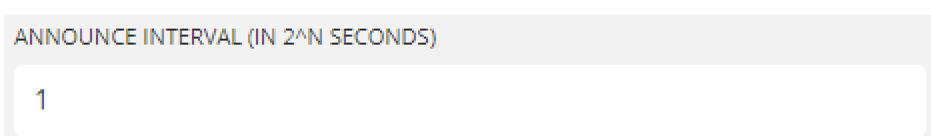
Figure 9-112. Setting the Peer Delay Request Interval



8. **Configure Announce Interval**
   The Announce interval specifies the time interval between successive Announce messages being sent to other PTP devices on the network.

   By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is 0-4 in $2^{\wedge n}$ seconds, or 1-16 seconds.

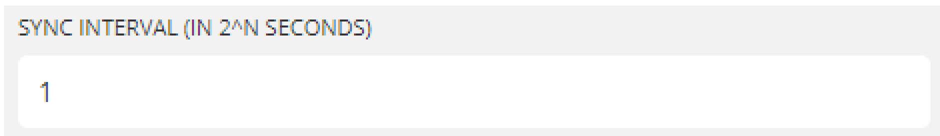
Figure 9-113. Setting the Announce Interval



9. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
10. **Configure Sync Interval**
   The Sync interval specifies the time interval between successive Sync messages being sent to other PTP devices on the network. This option only appears when the PTP clock is TimeTransmitter capable (When clock mode is set to auto or TimeTransmitter only).

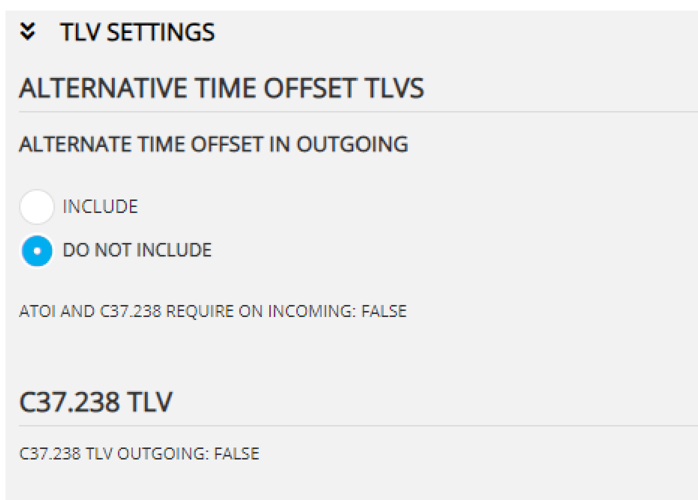
   By default, this is set to 1 in 2^n seconds, or 2 seconds. The supported range is -1 to 1 in 2^n seconds, or 0.5 to 2 seconds.

   Figure 9-114. Setting the Sync Interval

11. **BTCA**
   By default, **BTCA** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008
12. **Clock Class Rules**
   By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008
13. **Configure TLV Settings > Alternate Time Offset In Outgoing**
   In the E2E and P2P default profiles, there is an option to either include or exclude Alternative Time Offset TLVs (ATOI TLVs) in outgoing PTP messages by using the **TLV SETTINGS > ALTERNATE TIME OFFSET IN OUTGOING** setting.

   Figure 9-115. TLV Settings

14. **TLV Settings> ATOI and C37.238 Require on incoming**
   By default, the **ATOI AND C37.238 REQUIRE ON INCOMING** setting is set to **FALSE**.
15. **TLV Settings> C37.238 TLV Outgoing**
   By default, the **C37.238 TLV OUTGOING** is set to **FALSE**, preventing the C37.238 TLV from being sent on outgoing packets.
16. **Save Settings**

To write the settings to GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-116. Successful Save Notification

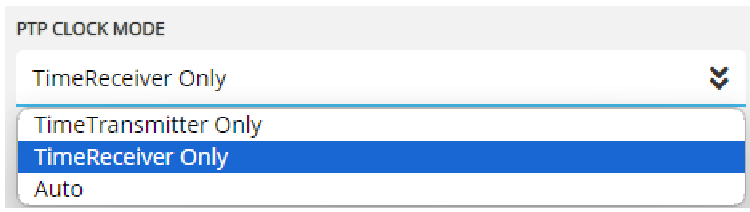
9.5.7.1.3 Peer to Peer Default Profile TimeReceiver Only Mode

This section describes how to provision a PTP Peer to Peer Default Profile TimeReceiver Only Mode Clock.

1. **Select TimeReceiver Only for PTP Clock Mode**

   From the **PTP CLOCK MODE** drop-down list, select **TimeReceiver Only**.

   Figure 9-117. PTP Clock Mode Setting

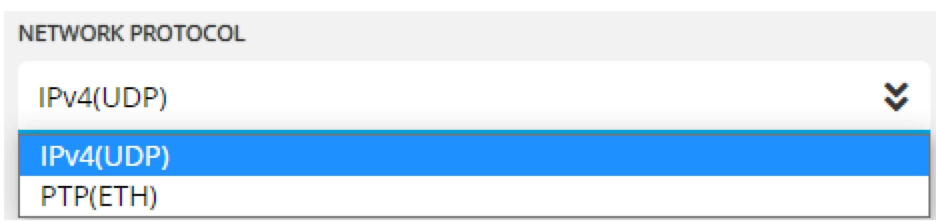
   

2. **Select Network Protocol**

   From the **NETWORK PROTOCOL** drop-down list, select the network protocol that the PTP will operate on.

   The Network protocol should be consistent across the network subnet. The supported options are IPv4 (layer 4) and PTP over Ethernet (layer 2). By default, the network protocol is set to **IPv4 (UDP)**.

   Figure 9-118. Network Protocol Settings

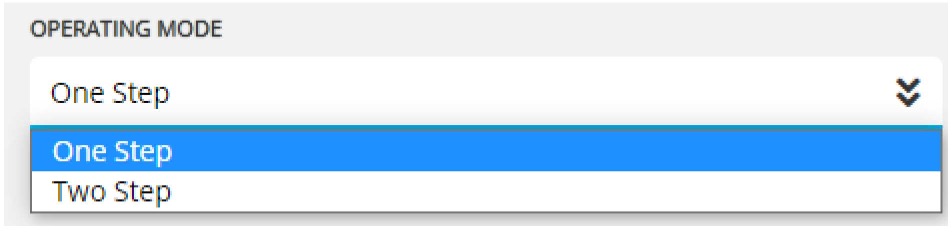
   Note: IPv4 is the most common PTP Network Protocol.

3. **Select Operating Mode**

   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-119. Setting the Operating Mode

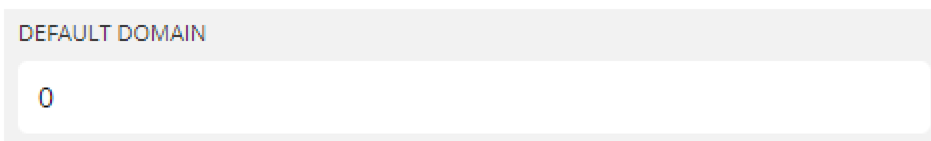


Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to **P2P**, which will set the delay mechanism to peer to peer as defined in IEEE 1588v2-2008.
5. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of **0**.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with domain '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

Figure 9-120. Default Domain Settings



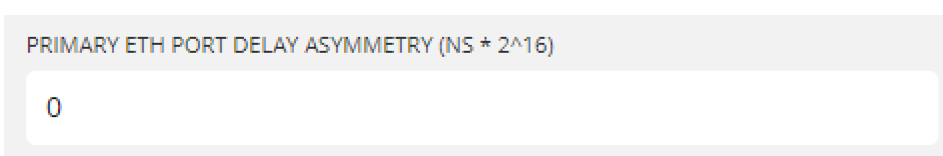
6. **Configure Delay Asymmetry**
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.

   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces PTP time accuracy.

   Delay asymmetry is a calculation consisting of the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the error caused by asymmetry delay in the PTP delay calculation mechanism.

   If the delay asymmetry is known, entering it manually will allow it to be compensated for, and improve time accuracy. The input range is 3.2768e+14 ns×2$^{\wedge 16}$ to −3.2768e+14 ns×2$^{\wedge 16}$ (-5 to 5 seconds).

Figure 9-121. Setting the Delay Asymmetry

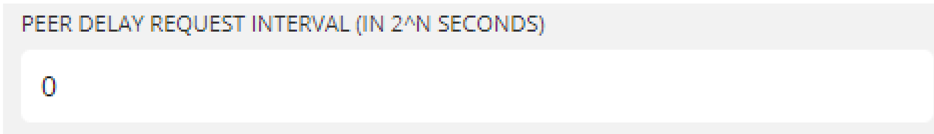


7. **Configure Peer Delay Request Interval**

The Peer Delay Request interval specifies the time interval between successive Peer Delay Request messages being sent to other PTP devices on the network. This option only appears when a profile that uses the Peer-to-Peer delay mechanism is selected.

By default, this is set to 0 in $2^{\wedge n}$ seconds, or 1 second. The supported range is 0-5 in $2^{\wedge n}$ seconds, or 1-32 seconds.

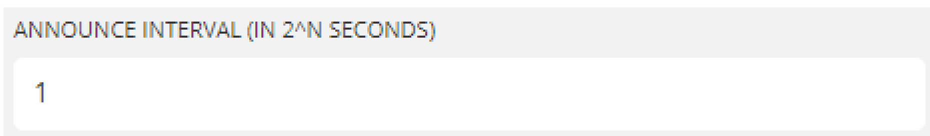
Figure 9-122. Setting the Peer Delay Request Interval



8. **Configure Announce Interval**
   The Announce interval specifies the time interval between successive Announce messages being sent to other PTP devices on the network.

   By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is 0-4 in $2^{\wedge n}$ seconds, or 1-16 seconds.

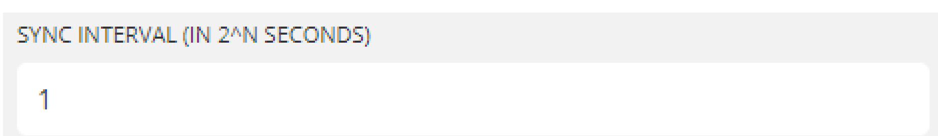
   Figure 9-123. Setting the Announce Interval

9. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
10. **Configure Sync Interval**
    The Sync interval specifies the time interval between successive Sync messages being sent to other PTP devices on the network. This option only appears when the PTP clock is TimeTransmitter capable.

    By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is -1 to 1 in $2^{\wedge n}$ seconds, or 0.5 to 2 seconds.

    Figure 9-124. Setting the Sync Interval

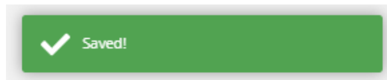
    

11. **BTCA**
    By default, **BTCA** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
12. **Clock Class Rules**
    By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
13. **TLV Settings > Alternate Time Offset in Outgoing**
    By default the **ALTERNATE TIME OFFSET IN OUTGOING** is set to false, preventing the ATOI TLV from being sent on outgoing packets.
14. **TLV Settings > ATOI and C37.238 Require on Incoming**
    By default, the **ATOI AND C37.238 REQUIRE ON INCOMING** setting is set to false.

15. **TLV Settings > C37.238 TLV Outgoing**
    By default, the **C37.238 TLV OUTGOING** is set to false, preventing the C37.238 TLV from being sent on outgoing packets.
16. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-125. Successful Save Notification

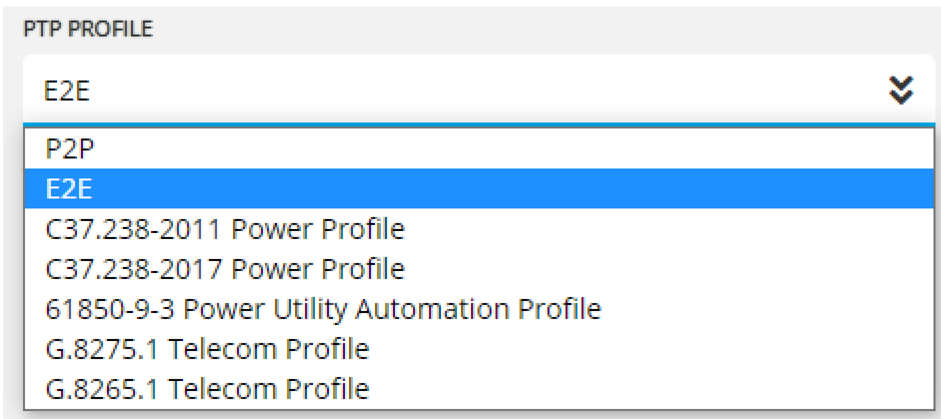


9.5.7.2 End to End Default Profile

This section describes how to provision a GridTime 3000 with the End to End Default Profile.

1. **Select End to End Default Profile**
   From the **PTP PROFILE** drop-down list, select **E2E**.

Figure 9-126. Setting the E2E Profile



2. Follow the instructions in one of the following sections depending on your desired PTP Clock Mode:
   - End to End Default Profile Auto Mode
   - End to End Default Profile TimeTransmitter Only Mode
   - End to End Default Profile TimeReceiver Only Mode

PTP Clock Mode Descriptions

Auto mode allows the port to operate either in the TimeTransmitter or TimeReceiver state depending on whether the GridTime 3000 is in sync or not. When the GridTime 3000 is in sync or in holdover, the port will be in the TimeTransmitter or passive TimeTransmitter state; when the GridTime 3000 is out of sync the port will be in the TimeReceiver state.

In TimeTransmitter only mode, the port will always either be in the TimeTransmitter or passive TimeTransmitter state depending on whether it has won the BTCA .

In TimeReceiver only mode, the port will always be in the TimeReceiver or listening state depending on whether there is a PTP TimeTransmitter available to sync to.

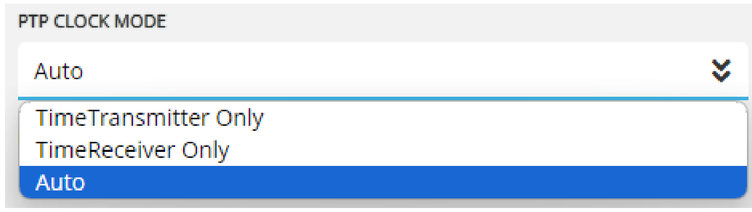
9.5.7.2.1 End to End Default Profile Auto Mode

This section describes how to provision a PTP End to End Default Profile Auto Mode Clock.

1. **Select Auto for PTP Clock Mode**

   From the **PTP CLOCK MODE** drop-down list, select **Auto**.

   Figure 9-127. PTP Clock Mode Settings

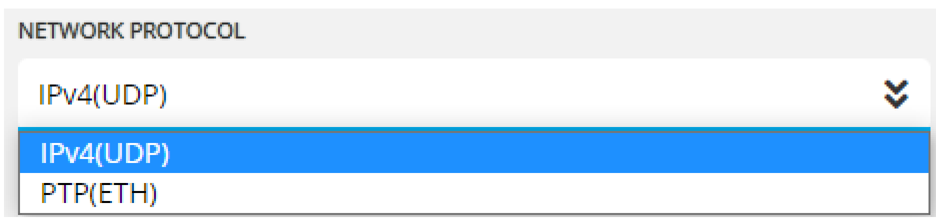
   

2. **Select Network Protocol**

   From the **NETWORK PROTOCOL** drop-down list, select the network protocol that the PTP will operate on.

   The Network protocol should be consistent across the network subnet. The supported options are IPv4 (layer 4) and PTP over Ethernet (layer 2). By default the network protocol is set to **IPv4 (UDP)**.

   Figure 9-128. Network Protocol Settings

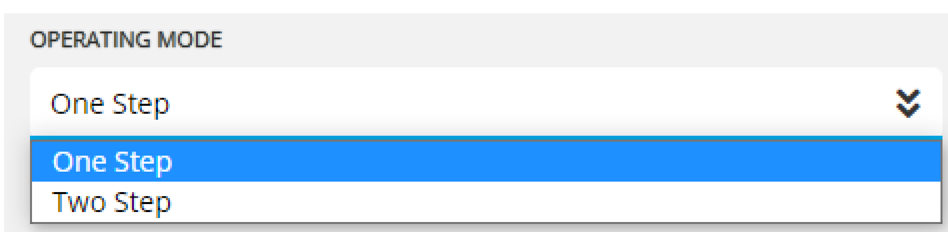
   Note: IPv4 is the most common PTP Network Protocol.

3. **Select Operating Mode**

   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

   Figure 9-129. Setting the Operating Mode

   Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**

   By default, the **DELAY MECHANISM** is set to **E2E**, which will set the delay mechanism to end to end as defined in IEEE 1588v2-2008.

5. **Configure Priority 1 and Priority 2 Fields**

   Modify the **PRIORITY #1** and **PRIORITY #2** fields if required, otherwise it is recommended to retain the default values.

These parameters modify the automatic selection of TimeTransmitter clocks in PTP networks. Lower values mean that the unit will be preferred against other TimeTransmitter capable clocks during the selection process. The priority 1 value is used to manually select which TimeTransmitter capable clock will become the grandmaster and will be used in preference over other selection criteria including clock accuracy , so should be modified very carefully. The priority 2 value is treated as the least important criteria, providing greater selection control between otherwise-equal clocks

For both priority fields, the input range is 0 to 255, where 0 is the highest priority. The default setting is 128.

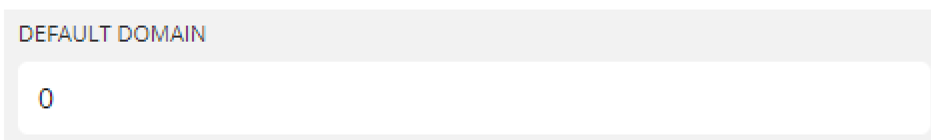
Figure 9-130. Setting the TimeTransmitter Clock Priority

6. **Configure Default Domain**

   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with domain '0'. Changing the domain causes only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

Figure 9-131. Default Domain Settings



7. **Configure Delay Asymmetry**

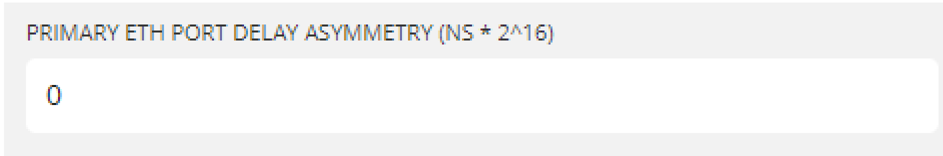
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.

   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces PTP time accuracy.

   Delay asymmetry is the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the error caused by delay in asymmetry in the PTP delay calculation mechanism.

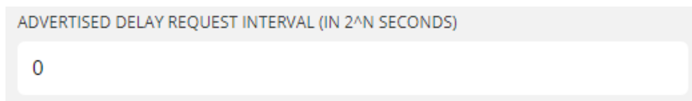
   If the delay asymmetry is known, entering it manually will allow it to be compensated for, and improve time accuracy. The input range is 3.2768e+14 ns×$2^{\wedge 16}$ to −3.2768e+14 ns×$2^{\wedge 16}$ (-5 to 5 seconds).

Figure 9-132. Setting the Delay Asymmetry



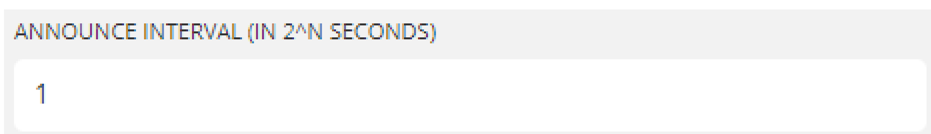
8. **Configure Advertised Delay Request Interval**
   The **ADVERTISED DELAY REQUEST INTERVAL** specifies the time interval between successive Delay Request messages being sent to other PTP devices on the network. This option only appears when the End to End Default Profile is selected. This option does not appear when the port is configured as a Forced TimeReceiver.
   By default, this is set to 0 in $2^{\wedge n}$ seconds, or 1 second. The supported range is 0-5 in $2^{\wedge n}$ seconds, or 1-32 seconds.

Figure 9-133. Advertised Delay Request Interval Settings



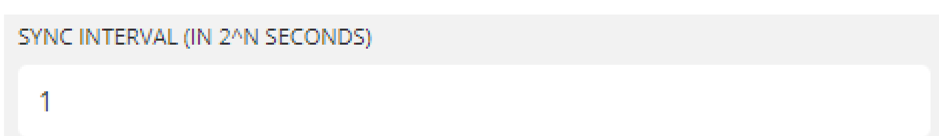
9. **Configure Announce Interval**
   The Announce interval specifies the time interval between successive Announce messages being sent to other PTP devices on the network.
   By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is 0-4 in $2^{\wedge n}$ seconds, or 1-16 seconds.

Figure 9-134. Setting the Announce Interval



10. **Announce Receipt Timeout**
    By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
11. **Configure Sync Interval**
    The Sync interval specifies the time interval between successive Sync messages being sent to other PTP devices on the network. This option only appears when the PTP clock is TimeTransmitter capable.
    By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is -1 to 1 in $2^{\wedge n}$ seconds, or 0.5 to 2 seconds.

Figure 9-135. Setting the Sync Interval

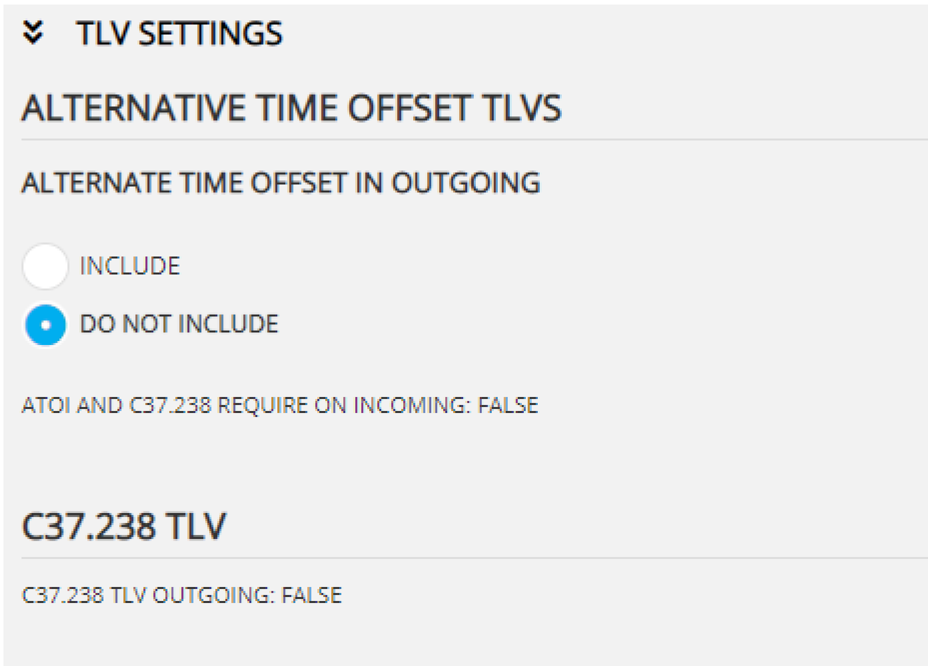


12. **BTCA**
    By default, **BTCA** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
13. **Clock Class Rules**

By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.

14. **Configure TLV Settings > Alternate Time Offset In Outgoing**
    In the E2E and P2P default profiles, there is an option to either include or exclude Alternative Time Offset TLVs (ATOI TLVs) in outgoing PTP messages by using the **TLV SETTINGS > ALTERNATE TIME OFFSET IN OUTGOING** setting.

Figure 9-136. TLV Settings



15. **TLV Settings > ATOI and C37.238 Require on Incoming**
    By default, the **ATOI AND C37.238 REQUIRE ON INCOMING** setting is set to **FALSE**.
16. **TLV Settings > C37.238 TLV Outgoing**
    By default, the **C37.238 TLV OUTGOING** is set to **FALSE**, preventing the C37.238 TLV from being sent on outgoing packets.
17. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

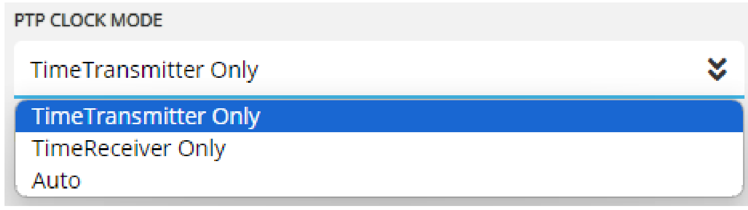
Figure 9-137. Successful Save Notification

9.5.7.2.2 End to End Default Profile TimeTransmitter Only Mode

This section describes how to provision a PTP End to End Default Profile TimeTransmitter Only Mode Clock.

1. **Select TimeTransmitter Only for PTP Clock Mode**
   From the **PTP Clock Mode** drop-down list, select **TimeTransmitter Only**.

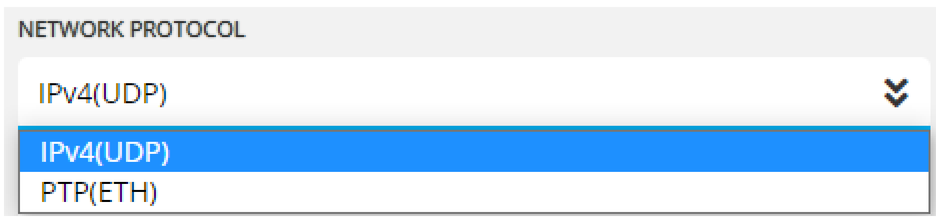
Figure 9-138. PTP Clock Mode Settings



2. **Select Network Protocol**
   From the **NETWORK PROTOCOL** drop-down list, select the network protocol that the PTP will operate on.

   The Network protocol should be consistent across the network subnet. The supported options are IPv4 (layer 4) and PTP over Ethernet (layer 2). By default the network protocol is set to **IPv4(UDP)**.

   Figure 9-139. Network Protocol Settings

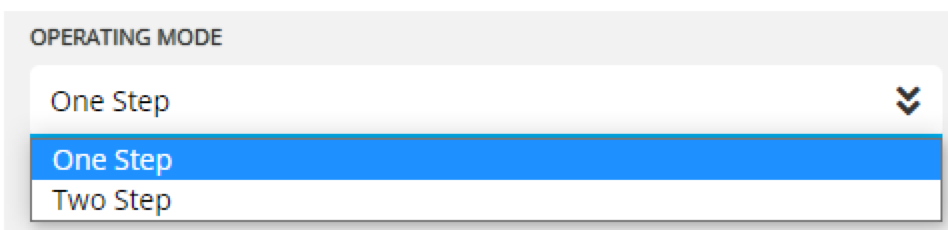
   

   Note: IPv4 is the most common PTP Network Protocol.

3. **Select Operating Mode**
   From the OPERATING MODE drop-down list, select the operating mode for the PTP network .

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

   Figure 9-140. Setting the Operating Mode

   Note: Select **Two Step** if the Operating Mode is unknown.

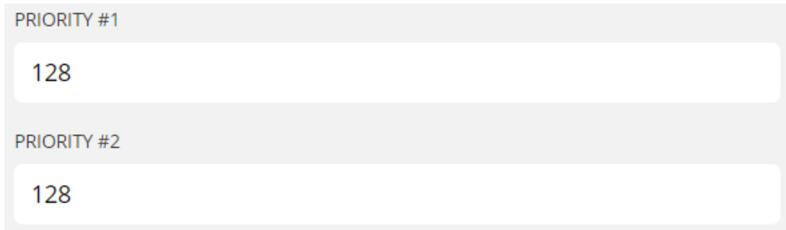
4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to **E2E**, which will set the delay mechanism to end-to-end as defined in IEEE 1588v2-2008.

5. **Configure Priority 1 and Priority 2 Fields**
   Modify the **PRIORITY #1** and **PRIORITY #2** fields if required, otherwise it is recommended to retain the default values.

   These parameters modify the automatic selection of TimeTransmitter clocks in PTP networks. Lower values mean that the unit will be preferred against other TimeTransmitter capable clocks during the selection process. The priority 1 value is used to manually select which TimeTransmitter capable clock will become the grandmaster and will be used in preference over other selection criteria including clock accuracy , so should be modified very carefully. The priority 2 value is treated as the least important criteria, providing greater selection control between otherwise-equal clocks

For both priority fields, the input range is 0 to 255, where 0 is the highest priority. The default setting is 128.

Figure 9-141. Setting the TimeTransmitter Clock Priority

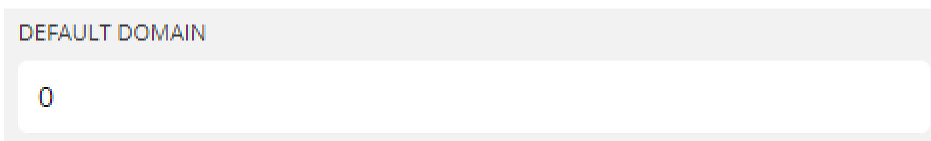


6. **Configure Default Domain**

   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with domain '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

Figure 9-142. Default Domain Settings

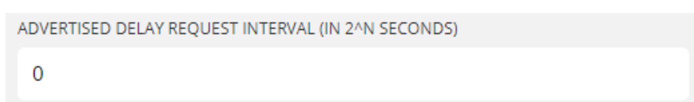


7. **Configure Advertised Delay Request Interval**

   The **ADVERTISED DELAY REQUEST INTERVAL** specifies the time interval between successive Delay Request messages being sent to other PTP devices on the network. This option only appears when the End to End Default Profile is selected. This option does not appear when the port is configured as a Forced TimeReceiver.

   By default, this is set to 0 in $2^{\wedge n}$ seconds, or 1 second. The supported range is 0-5 in $2^{\wedge n}$ seconds, or 1-32 seconds.

Figure 9-143. Advertised Delay Request Interval Setting

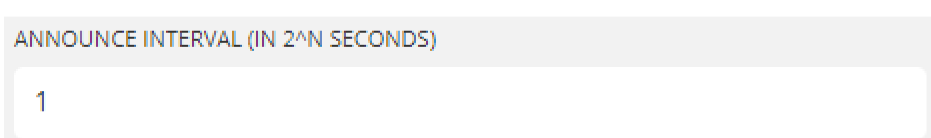


8. **Configure Announce Interval**

   The Announce interval specifies the time interval between successive Announce messages being sent to other PTP devices on the network.

   By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is 0-4 in $2^{\wedge n}$ seconds, or 1-16 seconds.

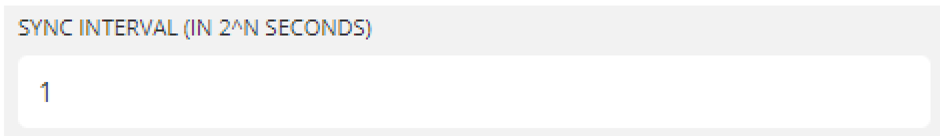
Figure 9-144. Setting the Announce Interval



9. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
10. **Configure Sync Interval**
   The Sync interval specifies the time interval between successive Sync messages being sent to other PTP devices on the network. This option only appears when the PTP clock is TimeTransmitter capable..

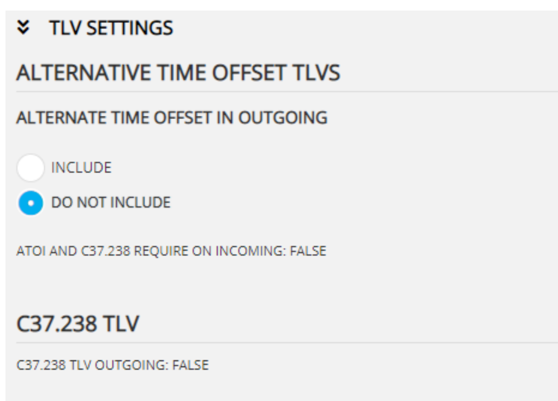
   By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is -1 to 1 in $2^{\wedge n}$ seconds, or 0.5 to 2 seconds.

   Figure 9-145. Setting the Sync Interval

11. **BTCA**
   By default, **BTCA** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008
12. **Clock Class Rules**
   By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008
13. **Configure TLV Settings > Alternate time Offset In Outgoing**
   In the E2E and P2P default profiles, there is an option to either include or exclude Alternative Time Offset TLVs (ATOI TLVs) in outgoing PTP messages.

   Figure 9-146. TLV Settings

14. **TLV Settings > ATOI and C37.238 Require on Incoming**
   By default, the 'ATOI AND C37.238 REQUIRE ON INCOMING' setting is set to false.
15. **TLV Settings > C37.238 TLV Outgoing**
   By default, the **C37.238 TLV OUTGOING** is set to **FALSE**, preventing the C37.238 TLV from being sent on outgoing packets.
16. **Save Settings**
   To write the settings to GridTime 3000, click **SAVE**.

   A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

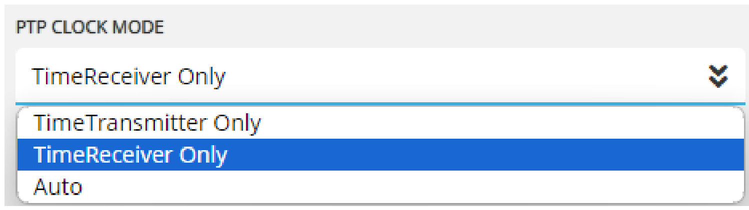
Figure 9-147. Successful Save Notification

9.5.7.2.3 End to End Default Profile TimeReceiver Only Mode

This section describes how to provision a PTP End to End Default Profile TimeReceiver Only Mode Clock.

1. **Select TimeReceiver Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeReceiver Only**.

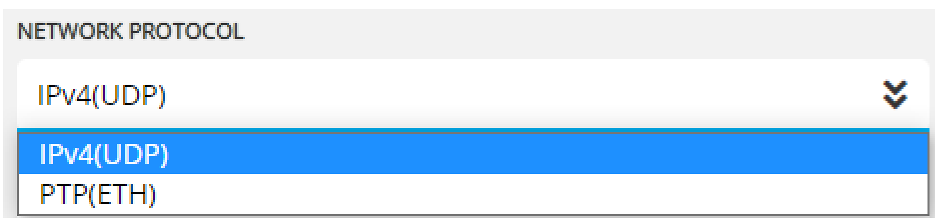
   Figure 9-148. PTP Clock Mode Setting

2. **Select Network Protocol**
   From the **NETWORK PROTOCOL** drop-down list, select the network protocol that the PTP will operate on.

   The Network protocol should be consistent across the network subnet. The supported options are IPv4 (layer 4) and PTP over Ethernet (layer 2). By default, the network protocol is set to **IPv4 (UDP)**.

   Figure 9-149. Network Protocol Settings

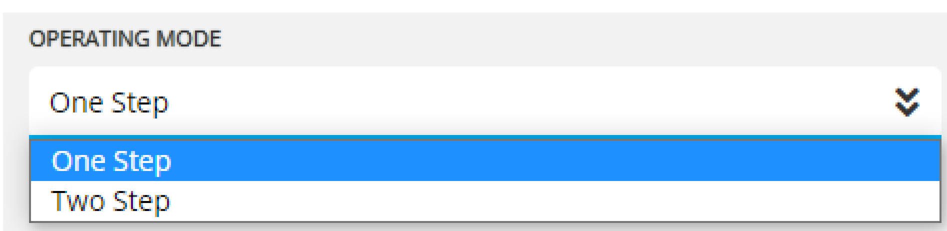
   

   Note: IPv4 is the most common PTP Network Protocol.

3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

   Figure 9-150. Setting the Operating Mode

   Note: Select **Two Step** if the Operating Mode is unknown.

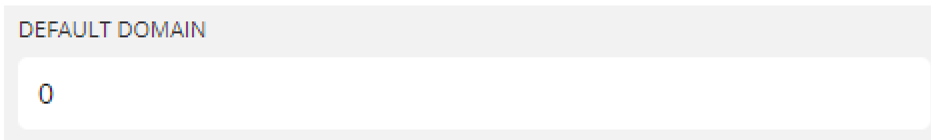
4. **Delay Mechanism**

By default, the **DELAY MECHANISM** is set to **E2E**, which sets the delay mechanism to end-to-end as defined in IEEE 1588v2-2008.

5. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of **0**.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

Figure 9-151. Default Domain Settings



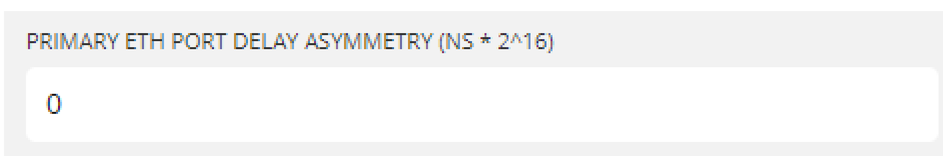
6. **Configure Delay Asymmetry**
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.

   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces PTP time accuracy.

   Delay asymmetry is calculated from the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the delay asymmetry error caused in the PTP delay calculation mechanism.

   If the delay asymmetry is known, entering it manually will allow it to be compensated for, and improve time accuracy. The input range is 3.2768e+14 ns×$2^{\wedge 16}$ to −3.2768e+14 ns×$2^{\wedge 16}$ (-5 to 5 seconds).

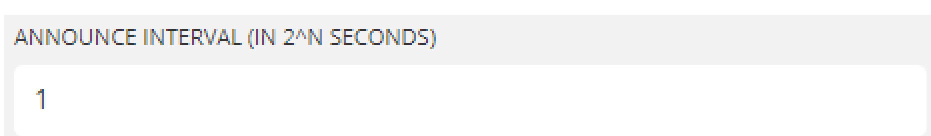
Figure 9-152. Setting the Delay Asymmetry



7. **Configure Announce Interval**
   The Announce interval specifies the time interval between successive Announce messages being sent to other PTP devices on the network.

   By default, this is set to 1 in $2^{\wedge n}$ seconds, or 2 seconds. The supported range is 0-4 in $2^{\wedge n}$ seconds, or 1-16 seconds.

Figure 9-153. Setting the Announce Interval



8. **Announce Receipt Timeout**

By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.

9. **BTCA**
   By default, **BTCA** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
10. **Clock Class Rules**
    By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
11. **TLV Settings > Alternate Time Offset in Outgoing**
    By default the **ALTERNATE TIME OFFSET IN OUTGOING** is set to false, preventing the ATOI TLV from being sent on outgoing packets.
12. **TLV Settings > ATOI and C37.238 Require on Incoming**
    By default, the **ATOI AND C37.238 REQUIRE ON INCOMING** setting is set to false.
13. **TLV Settings > C37.238 TLV Outgoing**
    By default, the **C37.238 TLV OUTGOING** is set to false, preventing the C37.238 TLV from being sent on outgoing packets.
14. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

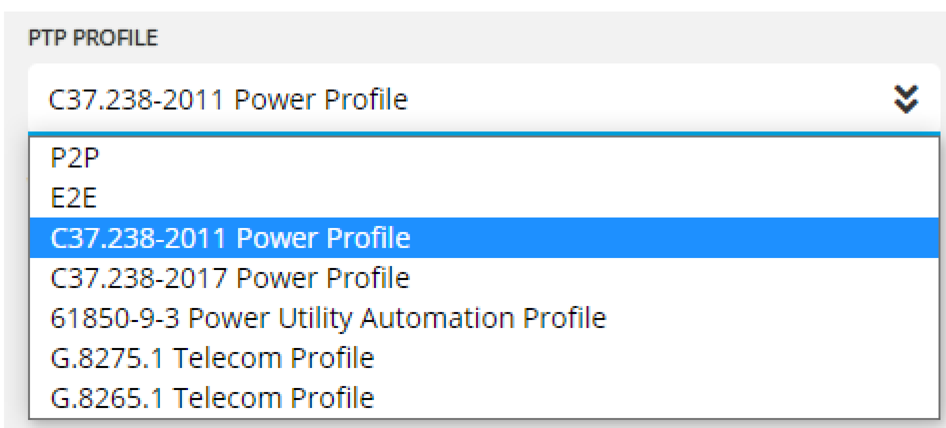
Figure 9-154. Successful Save Notification

9.5.7.3 C37.238-2011 Power Profile

This section describes how to provision a GridTime 3000 with the C37.238-2011 Power Profile.

1. **Select C37.238-2011 Power Profile**
   From the **PTP PROFILE** drop-down list, select **C37.238-2011 Power Profile**.

Figure 9-155. PTP Profile Settings



2. Follow the instructions in one of the following sections depending on your desired PTP Clock Mode:
   – C37.238-2011 Power Profile Auto Mode
   – C37.238-2011 Power Profile TimeTransmitter Only Mode

– C37.238-2011 Power Profile TimeReceiver Only Mode

PTP Clock Mode Descriptions

Auto mode allows the port to operate either in the TimeTransmitter or TimeReceiver state depending on whether the GridTime 3000 is synchronized or not. When the GridTime 3000 is in sync or in holdover, the port will be in the TimeTransmitter or passive TimeTransmitter state, when the GridTime 3000 is out of sync the port will be in the TimeReceiver state.

In TimeTransmitter only mode, the port will always either be in the TimeTransmitter or passive TimeTransmitter state depending on whether it has won the BTCA or not.

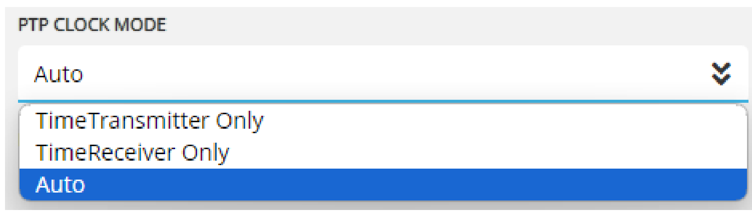
In TimeReceiver only mode, the port will always be in the TimeReceiver or listening state depending on whether there is a PTP TimeTransmitter available to sync to.

9.5.7.3.1 C37.238-2011 Power Profile Auto Mode

This section describes how to provision a PTP C37.238-2011 Power Profile Auto Mode Clock.

1. **Select Auto for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **Auto**.

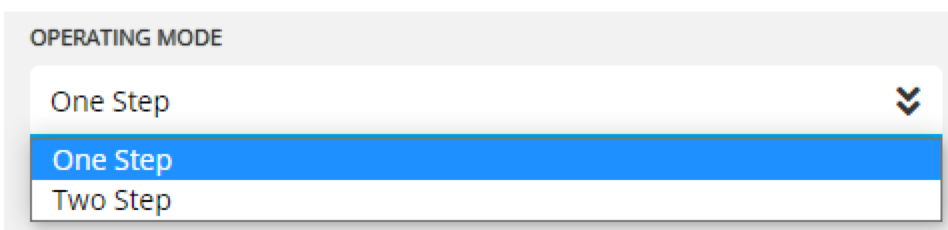
   Figure 9-156. PTP Clock Mode Settings



2. **Network Protocol**
   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer
3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

   Figure 9-157. Operating Mode Settings

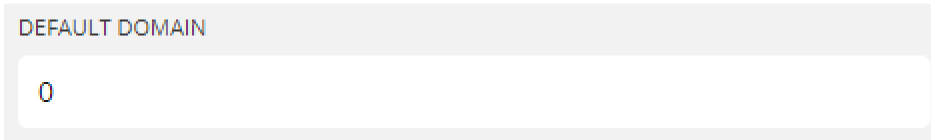


   Note: Select **Two Step** if the Operating Mode is unknown.
4. **Delay Mechanism**

   By default, the **DELAY MECHANISM** is set to **P2P**, which will set the delay mechanism to peer-to-peer as defined in IEEE 1588v2-2008.
5. **Priority #1 and Priority #2**
   By default, both Priority #1 and Priority #2 are set to 128 and cannot be changed.
6. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

Figure 9-158. Default Domain Settings



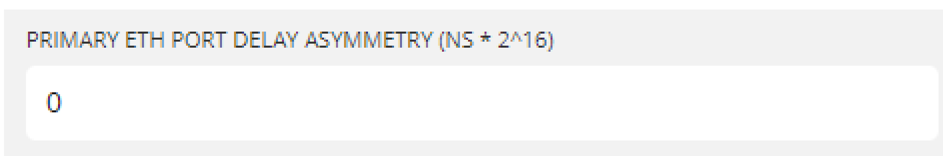
7. **Configure Delay Asymmetry**
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.

   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces PTP time accuracy.

   Delay asymmetry is determined by the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the error caused by delay in asymmetry in the PTP delay calculation mechanism.

   If the delay asymmetry is known, entering it manually will allow it to be compensated for, and improve time accuracy. The input range is 3.2768e+14 $\text{ns}\times 2^{\wedge 16}$ to −3.2768e+14 $\text{ns}\times 2^{\wedge 16}$ (-5 to 5 seconds).

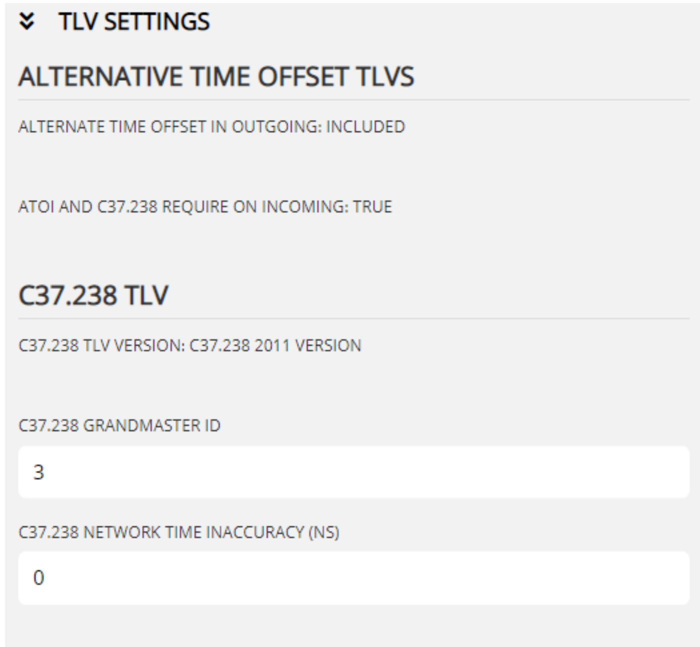
Figure 9-159. Delay Asymmetry Settings



8. **Peer Delay Request Interval**
   By default, the **PEER DELAY REQUEST INTERVAL** is set to 1 second.
9. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1 second.
10. **Announce Receipt Timeout**
    By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
11. **Sync Interval**
    By default, the **SYNC INTERVAL** is set to 1 second.
12. **BTCA**
    By default, the BTCA operations are set to **BASIC** and will operate as defined in IEEE 1588v2-2008.
13. **Clock Class Rules**
    By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
14. **Configure TLV Settings**
    With the C37.238-2011 profile, the ATOI TLV is always included in outgoing messages, and is required on incoming messages — otherwise they will be ignored. The same applies for

the C37.238 TLV, however, the C37.238 TLV includes two configurable settings — the C37.238 Grandmaster ID, and the C37.238 Network Time Inaccuracy.

Figure 9-160. TLV Settings

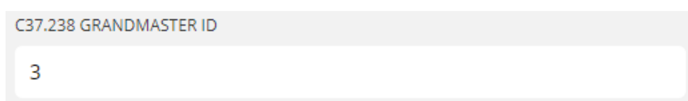


TLV Settings > GrandMaster ID

Set the C37.238 Grandmaster ID setting using the **C37.238 GRANDMASTER ID** text box.

This is the GMIdentity or Grandmaster Identity as defined in C37.238-2011. Grandmaster Identity is transmitted in IEEE_C37_238 TLV (2 bytes). The configurable range is 3 to 254. By default, it is set to 3.

Figure 9-161. Grandmaster ID Settings



TLV Settings > C37.238 Network Time Inaccuracy

Set the C37.238 Network Time Inaccuracy setting using the **C37.238 NETWORK TIME INACCURACY (NS)** text box.

This configurable field sets the networkTimeInaccuracy as defined in C37.238-2011. It will set the estimated worst-case error in nanoseconds from the grandmaster. The configurable range is 0 (default) to 2,147,483,647 ns.

Figure 9-162. Network Time Inaccuracy Settings

15. **Save Settings**

    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

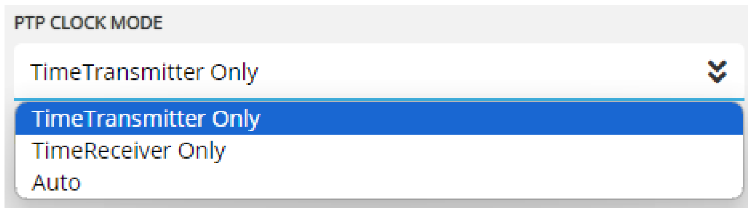
Figure 9-163. Successful Save Notification

9.5.7.3.2 C37.238-2011 Power Profile TimeTransmitter Only Mode

This section describes how to provision a PTP C37.238-2011 Power Profile TimeTransmitter Only Mode Clock.

1. **Select TimeTransmitter Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeTransmitter Only**.

   Figure 9-164. PTP Clock Mode Settings

2. **Network Protocol**

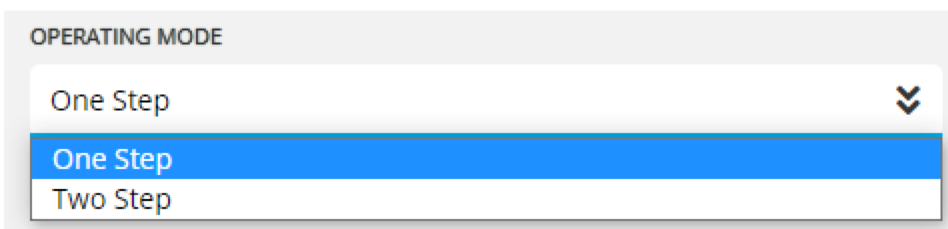
   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer

3. **Select Operating Mode**

   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

   Figure 9-165. Operating Mode Settings

   Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to **P2P**, which sets the delay mechanism to peer-to-peer as defined in IEEE 1588v2-2008.

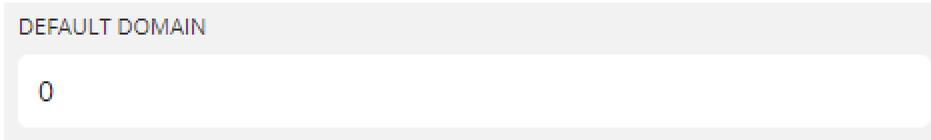
5. **Priority #1 and Priority #2**
   By default, both Priority #1 and Priority #2 are set to 128 and cannot be changed.

6. **Configure Default Domain**

   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

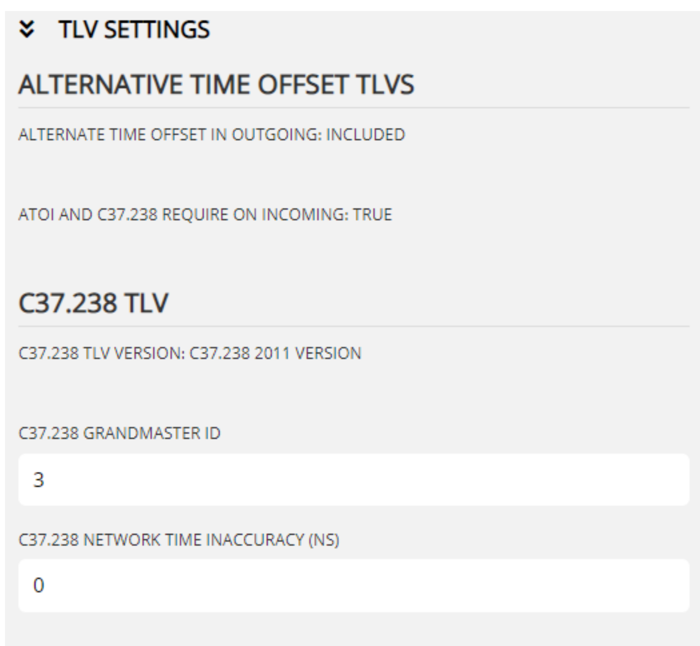
   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

Figure 9-166. Default Domain Settings



7. **Peer Delay Request Interval**
   By default, the **PEER DELAY REQUEST INTERVAL** is set to 1 second.
8. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1 second.
9. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
10. **Sync Interval**
    By default, the **SYNC INTERVAL** is set to 1 second.
11. **BTCA**
    By default, the BTCA operations are set to **BASIC** and will operate as defined in IEEE 1588v2-2008.
12. **Clock Class Rules**
    By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
13. **Configure TLV Settings**
    With the C37.238-2011 profile the ATOI TLV is always included in outgoing messages, and is required on incoming messages — otherwise they will be ignored. The same applies for the C37.238 TLV, however, the C37.238 TLV includes two configurable settings — the C37.238 Grandmaster ID, and the C37.238 Network Time Inaccuracy.

Figure 9-167. TLV Settings



GrandMaster ID

Set the C37.238 Grandmaster ID setting using the **C37.238 GRANDMASTER ID** text box.

This is the GMIdentity or Grandmaster Identity as defined in C37.238-2011. Grandmaster Identity is transmitted in IEEE_C37_238 TLV (2 bytes). The configurable range is 3 to 254. By default it is set to 3.

Figure 9-168. Grandmaster ID Settings

C37.238 Network Time Inaccuracy

Set the C37.238 Network Time Inaccuracy setting using the **C37.238 NETWORK TIME INACCURACY (NS)** text box.

This configurable field sets the networkTimeInaccuracy as defined in C37.238-2011. It will set the estimated worst-case error in nanoseconds from the grandmaster. The configurable range is 0 (default) to 2,147,483,647 ns.

Figure 9-169. Network Time Inaccuracy Settings

14. **Save Settings**

    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

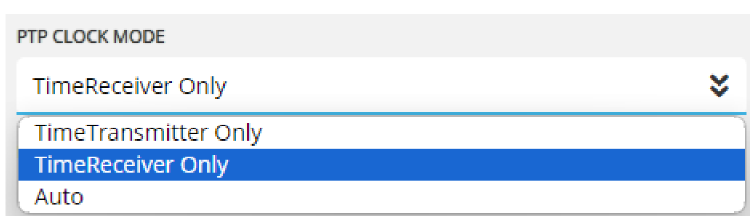
Figure 9-170. Successful Save Notification

9.5.7.3.3 C37.238-2011 Power Profile TimeReceiver Only Mode

This section describes how to provision a PTP C37.238-2011 Power Profile TimeReceiver Only Mode Clock.

1. **Select TimeReceiver Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeReceiver Only**.

Figure 9-171. PTP Clock Mode Settings



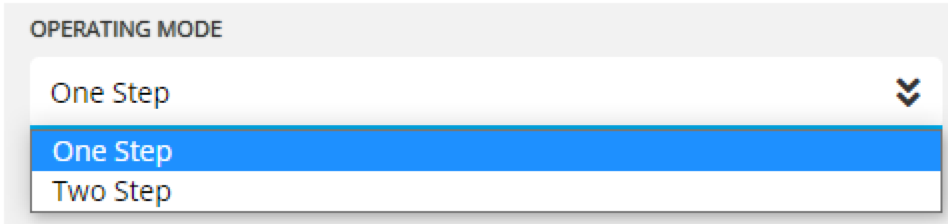
2. **Network Protocol**

   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer
3. **Select Operating Mode**

From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-172. Operating Mode Settings

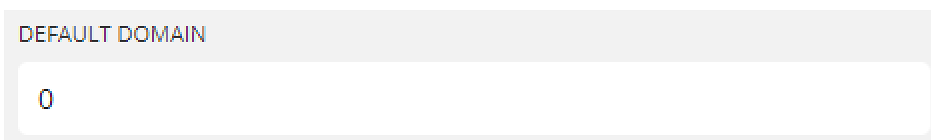


Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to **P2P**, which sets the delay mechanism to peer-to-peer as defined in IEEE 1588v2-2008.
5. **Priority #1 and Priority #2**
   By default, both Priority #1 and Priority #2 are set to 128 and cannot be changed.
6. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

Figure 9-173. Default Domain Settings



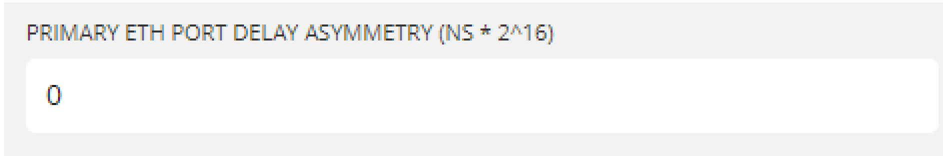
7. **Configure Delay Asymmetry**
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.

   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces PTP time accuracy.

   Delay asymmetry is determined by the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the error caused by delay in asymmetry in the PTP delay calculation mechanism.

   If the delay asymmetry is known, entering it manually will allow it to be compensated for, and improve time accuracy. The input range is 3.2768e+14 ns×$2^{\wedge 16}$ to −3.2768e+14 ns×$2^{\wedge 16}$ (-5 to 5 seconds).

Figure 9-174. Delay Asymmetry Settings



8. **Peer Delay Request Interval**

   By default, the **PEER DELAY REQUEST INTERVAL** is set to 1 second.
9. **Announce Interval**

   By default, the **ANNOUNCE INTERVAL** is set to 1 second.
10. **Announce Receipt Timeout**

    By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
11. **BTCA**

    By default, the BTCA operations are set to **BASIC** and will operate as defined in IEEE 1588v2-2008.
12. **Clock Class Rules**

    By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
13. **Save Settings**

    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-175. Successful Save Notification

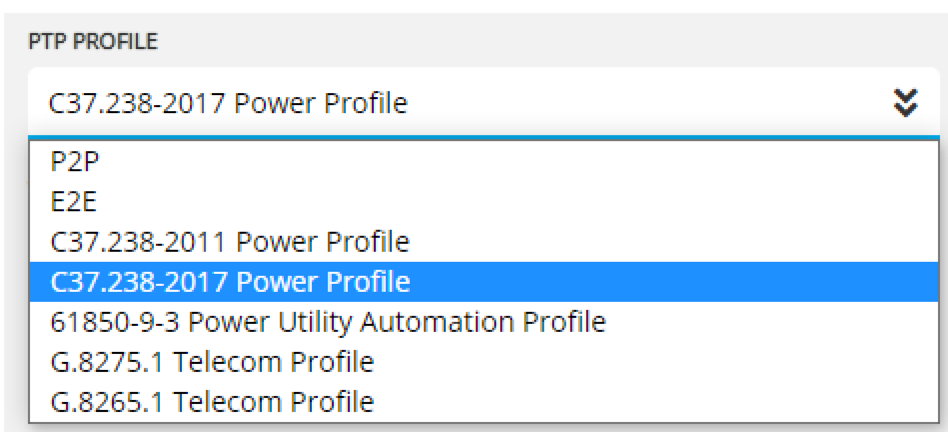
9.5.7.4 C37.238-2017 Power Profile

This section describes how to provision a GridTime 3000 with the C37.238-2017 Power Profile.

1. **Select C37.238-2017 Power Profile**

   From the **PTP PROFILE** drop-down list, select **C37.238-2017 Power Profile**.

Figure 9-176. PTP Profile Settings



2. Follow the instructions in one of the following sections depending on your desired PTP Clock Mode:
   – C37.238-2017 Power Profile Auto Mode
   – C37.238-2017 Power Profile TimeTransmitter Only Mode
   – C37.238-2017 Power Profile TimeReceiver Only Mode

PTP Clock Mode Descriptions

Auto mode allows the port to operate either in the TimeTransmitter or TimeReceiver state depending on whether the GridTime 3000 is in sync. When the GridTime 3000 is in sync or in holdover, the port will be in the TimeTransmitter or passive TimeTransmitter state, when the GridTime 3000 is out of sync the port will be in the TimeReceiver state.

In TimeTransmitter only mode, the port will always either be in the TimeTransmitter or passive TimeTransmitter state depending on whether it has won the BTCA.

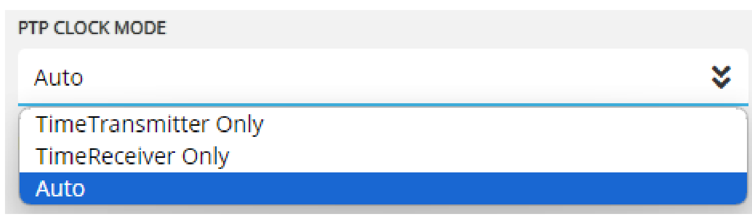
In TimeReceiver only mode, the port will always be in the TimeReceiver or listening state depending on whether there is a PTP TimeTransmitter available to sync to.

9.5.7.4.1 C37.238-2017 Power Profile Auto Mode

This section describes how to provision a PTP C37.238-2017 Power Profile Auto Mode Clock.

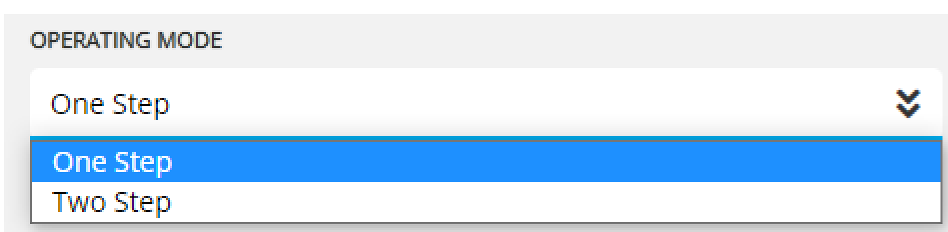
1. **Select Auto for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **Auto**.

Figure 9-177. PTP Clock Mode Settings



2. **Network Protocol**
   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer
3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.
   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-178. Operating Mode Settings



Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to **P2P**, which will set the delay mechanism to peer-to-peer as defined in IEEE 1588v2-2008.

5. **Configure Priority 1 and Priority 2 Fields**

   Modify the **PRIORITY #1** and **PRORITY #2** settings if required, otherwise it is recommended that these are left as their default values.

   These parameters modify the automatic selection of TimeTransmitter clocks in PTP networks. Lower values mean that the unit will be preferred against other TimeTransmitter capable clocks during the selection process. The priority 1 value is used to manually select which TimeTransmitter capable clock will become the grandmaster and will be used in preference over other selection criteria including clock accuracy , so should be modified very carefully. The priority 2 value is treated as the least important criteria, providing greater selection control between otherwise-equal clocks

   For both priority fields, the input range is 0 to 255, where 0 is the highest priority. The default setting is 128.

   Figure 9-179. Priority #1 and #2 Settings

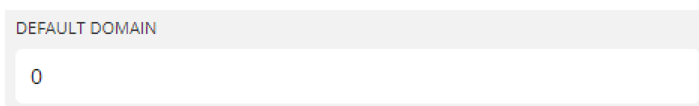
   

6. **Configure Default Domain**

   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127.

   Figure 9-180. Default Domain Settings

7. **Configure Delay Asymmetry**

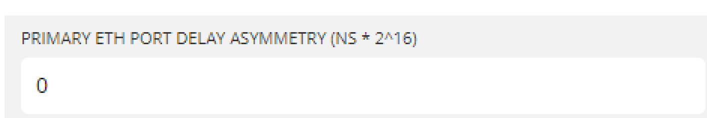
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.

   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces the PTP time accuracy.

   Delay asymmetry is determined by the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the error caused by delay in asymmetry in the PTP delay calculation mechanism.

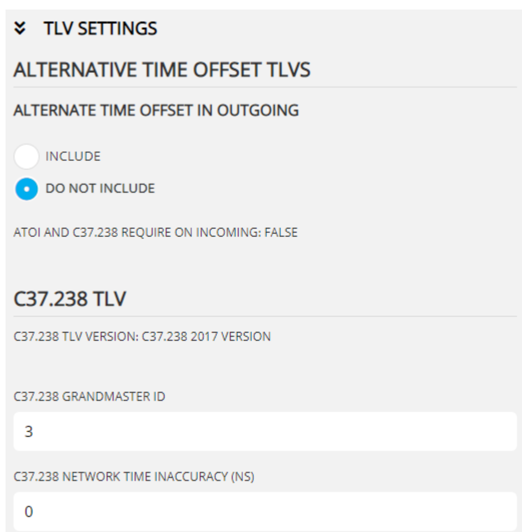
   If the delay asymmetry is known, entering it manually will allow it to be compensated for, and improve time accuracy. The input range is 3.2768e+14 ns×$2^{\wedge 16}$ to −3.2768e+14 ns×$2^{\wedge 16}$ (-5 to 5 seconds).

   Figure 9-181. Delay Asymmetry Settings

8. **Peer Delay Request Interval**
   By default, the **PEER DELAY REQUEST INTERVAL** is set to 1 second.
9. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1 second.
10. **Announce Receipt Timeout**
    By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
11. **Sync Interval**
    By default, the **SYNC INTERVAL** is set to 1 second.
12. **BTCA**
    By default, the BTCA operations are set to **BASIC** and will operate as defined in IEEE 1588v2-2008.
13. **Clock Class Rules**
    By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
14. **Configure TLV Settings**
    With the C37.238-2017 profile, neither the ATOI TLV nor the C37.238 TLV is required on incoming traffic. The ATOI TLV can be included in outgoing traffic using the **ALTERNATIVE TIME OFFSET IN OUTGOING** setting, and the C37.238 TLV is always included in outgoing traffic. The C37.238 TLV includes two configurable settings — the C37.238 Grandmaster ID, and the C37.238 Network Time Inaccuracy.

Figure 9-182. TLV Settings



TLV Settings > GrandMaster ID

Set the C37.238 Grandmaster ID setting using the **C37.238 GRANDMASTER ID** text box.

This is the GMIdentity or the Grandmaster Identity as defined in C37.238-2017. Grandmaster Identity is transmitted in IEEE_C37_238 TLV (2 bytes). The configurable range is 0 to 65,535. By default, it is set to 3.

Figure 9-183. Grandmaster ID Settings

TLV Settings > C37.238 Network Time Inaccuracy

Set the C37.238 Network Time Inaccuracy setting using the **C37.238 NETWORK TIME INACCURACY (NS)** text box.

This configurable field sets the networkTimeInaccuracy as defined in C37.238-2011. It will set the estimated worst-case error in nanoseconds from the grandmaster. The configurable range is 0 (default) to 2,147,483,647 ns.

Figure 9-184. Network Time Inaccuracy Settings

15. **Save Settings**

    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-185. Successful Save Notification

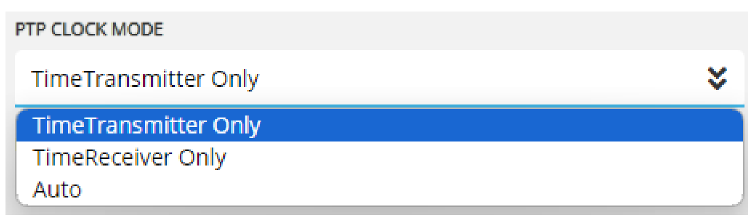
9.5.7.4.2 C37.238-2017 Power Profile TimeTransmitter Only Mode

This section describes how to provision a PTP C37.238-2017 Power Profile TimeTransmitter Only Mode Clock.

1. **Select TimeTransmitter Only for PTP Clock Mode**

   From the **PTP CLOCK MODE** drop-down list, select **TimeTransmitter Only**.

Figure 9-186. PTP Clock Mode Settings



2. **Network Protocol**

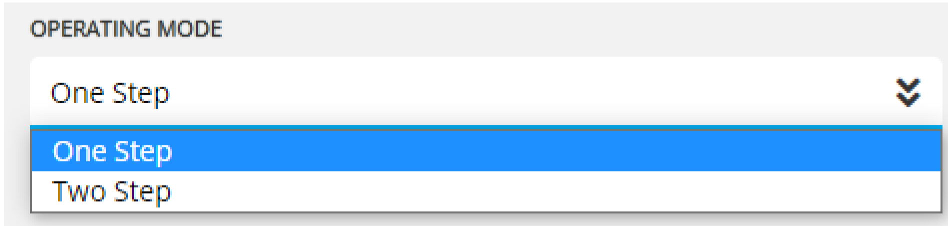
   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer

3. **Select Operating Mode**

   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-187. Operating Mode Settings



Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**

   By default, the **DELAY MECHANISM** is set to **P2P**, which sets the delay mechanism to peer-to-peer as defined in IEEE 1588v2-2008.

5. **Configure Priority 1 and Priority 2 Fields**

   Modify the **PRIORITY #1** and **PRORITY #2** settings if required, otherwise it is recommended that these are left as their default values.

   These parameters modify the automatic selection of TimeTransmitter clocks in PTP networks. Lower values mean that the unit will be preferred against other TimeTransmitter capable clocks during the selection process. The priority 1 value is used to manually select which TimeTransmitter capable clock will become the grandmaster and will be used in preference over other selection criteria including clock accuracy , so should be modified very carefully. The priority 2 value is treated as the least important criteria, providing greater selection control between otherwise-equal clocks

   For both priority fields, the input range is 0 to 255, where 0 is the highest priority. The default setting is 128.

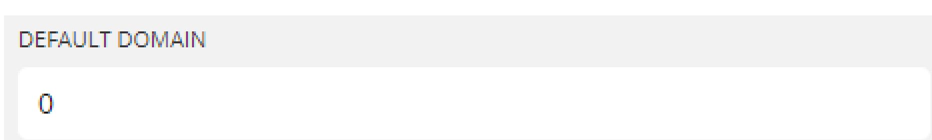
Figure 9-188. Priority #1 and #2 Settings

6. **Configure Default Domain**

   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127 and 254.

Figure 9-189. Default Domain Settings

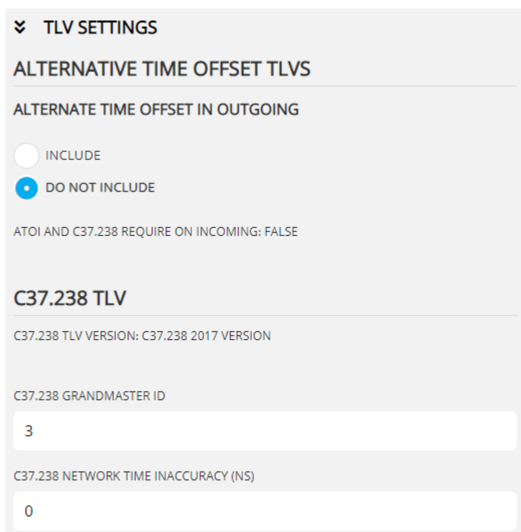


7. **Peer Delay Request Interval**

   By default, the **PEER DELAY REQUEST INTERVAL** is set to 1 second.

8. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1 second.
9. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
10. **Sync Interval**
    By default, the **SYNC INTERVAL** is set to 1 second.
11. **BTCA**
    By default, the BTCA operations are set to **BASIC** and will operate as defined in IEEE 1588v2-2008.
12. **Clock Class Rules**
    By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
13. **Configure TLV Settings**
    With the C37.238-2017 profile, neither the ATOI TLV or the C37.238 TLV are required on incoming traffic. The ATOI TLV can be included in outgoing traffic using the **ALTERNATIVE TIME OFFSET IN OUTGOING** setting, and the C37.238 TLV is always included in outgoing traffic. The C37.238 TLV includes two configurable settings — the C37.238 Grandmaster ID, and the C37.238 Network Time Inaccuracy.

Figure 9-190. TLV Settings

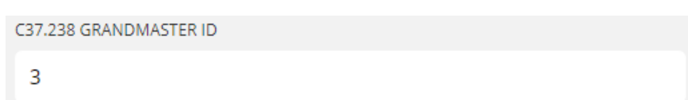


GrandMaster ID

Set the C37.238 Grandmaster ID setting using the **C37.238 GRANDMASTER ID** text box.

This is the GMIdentity or Grandmaster Identity as defined in C37.238-2017. Grandmaster Identity is transmitted in IEEE_C37_238 TLV (2 bytes). The configurable range is 0 to 65,535. By default it is set to 3.

Figure 9-191. Grandmaster ID Settings



C37.238 Network Time Inaccuracy

Set the C37.238 Network Time Inaccuracy setting using the **C37.238 NETWORK TIME INACCURACY (NS)** text box.

This configurable field sets the networkTimeInaccuracy as defined in C37.238-2011. It sets the estimated worst-case error in nanoseconds from the Grandmaster. The configurable range is 0 (default) to 2,147,483,647 ns.

Figure 9-192. Network Time Inaccuracy Settings

14. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

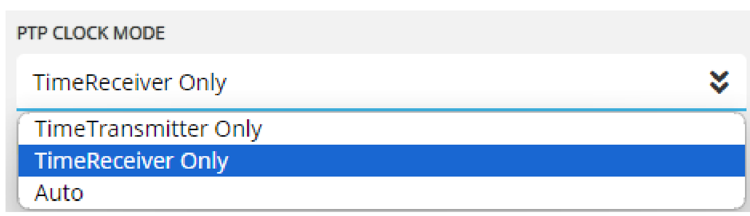
Figure 9-193. Successful Save Notification

9.5.7.4.3 C37.238-2017 Power Profile TimeReceiver Only Mode

This section describes how to provision a PTP C37.238-2017 Power Profile TimeReceiver Only Mode Clock.

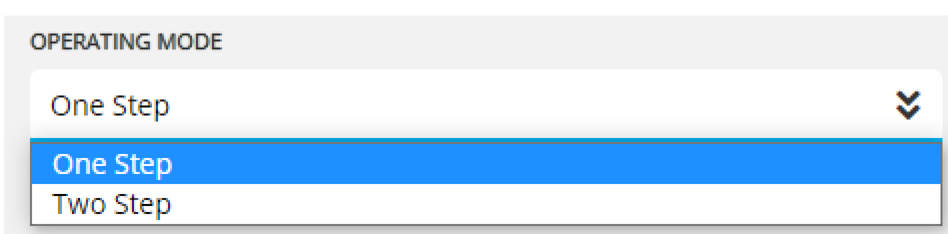
1. **Select TimeReceiver Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeReceiver Only**.

Figure 9-194. PTP Clock Mode Settings



2. **Network Protocol**
   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer
3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.
   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-195. Operating Mode Settings

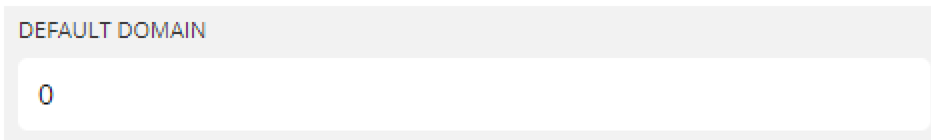


Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to **P2P**, which sets the delay mechanism to peer-to-peer as defined in IEEE 1588v2-2008.
5. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127 and 254.

   Figure 9-196. Default Domain Settings

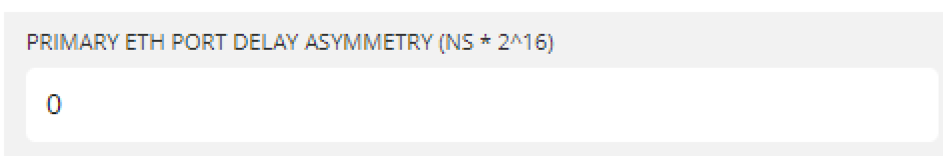
6. **Configure Delay Asymmetry**
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.

   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces PTP time accuracy.

   Delay asymmetry is calculated from the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the error caused by delay in asymmetry in the PTP delay calculation mechanism.

   If the delay asymmetry is known, entering it manually will allow it to be compensated for, and improve time accuracy. The input range is 3.2768e+14 ns×2^{16} to −3.2768e+14 ns×2^{16} (-5 to 5 seconds).

   Figure 9-197. Delay Asymmetry Settings

7. **Peer Delay Request Interval**

   By default, the **PEER DELAY REQUEST INTERVAL** is set to 1 second.
8. **Announce Interval**

   By default, the **ANNOUNCE INTERVAL** is set to 1 second.
9. **Announce Receipt Timeout**

   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
10. **BTCA**

    By default, the BTCA operations are set to **BASIC** and will operate as defined in IEEE 1588v2-2008.

11. **Clock Class Rules**
    By default, **CLOCK CLASS RULES** operations are set to **BASIC** and operates as defined in IEEE 1588v2-2008.
12. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

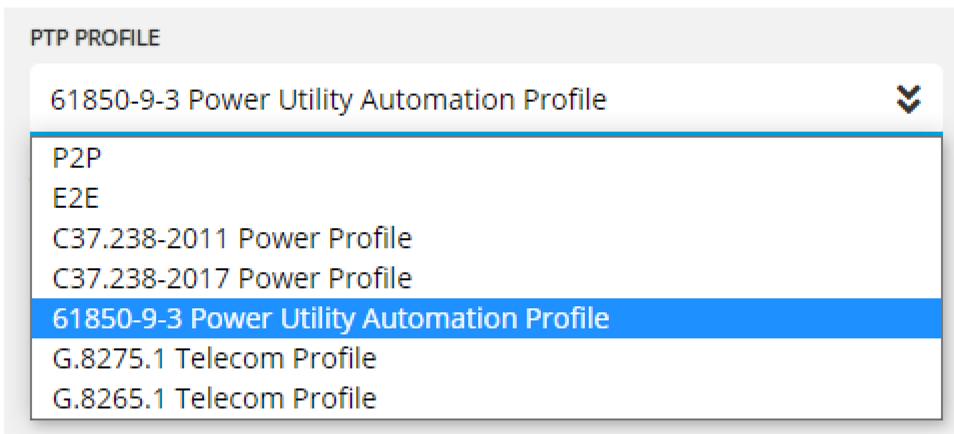
Figure 9-198. Successful Save Notification

9.5.7.5 61850-9-3 Power Utility Profile

This section describes how to provision a GridTime 3000 with the 61850-9-3 Power Utility Profile.

1. **Select 61850-9-3 Power Utility Profile**
   From the **PTP PROFILE** drop-down list, select **61850-9-3 Power Utility Automation Profile**.

Figure 9-199. PTP Profile Settings



2. Follow the instructions in one of the following sections depending on your desired PTP Clock Mode:
   - 61850-9-3 Power Utility Profile Auto Mode
   - 61850-9-3 Power Utility Profile TimeTransmitter Only Mode
   - 61850-9-3 Power Utility Profile TimeReceiver Only Mode

PTP Clock Mode Descriptions

Auto mode allows the port to operate either in the TimeTransmitter or TimeReceiver state depending on whether the GridTime 3000 is in sync or not. When the GridTime 3000 is in sync or in holdover, the port will be in the TimeTransmitter or passive TimeTransmitter state, when the GridTime 3000 is out of sync, the port will be in the TimeReceiver state.

In TimeTransmitter only mode, the port will always either be in the TimeTransmitter or passive TimeTransmitter state depending on whether it has won the BTCA or not.

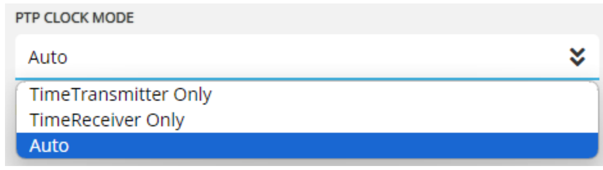
In TimeReceiver only mode, the port will always be in the TimeReceiver or listening state depending on whether there is a PTP TimeTransmitter available to sync to.

9.5.7.5.1 61850-9-3 Power Utility Profile Auto Mode

This section describes how to provision a PTP 61850-9-3 Power Utility Profile Auto Mode Clock.

1. **Select Auto for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **Auto**.

   Figure 9-200. PTP Clock Mode Settings

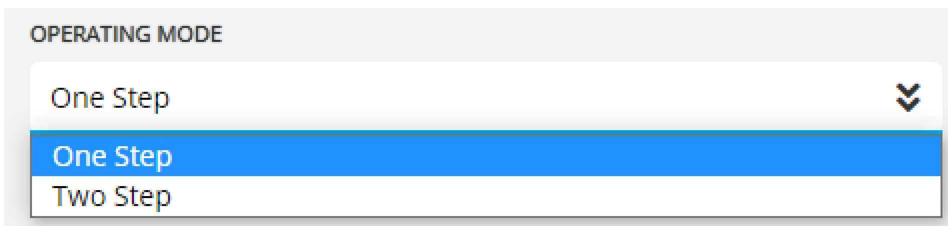
2. **Network Protocol**

   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer

3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

   Figure 9-201. Operating Mode Settings

   Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to **P2P**, which will set the delay mechanism to peer-to-peer as defined in IEEE 1588v2-2008.

5. **Configure Priority 1 and Priority 2 Fields**
   Modify the **PRIORITY #1** and **PRORITY #2** settings if required, otherwise it is recommended that these are left as their default values.

   These parameters modify the automatic selection of TimeTransmitter clocks in PTP networks. Lower values mean that the unit will be preferred against other TimeTransmitter capable clocks during the selection process. The priority 1 value overrides all other selection criteria including clock accuracy, so should be modified carefully. The priority 2 value is treated as the least important criteria, providing greater selection control between otherwise-equal clocks.

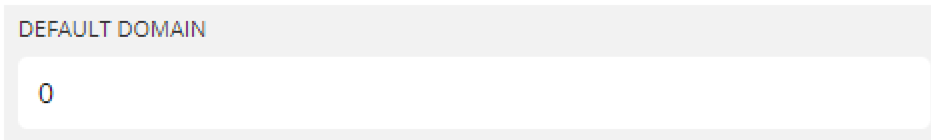
   For both priority fields, the input range is 0 to 255, where 0 is the highest priority. The default setting is 128.

   Figure 9-202. Priority #1 and #2 Settings

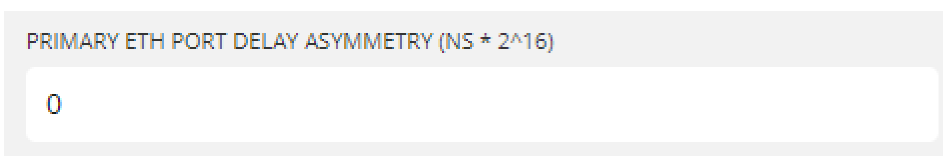
6. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.
   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127 and 254.

   Figure 9-203. Default Domain Settings



7. **Configure Delay Asymmetry**
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.
   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces PTP time accuracy.
   Delay asymmetry is calculated from the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the error caused by delay in asymmetry in the PTP delay calculation mechanism.
   If the delay asymmetry is known, entering it manually will allow it to be compensated for, and improve time accuracy. The input range is 3.2768e+14 ns*2^16 to -3.2768e+14 ns*2^16 (-5 to 5 seconds).

   Figure 9-204. Delay Asymmetry Settings

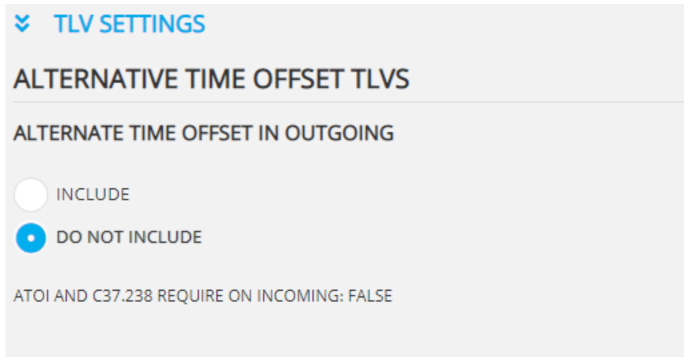


8. **Peer Delay Request Interval**
   By default, the **PEER DELAY REQUEST INTERVAL** is set to 1 second.
9. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1 second.
10. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
11. **Sync Interval**
   By default, the **SYNC INTERVAL** is set to 1 second.
12. **BTCA**
   By default, the BTCA operations are set to **BASIC** and will operate as defined in IEEE 1588v2-2008.
13. **Clock Class Rules**

By default, the **CLOCK CLASS RULES** operations are set to **61850** and operates as defined in IEC 61850-9-3

14. **Configure TLV Settings > Alternate Time Offset In Outgoing**
    With the 61850-9-3 Power Utility Profile, no TLVs are required on incoming traffic. The ATOI TLV can be included in outgoing traffic using the **ALTERNATIVE TIME OFFSET IN OUTGOING** setting.

Figure 9-205. TLV Settings



15. **TLV Settings > ATOI and C37.238 Require on Incoming**
    By default, the **ATOI AND C37.238 REQUIRE ON INCOMING** is set to **FALSE**.
16. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

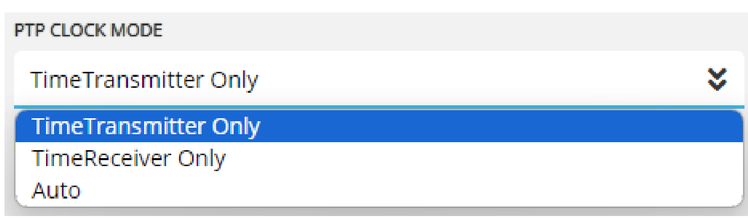
Figure 9-206. Successful Save Notification

9.5.7.5.2 61850-9-3 Power Utility Profile TimeTransmitter Only Mode

This section describes how to provision a PTP 61850-9-3 Power Utility Profile TimeTransmitter Only Mode Clock.

1. **Select TimeTransmitter Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeTransmitter Only**.

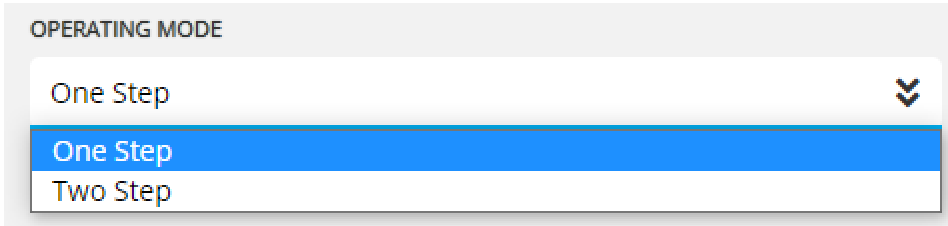
Figure 9-207. PTP Clock Mode Settings



2. **Network Protocol**
   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer
3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-208. Operating Mode Settings



Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to P2P, which sets the delay mechanism to peer-to-peer as defined in IEEE 1588v2-2008.
5. **Configure Priority 1 and Priority 2 Fields**
   Modify the **PRIORITY #1** and **PRORITY #2** settings if required, otherwise it is recommended that these are left as their default values.

   These parameters modify the automatic selection of TimeTransmitter clocks in PTP networks. Lower values mean that the unit will be preferred against other TimeTransmitter capable clocks during the selection process. The priority 1 value overrides all other selection criteria including clock accuracy, so should be modified very carefully. The priority 2 value is treated as the least important criteria, providing greater selection control between otherwise-equal clocks.

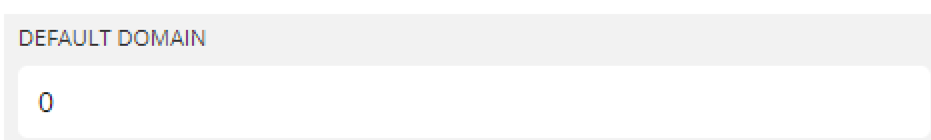
   For both priority fields, the input range is 0 to 255, where 0 is the highest priority. The default setting is 128.

Figure 9-209. Priority #1 and #2 Settings

6. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127 and 254.

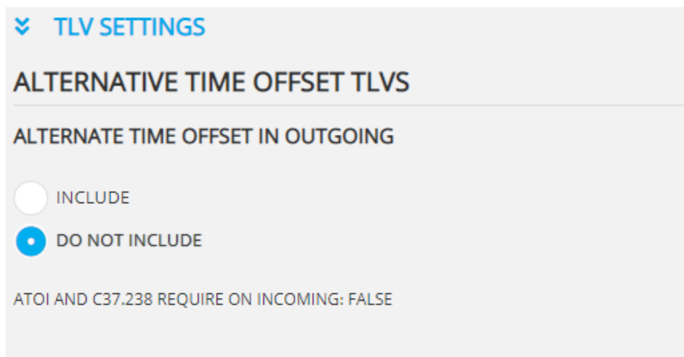
Figure 9-210. Default Domain Settings



7. **Peer Delay Request Interval**
   By default, the **PEER DELAY REQUEST INTERVAL** is set to 1 second.
8. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1 second.

9. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
10. **Sync Interval**
    By default, the **SYNC INTERVAL** is set to 1 second.
11. **BTCA**
    By default, the BTCA operations are set to **BASIC** and will operate as defined in IEEE 1588v2-2008.
12. **Clock Class Rules**
    By default, the **CLOCK CLASS RULES** operations are set to **61850** and operates as defined in IEC 61850-9-3
13. **Configure TLV Settings > Alternate Time Offset In Outgoing**
    With the 61850-9-3 Power Utility Profile, no TLVs are required on incoming traffic. The ATOI TLV can be included in outgoing traffic using the **ALTERNATIVE TIME OFFSET IN OUTGOING** setting.

Figure 9-211. TLV Settings



14. **TLV Settings > ATOI and C37.238 Require on Incoming**
    By default, the **ATOI AND C37.238 REQUIRE ON INCOMING** is set to **FALSE**.
15. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

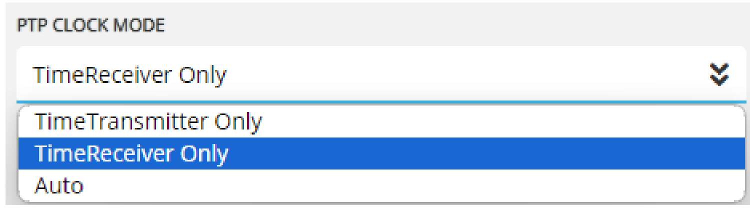
Figure 9-212. Successful Save Notification

9.5.7.5.3 61850-9-3 Power Utility Profile TimeReceiver Only Mode

This section describes how to provision a PTP 61850-9-3 Power Utility Profile TimeReceiver Only Mode Clock.

1. **Select TimeReceiver Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeReceiver Only**.

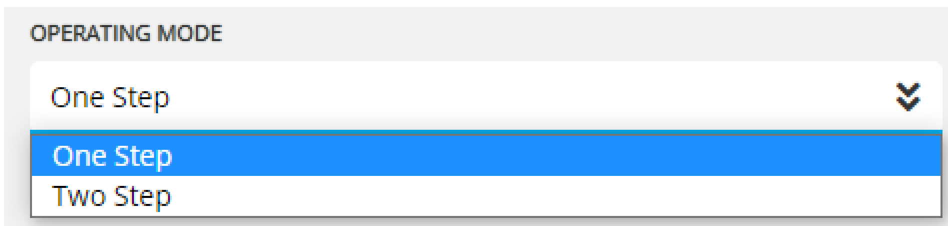
Figure 9-213. PTP Clock Mode Settings



2. **Network Protocol**
   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer
3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-214. Operating Mode Settings

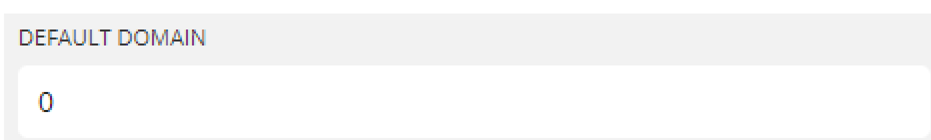


Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default, the **DELAY MECHANISM** is set to P2P, which sets the delay mechanism to peer-to-peer as defined in IEEE 1588v2-2008.
5. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of '0'.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain will cause only devices with the specified domain to communicate using the PTP protocol. The input range is 0 to 127 and 254.

Figure 9-215. Default Domain Settings



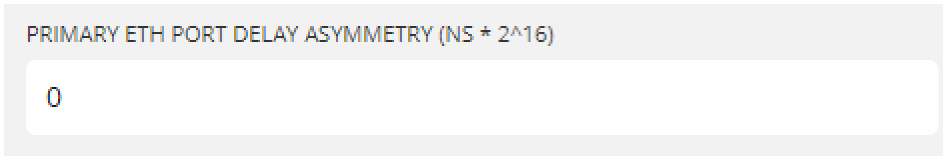
6. **Configure Delay Asymmetry**
   Modify the **PRIMARY ETH PORT DELAY ASYMMETRY (NS* 2^16)** setting if the delay asymmetry in the network link is known, otherwise it is recommended that the setting is left as its default value of '0'.

   PTP automatically calculates the propagation delay between a TimeTransmitter and TimeReceiver, but this calculation assumes the delay in each direction of transmission is the same. PTP cannot measure and compensate for delay asymmetry, which means that the presence of delay asymmetry reduces PTP time accuracy.

Delay asymmetry is calculated from the TimeTransmitter to TimeReceiver path delay minus the TimeReceiver to TimeTransmitter path delay. A TimeReceiver uses the delay asymmetry value to compensate for the error caused by delay in asymmetry in the PTP delay calculation mechanism.

If the delay asymmetry is known, entering it manually will allow it to be compensated for, and improve time accuracy. The input range is 3.2768e+14 ns×$2^{\wedge 16}$ to −3.2768e+14 ns×$2^{\wedge 16}$ (-5 to 5 seconds).

Figure 9-216. Delay Asymmetry Settings



7. **Peer Delay Request Interval**
   By default, the **PEER DELAY REQUEST INTERVAL** is set to 1 second.
8. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1 second.
9. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
10. **BTCA**
    By default, the BTCA operations are set to **BASIC** and will operate as defined in IEEE 1588v2-2008.
11. **Clock Class Rules**
    By default, the **CLOCK CLASS RULES** operations are set to **61850** and operates as defined in IEC 61850-9-3
12. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

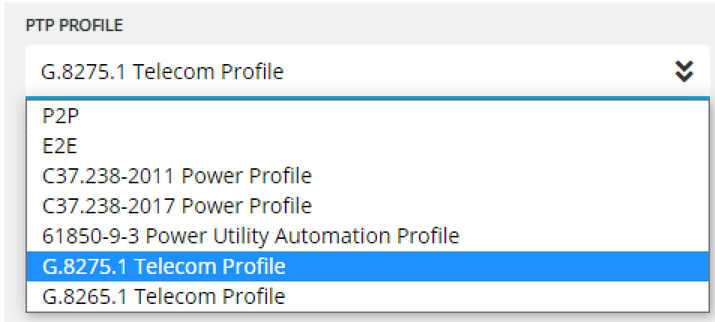
Figure 9-217. Successful Save Notification

9.5.7.6 G.8275.1 Telecom Profile

This section describes how to provision a GridTime 3000 with the G.8275.1 Telecom Profile.

1. **Select G.8275.1 Telecom Profile Profile**
   From the **PTP PROFILE** drop-down list, select **G.8275.1 Telecom Profile**.

Figure 9-218. PTP Profile Settings



2. Follow the instructions in one of the following sections depending on your desired PTP Clock Mode:
   - G.8275.1 Telecom Profile TimeTransmitter Only Mode
   - G.8275.1 Telecom Profile TimeReceiver Only Mode

PTP Clock Mode Descriptions

In TimeTransmitter only mode the port will always either be in the TimeTransmitter or passive TimeTransmitter state depending on whether it has won the BTCA or not.

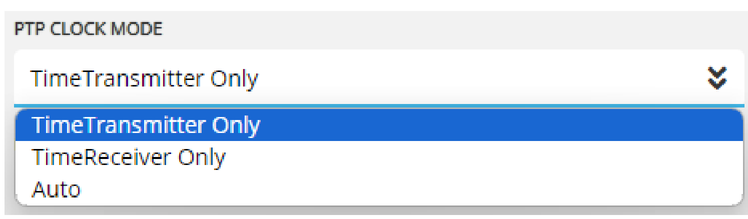
In TimeReceiver only mode, the port will always be in the TimeReceiver or listening state depending on whether there is a PTP TimeTransmitter available to sync to.

9.5.7.6.1 G.8275.1 Telecom Profile TimeTransmitter Only Mode

This section describes how to provision a PTP G.8275.1 Telecom Profile TimeTransmitter Only Mode Clock.

1. **Select TimeTransmitter Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeTransmitter Only**.

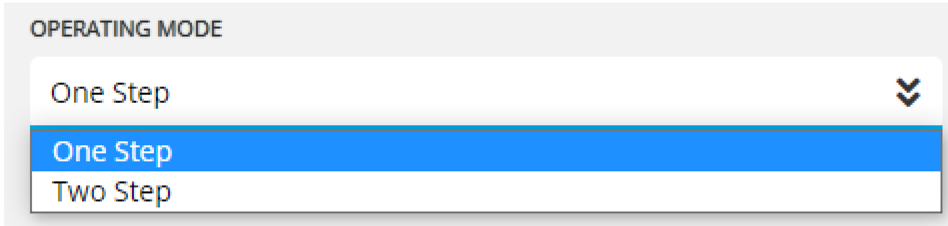
Figure 9-219. PTP Clock Mode Settings



2. **Network Protocol**
   By default, the network protocol is set to Layer 2 (Ethernet), which will send packets through the Ethernet data layer
3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-220. Operating Mode Settings



Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default the **DELAY MECHANISM** is set to E2E, which sets the delay mechanism to end--to-end as defined in IEEE 1588v2-2008.
5. **Configure Priority Fields**
   – The **PRIORITY #1** field is not used by the G.8275.1 alternate BTCA, so is not configurable for the G.8275.1 profile and thus appears with a default value of 128.
   – The **PRIORITY # 2** field is used by the alternate BTCA, in addition to two additional priority fields, the port local priority and clock local priority fields. These parameters modify the automatic selection of TimeTransmitter clocks in PTP networks.

   Priority 2

   In the alternate BTCA selection process, the priority 2 value is treated as the fourth most important selection criteria below clock class, clock accuracy, and clock variance in order, much like the traditional PTP BTCA except that the priority 1 field is not considered.

   Below the priority 2 field, the clock local priority and port local priority fields are compared.

   Clock Local Priority

   The **CLOCK LOCAL PRIORITY** is applied to the local clock when it is compared to a foreign TimeTransmitter. Setting this to a lower value gives preference to the local clock over foreign TimeTransmitters. The input range is 1 to 255, where 1 is the highest priority. The default setting is 128. This attribute is not used when operating as a Grandmaster. Modify these fields to achieve your desired BTCA outcome.

   Port Local Priority

   The **PORT LOCAL PRIORITY** is applied to the Announce messages received on the port from a potential TimeTransmitter when comparing that potential TimeTransmitter to the local clock or other potential TimeTransmitters. Setting this to a lower value gives preference to foreign TimeTransmitters connected to this port. The input range is 1 to 255, where 1 is the highest priority. The default setting is 128. This attribute is not used when operating as a Grandmaster.

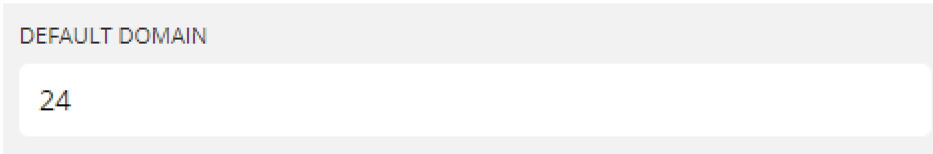
   Figure 9-221. Priority Settings

6. **Configure Default Domain**

Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of **24**.

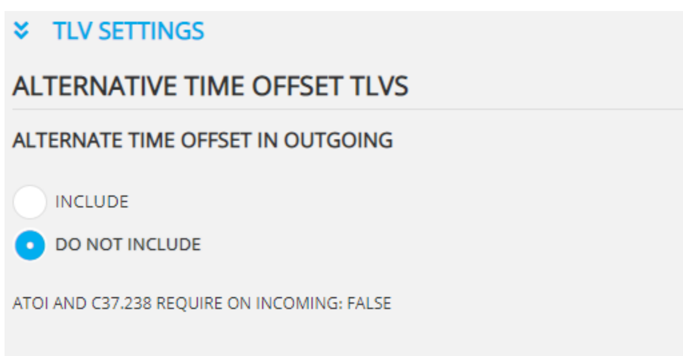
A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain causes only devices with the specified domain to communicate using the PTP protocol. The input range is 24-43.

Figure 9-222. Default Domain Settings



7. **Advertised Delay Request Interval**
   By default, the **ADVERTISED DELAY REQUEST INTERVAL** is set to 1/16 second.
8. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1/8 second.
9. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
10. **Sync Interval**
    By default, the **SYNC INTERVAL** is set to 1/16 second.
11. **BTCA**
    By default, the BTCA operations are set to **G.8275** and operates as defined in ITU-T G 8265.1.
12. **Clock Class Rules**
    By default, the **CLOCK CLASS RULES** operations are set to **G.8275** and operates as defined in ITU-T G 8275.1.
13. **Configure TLV Settings > Alternate Time Offset In Outgoing**
    With the ITU-T G8275.1 TelecomProfile, no TLVs are required on incoming traffic. The ATOI TLV can be included in outgoing traffic using the **ALTERNATIVE TIME OFFSET IN OUTGOING** setting.

Figure 9-223. TLV Settings



14. **TLV Settings > ATOI and C37.238 Require on Incoming**
    By default, the **ATOI AND C37.238 REQUIRE ON INCOMING** setting is set to **FALSE**.
15. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.
    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

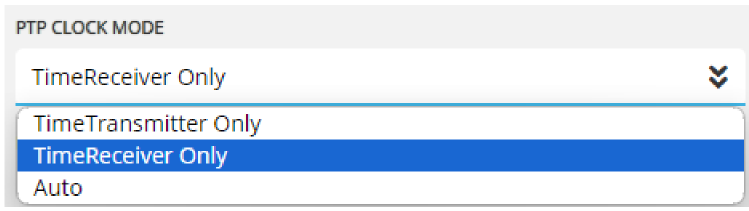
Figure 9-224. Successful Save Notification

9.5.7.6.2 G.8275.1 Telecom Profile TimeReceiver Only Mode

This section describes how to provision a PTP G.8275.1 Telecom Profile TimeReceiver Only Mode Clock.

1. **Select TimeReceiver Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeReceiver Only**.

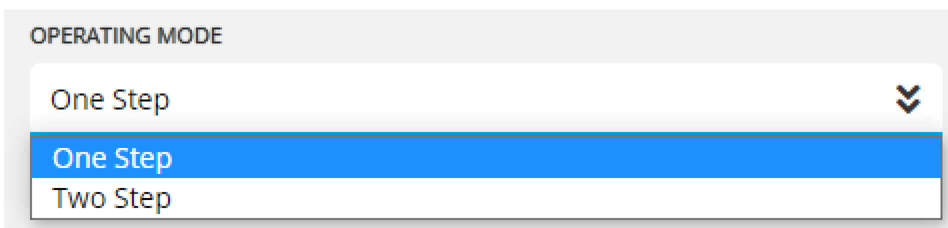
   Figure 9-225. PTP Clock Mode Settings

2. **Network Protocol**
   By default, the **NETWORK PROTOCOL** is set to Layer 2 (Ethernet), which sends packets through the Ethernet data layer
3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

   Figure 9-226. Operating Mode Settings

   Note: Select **Two Step** if the Operating Mode is unknown.
4. **Delay Mechanism**
   By default the **DELAY MECHANISM** is set to E2E, which sets the delay mechanism to end-to-end as defined in IEEE 1588v2-2008.
5. **Configure Priority Fields**
   The **PORT LOCAL PRIORITY** setting does not have a significant behavioral impact in TimeReceiver only mode and the clock local priority setting has no impact. The port local priority only affects the BTCA comparison of different TimeTransmitters it can see, as it can not consider itself as a TimeTransmitter candidate.

   Clock Local Priority

   The **CLOCK LOCAL PRIORITY** does not affect the execution of the BTCA in TimeReceiver only mode, as the port cannot consider itself as a potential TimeTransmitter in the BTCA process. Therefore, it can be left unchanged.

   Modify these fields to achieve your desired BTCA outcome.

   Port Local Priority

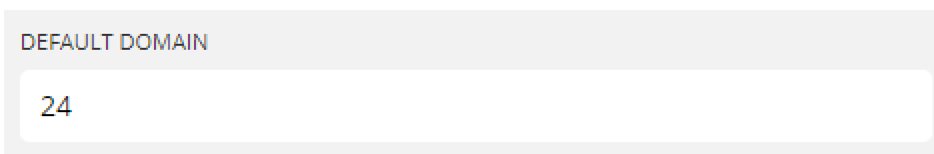
The **PORT LOCAL PRIORITY** is applied to the announce messages received on the port from a potential TimeTransmitter when comparing that potential TimeTransmitter to the local clock or other potential TimeTransmitter. Setting this to a lower value gives preference to foreign TimeTransmitters connected to this port, against TimeTransmitters connected to a different port. The input range is 1 to 255, where 1 is the highest priority. The default setting is 128. This attribute is not used when operating as a grandmaster.

Figure 9-227. Port Local Priority Settings

6. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of **24**.

   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with a domain of '0'. Changing the domain causes only devices with the specified domain to communicate using the PTP protocol. The input range is 24-43.

   Figure 9-228. Default Domain Settings

7. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1/8 second.
8. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
9. **BTCA**
   By default, the BTCA operations are set to **G.8275** and operates as defined in ITU-T G 8275.1.
10. **Clock Class Rules**
    By default, the **CLOCK CLASS RULES** operations are set to **G.8275** and operates as defined in ITU-T G 8275.1.
11. **TLV Settings > ATOI and C37.238 Require on Incoming**
    By default, the **ATOI AND C37.238 REQUIRE ON INCOMING** setting is set to FALSE.
12. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

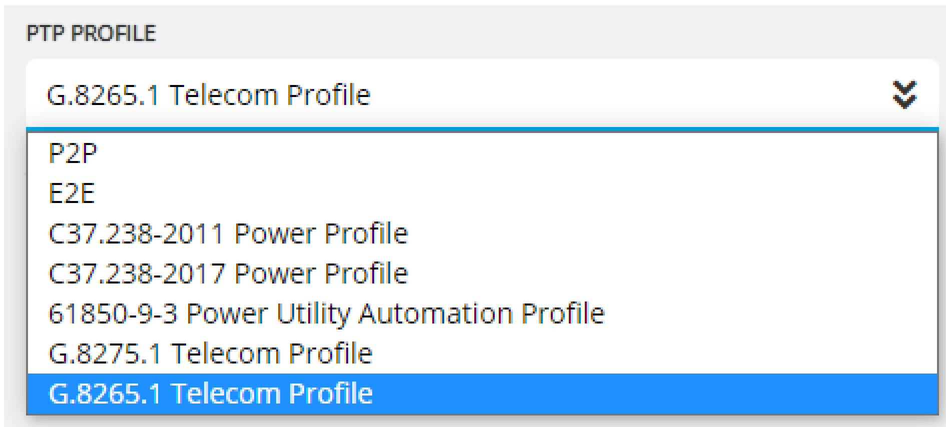
Figure 9-229. Successful Save Notification

9.5.7.7 G.8265.1 Telecom Profile

This section describes how to provision a GridTime 3000 with the G.8265.1 Telecom Profile.

1. **Select G.8265.1 Telecom Profile Profile**
   From the **PTP PROFILE** drop-down list, select **G.8265.1 Telecom Profile**.

Figure 9-230. PTP Profile Settings



2. Follow the instructions in one of the following sections depending on your desired PTP Clock Mode:
   - G.8265.1 Telecom Profile TimeTransmitter Only Mode
   - G.8265.1 Telecom Profile TimeReceiver Only Mode

PTP Clock Mode Descriptions

In TimeTransmitter only mode, the port will always either be in the TimeTransmitter or passive TimeTransmitter state depending on whether it has won the BTCA or not.

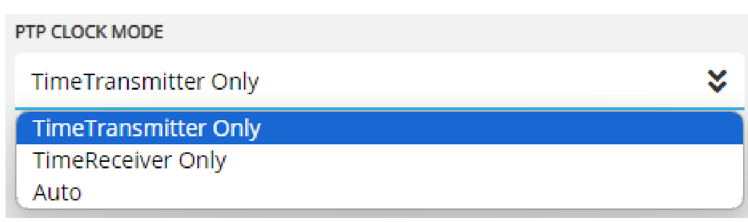
In TimeReceiver only mode, the port will always be in the TimeReceiver or listening state depending on whether there is a PTP TimeTransmitter available to sync to.

9.5.7.7.1 G.8265.1 Telecom Profile TimeTransmitter Only Mode

This section describes how to provision a PTP G.8265.1 Telecom Profile TimeTransmitter Only Mode Clock.

1. **Select TimeTransmitter Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeTransmitter Only**.

Figure 9-231. PTP Clock Mode Settings

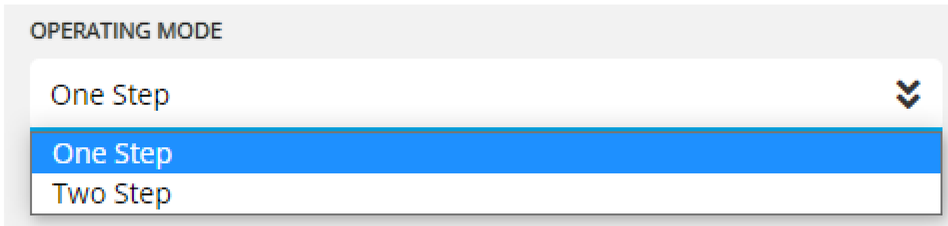


2. **Network Protocol**

By default, the network protocol is set to Layer 3 (UDP), which sends packets through the Ethernet data layer

3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.
   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

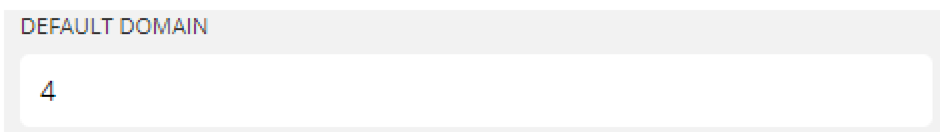
Figure 9-232. Operating Mode Settings



Note: Select **Two Step** if the Operating Mode is unknown.

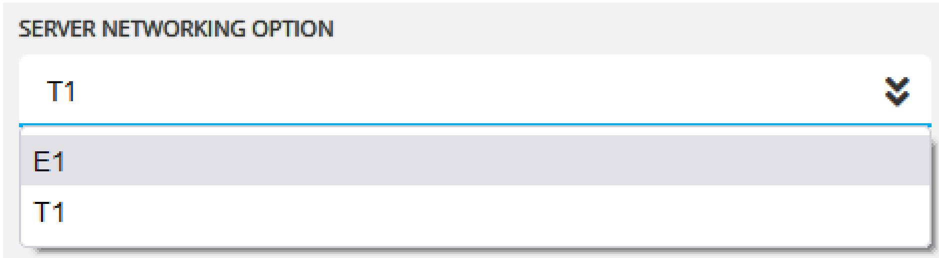
4. **Delay Mechanism**
   By default the **DELAY MECHANISM** is set to E2E, which sets the delay mechanism to end--to-end as defined in IEEE 1588v2-2008.
5. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of **4**.
   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with domain 4. Changing the domain causes only devices with the specified domain to communicate using the PTP protocol. The input range is 4-23.

Figure 9-233. Default Domain Settings



6. **Advertised Delay Request Interval**
   By default, the **ADVERTISED DELAY REQUEST INTERVAL** is set to 1/16 second.
7. **Announce Interval**
   By default, the **ANNOUNCE INTERVAL** is set to 1/8 second.
8. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
9. **Sync Interval**
   By default, the **SYNC INTERVAL** is set to 1/16 second.
10. **BTCA**
    By default, the BTCA operations are set to **G.8265** and operates as defined in ITU-T G 8265.1.
11. **Configure TimeTransmitter Networking Option**
    From the **SERVER NETWORKING OPTION** drop-down list, select the TimeTransmitter networking option from either **T1** or **E1**. The clock class rules changes to reflect the selected option.

Figure 9-234. TimeTransmitter Networking Option Settings



12. **Clock Class Rules**
    By default, the **CLOCK CLASS RULES** operations are set to **G.8265**. It appears as either **G.8265 (Option I)** if a **TimeTransmitter NETWORKING OPTION** of **T1** is selected or **G.8265 (Option II)** if **E1** is selected and operates as defined in ITU-T G.8265.1.
13. **Configure the TimeTransmitter Force Quality (Optional)**
    If this option is configured, then the GridTime 3000 reports its accuracy as being equal to the specified level, regardless of the quality of the sync sources or the actual accuracy of the GridTime 3000. The available options depend on the configured TimeTransmitter Networking Option, and are defined in clause 5.4.2 of [ITU-T G.781]. If the GridTime 3000 should report its true accuracy, select the **None** option.
14. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.

    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

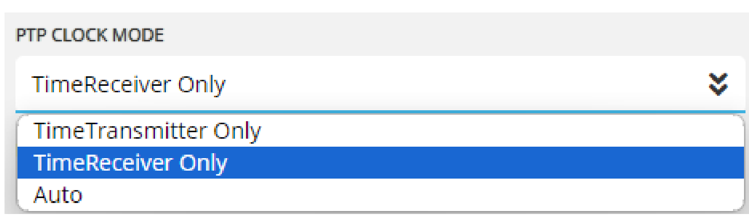
Figure 9-235. Successful Save Notification

9.5.7.7.2 G.8265.1 Telecom Profile TimeReceiver Only Mode

This section describes how to provision a PTP G.8265.1 Telecom Profile TimeReceiver Only Mode Clock.

1. **Select TimeReceiver Only for PTP Clock Mode**
   From the **PTP CLOCK MODE** drop-down list, select **TimeReceiver Only**.

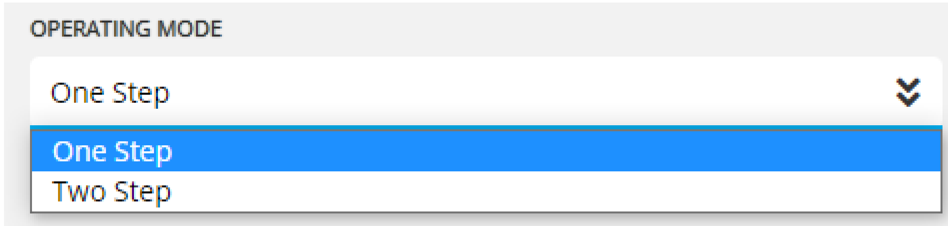
Figure 9-236. PTP Clock Mode Settings



2. **Network Protocol**
   By default, the **NETWORK PROTOCOL** is set to Layer 3 (UDP), which sends packets through the Network data layer
3. **Select Operating Mode**
   From the **OPERATING MODE** drop-down list, select the operating mode for the PTP network.

   Operating mode is a network wide parameter. The configurable options are **One Step** or **Two Step**.

Figure 9-237. Operating Mode Settings

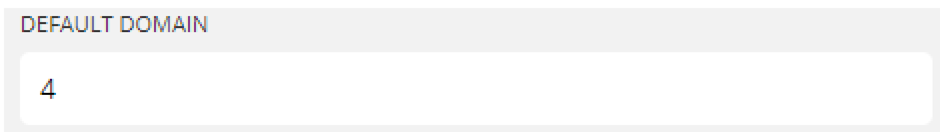


Note: Select **Two Step** if the Operating Mode is unknown.

4. **Delay Mechanism**
   By default the **DELAY MECHANISM** is set to E2E, which sets the delay mechanism to end-to-end as defined in IEEE 1588v2-2008.
5. **Configure Default Domain**
   Modify the **DEFAULT DOMAIN** number if required, otherwise it is recommended that it is left at its default value of **4**.

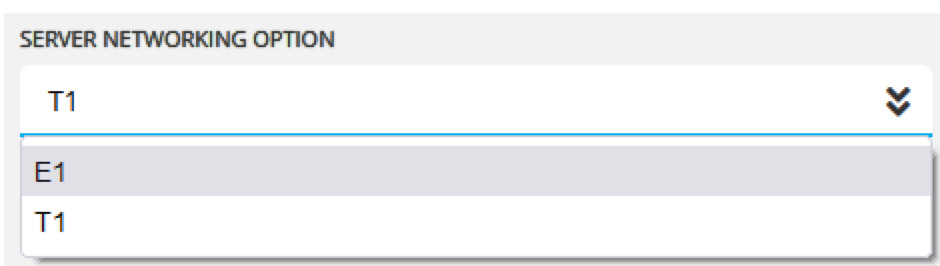
   A domain consists of one or more PTP devices communicating with each other. By default, PTP aware devices are configured with domain '0'. Changing the domain cause only devices with the specified domain to communicate using the PTP protocol. The input range is 4-23.

Figure 9-238. Default Domain Settings



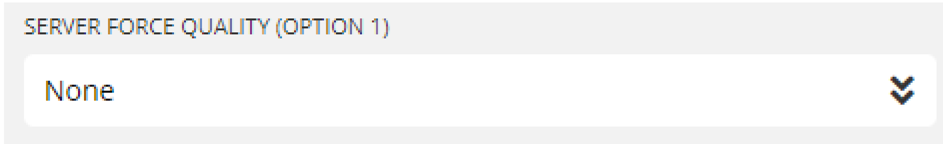
6. **Announce Receipt Timeout**
   By default, the **ANNOUNCE RECEIPT TIMEOUT** is set to 3. This means that after 3 announce intervals, if the device has not received an announce message, it triggers an announce receipt timeout event, which moves the port into a listening state.
7. **Configure TimeTransmitter Networking Option**
   From the **SERVER NETWORKING OPTION** drop-down list, select the TimeTransmitter networking option from either **T1** or **E1**. The clock class rules changes to reflect the selected option.

Figure 9-239. TimeTransmitter Networking Option Settings



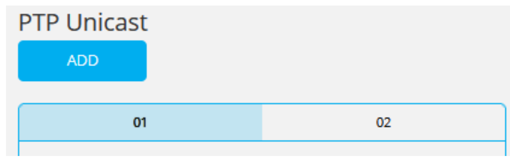
8. **Configure the Forced Quality**
   The TimeTransmitter force quality option should be set to **None** regardless of the TimeTransmitter Networking Option selected.

Figure 9-240. TimeTransmitter Force Quality Option Settings



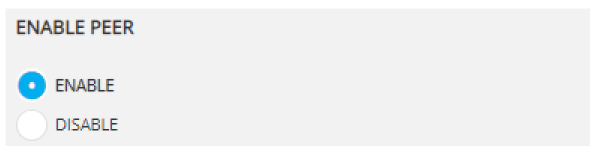
9. **Add the PTP Peer**
   Click the **ADD** button as shown in the following figure. A tabbed collection of settings are displayed. Multiple peers can be added and are accessible by selecting the numbered tabs. Each tab is numbered in the order they were created as shown in the following figure.

   Figure 9-241. PTP Peer Addition Settings



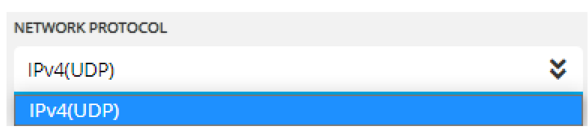
10. **Enable the Peer**
    By default, the enable settings are blank. To enable a peer, select the **ENABLE** radio button. If desired, an operator can later disable the peer without deleting it by selecting the **DISABLE** option. A disabled peer does not send signaling messages, or respond to sync messages.

    Figure 9-242. Enable/Disable Peer



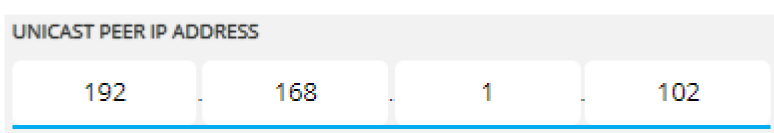
11. **Configure the IP settings**
    From the **NETWORK PROTOCOL** drop-down list, select **IPv4(UDP)**. It is the only available option to G.8265.1 peers, but the GridTime 3000 Ethernet port will not operate as a G.8265.1 TimeReceiver unless this option is selected.

    Figure 9-243. Network Protocol Settings

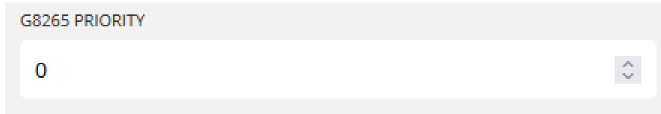


    Add the IP address of the TimeTransmitter to the **UNICAST PEER IP ADDRESS** section. The GridTime 3000 sends signaling messages to this IP address requesting announce and sync messages.

    Figure 9-244. TimeTransmitter IP Address Setting

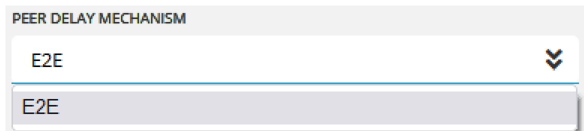


12. **Configure the G.8265 Priority**
    Enter the desired priority into the **G8265 PRIORITY** text box.



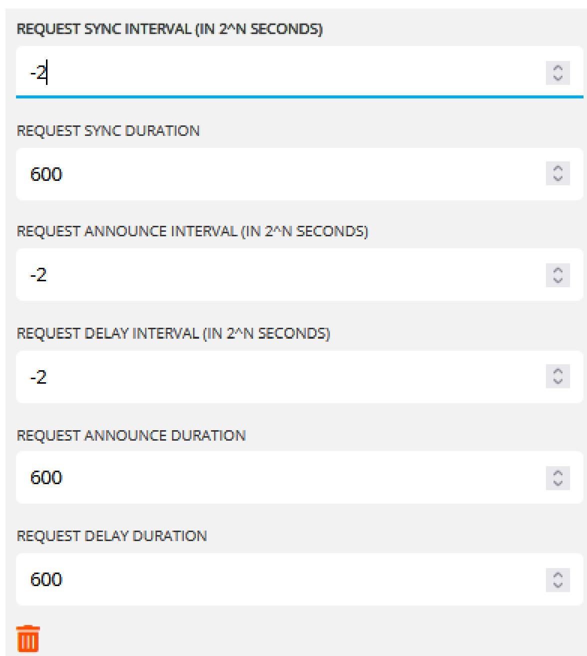
13. **Configure the Delay Mechanism**
    The G.8265.1 PTP profile only supports the End-to-End delay mechanism. Select this item from the drop-down as shown. This is the only option available, but the GridTime 3000 Ethernet port will not operate as a G.8265 TimeReceiver unless this setting is selected.

    Figure 9-245. Peer Delay Mechanism Setting

14. **Configure the Sync Interval, Announce Interval, and Delay Interval**
    These settings control the interval at which the G.8265.1 TimeTransmitter sends the associated packets. All of these fields take values from -7 to 4 seconds.
    The units for these fields are in units 2^{n}. For example, if '-2' is entered into one of these fields, then the TimeTransmitter will send the associated message every 0.5 seconds.

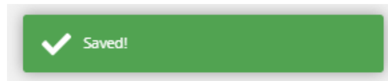
    Figure 9-246. TimeTransmitter Packet Settings

15. **Configure the Request Sync Duration, Request Announce Duration, and Request Delay Duration**
    These settings control the duration for which the G.8265.1 TimeTransmitter sends the associated packets. All these fields take values from 60 to 1000 seconds.
16. **Delete Unwanted Peers or Repeat Steps 6-12 to Add Additional Peers (Optional)**
    Unwanted peers can be deleted using the button at the bottom left of the PTP Unicast Peer pane. The GridTime 3000 imposes no software restrictions on the number of G.8265.1 peers that can be added.

17. **Save Settings**
    To write the settings to GridTime 3000, click **SAVE**.
    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-247. Successful Save Notification



9.6 Provisioning GNSS

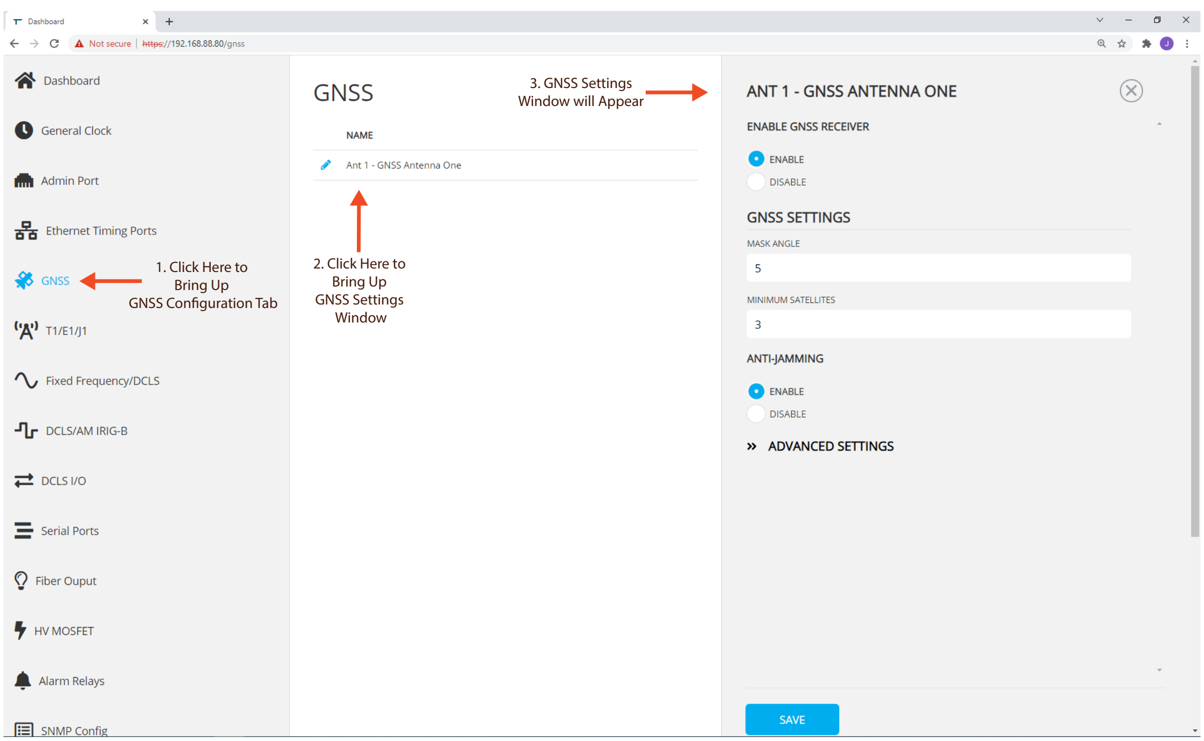
This section describes how to provision the antenna port settings on the GridTime 3000.

The GNSS configuration tab is used to configure the GridTime 3000 antenna ports. Choosing the correct settings ensures that the GridTime 3000 can receive GNSS time signals and accurately synchronize to time from GNSS satellites.

To configure the GridTime 3000 for GNSS time synchronization, perform the following steps:

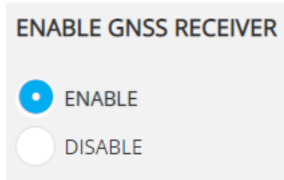
1. **Navigate to the GNSS Settings Window**
   To navigate to the GNSS configuration tab, on the left navigation pane, click **GNSS**, and then in the center of the screen, click the GNSS antenna name. This opens the corresponding GNSS antenna settings window on the right pane.

Figure 9-248. GNSS Configuration Tab



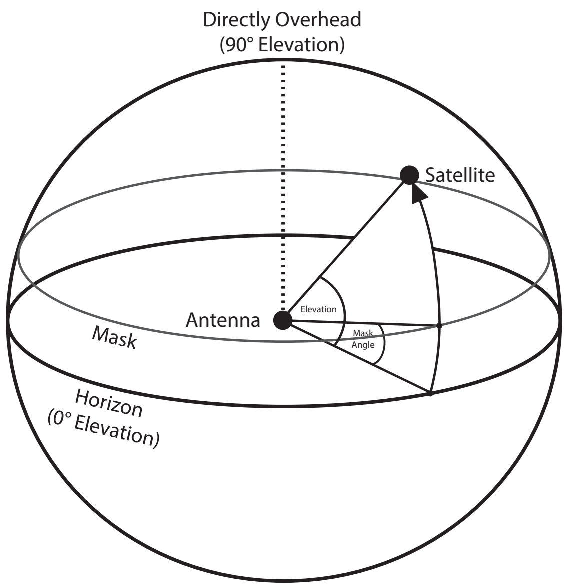
2. **Enable GNSS Receiver**
   Under the GNSS antenna settings pane, under the **ENABLE GNSS RECEIVER** section, select **ENABLE**.

Figure 9-249. Enable GNSS Receiver Settings



3. **Set Mask Angle**
   The mask angle threshold setting defines the minimum required elevation angle of GNSS satellites above the horizon when viewed from the antenna's current position. This angle is commonly referred to as elevation, and ranges from 0° - on the horizon, to 90° - directly overhead.

   Figure 9-250. Mask Angle Illustration

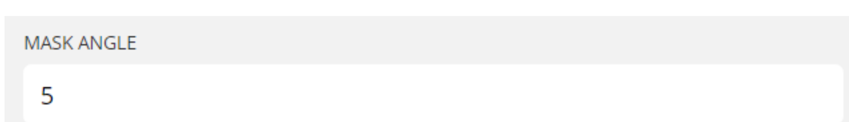
   Signals from satellites that are obstructed by objects on the horizon such as mountains may provide inconsistent GNSS coverage due to interference. The mask angle threshold setting provides a method to filter out these inconsistent signals ensuring the GridTime 3000 only uses stable and accessible satellites.

   By default, the mask angle is set to 5°, which means that only those satellites with an elevation of 5° or more is used for time synchronization.

   For a different mask angle, on the right pane, under the **GNSS Settings** section, in the **MASK ANGLE** text box, type a value between 0° and 90°.

   ,

   Figure 9-251. Mask Angle Settings

Tip:
A higher mask angle setting ensures that a more accurate time is received from GNSS satellites, as signal interference from objects in the environment is reduced.

However, as the mask angle is made higher, satellites that are closer to the horizon cannot be used, meaning there are less usable satellites. This creates a higher risk of a GNSS synchronization dropout occurring as satellites enter and exit the usable mask angle throughout the day. With a 90° mask angle, no satellites can be used at all.

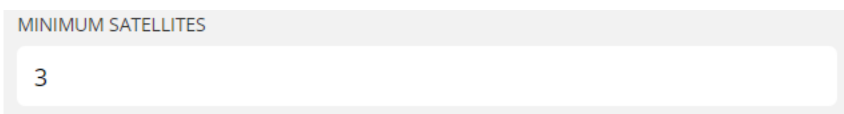
Important: Microchip do not recommend increasing the mask angle value above 20° for most use cases.

4. **Set Minimum Satellites**
   The minimum satellites threshold setting determines the minimum number of usable GNSS satellites that should be available at a given time. If the number of detected satellites is less than this, the low satellites alarm is triggered. For more information, see Alarm Conditions and Correction Actions.

   By default, this is set to three satellites, as three satellites is the minimum number required for the GridTime 3000 to calculate a position fix. Position fixes are required to calculate the time from GNSS satellite signals, so if less than three usable satellites are detected, the GridTime 3000 cannot synchronize to GNSS regardless of the minimum satellites threshold.

   For a different minimum satellites threshold, on the right pane, under the **GNSS Settings** section, in the **MINUMUM SATELLITES** text box, type a value between 0 and 184.

Figure 9-252. Minimum Satellites Settings



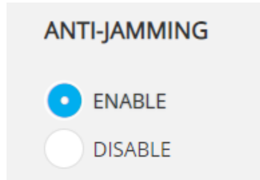
Tip:
A higher minimum satellites setting gives you more warning when your GridTime 3000 has insufficient satellites available, alerting you of the need to relocate your antenna to a site with better GNSS satellite reception before synchronization loss. This offers superior GNSS synchronization dropout prevention.

However, if the value is set too large, the GridTime 3000 frequently triggers the 'low satellites' alarm unnecessarily, flooding your system with meaningless alarms.

For this reason, we recommend not increasing this value above 10 for most cases.

5. **Set Anti-Jamming Mode**
   This setting enables the GridTime 3000 to utilize the anti-jamming and spoofing algorithms of the GNSS receiver that offers protection against jamming or spoofing GNSS attacks.

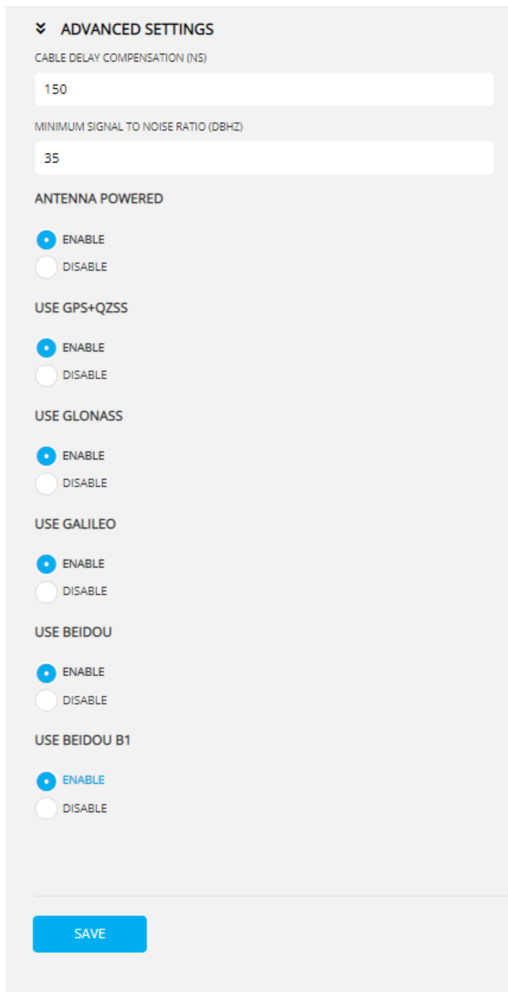
Figure 9-253. GNSS Anti-Jamming Settings



Note: This setting is enabled by default, and Microchip recommends leaving it enabled to ensure the most amount of protection from jamming and spoofing attacks.

6. **Expand Advanced Settings**
   The advanced settings drop down contains additional settings when it is expanded.

Figure 9-254. GNSS Advanced Settings



a. **Set Cable Delay Compensation**
   The **CABLE DELAY COMPENSATION (NS)** setting determines how much delay compensation the GridTime 3000 will apply to the calculated time when it is synchronized to GNSS. The GridTime 3000 adds the value of this setting to the calculated time in nanoseconds to compensate for the propagation delay of the GNSS signals as they pass through the antenna installation to the GridTime 3000's antenna port.

For optimal time accuracy, the propagation delay of the installation should be calculated using the following formula:

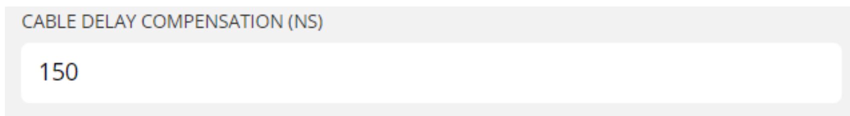
Figure 9-255. Formula to Calculate the Propagation Delay

$$\textit{Total Antenna Installation Delay}\ (ns) = \textit{Antenna Delay}\ (ns) + \textit{Cable Delay}\ (ns/m) \times \textit{Cable Length}\ (m)$$

This gives a fairly good approximation of the total antenna installation delay, but the delay values of inline amplifiers and lightning arrestors can be included as well if they are known. The delay values for the stock accessories provided with the GridTime 3000 are approximately 1–2 ns, low enough to be considered negligible. Other accessories, especially those with high-quality filters, may have more than 30 ns delay. If the cable delay is not known, 4 ns/m is a good approximation for most coaxial cable.

The default value of the cable delay compensation is 150 ns.

Figure 9-256. Cable Delay Compensation Setting



Note: If the antenna installation propagation delay is incorrectly compensated for, GNSS time synchronization will have an additional constant delay equal to the difference between the delay compensation setting and the true antenna installation delay

b. **Set Minimum Signal to Noise Ratio (DBHz)**
Signal to noise ratio (SNR) is the ratio of the usable component of a signal to the unusable noise component. It is defined as the signal power; the component of a signal containing only the transmitted information, divided by the noise power; the unwanted random disturbance component of the signal caused by environmental and electrical factors.

Figure 9-257. Signal To Noise Ratio Definition

$$SNR = \frac{\textit{Signal Power}\ (W)}{\textit{Noise Power}\ (W)}$$

When measured in logarithmic units, more commonly known as decibels (dB), SNR is defined as:

Figure 9-258. Signal To Noise Calculation

$$SNR\ (dB) = 10log_{10}(SNR) = 10log_{10}\left(\frac{\textit{Signal Power}\ (W)}{\textit{Noise Power}\ (W)}\right)$$

The **MINIMUM SIGNAL TO NOISE RATIO (DBHZ)** setting determines the minimum SNR (dB) expected from the GNSS satellite signals for satellites to be considered usable for time synchronization by the GridTime 3000.

GNSS signals with a low SNR are considered low quality, and are less reliably decoded. This results in less accurate time synchronization, hence, satellites that are below the signal to noise ratio threshold are filtered out.

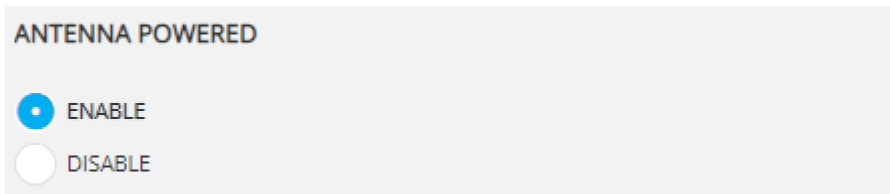
By default, the minimum signal to noise ratio is 35 dB.

Figure 9-259. Minimum SNR Setting

Note: Microchip recommends leaving this setting at 35 dBHz unless a large number of GNSS satellites are consistently available at the site of installation. A 35 dBHz SNR is sufficient for high-quality, accurate GNSS time synchronization.

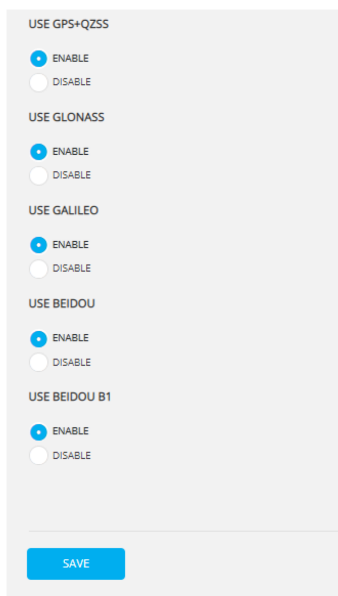
c. **Configure Internal Antenna Power Supply**
The GridTime 3000 can supply 5V and at most 80 mA to RF equipment through the antenna connector and cable. To enable or disable this supply, under the **ANTENNA POWERED** option, select the **ENABLE** or **DISABLE** radio button respectively.

Figure 9-260. Antenna Power Supply Settings



d. **Configure the GNSS Constellations**
The GNSS radio buttons determine the GNSS constellations used by the GridTime 3000 for time synchronization.

Figure 9-261. Enable/Disable the GNSS Constellations



Tip: Microchip recommends leaving all GNSS constellations enabled for time synchronization. This ensures as many GNSS satellites as possible are available at a given time, reducing the risk of GNSS synchronization dropouts.

Note: GPS and QZSS share signal properties and operates on same frequency band, that can cause problems in the receiver if only one is enabled. GridTime 3000 enables/disables GPS and QZSS together.

Note: At least one constellation must be enabled at all times.

e. **Save Settings**
To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

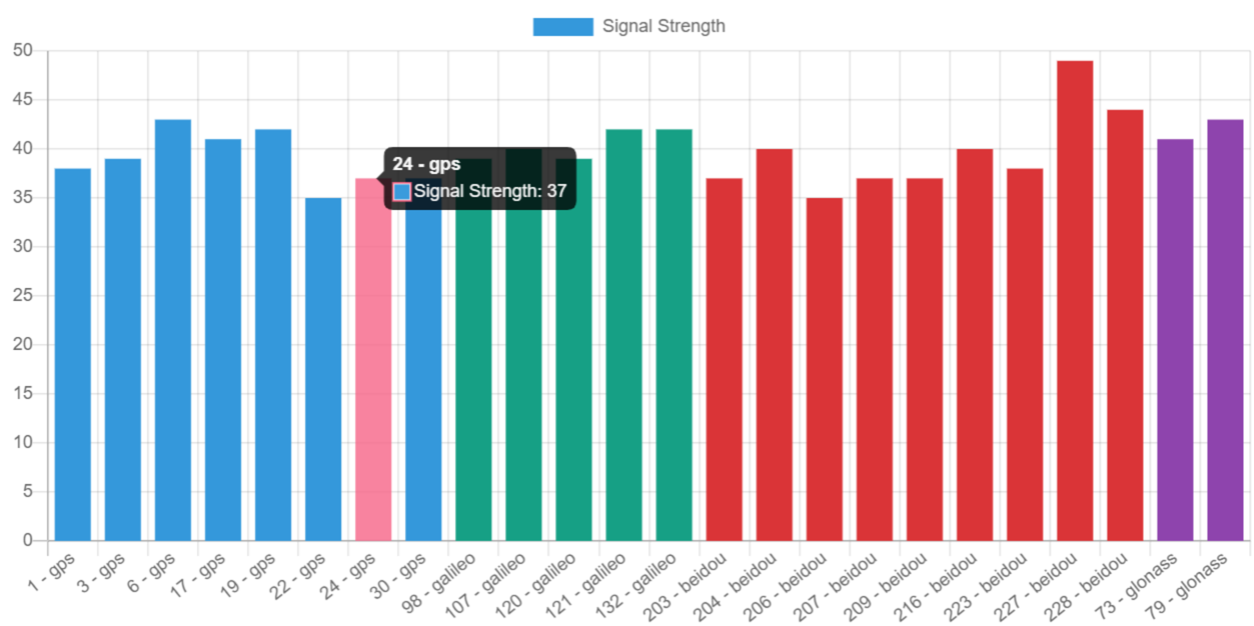
Figure 9-262. Settings Saved Notification

7. **Verify settings**
Validate the GNSS settings against the information on the Clock Management Tool (CMT) dashboard.

The satellite graph is a bar chart representing the SNR values of all the satellites used by the GridTime 3000, as well as the GNSS constellation they belong to. The satellite ID is shown at the base of each bar on the chart Satellite Graph.

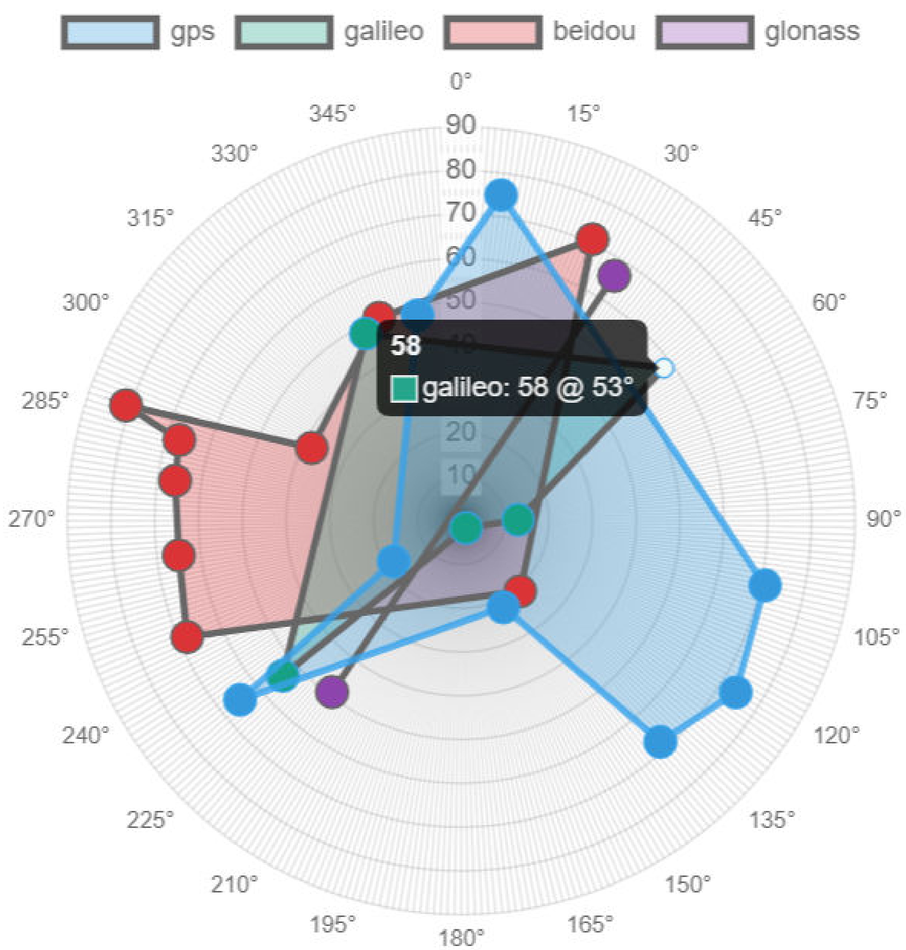
Check that the SNR values are above the signal to noise ratio threshold, and that only satellites from enabled constellations are present. Hover over individual satellites to check their signal strength.

Figure 9-263. Satellite Graph



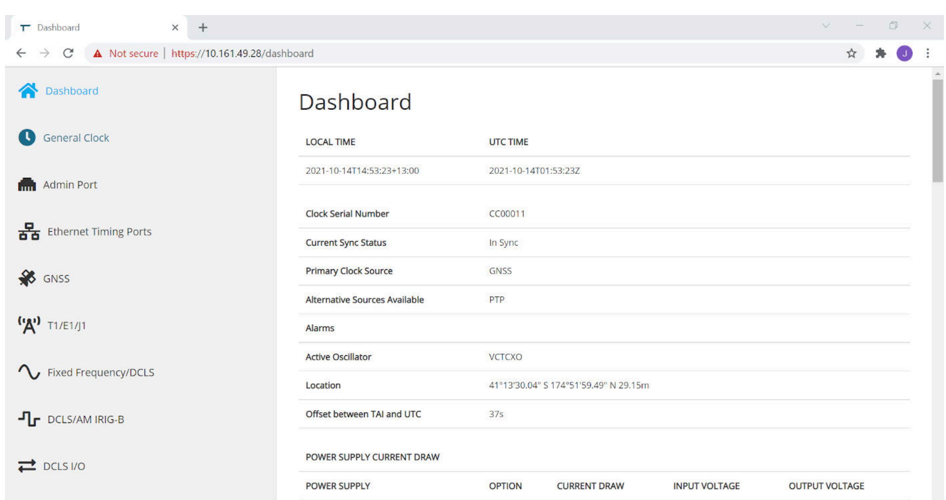
The satellite almanac shows the sky position of the satellites, including the elevations. Check that the satellite elevations are above the mask angle. The axis going up the middle of the almanac indicates elevation. When hovering on the satellite the first number that appears will also indicate the elevation. In the below example the satellite is at an elevation of 58 degrees and a position of 53 degrees from the receiver.

Figure 9-264. Satellite Almanac



Lastly, check that the GridTime 3000 is GNSS synchronized by navigating to the CMT dashboard. The GridTime 3000 should report that its current sync state is **In Sync** and that its primary clock source is **GNSS**.

Figure 9-265. CMT Dashboard

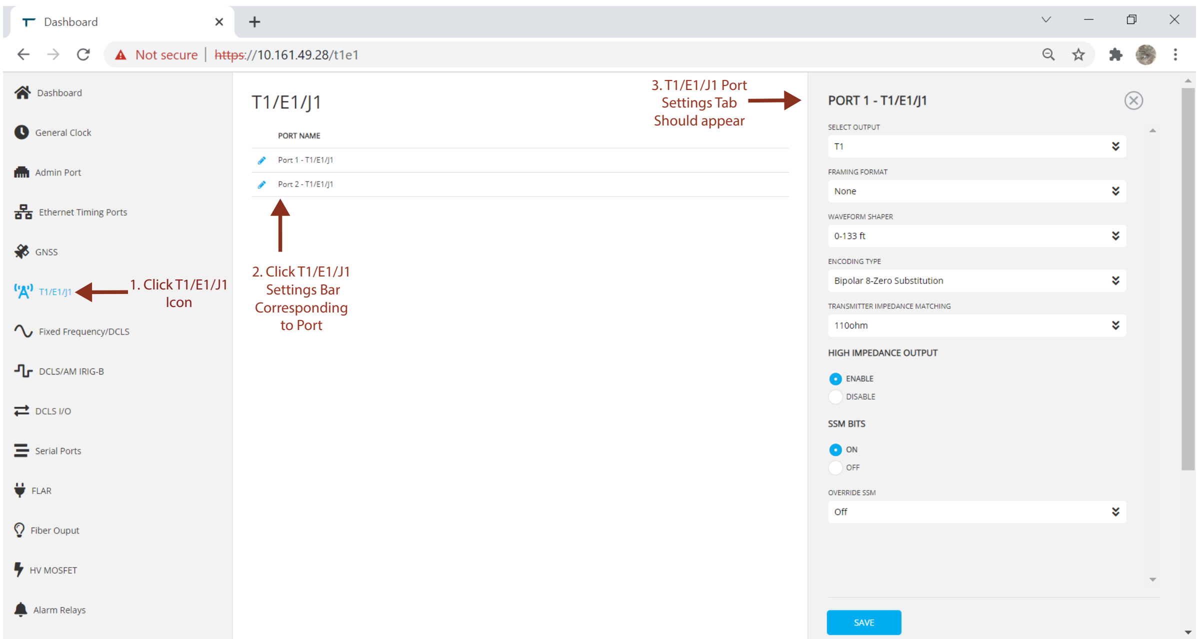


9.7 Provisioning the T1/E1/J1 Ports

This section describes how to provision the T1/E1/J1 ports.

1. **Navigate to the T1/E1/J1 Port Configuration Window**
   To navigate to the T1/E1/J1 Port configuration window, on the left navigation panel, click T1/E1/J1, and then click the settings bar corresponding to the port you want to configure. The **Port 01 - T1/E1/J1** settings tab is displayed on the right panel.

   Figure 9-266. T1/E1/J1 Configuration Window



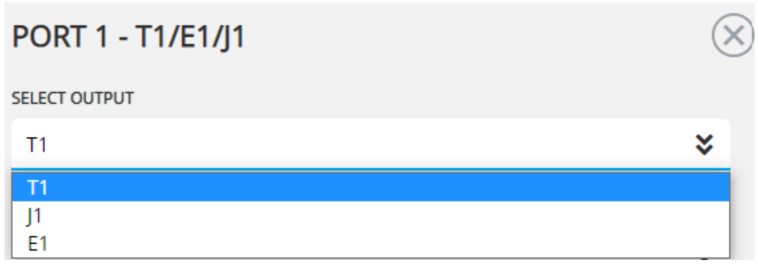
2. Follow the instructions in one of the following sections depending on the type of output signal you want to configure:
   – Provisioning T1 Output
   – Provisioning J1 Output
   – Provisioning E1 Output

9.7.1 Provisioning T1 Output

This section describes how to provision a T1/E1/J1 Port to output a T1 signal.

1. **Select Output**
   From the **SELECT OUTPUT** drop-down list, select **T1**. This reveals the T1-specific configuration options.
   Note: As the T1/E1/J1 ports must both output the same signal type (T1, J1, or E1), the signal output type for both ports is only configurable in the port 1 configuration window.

Figure 9-267. Selecting the T1 Output

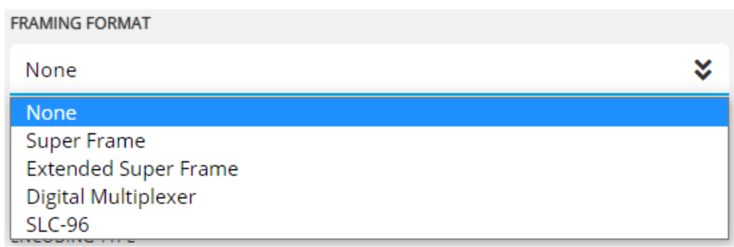


2. **Enable Port**
From the **High Impendance Output** radio buttons, select **ENABLE SIGNAL**. This displays the T1 output specific settings.

Figure 9-268. Enable Low Impedance Output

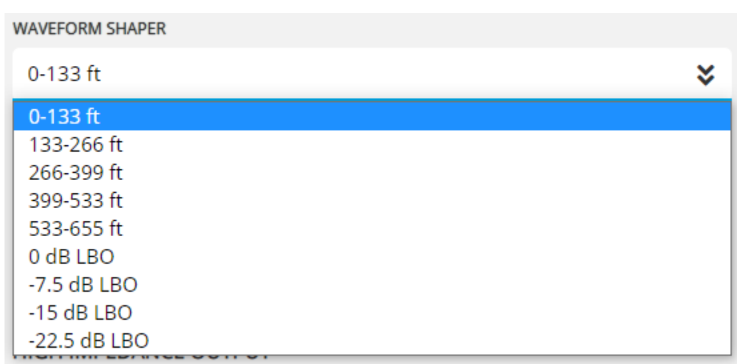
3. **Select Framing Format**
Select the appropriate framing format option from the **FRAMING FORMAT** drop-down list. By default, the framing format is set to **None**.

Figure 9-269. Select Framing Format



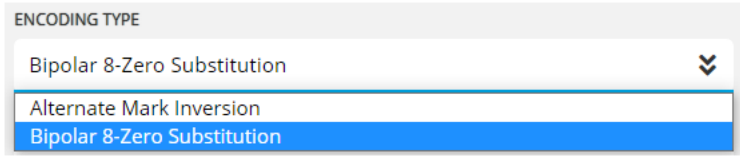
4. **Select Waveform Shaper**
Select the appropriate waveform shaper option from the **WAVEFORM SHAPER** drop-down list. By default, the waveform shaper is set to **0-133 ft**.

Figure 9-270. Select Waveform Shaper



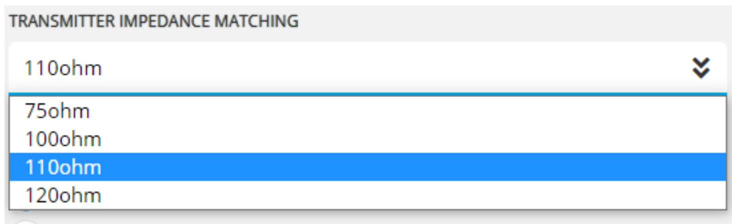
5. **Select Encoding Type**
Select the required encoding type from the **ENCODING TYPE** drop-down list. By default, the encoding type is set to **Bipolar 8-Zero Substitution**.

Figure 9-271. Select Encoding



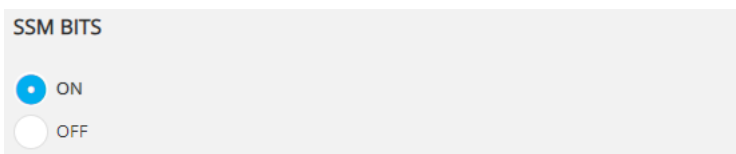
6. **Select Transmitter Impedance Matching**
   Select the correct transmitter impedance option from the **TRANSMITTER IMPEDANCE MATCHING** drop-down list. By default, this value is set to **110ohm**.

Figure 9-272. Set the Transmitter Impedance Matching



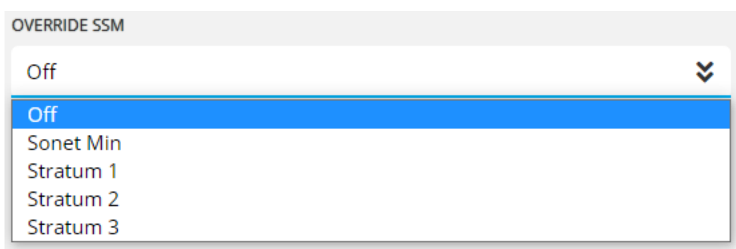
7. **Enable or Disable SSM Bits**
   Enable or disable SSM bits in the output signal using the **SSM BITS** radio buttons.

Figure 9-273. Enable/Disable SSM Bits



8. **Select Override SSM Behavior**
   Select the override SSM value from the **OVERRIDE SSM** drop-down list.

Figure 9-274. Select the Override SSM Value



9. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-275. Successful Save Notification

9.7.2 Provisioning J1 Output

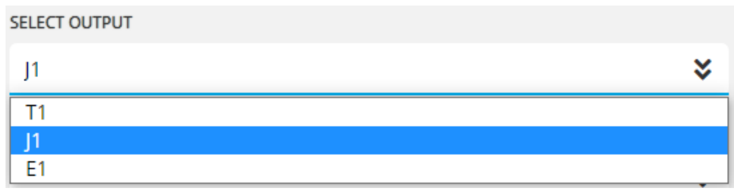
This section describes how to provision a T1/E1/J1 Port to output a J1 signal.

1. **Select Output**

   From the **SELECT OUTPUT** drop-down list, select **J1**. This reveals the J1-specific configuration options.

   Note: As the T1/E1/J1 ports must both output the same signal type (T1, J1, or E1), the signal output type for both ports is only configurable in the port 1 configuration window.

   Figure 9-276. Selecting the J1 Output

2. **Enable Port**

   From the **High Impendance Output** radio buttons, select **ENABLE SIGNAL**. This displays the J1 output specific settings.

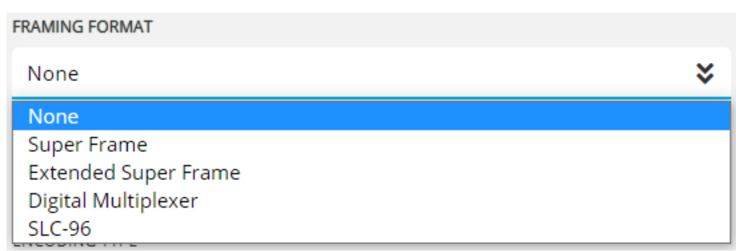
   Figure 9-277. Enable Low Impedance Output

3. **Select Framing Format**

   Select the appropriate framing format option from the **FRAMING FORMAT** drop-down list. By default, the framing format is set to **None**.

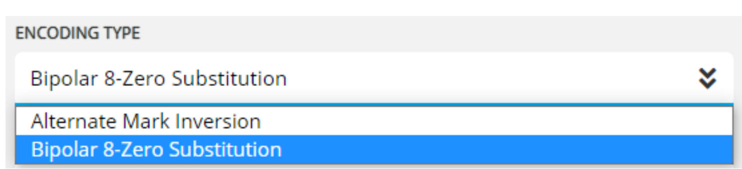
   Figure 9-278. Select Framing Format

4. **Select Encoding Type**

   Select the required encoding type from the **ENCODING TYPE** drop-down list. By default, the encoding type is set to **Bipolar 8-Zero Substitution**.

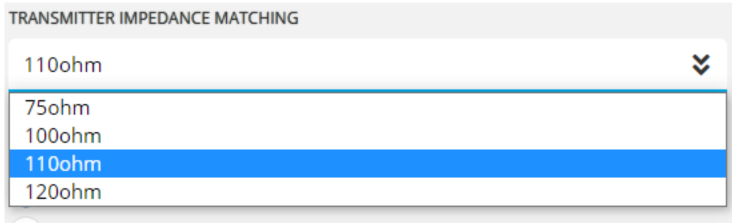
   Figure 9-279. Select Encoding

5. **Select Transmitter Impedance Matching**

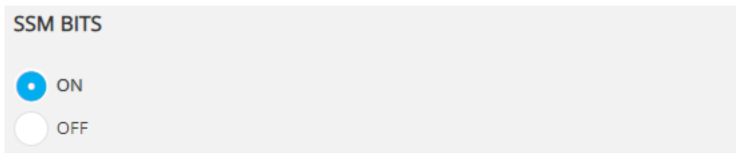
   Select the correct transmitter impedance option from the **TRANSMITTER IMPEDANCE MATCHING** drop-down list. By default, this value is set to **110ohm**.

Figure 9-280. Set the Transmitter Impedance Matching



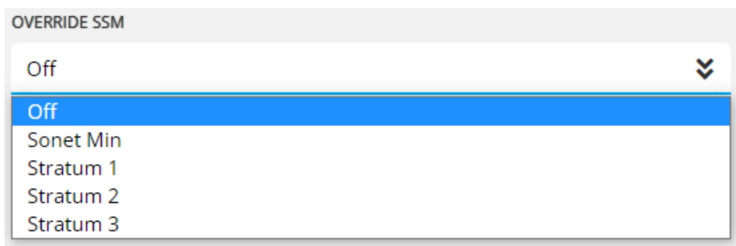
6. **Enable or Disable SSM Bits**
   Enable or disable SSM bits in the output signal using the **SSM BITS** radio buttons.

Figure 9-281. Enable/Disable SSM Bits



7. **Select Override SSM Behavior**
   Select the override SSM value from the **OVERRIDE SSM** drop-down list.

Figure 9-282. Select the Override SSM Value



8. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.

   A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-283. Successful Save Notification

Note:
Refer T1 section of translation of configuration files. J1 has similar digital transmission format to T1, but it is used in Japan instead of North America. J1 lines have the same total data transmission rate of 1.544 Mbps as T1 lines.

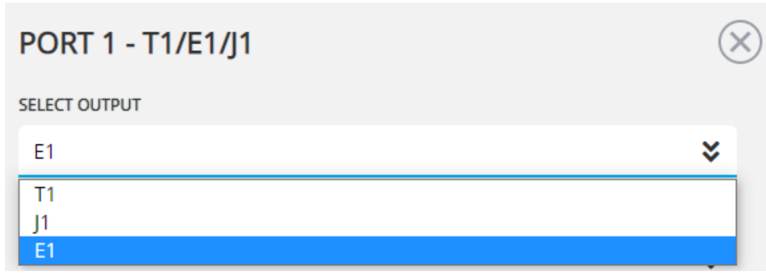
9.7.3 Provisioning E1 Output

This section describes how to provision a T1/E1/J1 Port to output a E1 signal.

1. **Select Output**
   From the **SELECT OUTPUT** drop-down list, select **E1**. This reveals the E1-specific configuration options.

   Note: As the T1/E1/J1 ports must both output the same signal type (T1, J1, or E1), the signal output type for both ports is only configurable in the port 1 configuration window.

Figure 9-284. Selecting the E1 Output

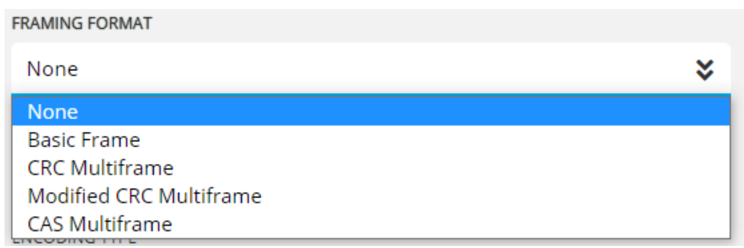


2. **Enable Port**
   From the **High Impedance Output** radio buttons, select **ENABLE SIGNAL**. This displays the E1 output specific settings.

Figure 9-285. Enable Low Impedance Output

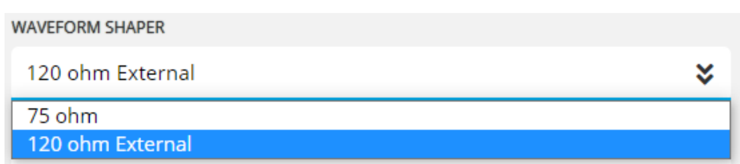
3. **Select Framing Format**
   Select the appropriate framing format option from the **FRAMING FORMAT** drop-down list. By default, the framing format is set to **None**.

Figure 9-286. Select Framing Format



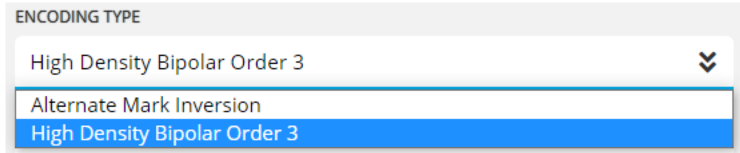
4. **Select Waveform Shaper**
   Select the appropriate waveform shaper option from the **WAVEFORM SHAPER** drop-down list. By default, the waveform shaper is set to **120 ohm External**.

Figure 9-287. Select Waveform Shaper



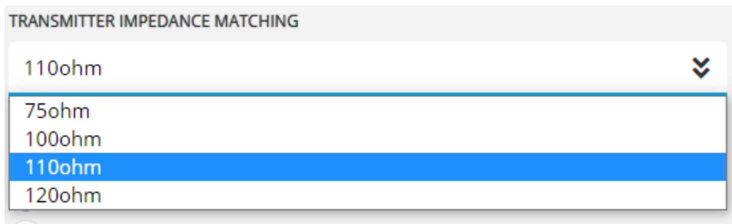
5. **Select Encoding Type**
   Select the required encoding type from the **ENCODING TYPE** drop-down list. By default, the encoding type is set to **High Density Bipolar Order 3**.

Figure 9-288. Select Encoding



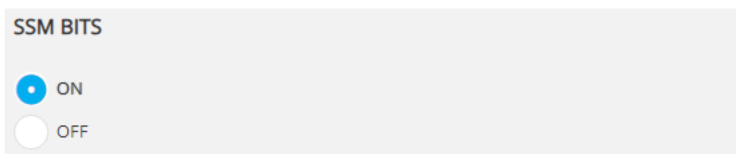
6. **Select Transmitter Impedance Matching**
   Select the correct transmitter impedance option from the **TRANSMITTER IMPEDANCE MATCHING** drop-down list. By default, this value is set to **110ohm**.

Figure 9-289. Set the Transmitter Impedance Matching



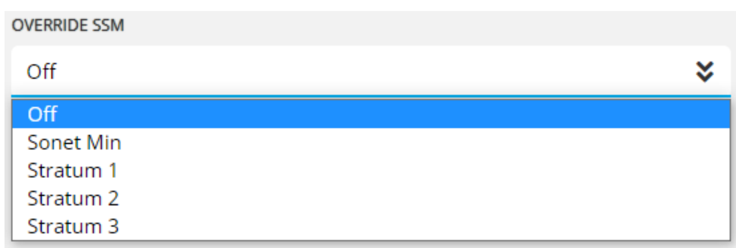
7. **Enable or Disable SSM Bits**
   Enable or disable SSM bits in the output signal using the **SSM BITS** radio buttons.

Figure 9-290. Enable/Disable SSM Bits



8. **Select Override SSM Behavior**
   Select the override SSM value from the **OVERRIDE SSM** drop-down list.

Figure 9-291. Select the Override SSM Value



9. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.
   A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-292. Successful Successful ave Notification

9.8 Provisioning the Pulse Ports

This section describes how to provision the GridTime 3000's pulse ports. The pulse ports include the BNC ports, the ST Fiber ports, and the HV MOSFET Port.

9.8.1 Provisioning Standard Pulse Outputs

This section describes how to provision pulse ports with standard pulse outputs. You can configure standard pulse outputs on any of the GridTime 3000 pulse ports. The different standard outputs include:

- Unmodulated IRIG-B
- Modified Manchester Modulated IRIG-B
- Simulated DCF77 Receiver Signal
- Programmable Pulses

For complete specifications of all the standard pulse outputs, see Time and Frequency Signals.

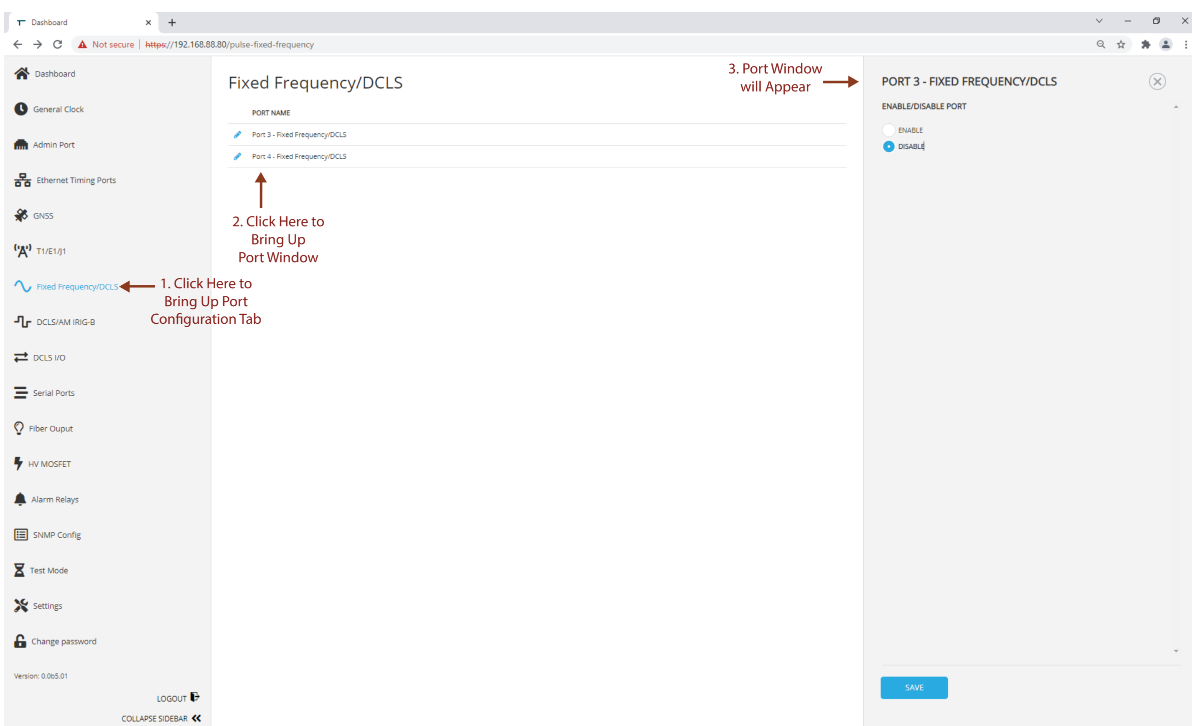
9.8.1.1 Unmodulated IRIG-B Output

This section describes how to provision a GridTime 3000 pulse port to output unmodulated IRIG-B.

Note: The unmodulated IRIG-B output provisioning process is the same for all BNC ports, the ST Fiber outputs, and the HV MOSFET port. The examples shown in this section uses port 3 - a fixed frequency/DCLS BNC port.

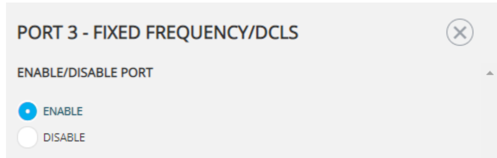
1. **Navigate to Port's Window**
   To navigate to the Fixed Frequency/DCLS port window, on the left navigation pane of the Dashboard, click **Frequency/DCLS**, and then on the center of the screen, click the port name you want to configure. This opens the corresponding port settings window on the right pane.

Figure 9-293. Dashboard-Fixed Frequency/DCLS



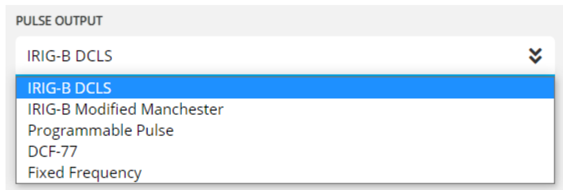
2. **Enable Port**
   On the port settings window on the right, select the **ENABLE** radio button to enable the port.

Figure 9-294. Enable Port



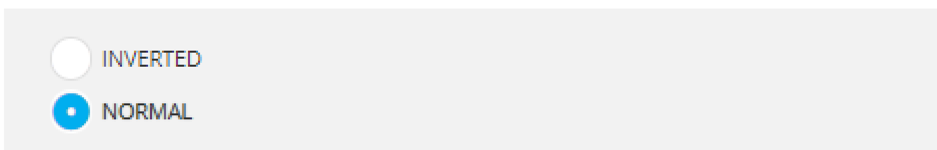
3. **Select Pulse Output**
   From the **PULSE OUTPUT** drop-down list, select **IRIG-B DCLS** (Unmodulated IRIG-B for ST Fiber outputs).

Figure 9-295. Pulse Output Settings



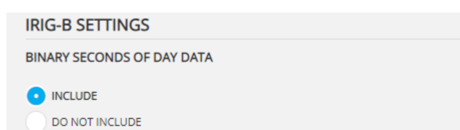
4. **Select Signal Inversion**
   Select whether the signal will be inverted or normal from the **Invert Signal** radio button options. By default, this is set to **NORMAL**.

Figure 9-296. Signal Inversion Settings



5. **Include or Exclude Binary Seconds of Day Data**
   Select whether binary seconds of day data is to be included in the output using the **BINARY SECONDS OF DAY DATA** radio buttons. By default, binary seconds of day data is set to **INCLUDE**.

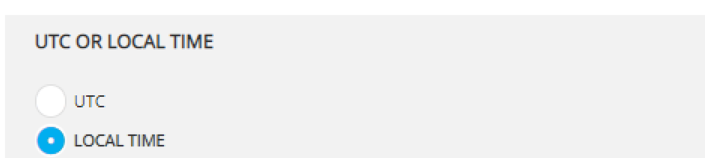
Figure 9-297. Include/Exclude Binary Seconds of Day Data



Note: Microchip recommends including binary seconds of day data in case it is required by the end device.

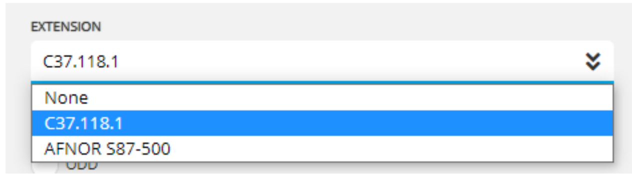
6. **UTC or Local Time**
   Select whether the output uses a UTC or Local Time format using the **UTC OR LOCAL TIME** radio buttons. By default, **LOCAL TIME** is selected.

Figure 9-298. Time Format Settings



7. **Select Extensions**
   Select what extensions are included in the control field of the output IRIG-B signal. By default, **C37.118.1** extensions are selected.

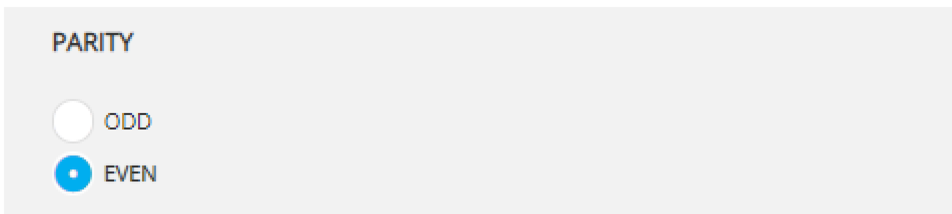
   Figure 9-299. Extension Settings



   Note: Microchip recommends using C37.118.1 extensions here as they are widely supported by end devices and contain useful information such as pending leap seconds and daylight savings jumps.

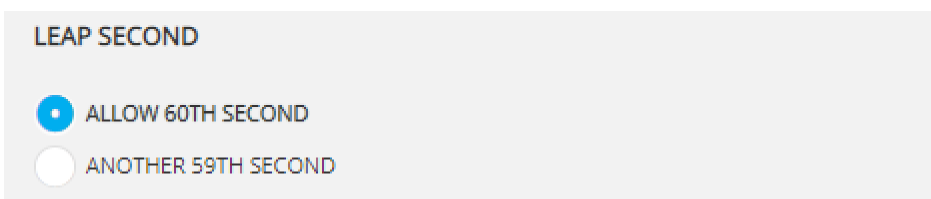
8. **Select Even or Odd Parity**
   Select whether the signal uses odd or even parity from the **PARITY** radio buttons. By default, the parity is set to **EVEN**.

   Figure 9-300. Parity Settings



9. **Select Leap Second Behavior**
   Choose the leap second behavior from the following options:

   Figure 9-301. Leap Second Behavior Settings



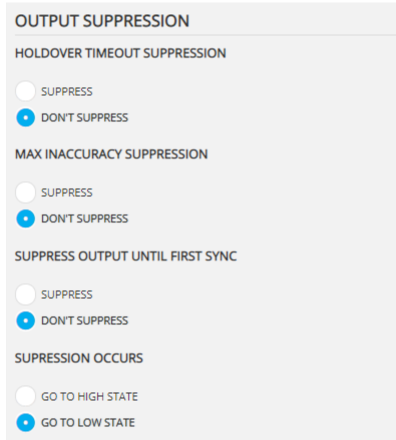
   – **ALLOW 60TH SECOND**: In the event of a leap second, the seconds counter in the IRIG-B signal will count an extra second up to 60 before rolling back to 0 and incrementing the minute counter.
   – **ANOTHER 59TH SECOND**: In the event of a leap second, the seconds counter in the IRIG-B signal will count to 59, then will repeat second 59 again a second later, before rolling back to 0 and incrementing the minute counter.

   By default, this is set to **ALLOW 60TH SECOND**.

   Note: Microchip recommends setting this to **ALLOW 60TH SECOND** unless the end device does not support a 60th second.

10. **Provision Output Suppression Behavior**
    The output suppression settings determine under what conditions the output will be suppressed, and whether it will be held high or low when suppressed.

Figure 9-302. Output Suppression Settings

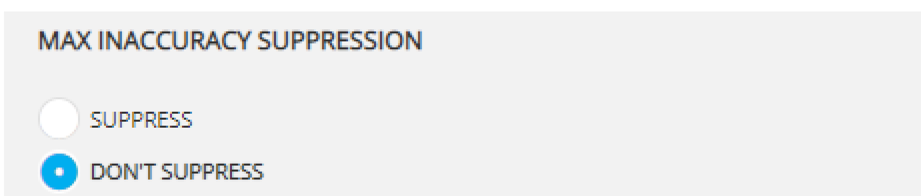


a. **Holdover Timeout Suppression**
Choose whether the IRIG-B output will be suppressed in the event of the GridTime 3000 experiencing a holdover timeout. By default, the **HOLDOVER TIMEOUT SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-303. Holdover Timeout Suppression Settings

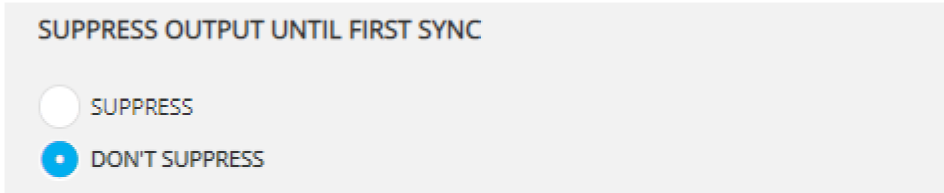
b. **Max Inaccuracy Suppression**
Choose whether the IRIG-B output will be suppressed in the event of the GridTime 3000 hitting its maximum inaccuracy threshold. By default, the **MAX INACCURACY SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-304. Max Inaccuracy Suppression Settings



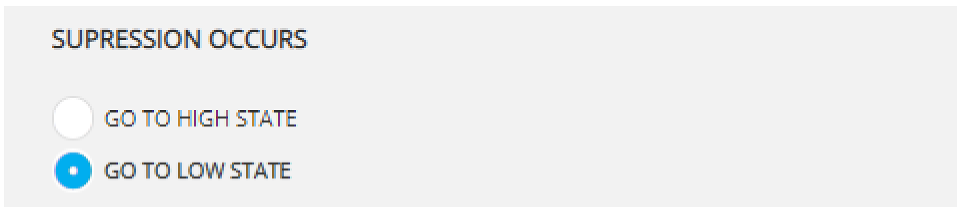
c. **Suppress Output Until First Sync**
Choose whether the IRIG-B output is to be suppressed until the GridTime 3000 has synchronized to its first time source on startup. By default, the **SUPPRESS OUTPUT UNTIL FIRST SYNC** radio button is set to **DON'T SUPPRESS**.

Figure 9-305. Suppress Output Until First Sync Settings



d. **Suppression Occurs**
Choose whether the output signal will get locked into a high or low (on the Fiber port these will be displayed as illuminated or dark and for the HV MOSFET open or closed) state during suppression. By default, the **SUPPRESSION OCCURS** radio button is set to **GO TO LOW STATE**.

Figure 9-306. High/Low State Output Signal Suppression Settings



11. **Save Settings**
To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-307. Successful Save Notification

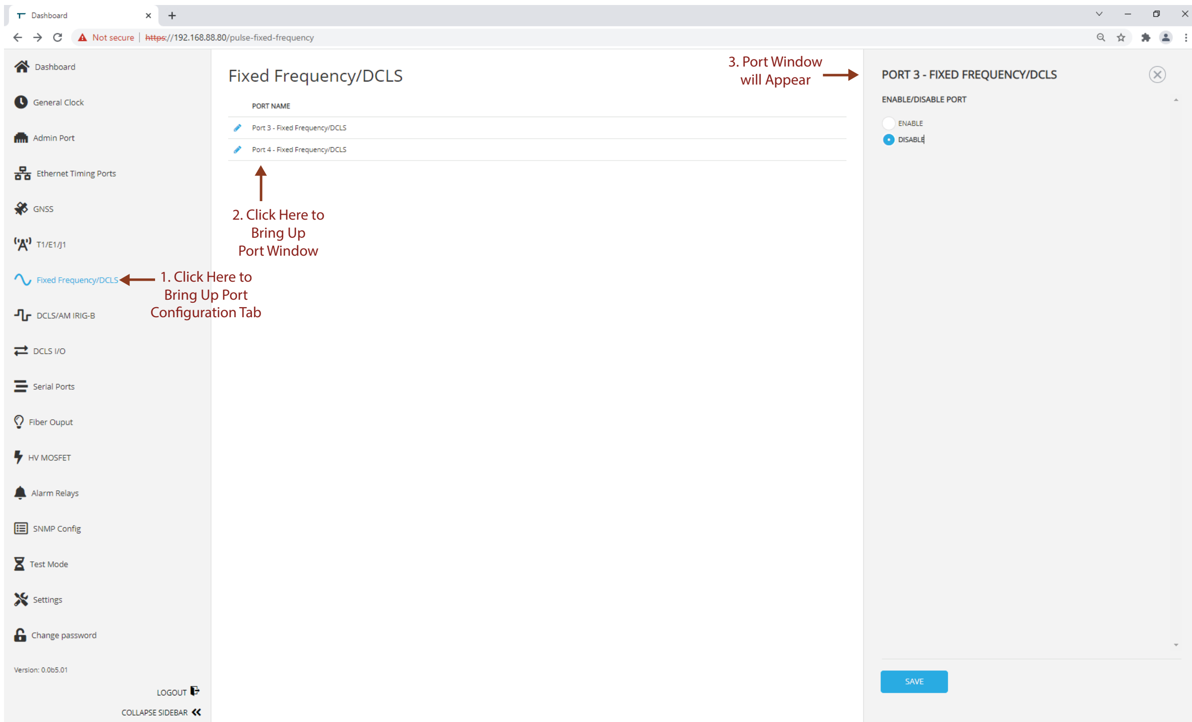
9.8.1.2 Modified Manchester Modulated IRIG-B Output

This section describes how to provision a GridTime 3000 pulse port to output modified manchester modulated IRIG-B.

Note: The IRIG-B Modified Manchester output provisioning process is the same for all BNC ports, the ST Fiber outputs, and the HV MOSFET port. The examples in this section is using Port 3 — a fixed frequency/DCLS BNC port as an example.

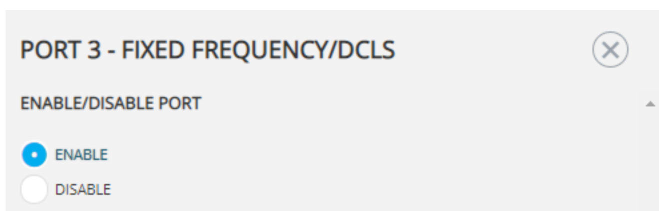
1. **Navigate to Port's Window**
To navigate to the port window that you want to configure, on the left navigation pane of the Dashboard window, click **Fixed Frequency/DCLS**, and then on the center of the window, click the port name you want to configure. This displays the settings for the selected port on the right pane.

Figure 9-308. Dashboard-Fixed Frequency/DCLS



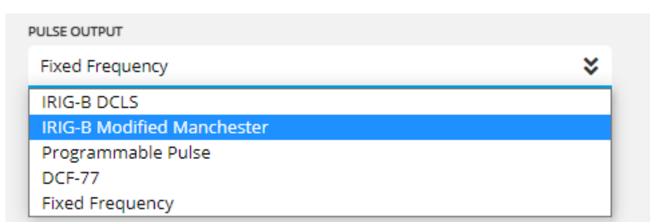
2. **Enable Port**
   On the port settings window on the right, select the **ENABLE** radio button to enable the port.

   Figure 9-309. Enable Port

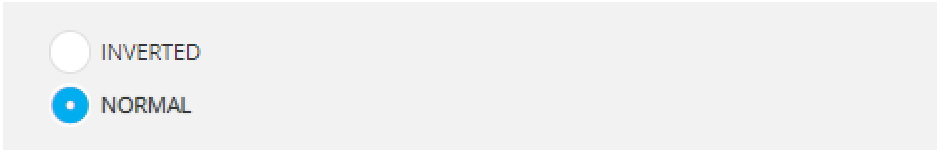
3. **Select Pulse Output**
   From the **PULSE OUTPUT** drop-down list, select **IRIG-B Modified Manchester**.

   Figure 9-310. Pulse Output Settings

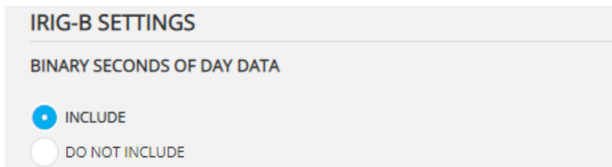
4. **Select Signal Inversion**
   Select whether the signal will be inverted or normal from the **Invert Signal** radio button options. By default, this is set to **NORMAL**.

Figure 9-311. Signal Inversion Settings



5. **Include or Exclude Binary Seconds of Day Data**
   Select whether binary seconds of day data is to be included in the output using the **BINARY SECONDS OF DAY DATA** radio buttons. By default, binary seconds of day data is set to **INCLUDE**.

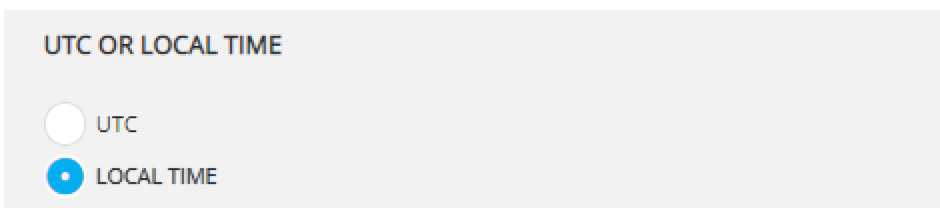
Figure 9-312. Include/Exclude Binary Seconds of Day Data



Note: Microchip recommends including binary seconds of day data in case it is required by the end device.

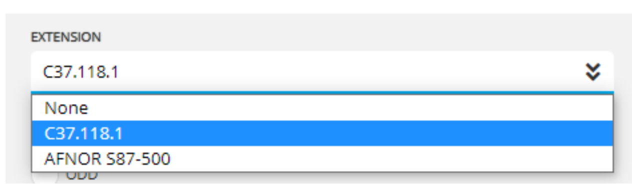
6. **UTC or Local Time**
   Select whether the output uses a UTC or Local Time format using the **UTC OR LOCAL TIME** radio buttons. By default, **LOCAL TIME** is selected.

Figure 9-313. Time Format Settings



7. **Select Extensions**
   Select what extensions are included in the control field of the output IRIG-B signal. By default, C37.118.1 extensions are selected.

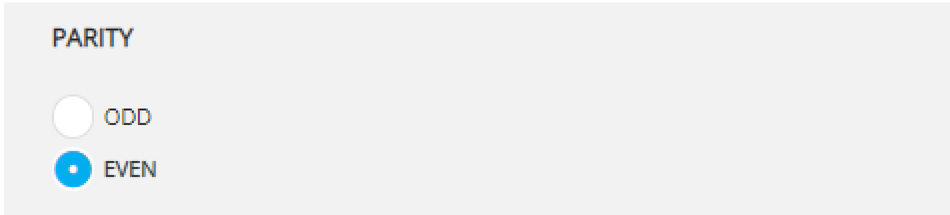
Figure 9-314. Extension Settings



Note: Microchip recommends using C37.118.1 extensions. They are widely supported by end devices and contain useful information such as pending leap seconds and daylight savings jumps.

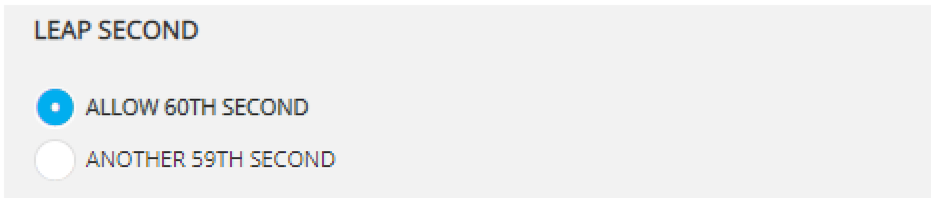
8. **Select Even or Odd Parity**
   Select whether the signal uses odd or even parity from the **PARITY** radio buttons. By default, the parity is set to **EVEN**.

Figure 9-315. Parity Settings



9. **Select Leap Second Behavior**
   Choose the leap second behavior from the following options:

   Figure 9-316. Leap Second Behavior Settings

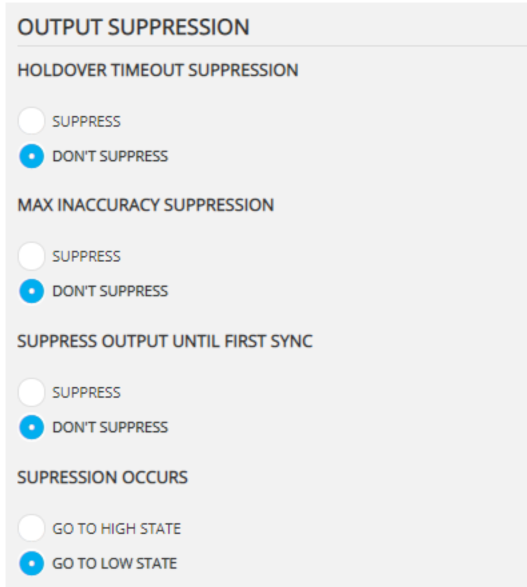
   – **ALLOW 60TH SECOND**: In the event of a leap second, the seconds counter in the IRIG-B signal will count an extra second up to 60 before rolling back to 0 and incrementing the minute counter.
   – **ANOTHER 59TH SECOND**: In the event of a leap second, the seconds counter in the IRIG-B signal will count to 59, then will repeat second 59 again a second later, before rolling back to 0 and incrementing the minute counter.

   By default, this is set to **ALLOW 60TH SECOND**.

   Note: Microchip recommends setting this to **ALLOW 60TH SECOND** unless the end device does not support a 60th second.

10. **Provision Output Suppression Behavior**
    The output suppression settings determine under what conditions the output will be suppressed, and whether it will be held high or low when suppressed.

Figure 9-317. Output Suppression Settings

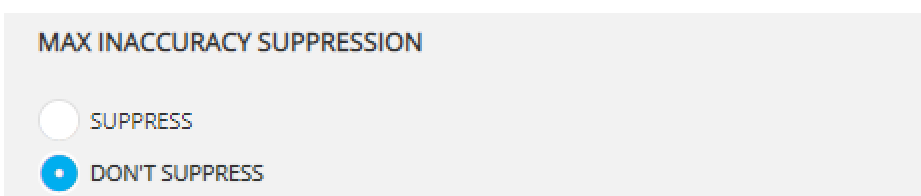


a. **Holdover Timeout Suppression**
Choose whether the Modified Manchester output will be suppressed in the event of the GridTime 3000 experiencing a holdover timeout. By default, the **HOLDOVER TIMEOUT SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-318. Holdover Timeout Suppression Settings

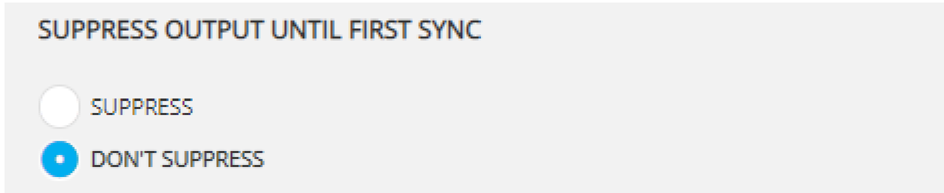
b. **Max Inaccuracy Suppression**
Choose whether the Modified Manchester output will be suppressed in the event of the GridTime 3000 hitting its maximum inaccuracy threshold. By default, the **MAX INACCURACY SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-319. Max Inaccuracy Suppression Settings



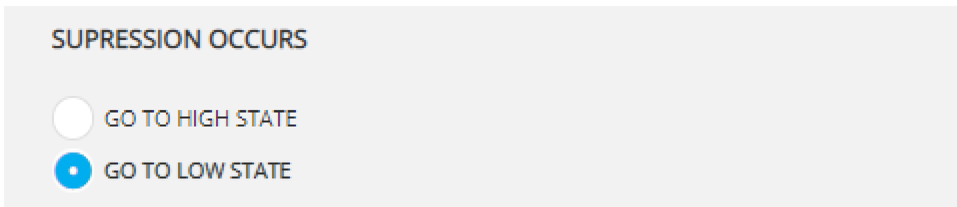
c. **Suppress Output Until First Sync**
Choose whether the Modified Manchester output is to be suppressed until the GridTime 3000 has synchronized to its first time source on startup. By default, the **SUPPRESS OUTPUT UNTIL FIRST SYNC** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-320. Suppress Output Until First Sync Settings



d. **Suppression Occurs**
Choose whether the output signal will get locked into a high or low (on the Fiber port these will be displayed as illuminated or dark and for the HV MOSFET open or closed) state during suppression. By default, the **SUPPRESSION OCCURS** radio button is set to **GO TO LOW STATE**.

Figure 9-321. High/Low State Output Signal Suppression Settings



11. **Save Settings**
To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-322. Successful Save Notification

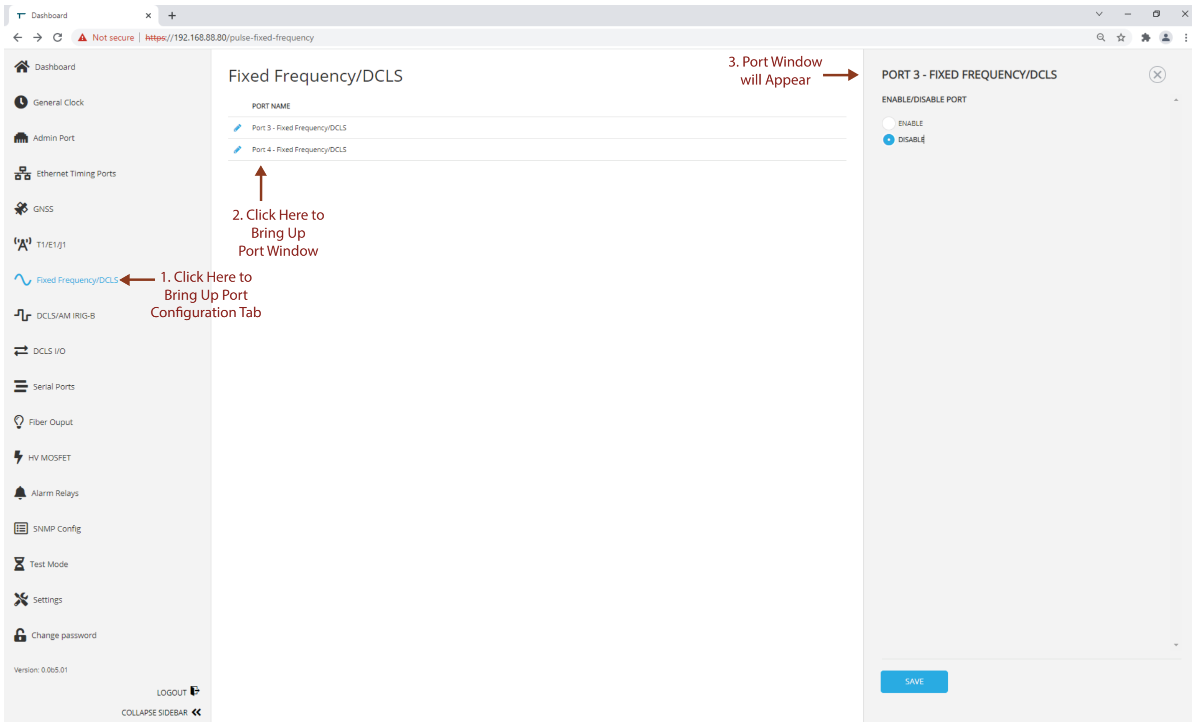
9.8.1.3 Simulated DCF77 Receiver Signal Output

This section describes how to provision a GridTime 3000 pulse port to output a simulated DCF77 receiver signal.

Note: The simulated DCF77 receiver signal output provisioning process is the same for all BNC ports, the ST Fiber outputs, and the HV MOSFET port. The example in this section is using Port 3 — a fixed frequency/DCLS BNC port.

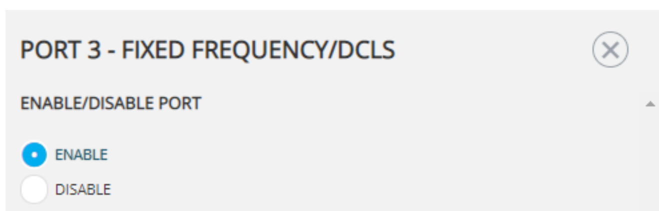
1. **Navigate to Port's Window**
To navigate to the port window that you want to configure, on the left navigation pane of the Dashboard window, click **Fixed Frequency/DCLS**, and then on the center of the window, click the port name you want to configure. This displays the settings for the selected port on the right pane.

Figure 9-323. Dashboard-Fixed Frequency/DCLS



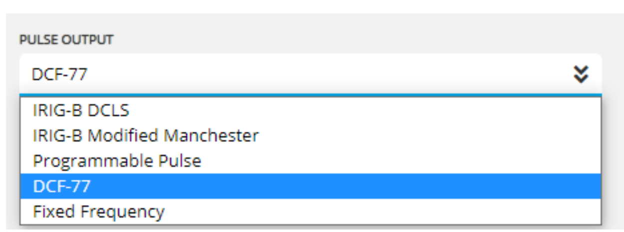
2. **Enable Port**
   Select **ENABLE** for the enable/disable port setting.

Figure 9-324. Enable Port



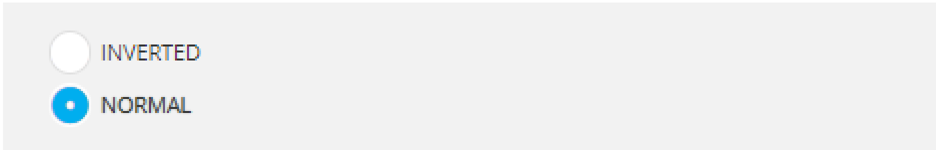
3. **Select Pulse Output**
   From the **PULSE OUTPUT** drop-down list, select **DCF-77**.

Figure 9-325. Pulse Output Settings



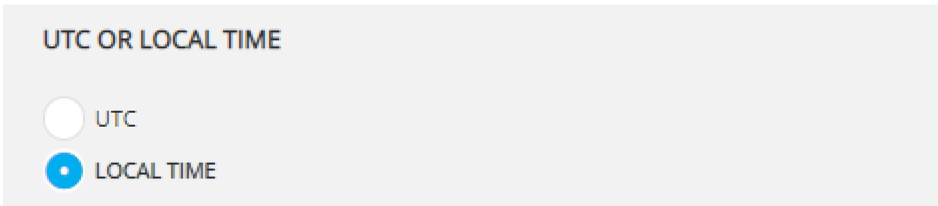
4. **Select Signal Inversion**
   Select whether the signal will be inverted or normal from the **Invert Signal** radio button options. By default, this is set to **NORMAL**.

Figure 9-326. Signal Inversion Settings



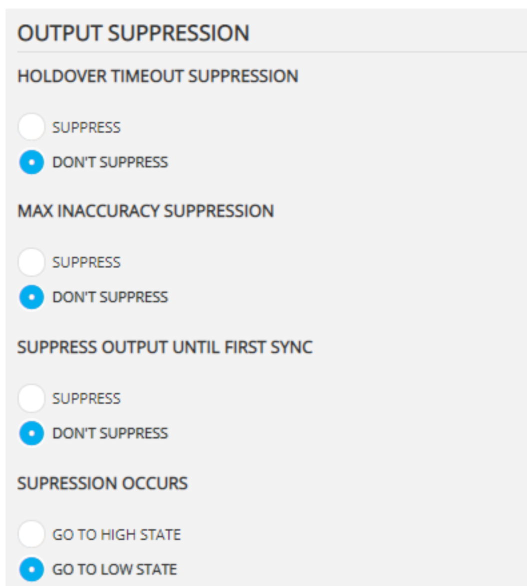
5. **UTC or Local Time**
   Select whether the output uses a UTC or Local Time format using the **UTC OR LOCAL TIME** radio buttons. By default, **LOCAL TIME** is selected.

Figure 9-327. Time Format Settings



6. **Provision Output Suppression Behavior**
   The output suppression settings determine under what conditions the DCF-77 output will be suppressed, and whether it will be held high or low when suppressed.

Figure 9-328. Output Suppression Settings

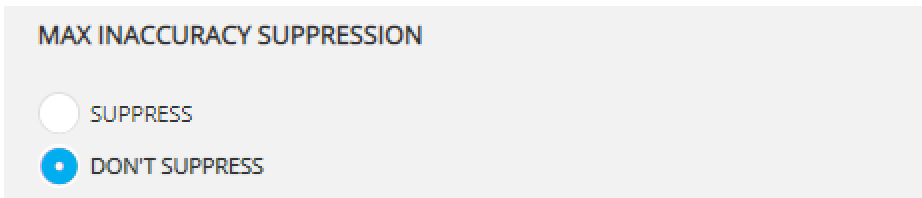


   a. **Holdover Timeout Suppression**
      Choose whether the DCF-77 output will be suppressed in the event of the GridTime 3000 experiencing a holdover timeout. By default, the **HOLDOVER TIMEOUT SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-329. Holdover Timeout Suppression Settings

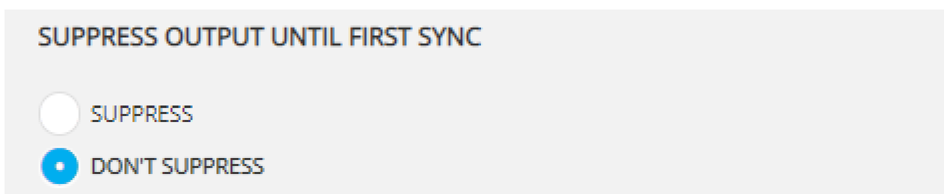
b. **Max Inaccuracy Suppression**
Choose whether the DCF-77 output will be suppressed in the event of the GridTime 3000 hitting its maximum inaccuracy threshold. By default, the **MAX INACCURACY SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-330. Max Inaccuracy Suppression Settings



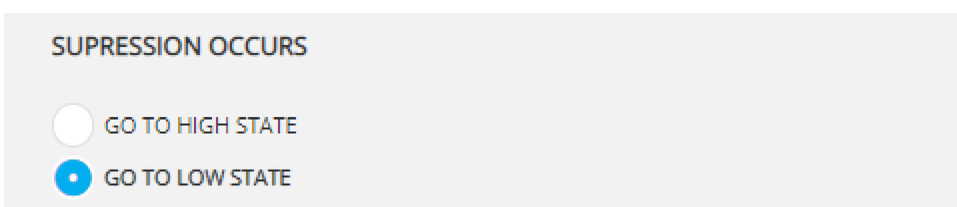
c. **Suppress Output Until First Sync**
Choose whether the DCF-77 output is to be suppressed until the GridTime 3000 has synchronized to its first time source on startup. By default, the **SUPPRESS OUTPUT UNTIL FIRST SYNC** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-331. Suppress Output Until First Sync Settings



d. **Suppression Occurs**
Choose whether the output signal will get locked into a high or low (on the Fiber port these will be displayed as illuminated or dark and for the HV MOSFET open or closed) state during suppression. By default, the **SUPPRESSION OCCURS** radio button is set to **GO TO LOW STATE**.

Figure 9-332. Output Signal Suppression State Settings



7. **Save Settings**
To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-333. Successful Save Notification

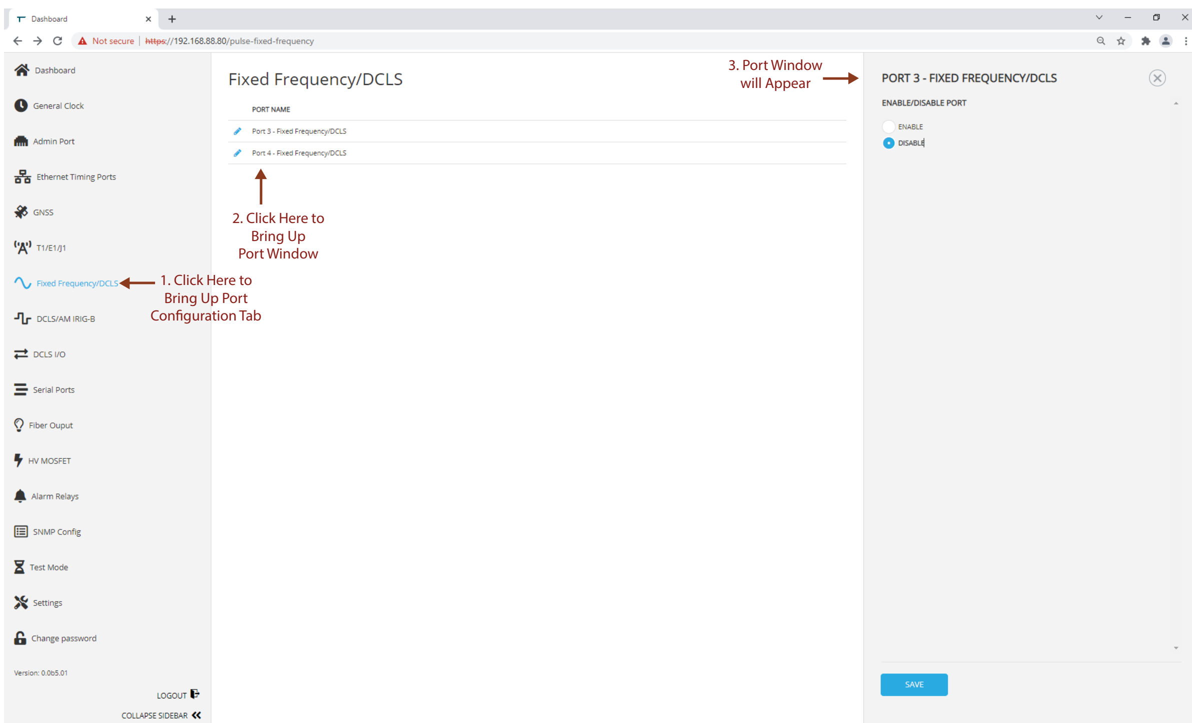
9.8.1.4 Programmable Pulse Output

This section describes how to provision a GridTime 3000 pulse port to output custom pulses.

Note: The programmable pulse output provisioning process is the same for all BNC ports, the ST Fiber outputs, and the HV MOSFET port. The example in this section is using Port 3 — a Frequency/ DCLS BNC port.

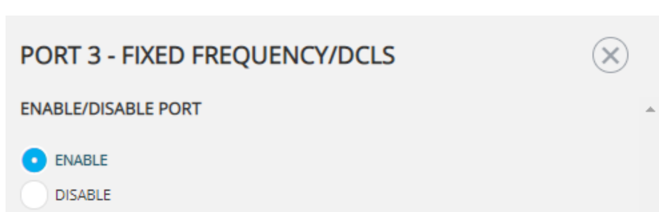
1. **Navigate to Port's Window**
   To navigate to the port window that you want to configure, on the left navigation pane of the Dashboard window, click **Fixed Frequency/DCLS**, and then on the center of the window, click the port name you want to configure. This displays the settings for the selected port on the right pane.

   Figure 9-334. Dashboard-Fixed Frequency/DCLS



2. **Enable Port**
   Select **ENABLE** for the enable/disable port setting.

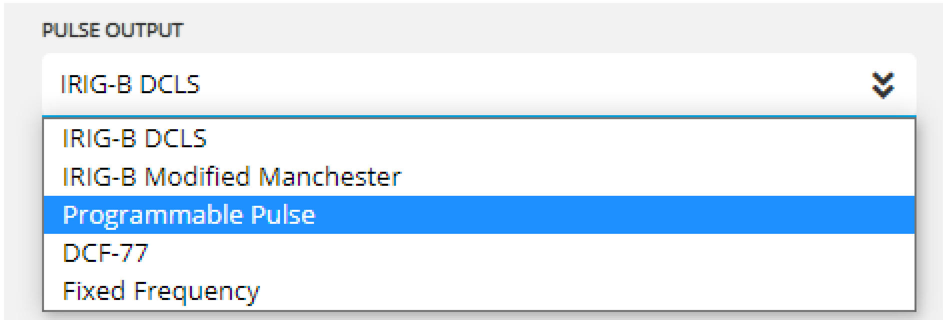
   Figure 9-335. Enable Port



3. **Select Pulse Output**

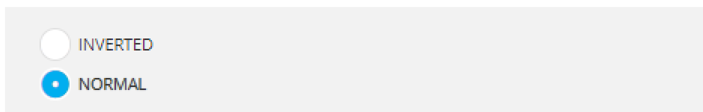
From the **PULSE OUTPUT** drop-down list, select **Programmable Pulse**.

Figure 9-336. Pulse Output Settings



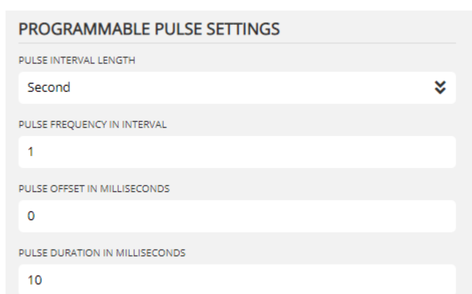
4. **Select Signal Inversion**
   Select whether the signal will be inverted or normal from the **Invert Signal** radio button options. By default, this is set to **NORMAL**.

   Figure 9-337. Signal Inversion Settings



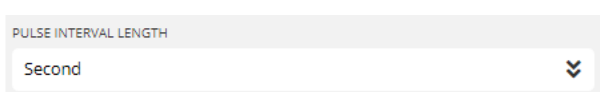
5. **Programmable Pulse Settings**
   The programmable pulse settings define the interval length, phase offset, frequency, and duration of the outputted pulses. By default, these specify a 1PPS signal with a 10ms pulse duration.

   Figure 9-338. Programmable Pulse Settings Window



   a. **Set Interval Length**
      The pulse interval length determines the time base for the programmable pulses. From the **PULSE INTERVAL LENGTH** drop-down list, select the interval length. By default, this is set to **Second**.

      Figure 9-339. Pulse Interval Settings

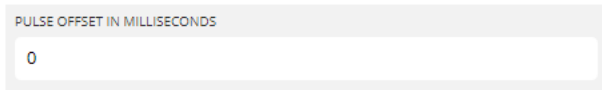


   b. **Set Pulse Frequency in Interval**
      The pulse frequency setting determines the number of pulses that occur in the interval length specified in the preceding step. previous step. By default, the 'PULSE FREQUENCY IN INTERNVAL' is set to 1.

Figure 9-340. Pulse Frequency Settings

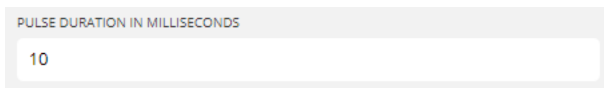
c. **Set Pulse Offset**
The pulse offset setting determines the phase offset the pulses will experience from the beginning of the time interval in milliseconds. By default, the **PULSE OFFSET IN MILLISECONDS** is set to 0 ms.

Figure 9-341. Pulse Offset Settings



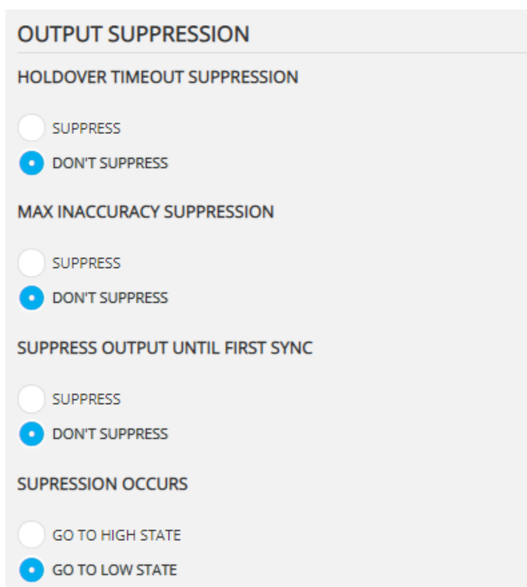
d. **Set Duration**
The pulse duration setting determines the duration of the pulses from the beginning of the time interval in milliseconds. By default, the **PULSE DURATION IN MILLISECONDS** is set to 10 ms.

Figure 9-342. Pulse Duration Settings



6. **Provision Output Suppression Behavior**
The output suppression settings determine under what conditions the DCF-77 output will be suppressed, and whether it will be held in a high or low state when suppressed.

Figure 9-343. Output Suppression Settings

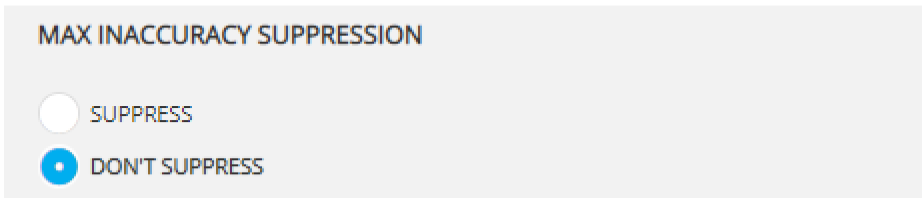


a. **Holdover Timeout Suppression**
Choose whether the programmable pulse output will be suppressed in the event of the GridTime 3000 experiencing a holdover timeout.
By default, the **HOLDOVER TIMEOUT SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-344. Holdover Timeout Suppression Settings

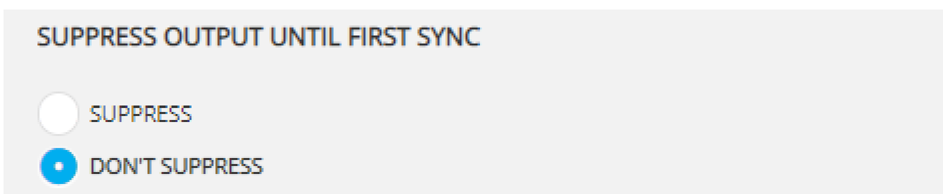
b. **Max Inaccuracy Suppression**
Choose whether the programmable pulse output will be suppressed in the event of the GridTime 3000 hitting its maximum inaccuracy threshold. By default, the **MAX INACCURACY SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-345. Max Inaccuracy Suppression Settings



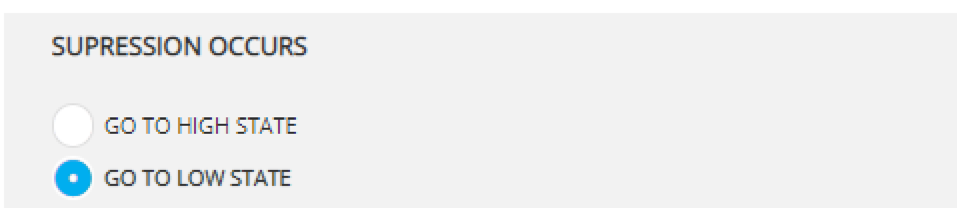
c. **Suppress Output Until First Sync**
Choose whether the programmable pulse output is to be suppressed until the GridTime 3000 has synchronized to its first time source on startup. By default, the **SUPPRESS OUTPUT UNTIL FIRST SYNC** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-346. Suppress Output Until First Sync Settings



d. **Suppression Occurs**
Choose whether the output signal will get locked into a high or low (on the Fiber port these will be displayed as illuminated or dark and for the HV MOSFET open or closed) state during suppression. By default, the **SUPPRESSION OCCURS** radio button is set to **GO TO LOW STATE**.

Figure 9-347. Output Signal Suppression State Settings



7. **Save Settings**
To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-348. Successful Save Notification

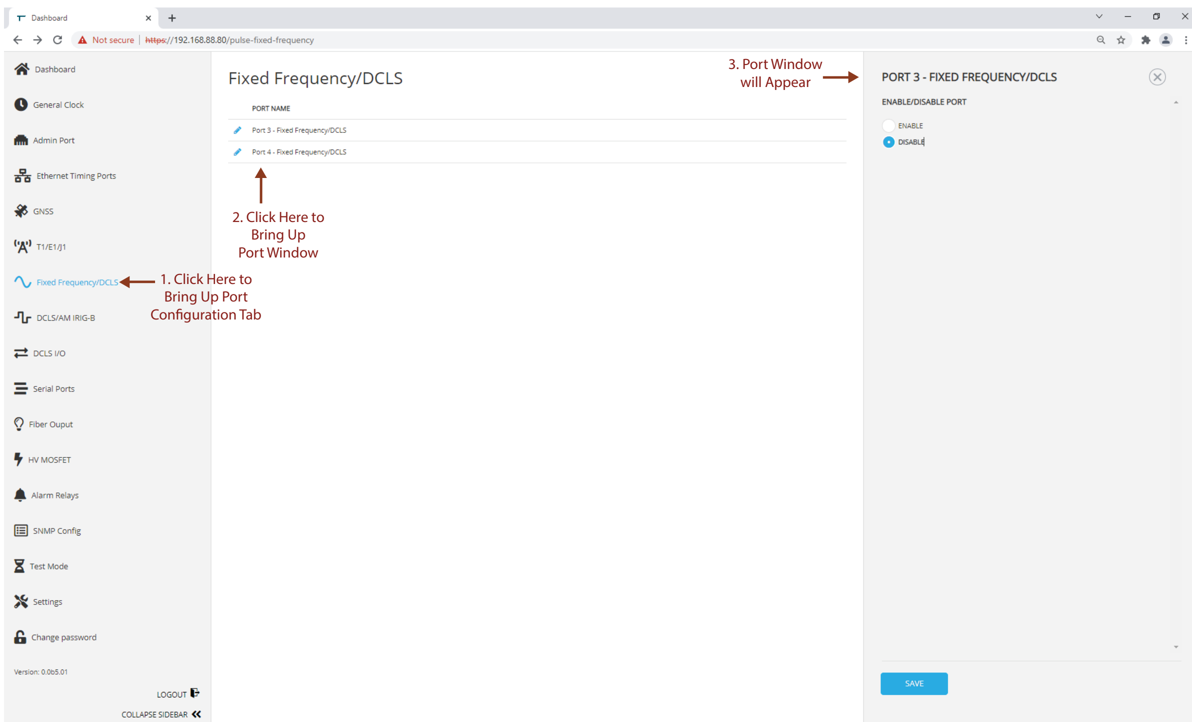
9.8.2 Provisioning G.703 Fixed Frequency Outputs

This section describes how to provision a GridTime 3000 Fixed Frequency/DCLS port to output a G.703 fixed frequency signal.

Note: Only the Fixed Frequency/DCLS BNC ports (Ports 3 and 4) can be used to output fixed frequency signals.

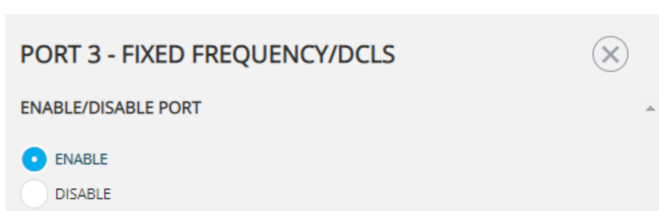
1. **Navigate to Port's Window**
   To navigate to the Fixed Frequency/DCLS port window, on the left navigation pane, click **Fixed Frequency/DCLS**, and then in the center of the screen, click the port you want to configure. This opens the corresponding port settings window on the right pane.

Figure 9-349. Fixed Frequency/DCLS Configuration Window



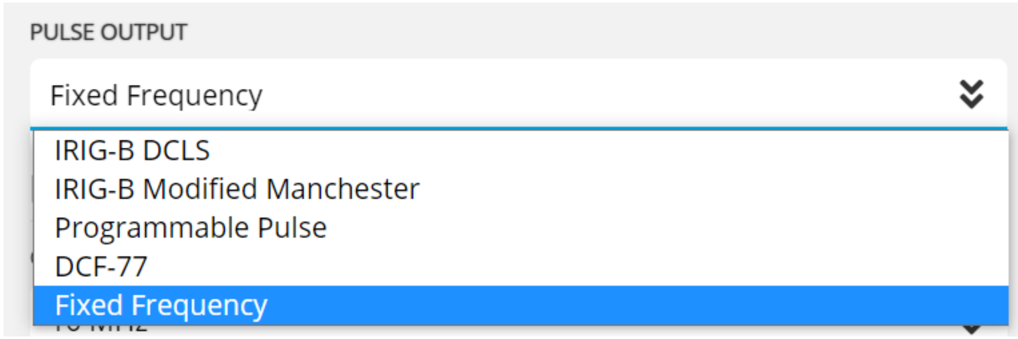
2. **Enable Port**
   On the port settings window on the right, select the **ENABLE** radio button to enable the port.

Figure 9-350. Enable/Disable Port Setting



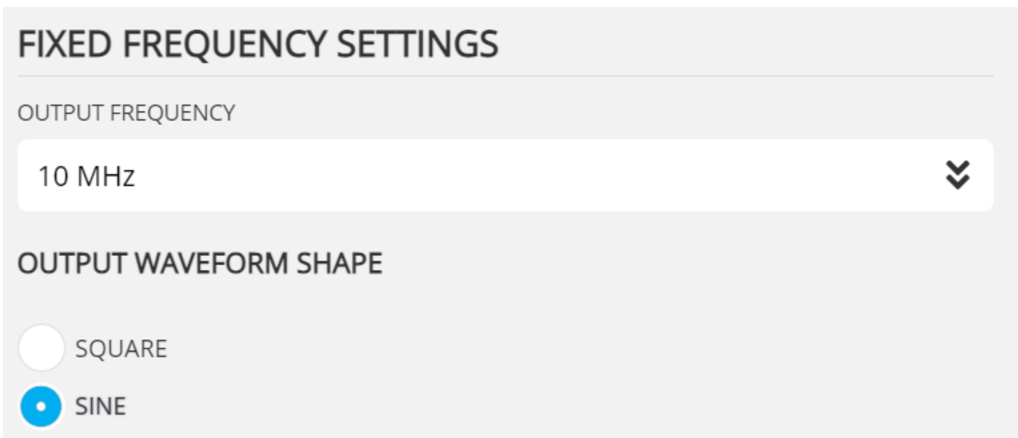
3. **Select Pulse Output**
   From the **PULSE OUTPUT** drop-down list, select **Fixed Frequency**.

Figure 9-351. Select Pulse Output



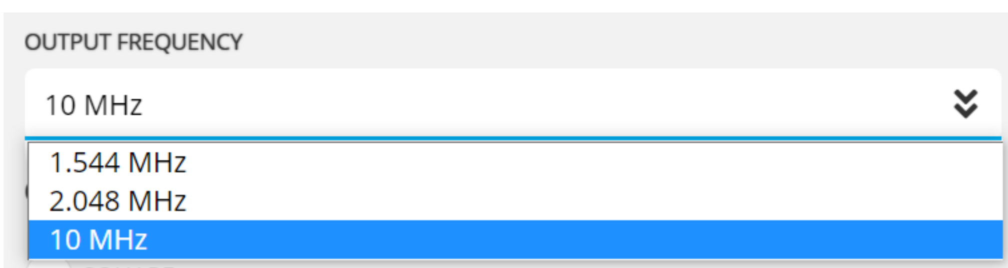
4. **Provision Fixed Frequency Settings**
   The fixed frequency settings define whether the output signal will be a sine or square wave, and what signal the frequency will be. By default, these settings specify a 10 MHZ sinusoidal wave.

   Figure 9-352. Set Fixed Frequency Settings

   a. **Select Output Frequency**
      From the **OUTPUT FREQUENCY** drop-down list, select the frequency of the output signal. By default, this is set to 10 MHz.

      Figure 9-353. Set Output Frequency

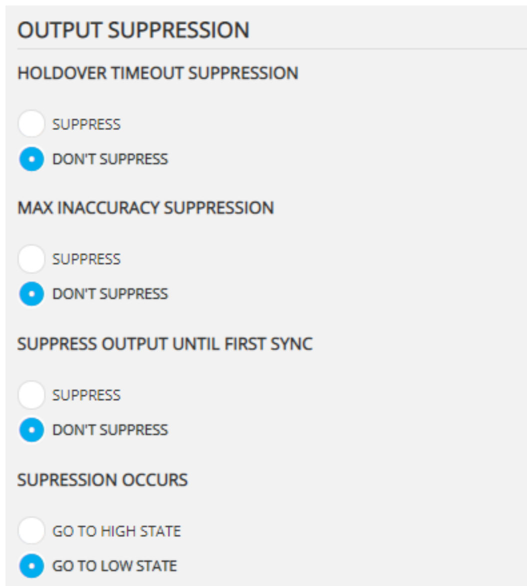
      

   b. **Select Waveform Shape**
      Select the waveform shape of the output signal using the **OUTPUT WAVEFORM SHAPE** setting radio buttons. By default, this is set to a sinusoidal wave (**SINE**).

Figure 9-354. Set Output Waveform Shape

5. **Provision Output Suppression Behavior**
   The output settings determine under what conditions the output will be suppressed, and whether it will be held in a high or low state when suppressed.

   Figure 9-355. Output Suppression Settings

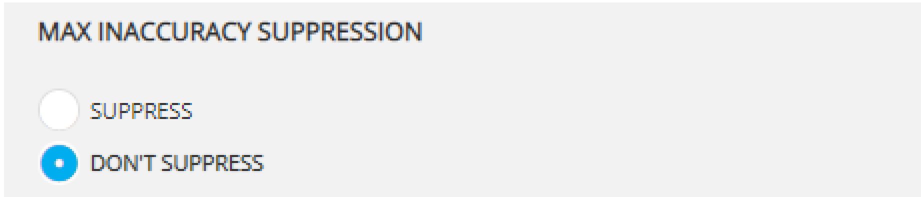


   a. **Holdover Timeout Suppression**
      Choose whether the frequency output will be suppressed in the event of the GridTime 3000 experiencing a holdover timeout. By default, the **HOLDOVER TIMEOUT SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

      Figure 9-356. Holdover Timeout Suppression Settings

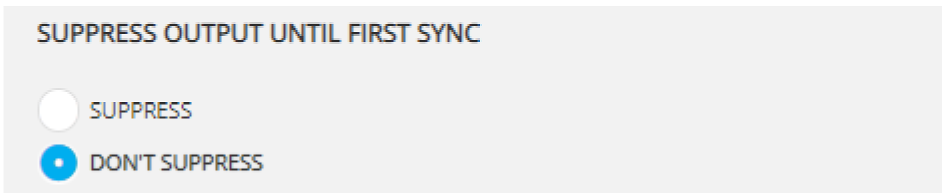
   b. **Max Inaccuracy Suppression**
      Choose whether the frequency output will be suppressed in the event of the GridTime 3000 hitting its maximum inaccuracy threshold. By default, the **MAX INACCURACY SUPPRESSION** radio button is set to **DON'T SUPPRESS**.

Figure 9-357. Max Inaccuracy Suppression Settings



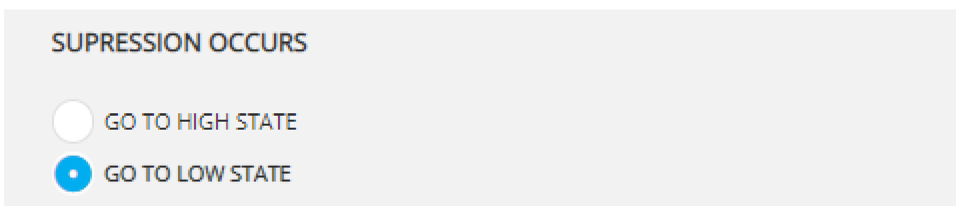
c. **Suppress Output Until First Sync**
Choose whether the frequency output is to be suppressed until the GridTime 3000 has synchronized to its first time source on startup. By default, the **SUPPRESS OUTPUT UNTIL FIRST SYNC** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-358. Suppress Output Until First Sync Settings



d. **Suppression Occurs**
Choose whether the output signal gets locked into a high or low (on the Fiber port these will be displayed as illuminated or dark and for the HV MOSFET open or closed) state during suppression. By default, the **SUPPRESSION OCCURS** radio button is set to **GO TO LOW STATE**.

Figure 9-359. High/Low State Output Signal Suppression Settings



6. **Save Settings**
To write the settings to the GridTime 3000, click **SAVE**.
A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-360. Successful Save Notification

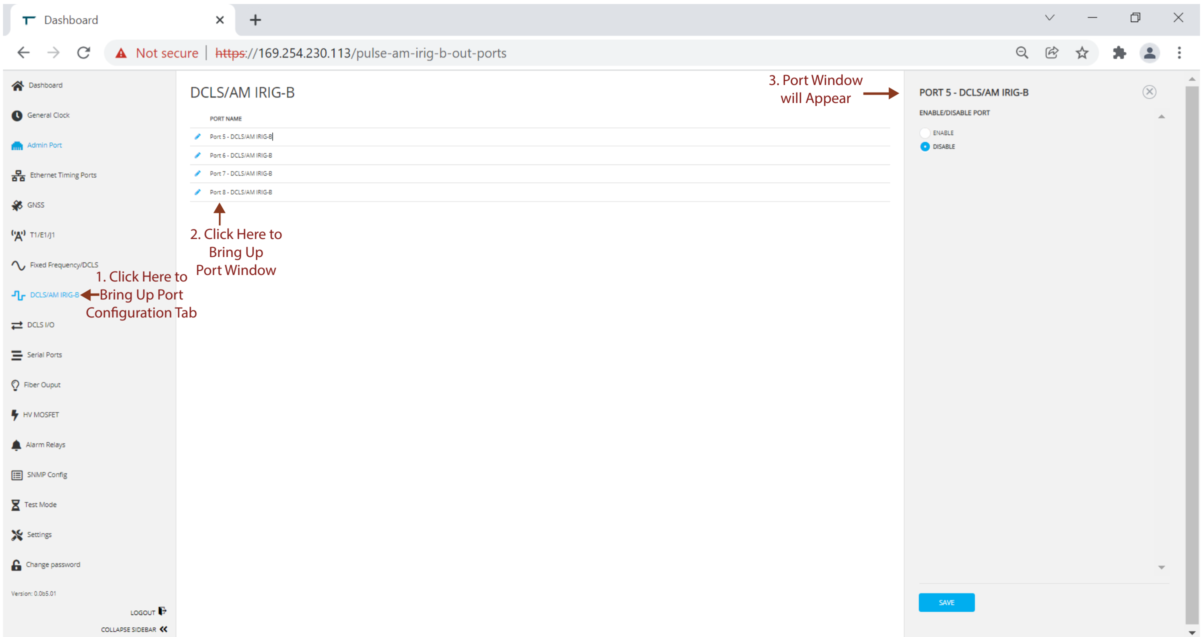
9.8.3 Provisioning AM IRIG-B Outputs

This section describes how to provision a GridTime 3000 AM IRIG/TTL port to output AM IRIG-B.

Note: Only the DCLS/AM IRIG-B BNC ports (Ports 5-8) can output AM IRIG-B.

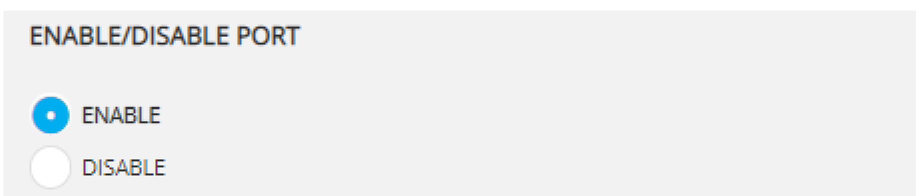
1. **Navigate to Port's Window**
To navigate to the IRIG/TTL port window, on the left navigation pane, click **DCLS/AM IRIG-B** , and then in the center of the screen, click the port you want to configure. This opens the corresponding port settings window on the right pane.

Figure 9-361. DCLS/AM IRIG-B Configuration Window



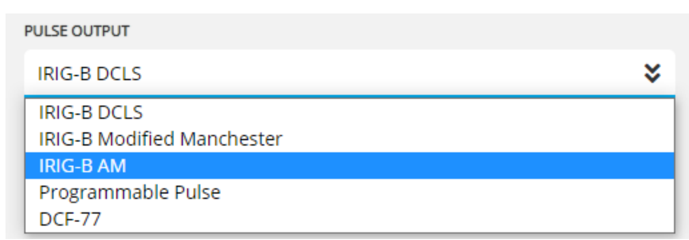
2. **Enable Port**
   On the port settings window on the right, select the **ENABLE** radio button to enable the port.

Figure 9-362. Enable/Disable Port Setting



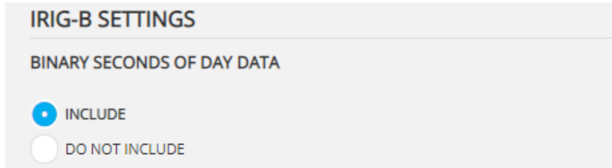
3. **Select Pulse Output**
   From the **PULSE OUTPUT** drop-down list, select **IRIG-B AM**.

Figure 9-363. Select Pulse Output



4. **Include or Exclude Binary Seconds of Day Data**
   Using the **BINARY SECONDS OF DAY DATA** radio buttons, select whether binary seconds of day data is to be included in the output. By default, binary seconds of day data is set to **INCLUDE**.

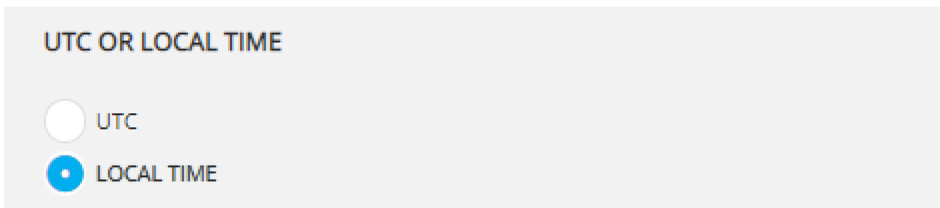
Figure 9-364. Set Binary Seconds of Day Data



Note: Microchip recommends including binary seconds of day data in case it is required by the end device.

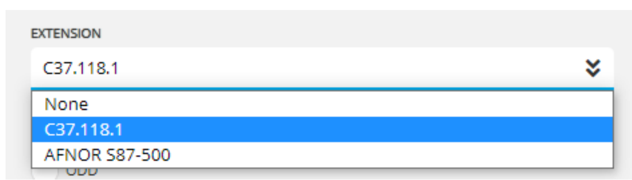
5. **UTC or Local Time**
   Select whether the output uses a UTC or Local Time format using the **UTC OR LOCAL TIME** radio buttons. By default, this is selected as **LOCAL TIME**.

Figure 9-365. Output Time Format Settings



6. **Select Extensions**
   Select what extensions is to be included in the control field of the output IRIG-B signal. By default, **C37.118.1** extensions is selected.

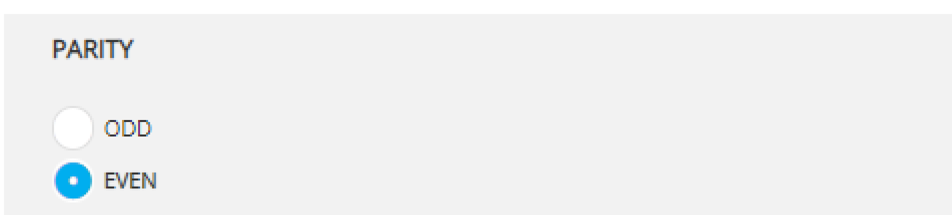
Figure 9-366. Signal Extension Settings



Note: Microchip recommends using C37.118.1 extensions as they are widely supported by end devices and contain useful information, such as pending leap seconds and daylight savings jumps.

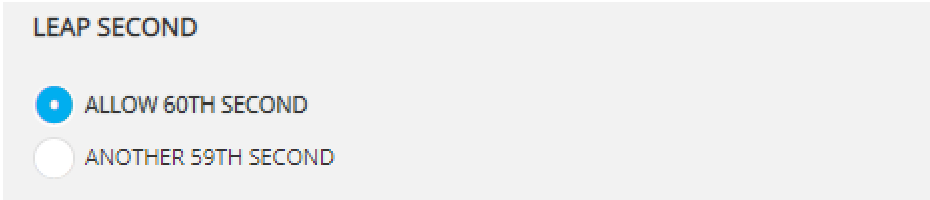
7. **Select Even or Odd Parity**
   From the **PARITY** radio buttons, select whether the signal uses odd or even parity . By default, this is set to **EVEN**.

Figure 9-367. Set Signal Parity



8. **Select Leap Second Behavior**
   Choose the leap second behavior from the following options:

Figure 9-368. Leap Second Behavior Settings



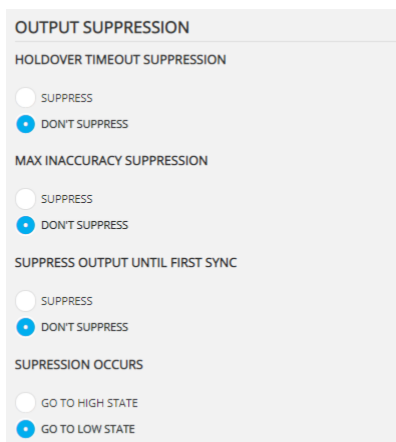
- **ALLOW 60TH SECOND**: In the event of a leap second, the seconds counter in the IRIG-B signal counts an extra second up to 60 before rolling back to 0 and incrementing the minute counter.
- **ANOTHER 59TH SECOND**: In the event of a leap second, the seconds counter in the IRIG-B signal counts to 59, then repeats second 59 again a second later, before rolling back to 0 and incrementing the minute counter.

By default, this is set to **ALLOW 60TH SECOND**.

Note: Microchip recommends setting this to **ALLOW 60TH SECOND** unless the end device does not support a 60th second.

9. **Provision Output Suppression Behavior**
The output settings determine under what conditions the output will be suppressed, and whether it will be held in a high or low state when suppressed.

Figure 9-369. Output Suppression Settings



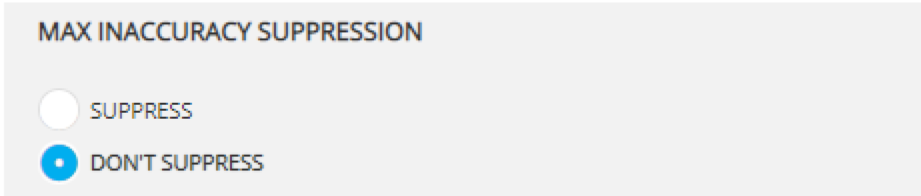
a. **Holdover Timeout Suppression**
Choose whether the AM IRIG-B frequency output will be suppressed in the event of the GridTime 3000 experiencing a holdover timeout. By default, the **HOLDOVER TIMEOUT SUPPRESSION** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-370. Holdover Timeout Suppression Settings

b. **Max Inaccuracy Suppression**

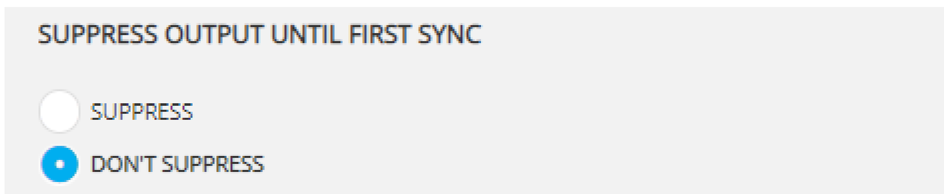
Choose whether the AM IRIG-B output will be suppressed in the event of the GridTime 3000 hitting its maximum inaccuracy threshold. By default, the **MAX INACCURACY SUPPRESSION** radio button is set to **DON'T SUPPRESS**.

Figure 9-371. Max Inaccuracy Suppression Settings



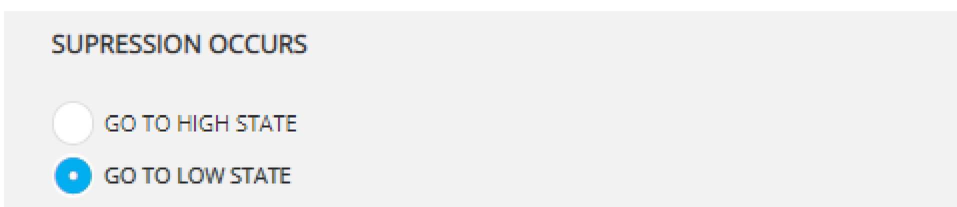
c. **Suppress Output Until First Sync**
Choose whether the AM IRIG-B output is to be suppressed until the GridTime 3000 has synchronized to its first time source on startup. By default, the **SUPPRESS OUTPUT UNTIL FIRST SYNC** radio buttons is set to **DON'T SUPPRESS**.

Figure 9-372. Suppress Output Until First Sync Settings



d. **Suppression Occurs**
Choose whether the output signal gets locked into a high or low (on the Fiber port these will be displayed as illuminated or dark and for the HV MOSFET open or closed) state during suppression. By default, the **SUPPRESSION OCCURS** radio button is set to **GO TO LOW STATE**.

Figure 9-373. High/Low State Output Signal Suppression Settings



10. **Save Settings**
To write the settings to the GridTime 3000, click **SAVE**.
A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-374. Successful Save Notification

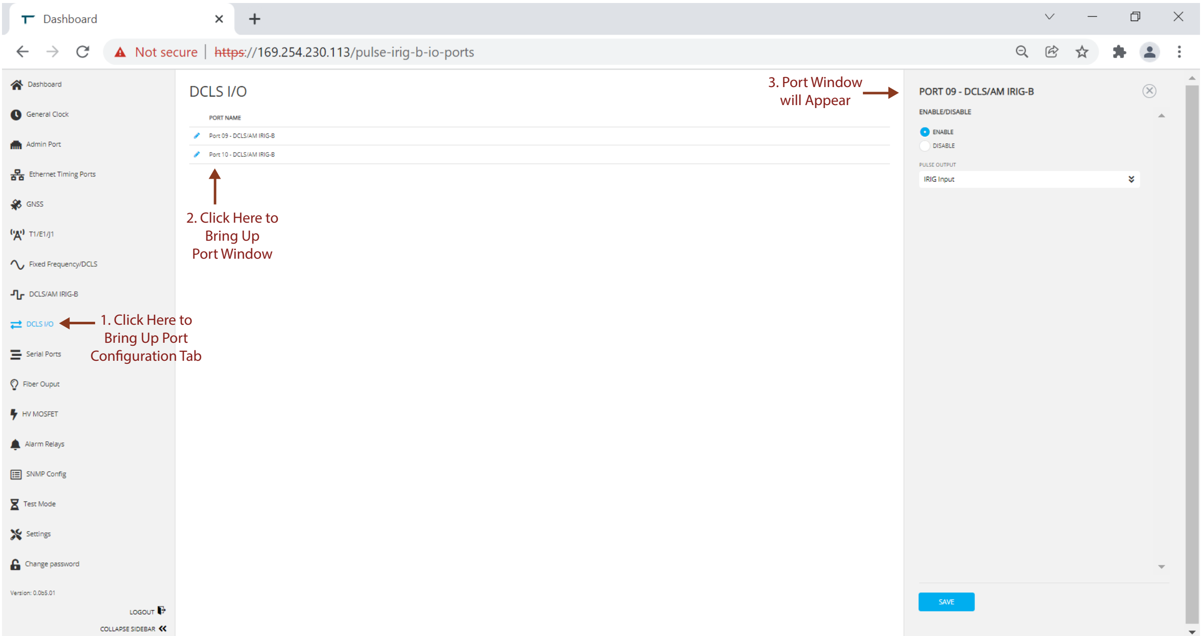
9.8.4 Provisioning IRIG-B Inputs

This section describes how to provision a GridTime 3000 DCLS I/O port to receive an IRIG-B signal.

Note: This port can only receive 0-5 V TTL IRIG-B004 with C37.118.1 Extensions. The GridTime 3000 will not be able to synchronize to the IRIG-B signal if it is not in this format.

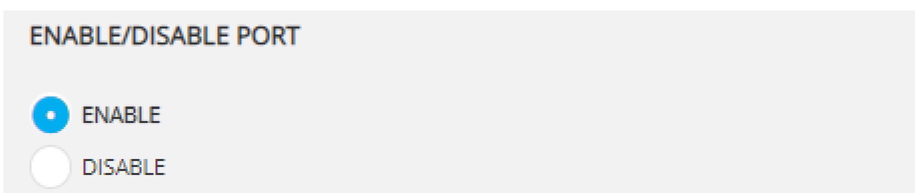
1. **Navigate to Port's Window**
   To navigate to the DCLS/IO port window, on the left navigation pane, click **DCLS/IO**, and then in the center of the screen, click the port you want to configure. This opens the corresponding port settings window on the right pane.

   Figure 9-375. DCLS I/O Port Configuration Window

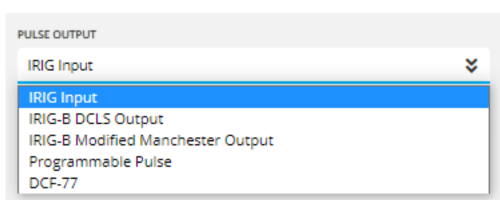
2. **Enable Port**
   On the port settings window on the right, select the **ENABLE** radio button to enable the port.

   Figure 9-376. Enable/Disable Port Setting

3. **Select IRIG Input Option**
   From the **PULSE OUTPUT** drop-down list, select **IRIG Input**.

   Figure 9-377. Pulse Output Setting

4. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.

   A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-378. Successful Save Notification

9.9 Provisioning the Serial String Ports

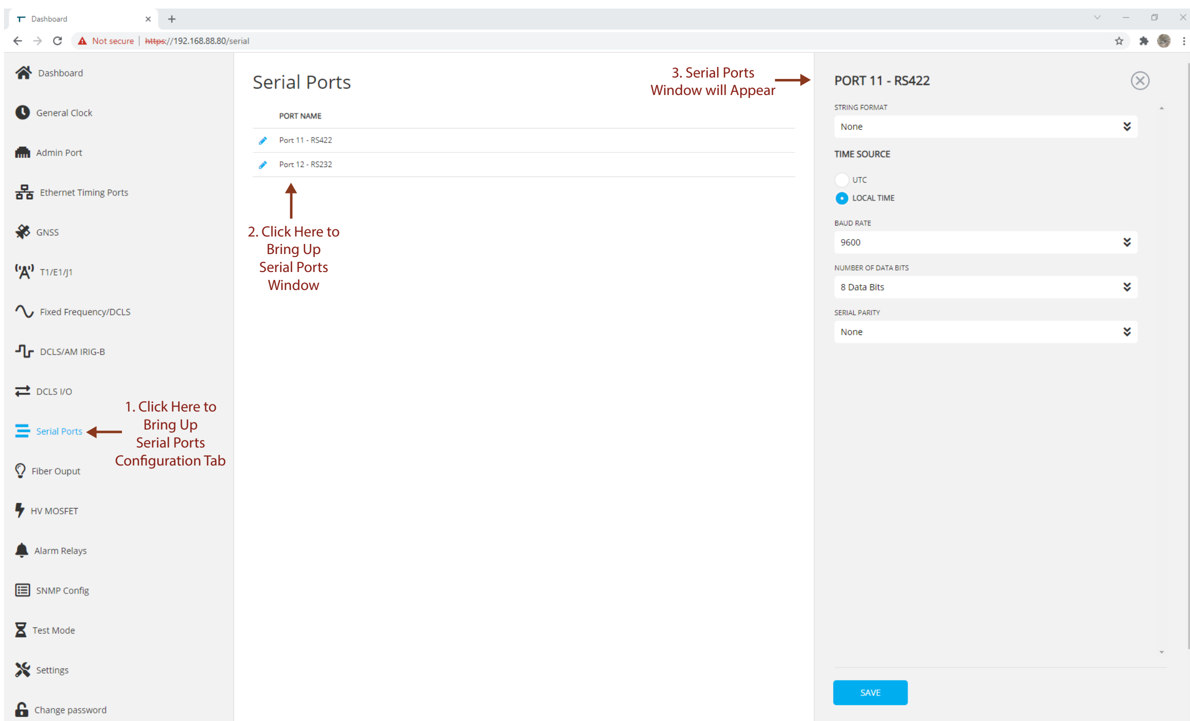
This section describes how to provision the serial string ports.

The Serial Ports configuration tab is used to configure the GridTime 3000 serial string ports. Choosing the correct settings ensures that the end device receiving the serial strings can successfully decode them once they are received.

To provision the GridTime 3000 serial string ports, follow these steps:

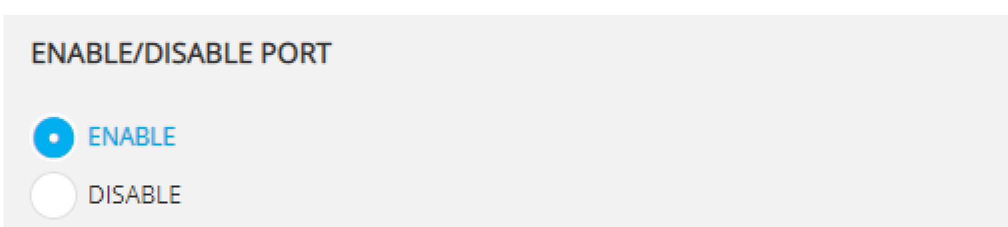
1. **Navigate to Serial String Ports Window**
   To navigate to the serial ports configuration window, on the left navigation pane, click **Serial Ports**, and then click the settings bar corresponding to the port (Port 11 for RS422 and Port 12 for RS232). The settings for the corresponding port is displayed on the right pane.

   Figure 9-379. Serial String Ports Configuration

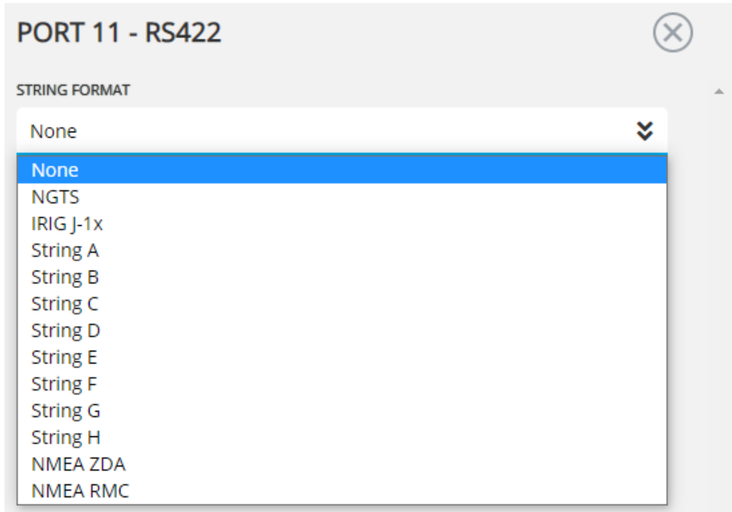
2. **Enable Serial String Port**
   To enable the port, select the **ENABLE** radio button.

   Figure 9-380. Enable/Disable Serial String Port

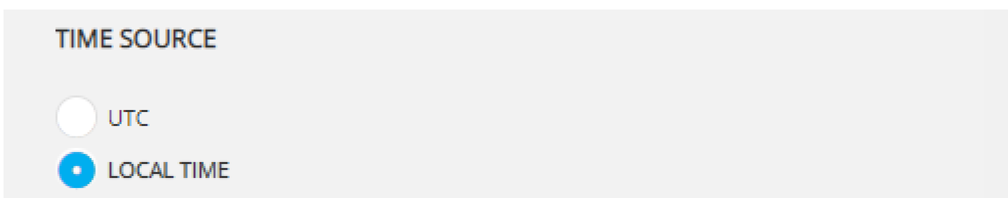
3. **Select the Serial String to Output**
   From the **STRING FORMAT** drop-down list, select the serial string format you wish the port to output. If **None** is selected, no serial string will be outputted by the port.

   Figure 9-381. Selecting the Serial String Output Format



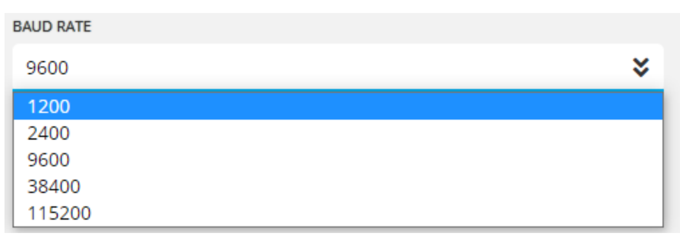
4. **Select whether UTC or Local Time will be used in the output**
   From the **TIME SOURCE** radio buttons, select the serial string output time source. By default, **LOCAL TIME** is selected.

   Figure 9-382. Selecting the Time Source



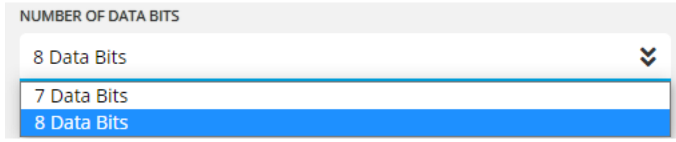
5. **Select Output Baud Rate**
   From the **BAUD RATE** drop-down list, select the serial string output baud rate. This determines the output baud of serial strings in units of Hz. By default, the baud rate is set to **9600**, allowing a maximum of 9600 bits per second.

   Figure 9-383. Selecting the Baud Rate



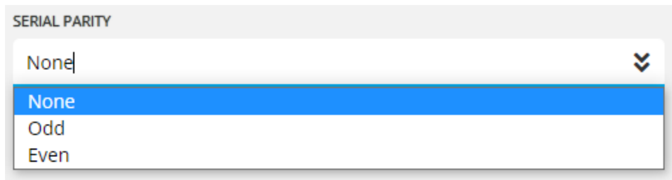
6. **Select the Number of Data Bits**
   From the **NUMBER OF DATA BITS** drop-down list, select the data bits. By default, the number of data bits is set to **8 Data Bits**.

Figure 9-384. Selecting the Number of Data Bits



7. **Select the Serial Parity**
   From the **SERIAL PARITY** drop-down list, select the serial parity option. The options are **None** (no parity), **Odd**, and **Even**. By default, the parity is set to **None**.

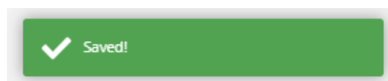
Figure 9-385. Select the Serial Parity



8. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.

   A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-386. Successful Save Notification



9.10 Provisioning the Alarm Relay Ports

This section describes how to provision the Alarm Relay Ports.

The Alarm Relays configuration tab is used to map alarms to the GridTime 3000's Alarm Relay ports.

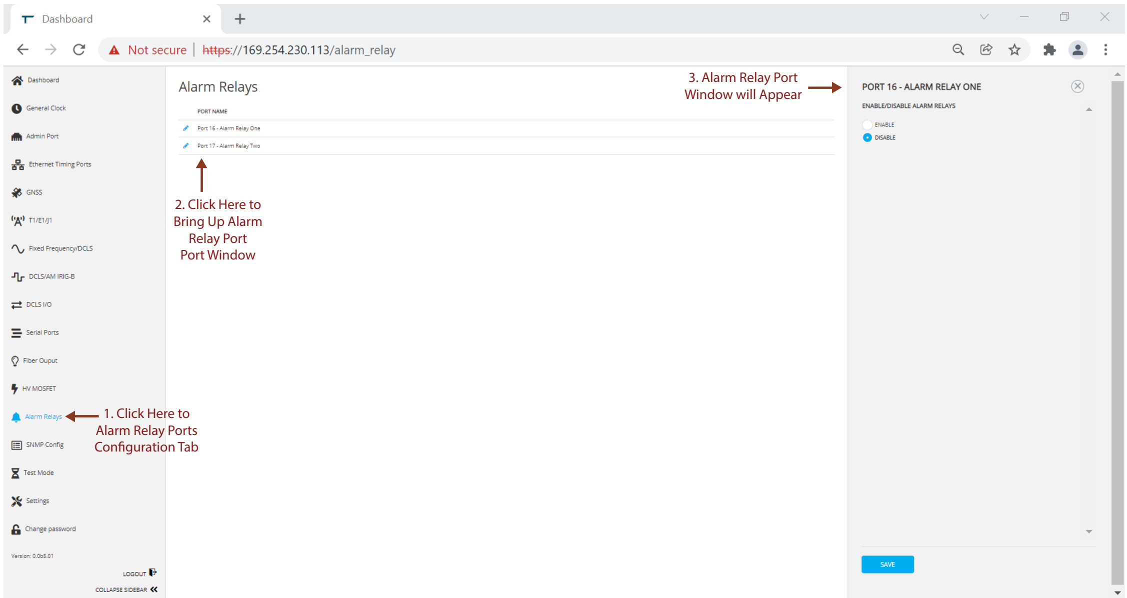
When any of the alarms mapped to an Alarm Relay port becomes active, the port transitions from the non-alarm state to the alarm state. When all active alarms on an Alarm Relay port clear, the port transitions from the alarm state to the non-alarm state.

For the trigger and clearance conditions of all the GridTime 3000 alarms, see Alarm Conditions and Correction Actions.

To provision the GridTime 3000's Alarm Relay ports, follow these steps:

1. **Navigate to Alarm Relay Port Window For Port 1**
   To navigate to the **Alarm Relays** window for the port you want to configure alarms for, on the left navigation pane, click **Alarm Relays**, and then click the settings bar corresponding to the Alarm Relay 1 or 2 (Port 16 or Port 17) port. The settings for the corresponding port appears on the right pane.

Figure 9-387. Alarm Relays Configuration Window



2. **Enable Port**
   To enable a port, select the **ENABLE** radio button.

Figure 9-388. Enable/Disable Alary Relays Port

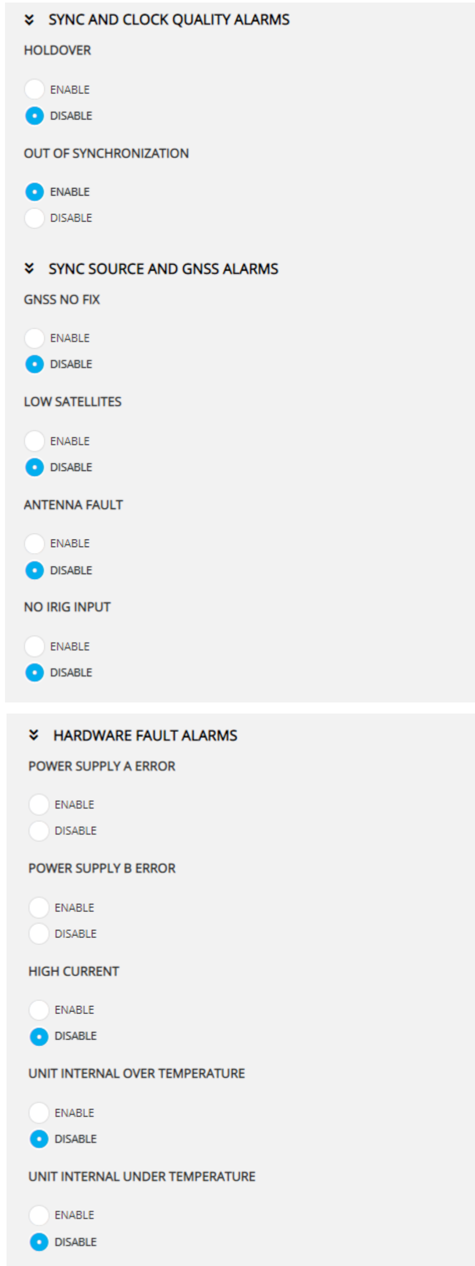
3. **Set Alarm Signal Delay**
   The alarm signal delay setting delays the trigger of the alarm relay by the configured value. Type this value in seconds in the **ALARM SIGNAL DELAY IN SECONDS** text box. By default, this is set to '0' seconds of delay.

Figure 9-389. Setting the Alarm Signal Delay

4. **Map Alarms to Alarm Relay Port**
   To map the alarms to the Alarm Relay port, select the **ENABLE** radio button next to the alarms you wish to map.

   By default, only the **OUT OF SYNCHRONIZATION** alarm is mapped to Alarm Relay One (Port 16), and only the **ANTENNA FAULT** alarm is mapped to Alarm Relay Two (Port 17). All other alarms are disabled.

Figure 9-390. Mapping the Alarms



For a complete description of the supported GridTime 3000 alarms, see Alarm Conditions and Correction Actions.

Note: Not all alarm conditions have an associated alarm relay option.

5. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.
   A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-391. Successful Save Notification

6. **Repeat on Port 2**
   Repeat this process on Alarm Relay Two (Port 17).

9.11 Provisioning an External Authentication Server

This section describes how to provision the GridTime 3000 to use an external authentication server (RADIUS or LDAP) to authenticate users.

9.11.1 Provisioning RADIUS

This section describes how to configure RADIUS authentication on the GridTime 3000.

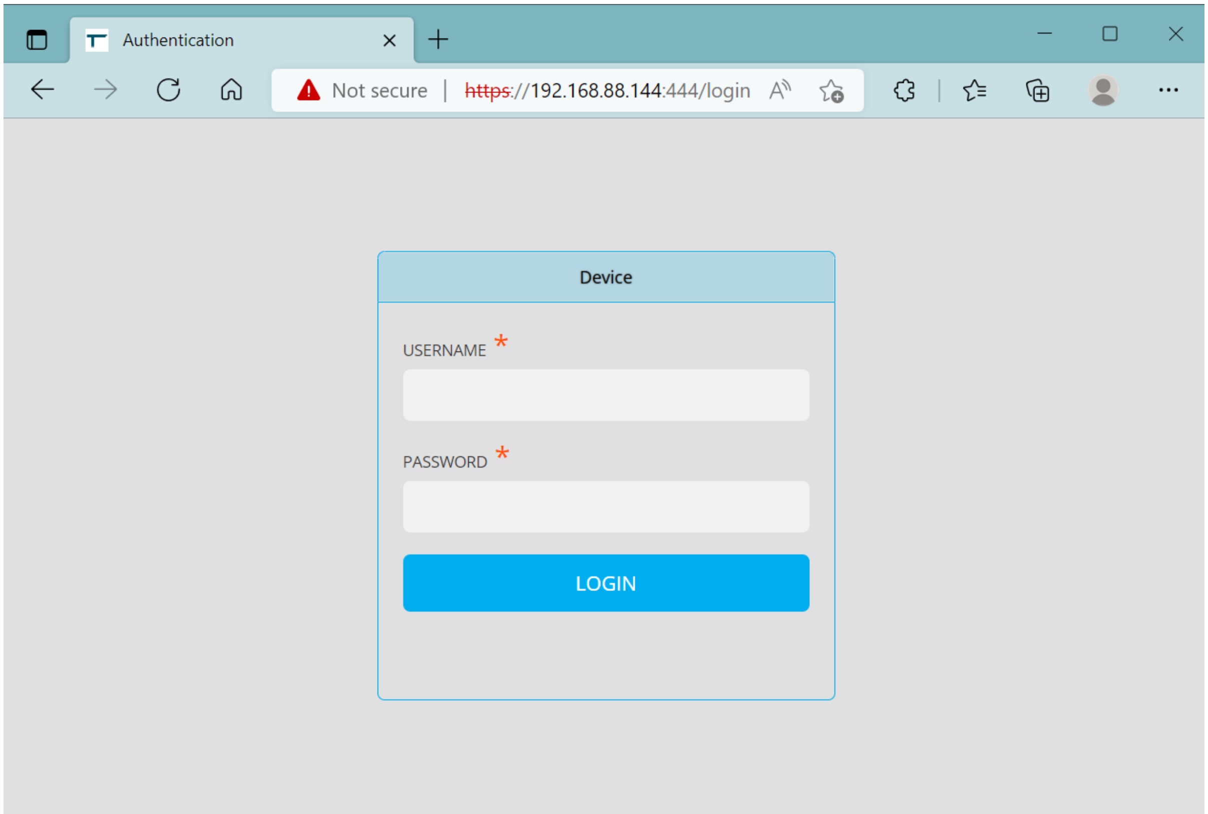
Note: By default, GridTime 3000 only allows the 'Administrator' role to have read and write access to all settings and advanced configuration menus. To set up additional roles, follow the instructions in Provisioning Roles.
By default, it also has a single Administrator user with the Administrator role mapped to it. The username for the Administrator user is 'Administrator', and the password will be what was entered during the first time login to CMT.

Important: Only a user with the role of 'Administrator' can provision users on the GridTime 3000.

Note: RADIUS requests will only be sent through the Admin Ethernet port.

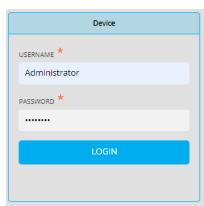
1. To navigate to the CMT authentication module, in your browser’s address bar, type the IP address you normally use to access the CMT and then add **:444** to the end of the address. The authentication module login screen is displayed.

Figure 9-392. CMT Authentication Module Login Screen



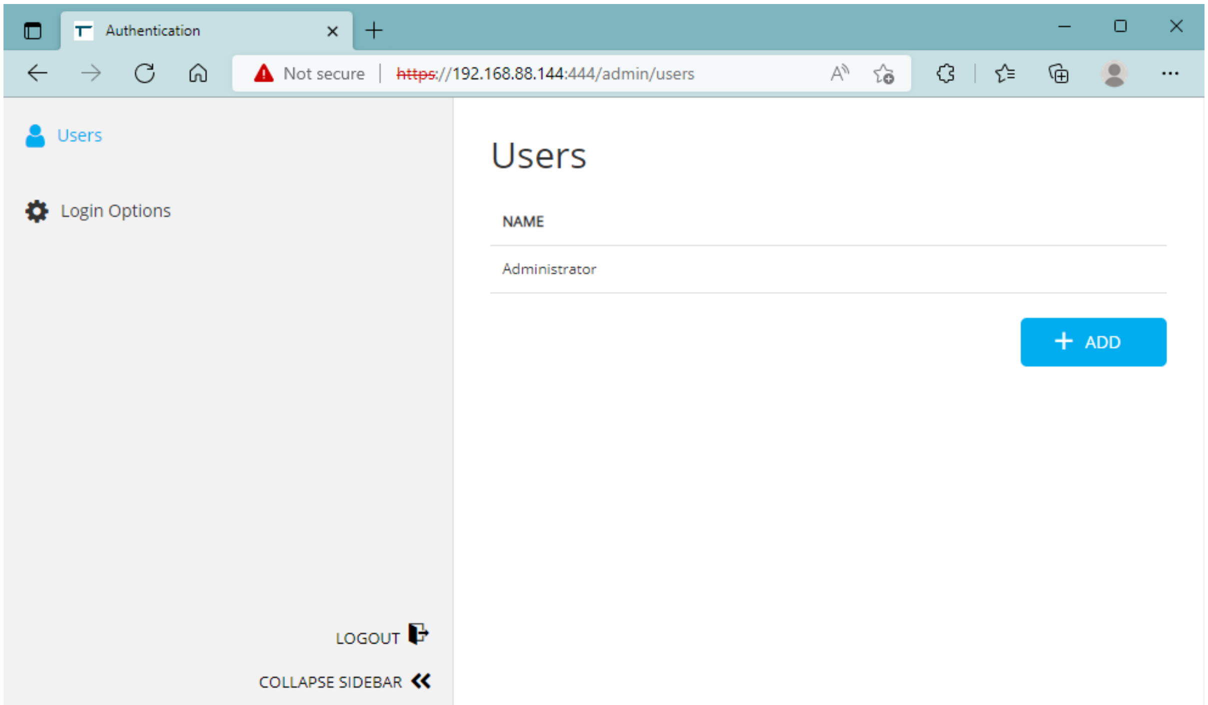
2. Enter the Administrator user login details and click **LOGIN**.

Figure 9-393. Logging In



3. Upon successful authentication, the **Users** tab of the authentication module is displayed.

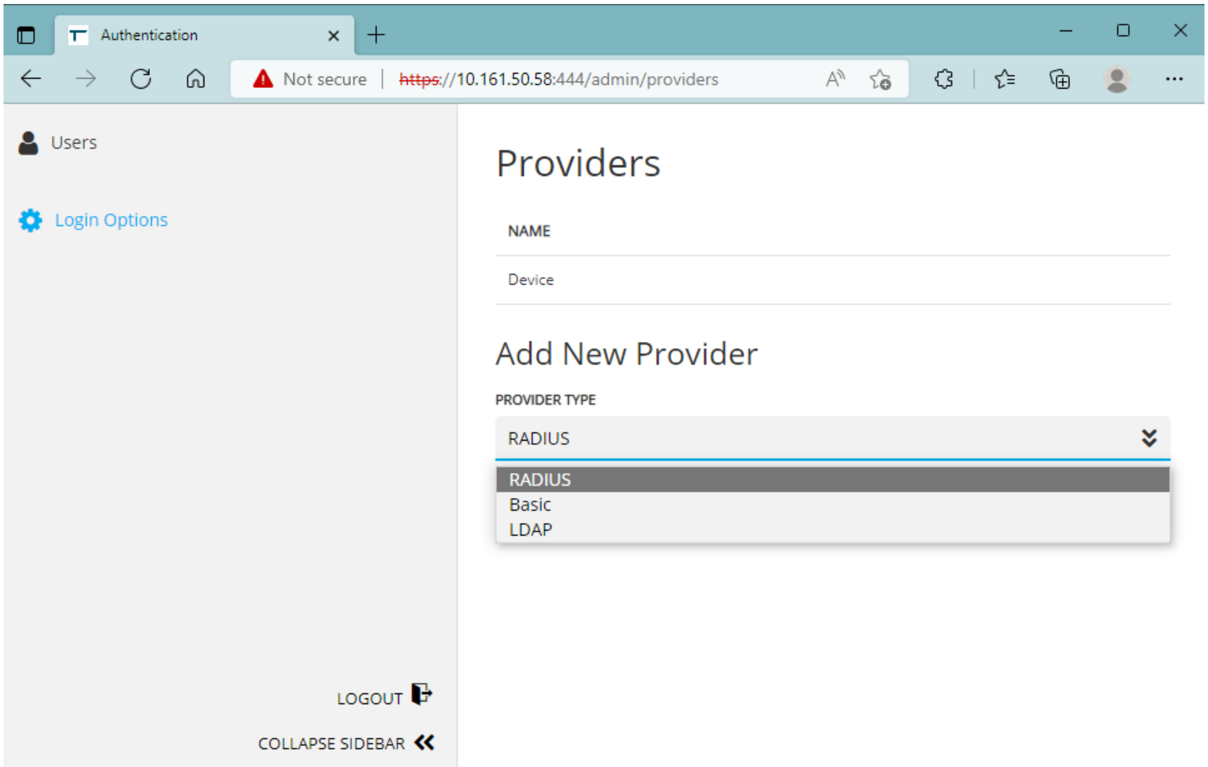
Figure 9-394. Authentication Module-Users Tab



Note: Unless previously modified, only the 'Administrator' user should be present as per the GridTime 3000's default settings.

4. To create a RADIUS provider:
   a. On the left navigation pane, click **Login Options**.

Figure 9-395. Adding a New RADIUS Provider

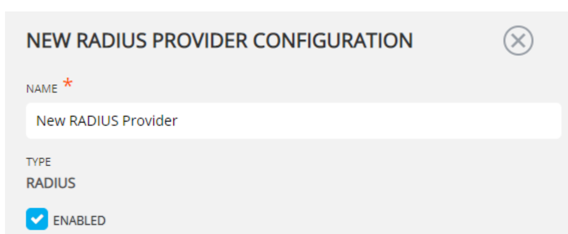


b. Click the **PROVIDER TYPE** drop-down list and select **RADIUS**, and then click **+ADD**.

   Note: The fields in the following screen shots are filled in with example inputs. The user should fill out the fields to fit their particular configuration parameters.

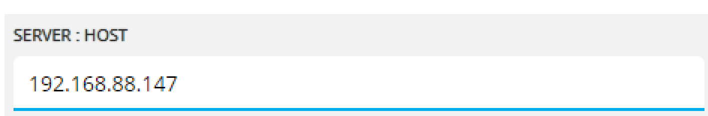
5. A new dialog box appears. Enter a name for the RADIUS provider in the **NAME *** text box.
   Note: This is not the server host address; this is simply a name used to identify the provider in the Providers Configuration Module.

   Figure 9-396. New RADIUS Provider Configuration

6. To enable this as a RADIUS provider, select the **ENABLED** check box .
7. Enter the IP address of the RADIUS server in the **SERVER : HOST** field.

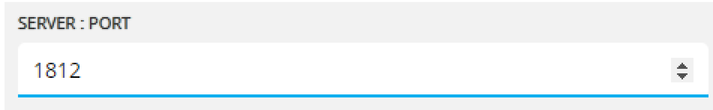
   Figure 9-397. Set the RADIUS Server IP Address

   Note: At the date of publication, the GridTime 3000 software only supports IPv4 addresses.

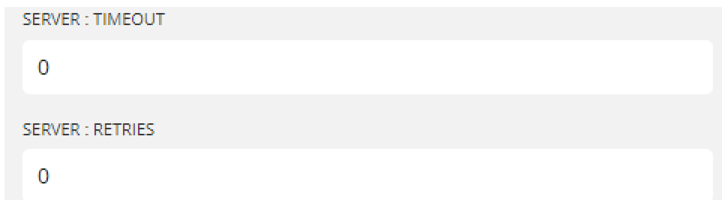
8. Enter the UDP port number that the RADIUS server is expecting to receive requests on. By default, this is configured to UDP port 1812, as per RFC 2865.

Figure 9-398. Set the UDP Port Number



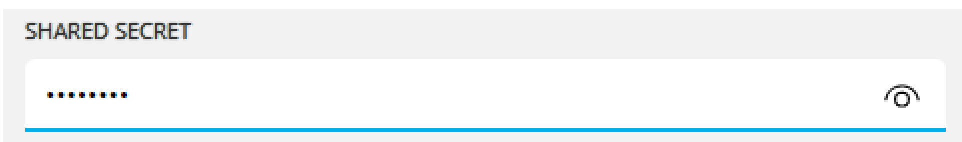
9. You can also change the default values for the **SERVER : TIMEOUT** and **SERVER : RETRIES** fields.
   – The **SERVER : TIMEOUT** field specifies the delay between retries for accessing the server, and is measured in milliseconds.
   – The **SERVER : RETRIES** field specifies how many times to send a RADIUS request in the event that a server response is not received. A value of '0' will disable the retries.

Figure 9-399. Timeout and Retry Settings



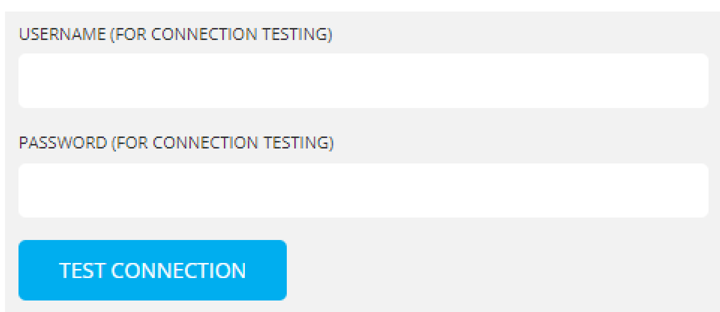
10. Enter the server secret in the **SHARED SECRET** field.

Figure 9-400. Set the Server Secret



11. Enter the username and password of a user in the RADIUS server and click **TEST CONNECTION** to validate the provider has been set up correctly, and that the GridTime 3000 can establish a connection with the RADIUS server.

Figure 9-401. Test New Connection



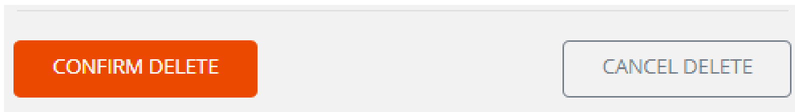
Note: This step is optional, but is useful to ensure that the connection is established correctly

12. **Save Settings**
    To write the settings to the GridTime 3000, click **SAVE**.
    A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-402. Successful Save Notification

13. To map a user to the RADIUS provider, see Provisioning Users - RADIUS
Note: To delete a provider, bring up the provider settings using steps 1, 2 and 3 and click **DELETE**. You will then be prompted to either confirm or cancel the deletion.

Figure 9-403. Confirm Deletion



9.11.2 Provisioning LDAP

This section describes how to configure LDAP authentication on the GridTime 3000.

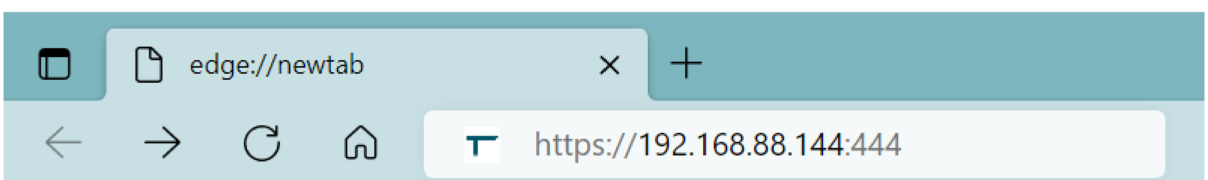
Note: By default, GridTime 3000 only allows the 'Administrator' role to have read and write access to all settings and advanced configuration menus. To set up additional roles, follow the instructions in Provisioning Roles.
By default, it also has a single Administrator user with the Administrator role mapped to it. The username for the Administrator user is 'Administrator', and the password will be what was entered during the first time login to CMT.

Important: Only a user with the role of 'Administrator' can provision users on the GridTime 3000.

Note: LDAP requests will only be sent through the Admin Ethernet port.

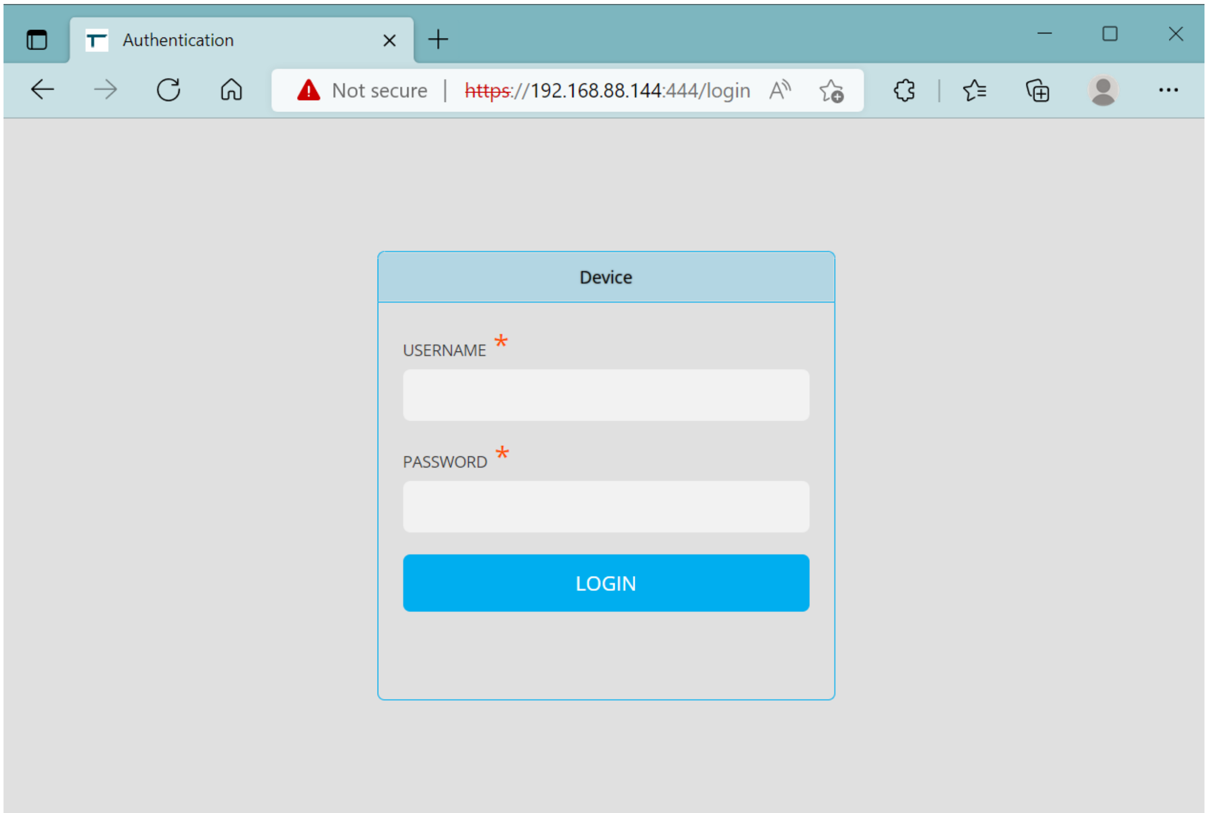
1. To navigate to the CMT authentication module, in your browser's address bar, type the IP address you normally use to access the CMT and then add **:444** to the end of the address.

Figure 9-404. CMT Authentication Module



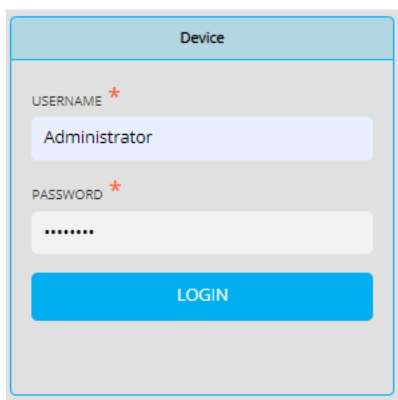
The authentication module login screen is displayed.

Figure 9-405. CMT Authentication Module Login Screen



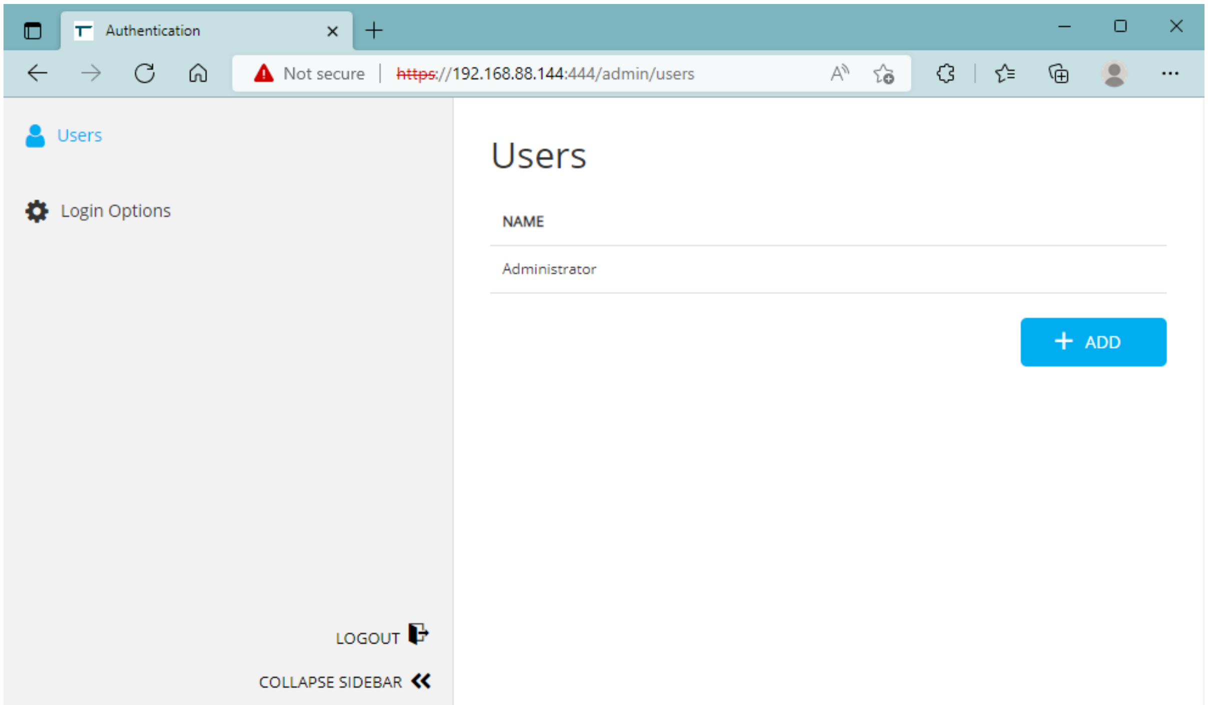
2. Enter the Administrator user login details and click **LOGIN**.

Figure 9-406. Logging In



3. Upon successful authentication, the **Users** tab of the authentication module is displayed.

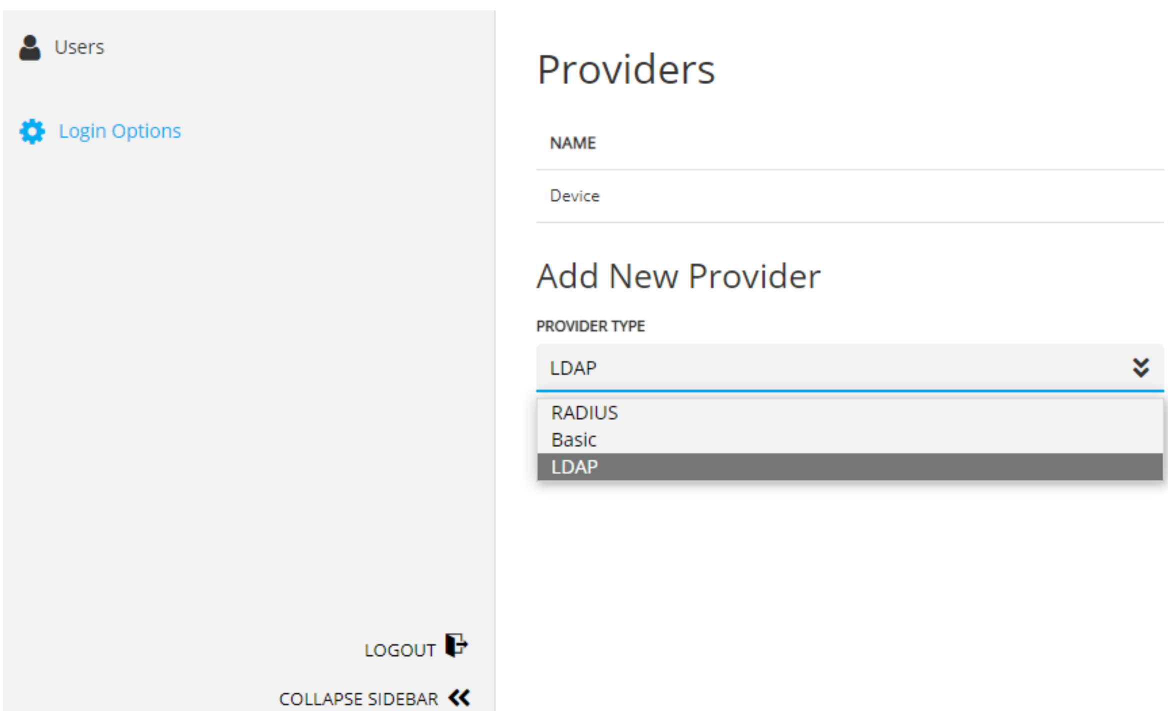
Figure 9-407. Authentication Module-Users Tab



Note: Unless previously modified, only the 'Administrator' user should be present as per the GridTime 3000's default settings.

4. To create a LDAP provider:
   a. On the left navigation pane, click **Login Options**.

Figure 9-408. Adding a New LDAP Provider



Note: The fields in the following screen shots are filled in with example inputs. The user should fill out the fields to fit their particular configuration parameters.

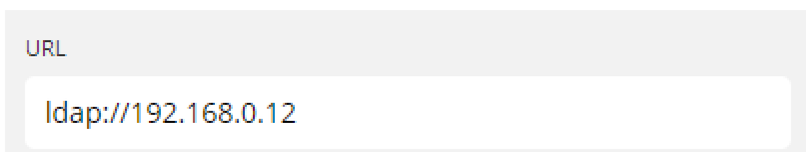
b. Click the **PROVIDER TYPE** drop-down list and select **LDAP**, and then click **+ADD**.

5. A new dialog box appears. Enter a name for the LDAP provider in the **NAME *** field.
Note: This is not the server host address; this is simply a name used to identify the provider in the Providers Configuration Module.

Figure 9-409. New LDAP Provider Configuration

6. To enable this as a LDAP provider, select the **ENABLED** check box.
7. Enter the address of the LDAP provider in the **URL** field.

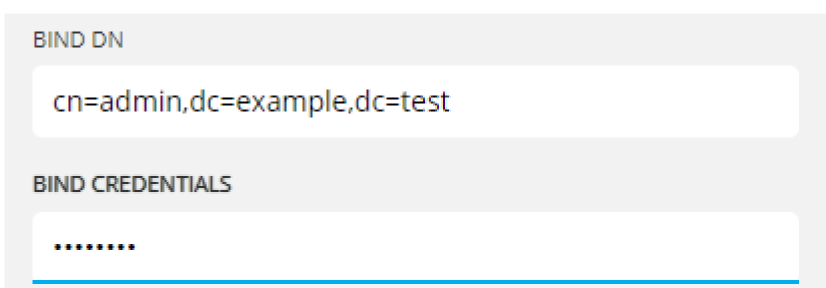
Figure 9-410. Set the LDAP URL



Note: At the date of publication, the GridTime 3000 software only supports IPv4 addresses.

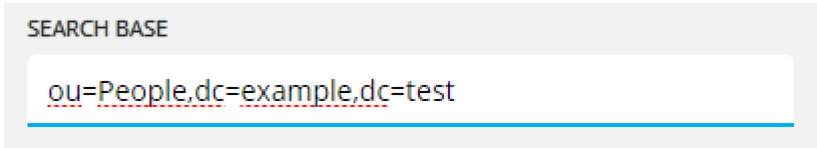
8. Fill the **BIND DN** field. This is the distinguished name of the user in the LDAP directory to bind as. If left empty, an anonymous bind will be performed. In the **BIND CREDENTIALS** field, enter the password for the user specified in the **BIND DN** field.

Figure 9-411. Set the LDAP User Distinguished Name



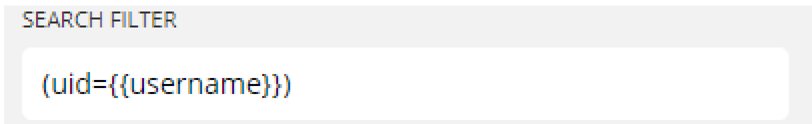
9. The **SEARCH BASE** field specifies the distinguished name of the base entry. User entries are expected to be found in subtrees under this entry. If left empty, the root of the directory will be searched.

Figure 9-412. Search Base Entry



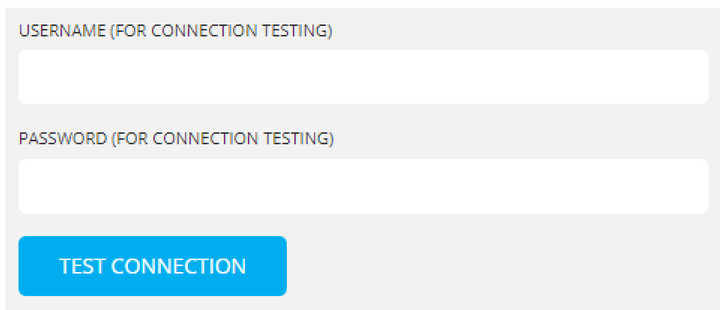
10. The **SEARCH FILTER** field specifies the search filter to be used to find an entry matching the user attempting to login. When the search filter is used, the placeholder **{{username}}** will be replaced with the username of the user attempting to login. It is expected that the search filter is only expected to match exactly one user; if more than one user is found, then the authentication will fail.

Figure 9-413. Search Filter Entry



11. Enter the username and password of a user in the LDAP server and click **TEST CONNECTION** to validate the provider has been set up correctly, and that the GridTime 3000 can establish a connection with the LDAP server.

Figure 9-414. Test New Connection



Note: This step is optional, but is useful to ensure that the connection is established correctly

12. **Save Settings**

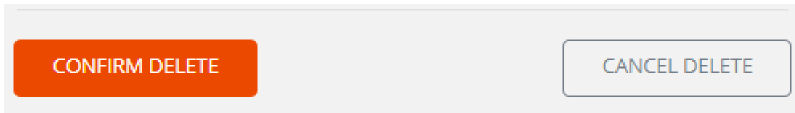
To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-415. Successful Save Notification

13. To map a user to the LDAP provider, see Provisioning Users - LDAP.

Note: To delete a provider, bring up the provider settings using steps 1, 2 and 3 and click **DELETE**. You will then be prompted to either confirm the deletion or cancel it.

Figure 9-416. Confirm Provider Deletion



9.12 Provisioning Roles

This section describes how to provision roles for the GridTime 3000.

Note: Only an 'Administrator' user can configure Roles on the GridTime 3000.

All CMT and SNMP users set up on the GridTime 3000 have a role mapped to them. The role defines what settings the user can view and edit (read and write permissions).

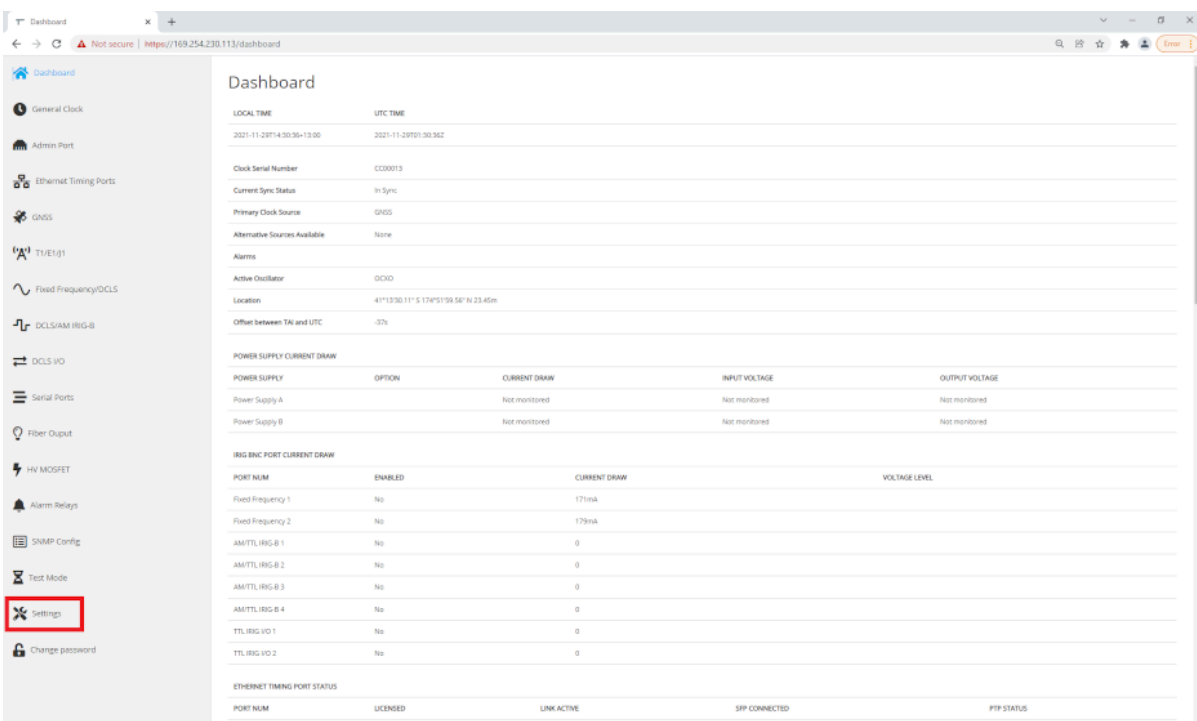
By default, the GridTime 3000 only has the 'Administrator' role set up, additional roles have to be set up using the instructions in this section. Along with the Administrator role, an Administrator user is also set up by default which has the Administrator role mapped to it.

The Administrator role is hidden in CMT as it cannot be edited or removed. The Administrator role allows full access to all of the GridTime 3000 settings. It is also the only role that can access the CMT settings menu, and is the only role that can access the CMT's Users module — where CMT user settings are modified and users are added or removed.

To set up additional roles for the GridTime 3000 apart from the Administrator role, follow these instructions. If no additional roles are required apart from the Administrator role, you can skip this section.

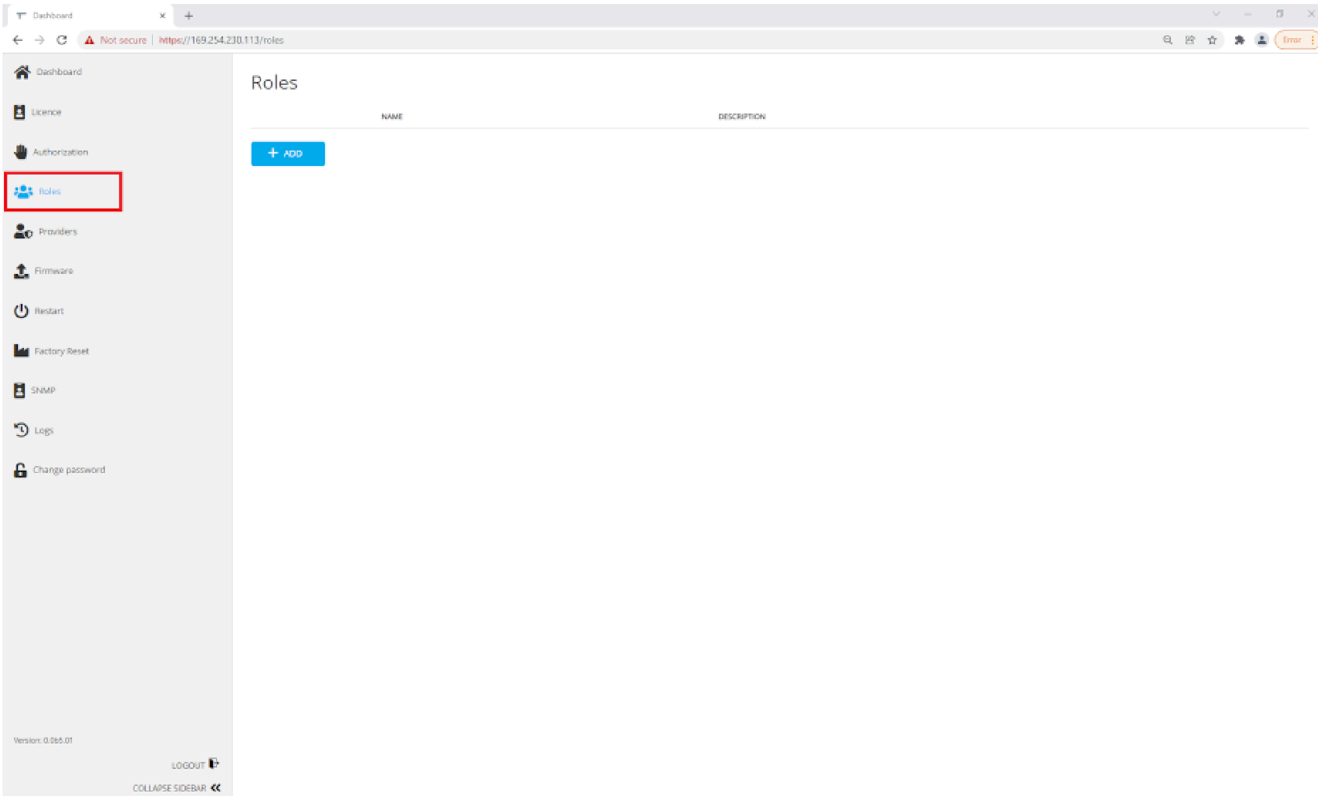
1. **Navigate to the Roles Tab**
   On the left navigation pane of the Dashboard, click **Settings**.

Figure 9-417. Settings Tab



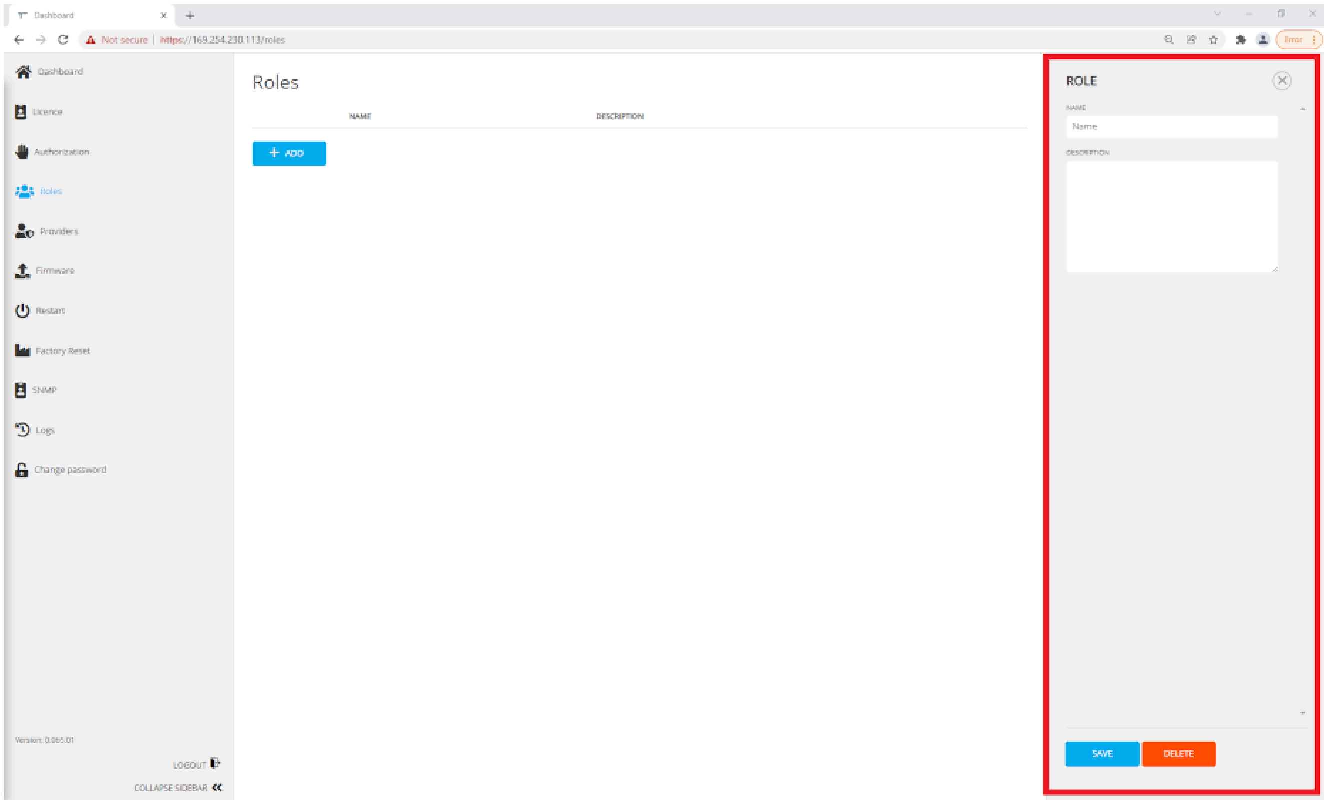
To bring up the Roles window, click **Roles**. All of the GridTime 3000's user roles are shown here apart from the Administrator role.

Figure 9-418. Roles Window



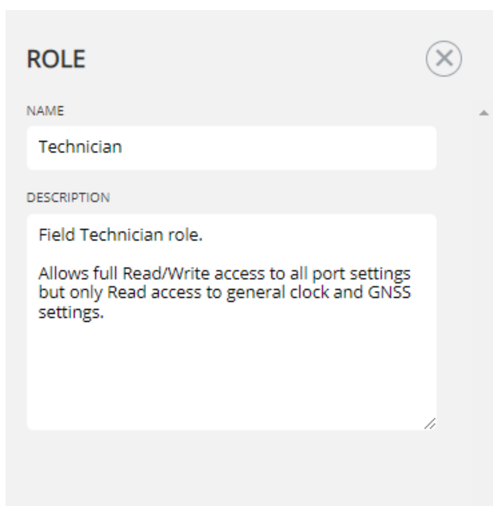
2. **Add New Role**
   To add a new role, click the **+ ADD** button. This brings up the **ROLE** settings window on the right hand side.

Figure 9-419. Role Settings Window



3. **Enter New Role Name and Description**
   Type the name and description for the new role into the respective textboxes.

Figure 9-420. Role Name and Description Details

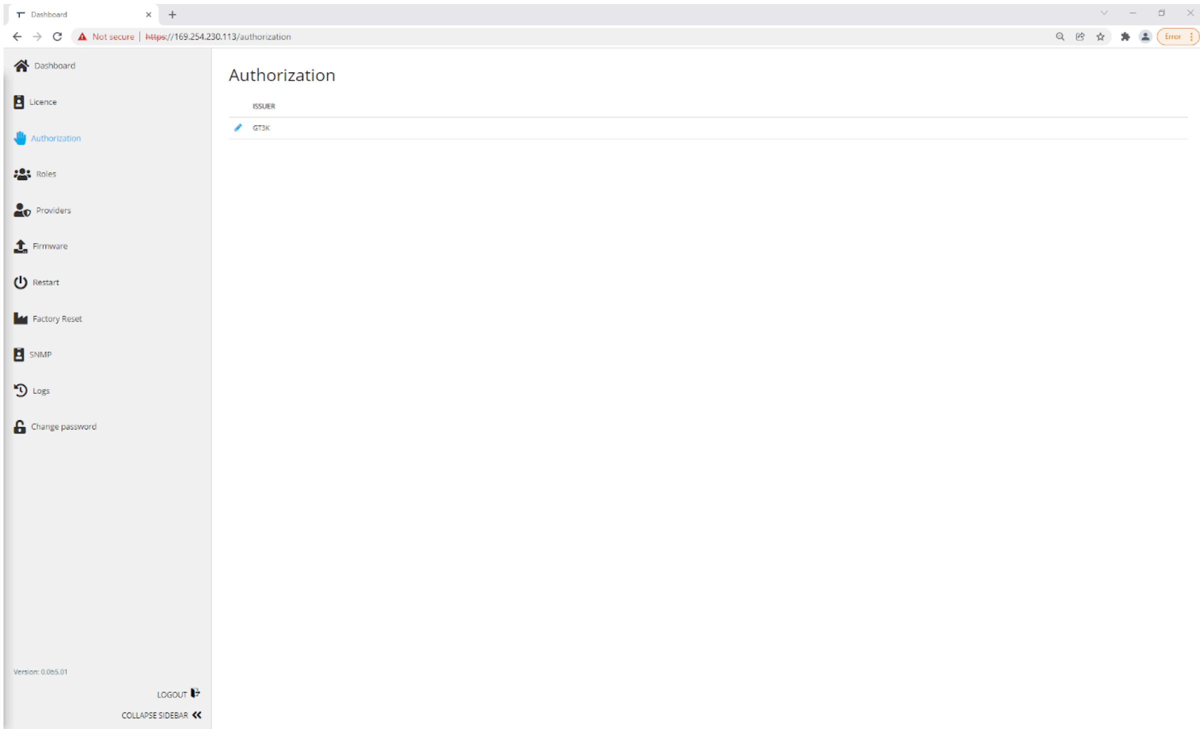


4. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-421. Successful Save Notification

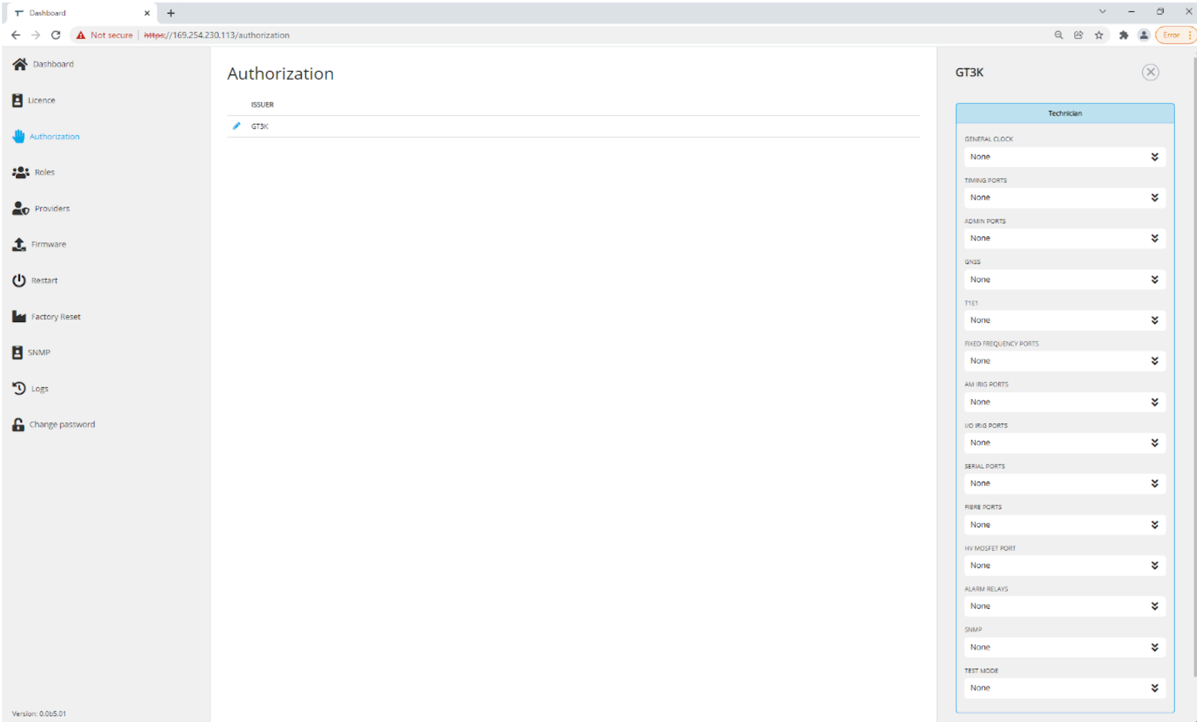
5. **Navigate to the Authorization Tab**
   Click **Authorization** to bring up the Authorization window.

Figure 9-422. Authorization Window



6. **Open Settings Window for New Role**
   Click **GT3K** issuer to load up the role authorization window. Click on the name of the role you have just configured in the right-hand window to bring up its associated permissions.

Figure 9-423. Configuring the New User Settings



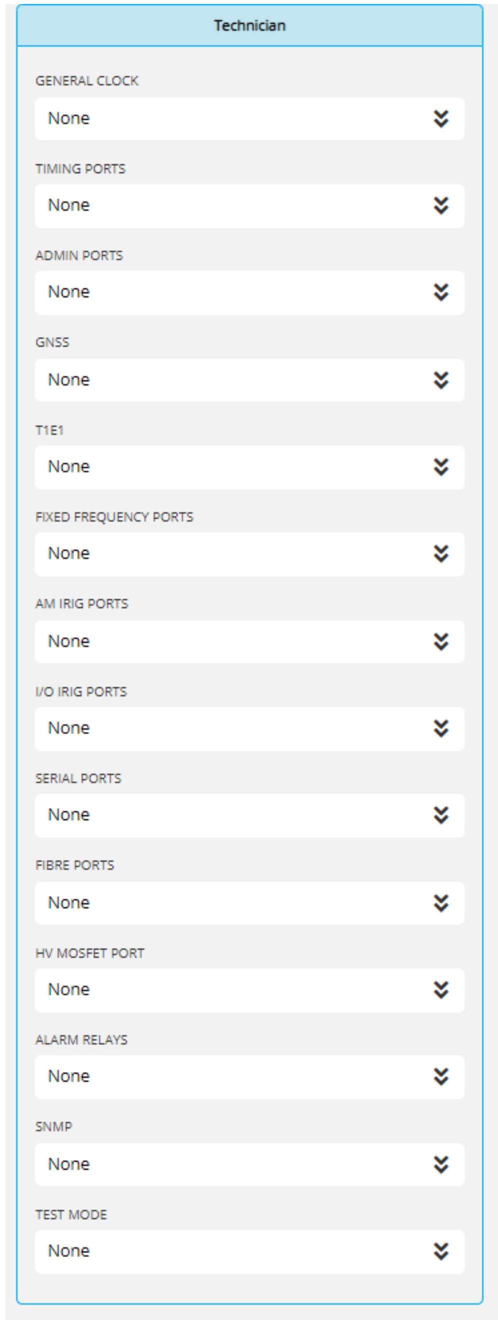
A series of drop-downs appears, each corresponding to a group of settings.

Each group of settings — that is general clock settings, have its own drop-down showing the role's access permissions for that group of settings.

Settings are grouped by port type or by functionality.

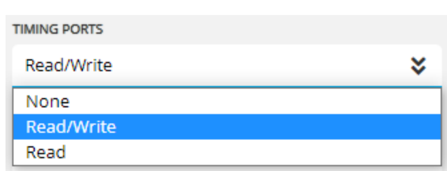
By default, a new role will have 'None' (no access), for all settings.

Figure 9-424. New Role Settings Window



7. **Edit Permissions**
   Go through and modify the role's access to each group of settings, using the drop-down options.

Figure 9-425. Modify Permissions



8. **Save Settings**

To write the settings to the GridTime 3000, click **SAVE**.

A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-426. Successful Save Notification

9.13 Provisioning SNMP Settings

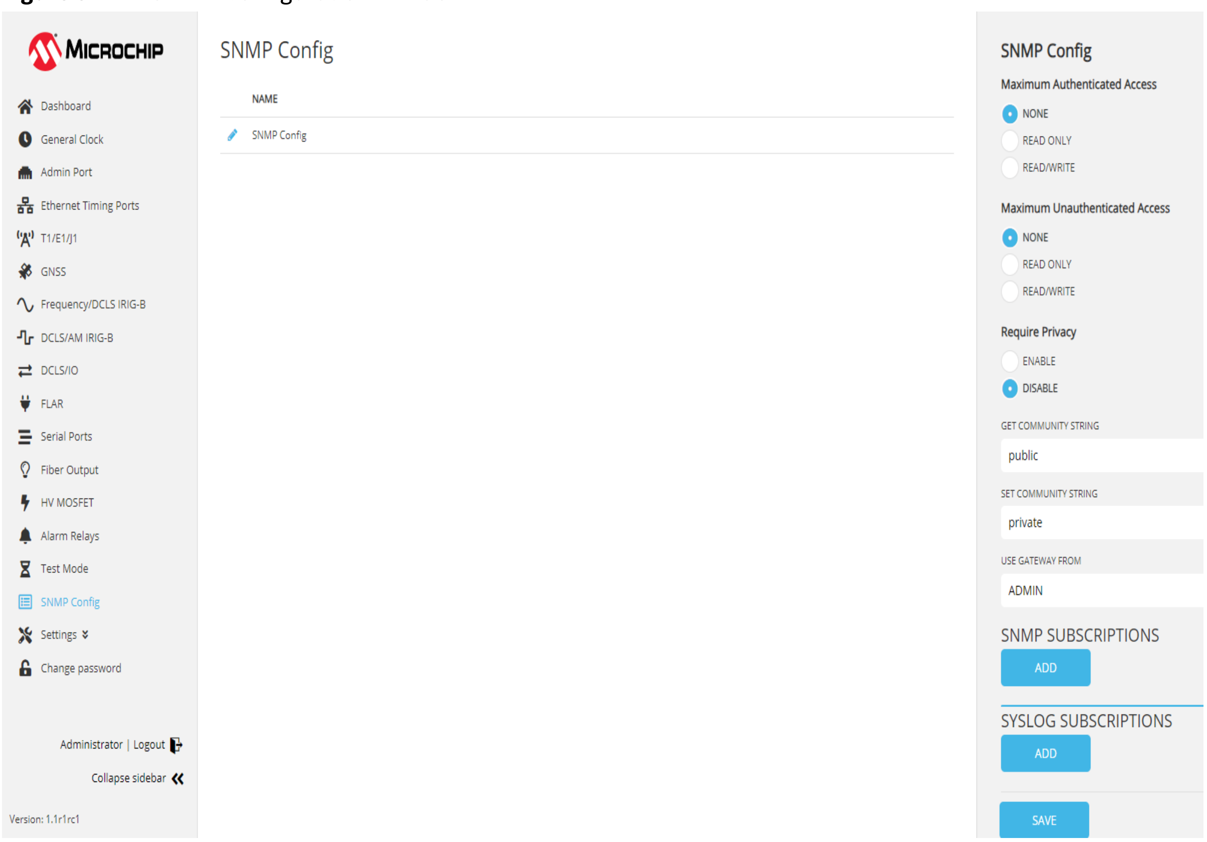
This section describes how to provision the SNMP settings on the GridTime 3000.

The SNMP configuration tab is used to configure the GridTime 3000's SNMP related settings.

To provision the GridTime 3000's SNMP agent, follow these steps:

1. **Navigate to SNMP Config Window**
   To navigate to the SNMP configuration window, on the left navigation pane, click **SNMP Config**, and then click the SNMP Config settings bar on the center of the screen. The **SNMP CONFIG** settings window appears on the right pane.

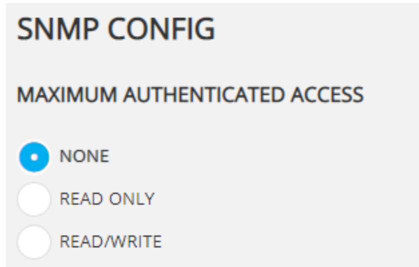
Figure 9-427. SNMP Configuration Window



2. **Set Maximum Authenticated Access**
   This field sets the access limits for authenticated clients using SNMPv3 with User-based Security Model (USM) Authentication. The configurable access levels are:
   – None
   – Read only
   – Read/Write

By default, this is set to **NONE**, meaning no access.

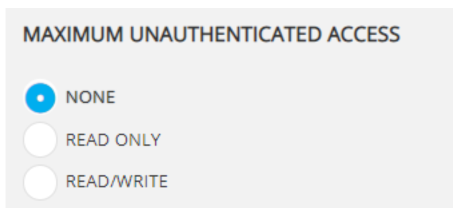
Figure 9-428. Maximum Authenticated Access Settings



3. **Set Maximum Unauthenticated Access**
   This field sets the access limits for unauthenticated clients using SNMPv1, SNMPv2c and SNMPv3 without USM Authentication. The configurable levels are:
   - None
   - Read only
   - Read/Write

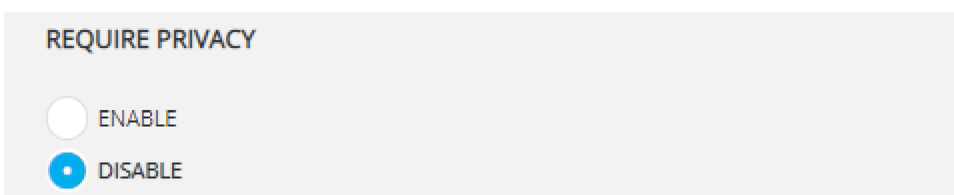
   By default, this is set to **NONE**, meaning no access.

Figure 9-429. Maximum Unauthenticated Access Settings



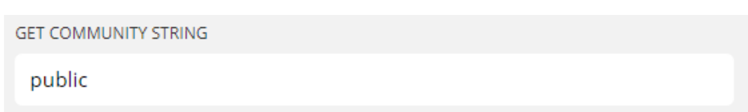
4. **Require or do not require privacy setting**
   The **REQUIRE PRIVACY** radio buttons determine whether SNMPv3 USM privacy is required on SNMP requests.
   By default, this is set to **DISABLE**, meaning SNMPv3 USM privacy is not required.

Figure 9-430. Enable/Disable USM Privacy



5. **Enter Get Community String (SNMPv1, SNMPv2c)**
   This field is the Public string access key. By default, this is set to **public**.

Figure 9-431. Get Community String Settings



6. **Enter Set Community String (SNMPv1, SNMPv2c)**
   This field is the Private string access key. By default, this is set to **private**.

Figure 9-432. Set Community String Setting

7. **Use Gateway From**
   Outgoing notifications with destinations outside the subnet accessible to the management ports are sent through the default gateway of the designated Ethernet port. If the designated Ethernet port has no assigned gateway, notifications are routed through the admin port instead.

Figure 9-433. Select the Gateway Source

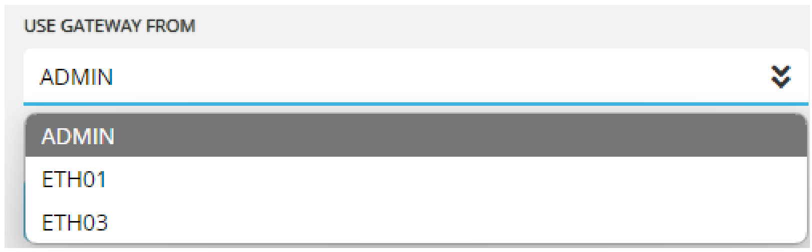
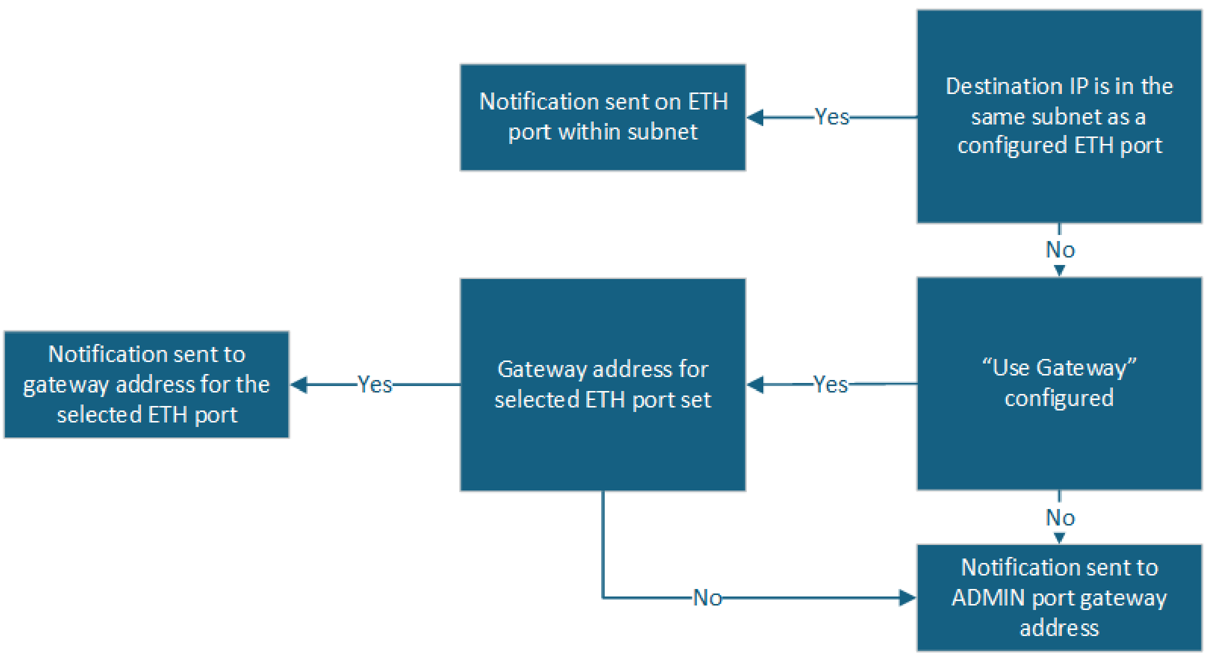


Figure 9-434. Gateway Flow



8. **Setting up Subscriptions**
   If SNMP or Syslog subscriptions are set up on the network, follow the instructions from one of the following sections:
   – Provisioning SNMP Notifications
   – Provisioning Syslog Notifications

   Note: All SNMP and Syslog notifications are sent from the GridTime 3000's admin Ethernet port only, ensure SNMP trap clients are set up with the IP address of the admin Ethernet port.
9. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.

A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-435. Successful Save Notification

10. **Set up SNMPv3 Users**

    Follow the instructions in Provisioning SNMP Users if SNMPv3 USM privacy is to be used.

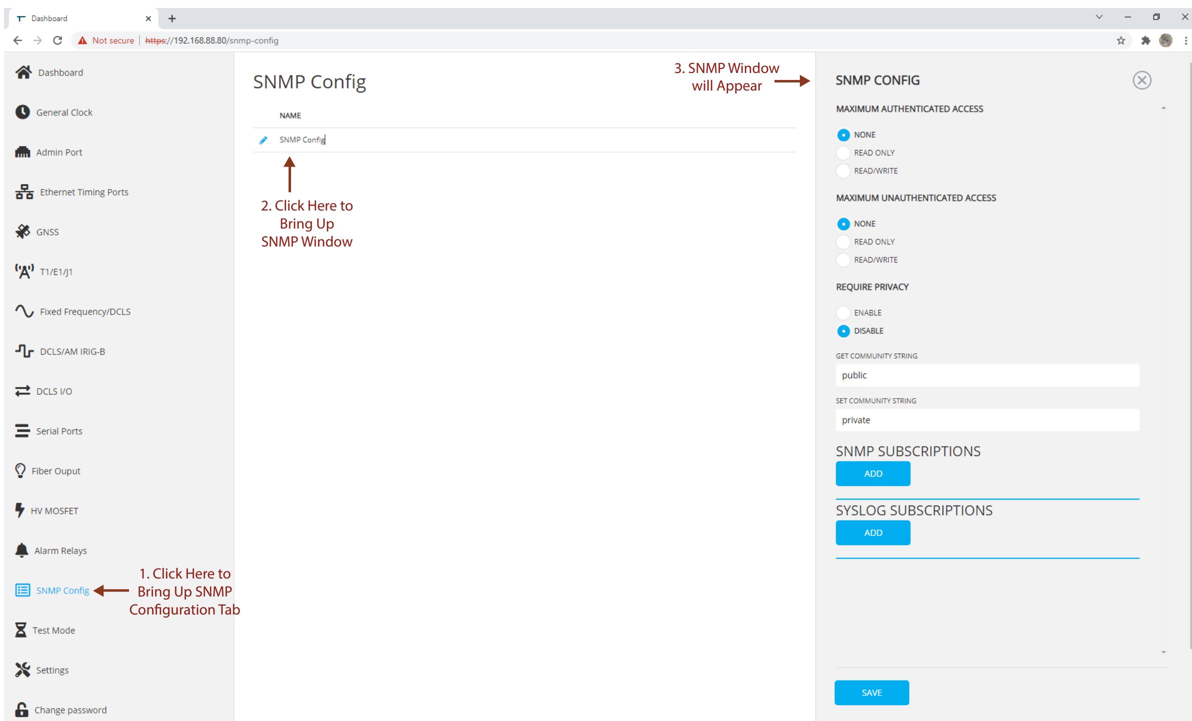
9.13.1 Provisioning SNMP Notifications

This section describes how to provision SNMP notifications.

1. **Navigate to SNMP Config Window**

   To navigate to the SNMP Configuration window, on the left navigation pane, click **SNMP Config**, and then click the SNMP Config settings bar in the center of the screen. The **SNMP CONFIG** settings window appears on the right pane.

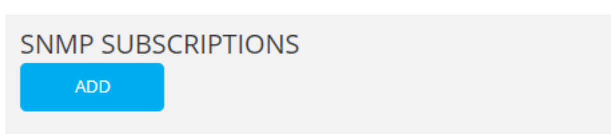
   Figure 9-436. SNMP Configuration Window



2. **Add New SNMP Subscription**

   To add a new SNMP subscription, under **SNMP SUBSCRIPTIONS**, click **ADD**.

   Figure 9-437. Add New SNMP Subscription

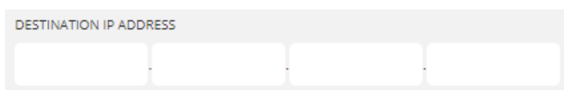


   This displays the new SNMP subscription settings.

Figure 9-438. SNMP Subscriptions Settings

3. **Enter Subscription's Destination IP Address**
   Enter the IP address of the SNMP client subscribing to GridTime 3000 notifications.

   Figure 9-439. SNMP Destination IP Address

4. **Enter Subscription's User Name**
   When the SNMP version selected is SNMPv2, this field will be used as the security key. The key can consist of any character combination, up to 32 characters maximum length.

   If the SNMP version selected is SNMPv3, and the username of a user set up in the 'SNMP Users' window is entered, then the user authentication settings will be applied. See Provisioning SNMP Users.

   If SNMPv3 is used and the username does not map to an SNMP user, SNMP notifications will be unauthenticated and unencrypted.

   Enter the user name for the SNMP subscriber.

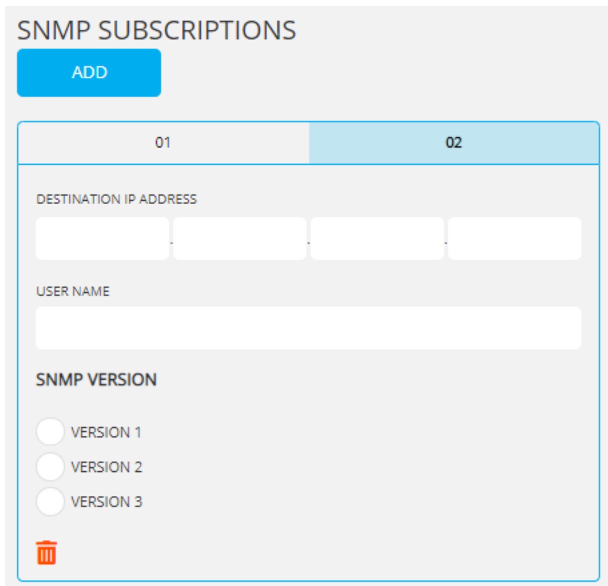
   Figure 9-440. Set SNMP Subscriber User Name

5. **Select SNMP Version Used by Subscription**
   Select the SNMP version to be used by the SNMP subscriber from SNMPv1, SNMPv2c, and SNMPv3.

Figure 9-441. Set SNMP Version

6. **Repeat Steps 2-5 for Each Additional Subscriber**
   To add another SNMP subscriber, click **ADD** again, and click the **02** tab under the **ADD** button to navigate to the settings for the new SNMP subscriber setting. The **01** tab contains the settings for the subscriber that was previously set up.

   Figure 9-442. Add Multiple SNMP Subscribers

   Repeat for as many subscriptions as are present on the network.

   > **Tip:**
   > To remove a SNMP subscription, click the icon.

7. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.
   A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

   Figure 9-443. Successful Save Notification

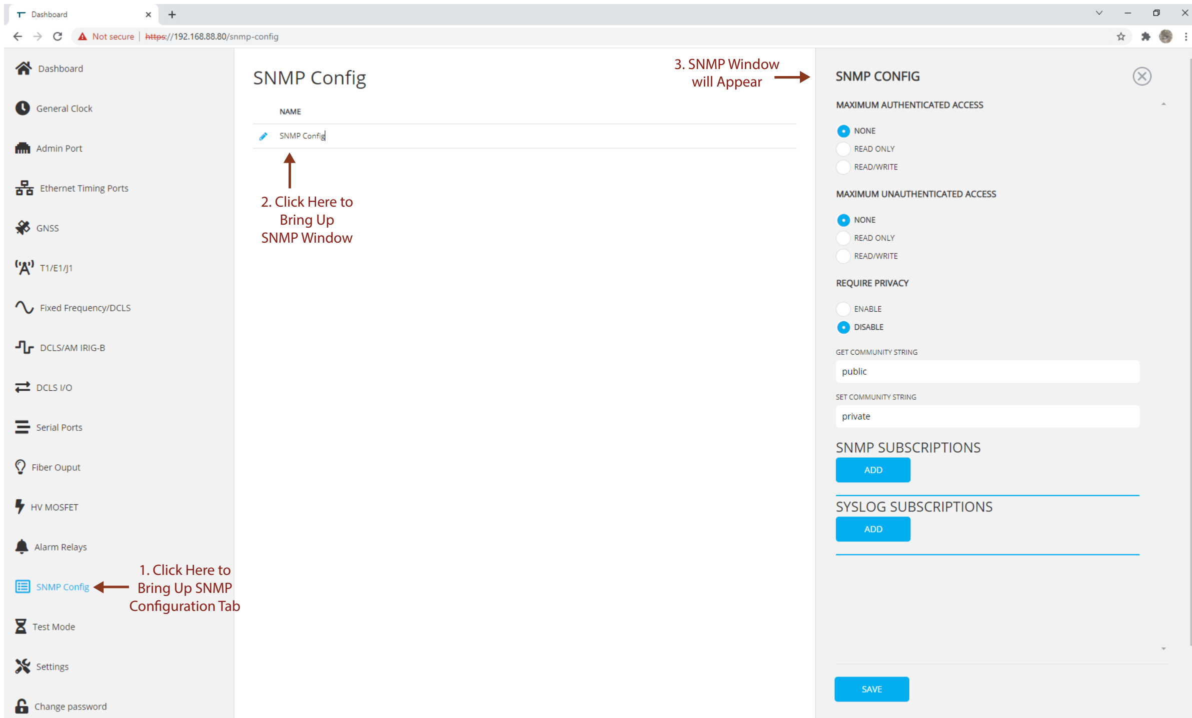
9.13.2 Provisioning Syslog Notifications

This section describes how to provision Syslog notifications.

1. **Navigate to SNMP Config Window**

To navigate to the SNMP configuration window, on the left navigation pane, click **SNMP Config**, and then click the SNMP Config settings bar in the center of the screen. The **SNMP CONFIG** settings window appears on the right pane.

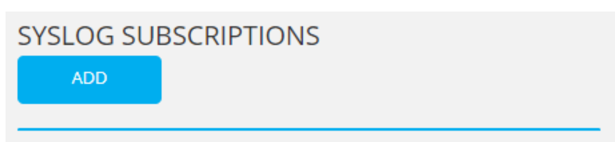
Figure 9-444. SNMP Configuration Window



2. **Add New Syslog Subscription**

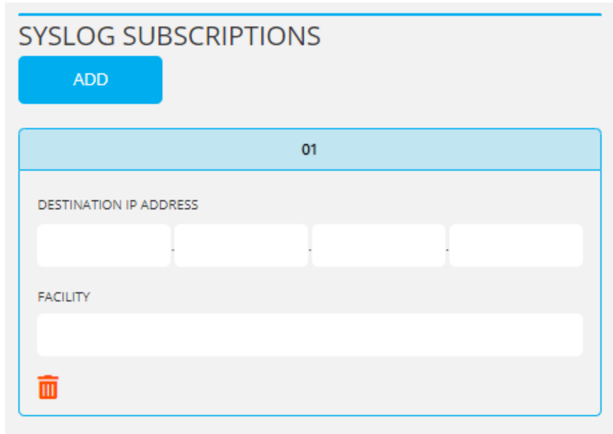
   To add a new SNMP subscription, under **SYSLOG SUBSCRIPTIONS**, click **ADD**.

Figure 9-445. Add New Syslog Subscriptions



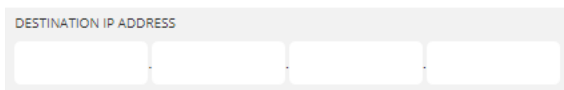
This displays the new Syslog subscription settings.

Figure 9-446. Syslog Subscription Settings



3. **Enter Subscriber's Destination IP Address**
   Enter the IP address of the Syslog subscriber.

   Figure 9-447. Syslog Destination IP Address

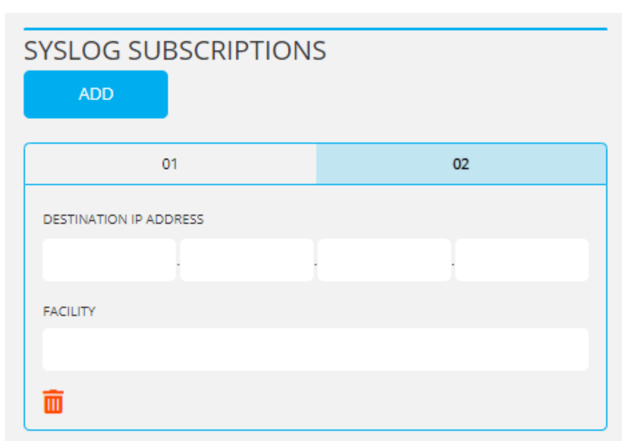
4. **Enter Subscriber's Facility Number**
   This is the setting for the Syslog facility number. It represents the “Local Use” value range 0 to 7 (that is Facility Number range between 16 to 23).

   Enter the facility number of the Syslog subscriber.

   Figure 9-448. Set Syslog Subscriber Facility Number

5. **Repeat Steps 2-4 for Each Additional Subscriber**
   To add another Syslog subscriber, click **ADD** again, and click the **02** tab under the **ADD** button to navigate to the settings for the new Syslog subscriber settings. The **01** tab contains the settings for the subscriber that was previously set up.

   Figure 9-449. Add Multiple Syslog Subscribers

Repeat for as many subscriptions as are present on the network.

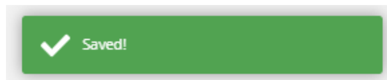
Tip:

To remove a Syslog subscription, click the icon.

6. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.

   A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-450. Successful Save Notification



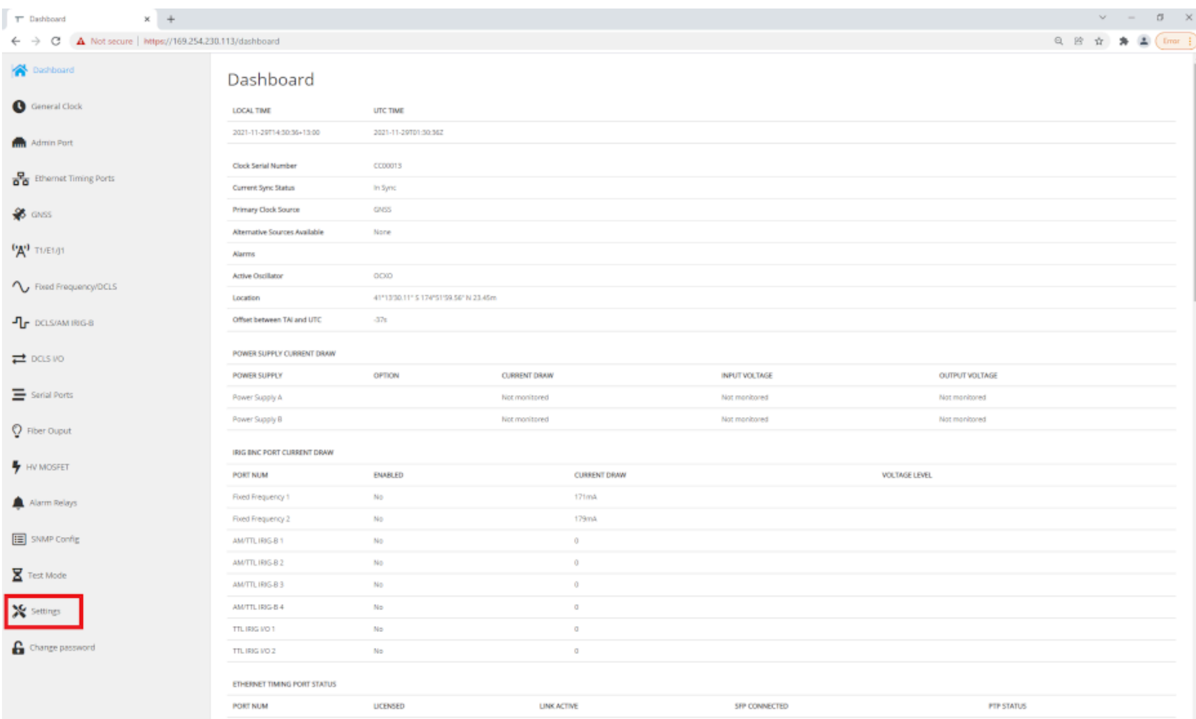
9.13.3 Provisioning SNMP Users

This section describes how to provision SNMPv3 USM users.

Note: Only an 'Administrator' user can configure SNMP Users on the GridTime 3000

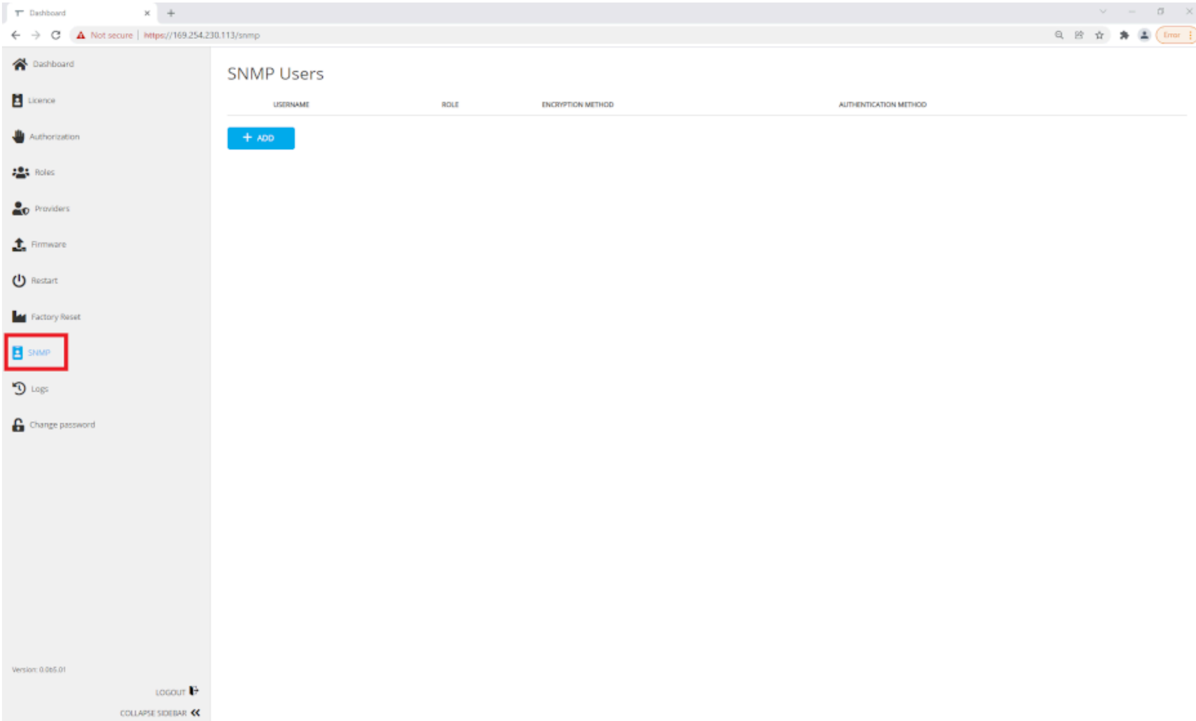
1. **Navigate to SNMP Users Tab**
   To navigate to the SNMP Users window, on the left navigation pane of the Dashboard, click Settings and then click **SNMP Users**.

Figure 9-451. SNMP Users Tab



The SNMP Users Window is displayed.

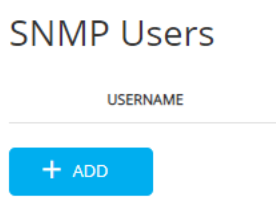
Figure 9-452. SNMP Users Tab



2. **Add User**

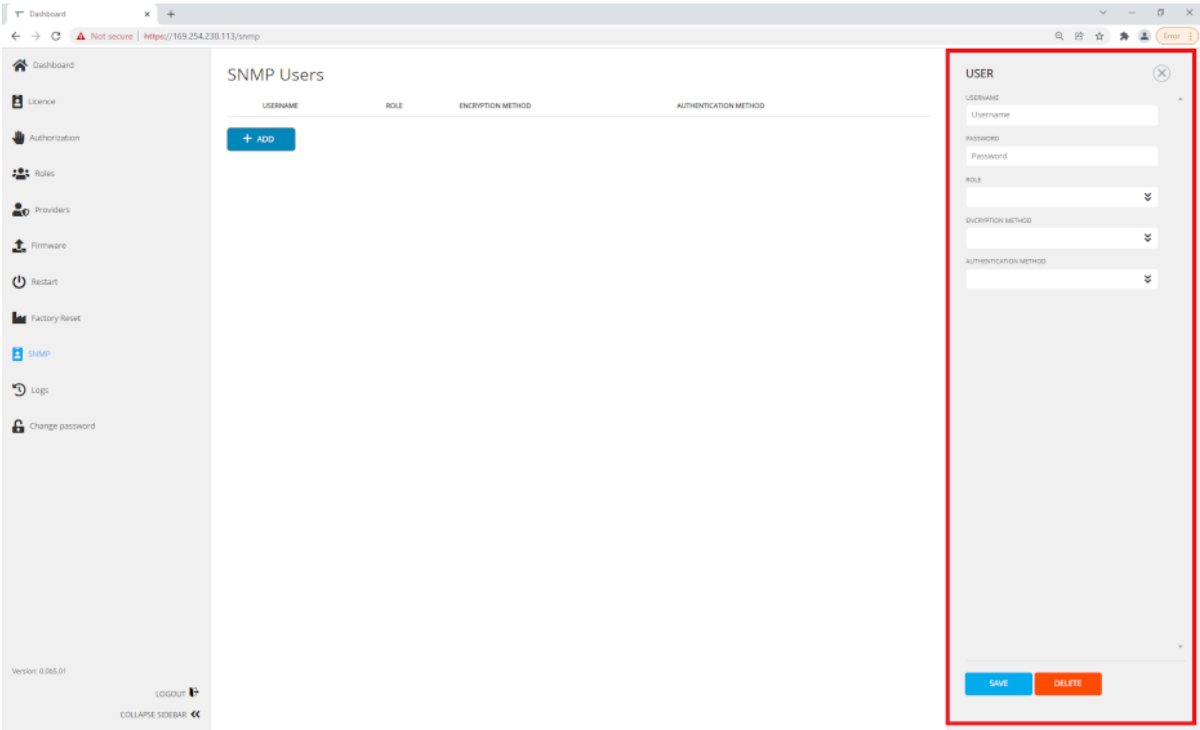
   To add a new SNMP user, click **+ ADD**.

Figure 9-453. Add a New SNMP User



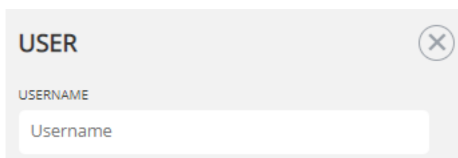
This displays the settings window for the new user on the right pane.

Figure 9-454. Configure User Settings



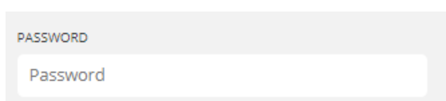
3. **Enter Username**
   Enter the SNMPv3 USM username for the new user.

Figure 9-455. Set Username



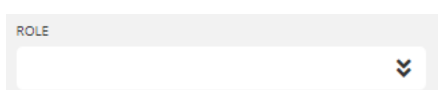
4. **Enter Password**
   Enter the SNMPv3 USM password for the new user.

Figure 9-456. Set Password



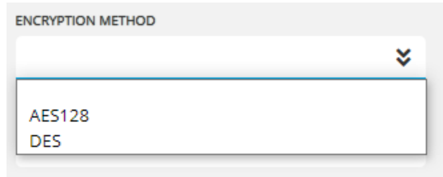
5. **Select Role**
   From the **ROLE** drop-down list, select the mapped user role. Read the Provisioning Roles section before proceeding with this step.

Figure 9-457. Set Role for the New User



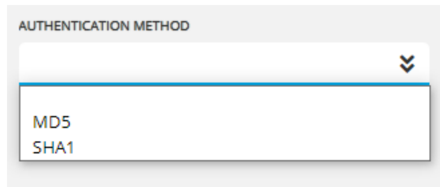
6. **Select Encryption Method**
   From the ENCRYPTION METHOD drop-down list, select the encryption type to be used.

Figure 9-458. Set the Encryption Method



7. **Select Authentication Method**
   From the **AUTHENTICATION METHOD** drop-down list, select the authentication method to be used.

   Figure 9-459. Set the Authentication Method



8. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.

   A **Saved!** notification appears on the bottom right corner of the page, indicating that the settings have successfully been written to the GridTime 3000.

   Figure 9-460. Successful Save Notification

9.14 Provisioning Users

9.14.1 Provisioning Users - Local Users

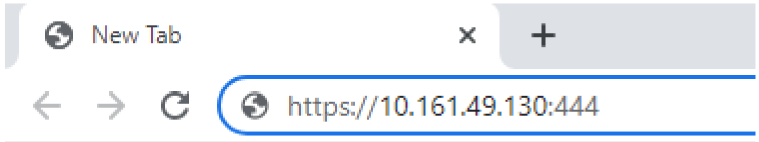
This section describes how to provision users for the GridTime 3000 when using the default basic provider.

Note: By default, GridTime 3000 only allows the 'Administrator' role to have read and write access to all settings and advanced configuration menus. To set up additional roles, follow the instructions in Provisioning Roles.
By default, it also has a single Administrator user with the Administrator role mapped to it. The username for the Administrator user is 'Administrator', and the password will be what was entered during the first time login to CMT.

Important: Only a user with the role of 'Administrator' can provision users on the GridTime 3000.

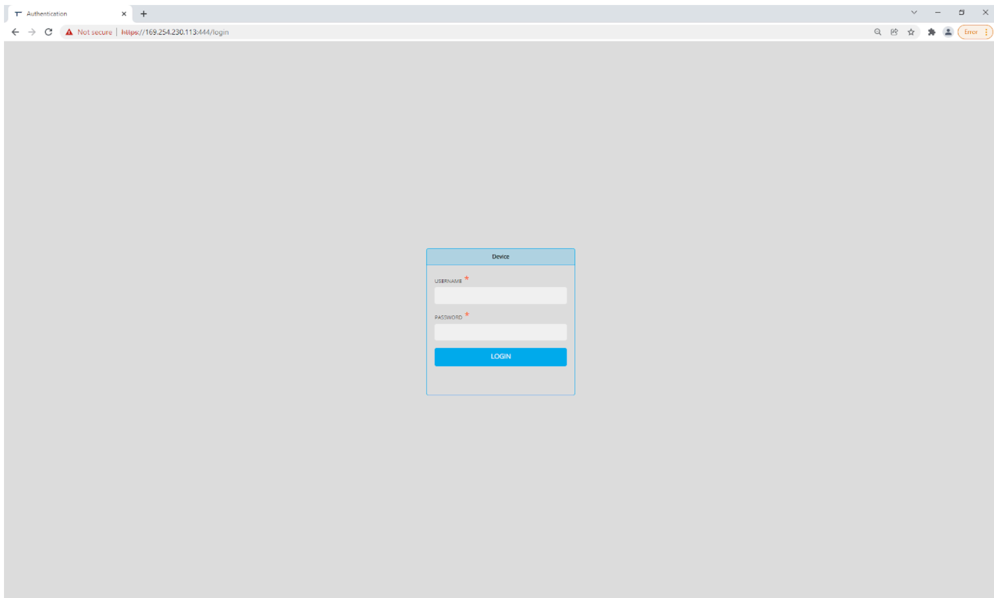
1. To navigate to the CMT authentication module, in your browser’s address bar, type the IP address you normally use to access the CMT and then add **:444** to the end of the address.

Figure 9-461. Log Into CMT Authentication Module



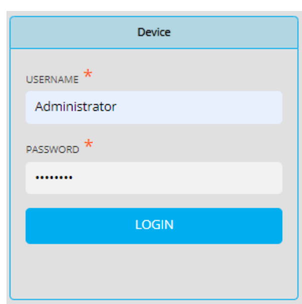
The authentication module login screen is displayed.

Figure 9-462. CMT Authentication Module Login Screen



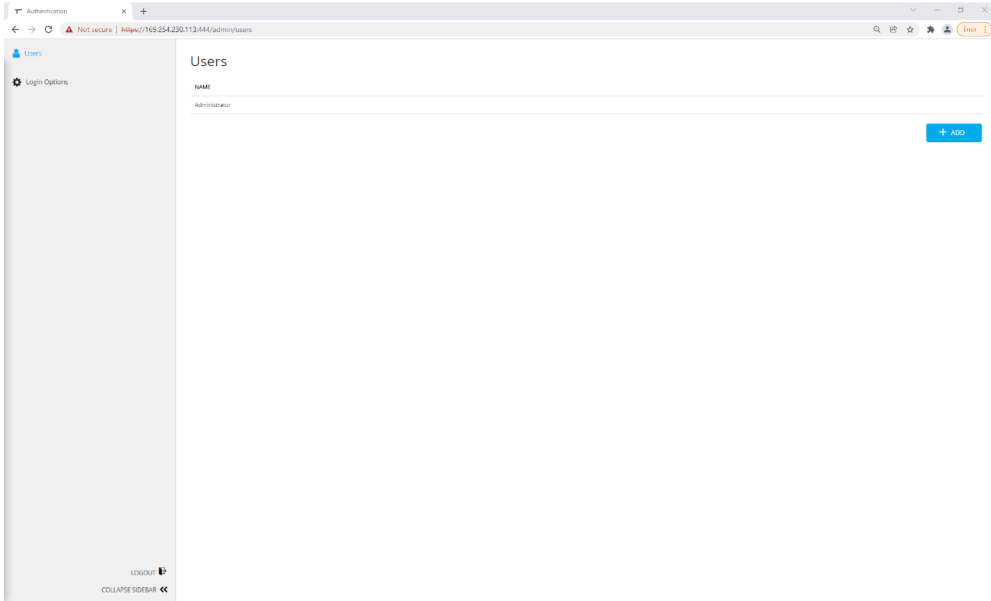
2. Enter the Administrator user login details and click **LOGIN**.

Figure 9-463. Logging In



Upon successful authentication, the **Users** tab of the authentication module is displayed.

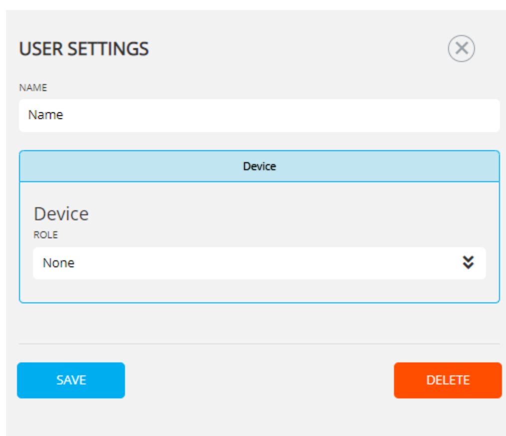
Figure 9-464. Authentication Module Users Tab



Note: Unless previously modified, only the 'Administrator' user should be present as per the GridTime 3000's default settings.

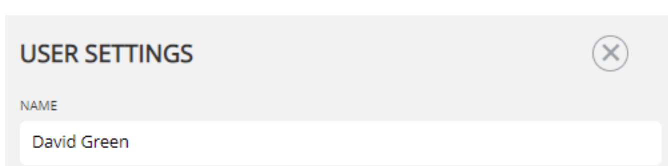
3. To add a new user, click the **+ADD** button. The **USER SETTINGS** window appears on the right pane.

Figure 9-465. User Settings Window



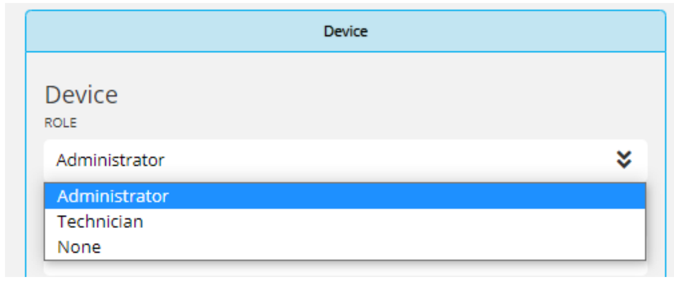
4. **Enter Name**
   Type the Name of the user into the **NAME** text box.
   Note: This is not the username used by the user during login, this is simply a name used to identify the user in the Users Configuration Module.

Figure 9-466. Example- Username Setting



5. **Select Role Mapped to User**
   From the **ROLE** drop-down list, select the role mapped to the user. If the role still needs to be set up, see Provisioning Roles.

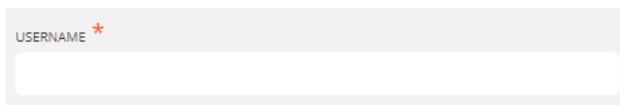
Figure 9-467. Map the User With Role



   This reveals additional user settings.

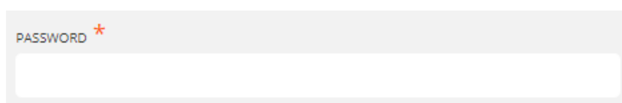
6. **Enter Username**
   Enter the login username in the **USERNAME*** text box.

Figure 9-468. Enter Username



7. **Enter Password**
   Enter the login password for the user in the **PASSWORD** text box.

Figure 9-469. Enter Password



   Note: FAILED ATTEMPTS and **LOCK OUT UNTIL** settings are available in the Clock Management Tool, but do not have any effect on the configured user.

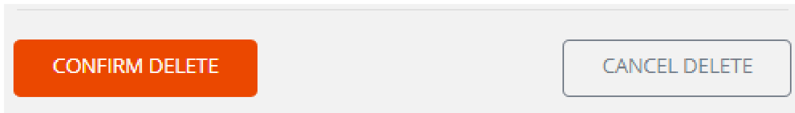
8. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**. A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

Figure 9-470. Settings Saved Notification

9. **Repeat Across All Required Users**
   Repeat the steps above until all required users are added.

Note: To delete a user, bring up the user settings using steps 1, 2 and 3, and click **DELETE**. You will then be prompted to either confirm or cancel the deletion.

Figure 9-471. Confirm Deletion



Note: The login username, password, and other details for the default 'Administrator' user can be changed, but the user cannot be deleted.

9.14.2 Provisioning Users - RADIUS

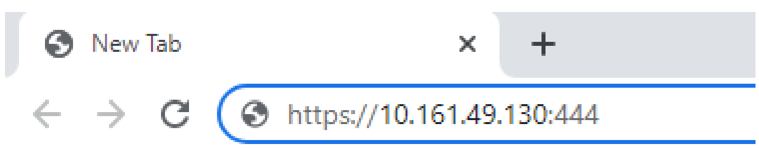
This section describes how to provision users for the GridTime 3000 when using RADIUS.

Note: By default, The GridTime 3000 only allows the 'Administrator' role to have read and write access to all settings and advanced configuration menus. Follow the instructions in Provisioning Roles to set up additional roles.
By default, it also has a single Administrator user with the Administrator role mapped to it. The username for the Administrator user is 'Administrator', and the password will be what was entered during the first time login to CMT.

Important: Only a user with the role of 'Administrator' can provision users on the GridTime 3000.

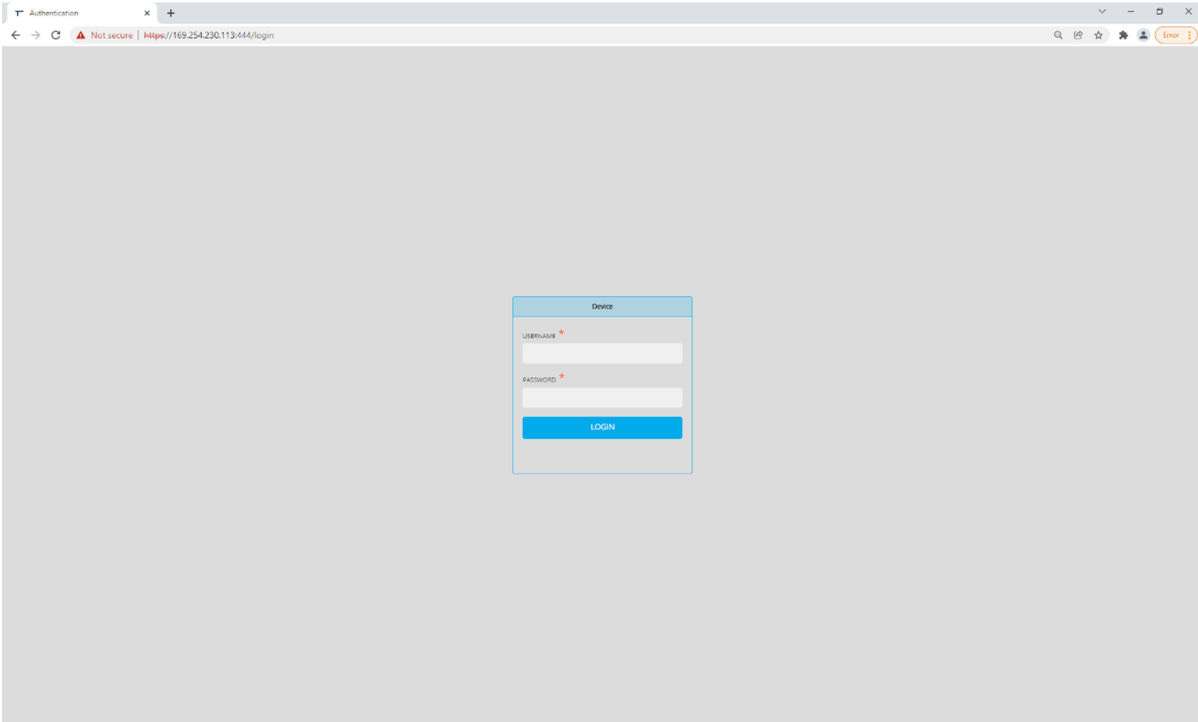
1. To navigate to the CMT authentication module, in your browser's address bar, type the IP address you normally use to access the CMT and then add **:444** to the end of the address.

Figure 9-472. Log into CMT Authentication Module



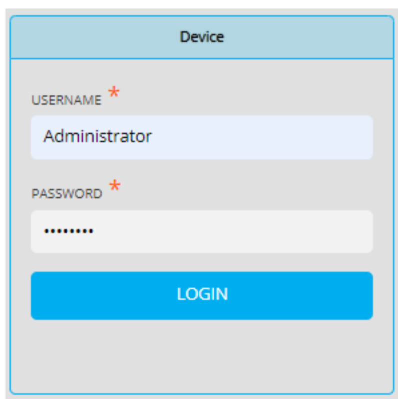
The authentication module login screen is displayed.

Figure 9-473. CMT Authentication Module Login Screen



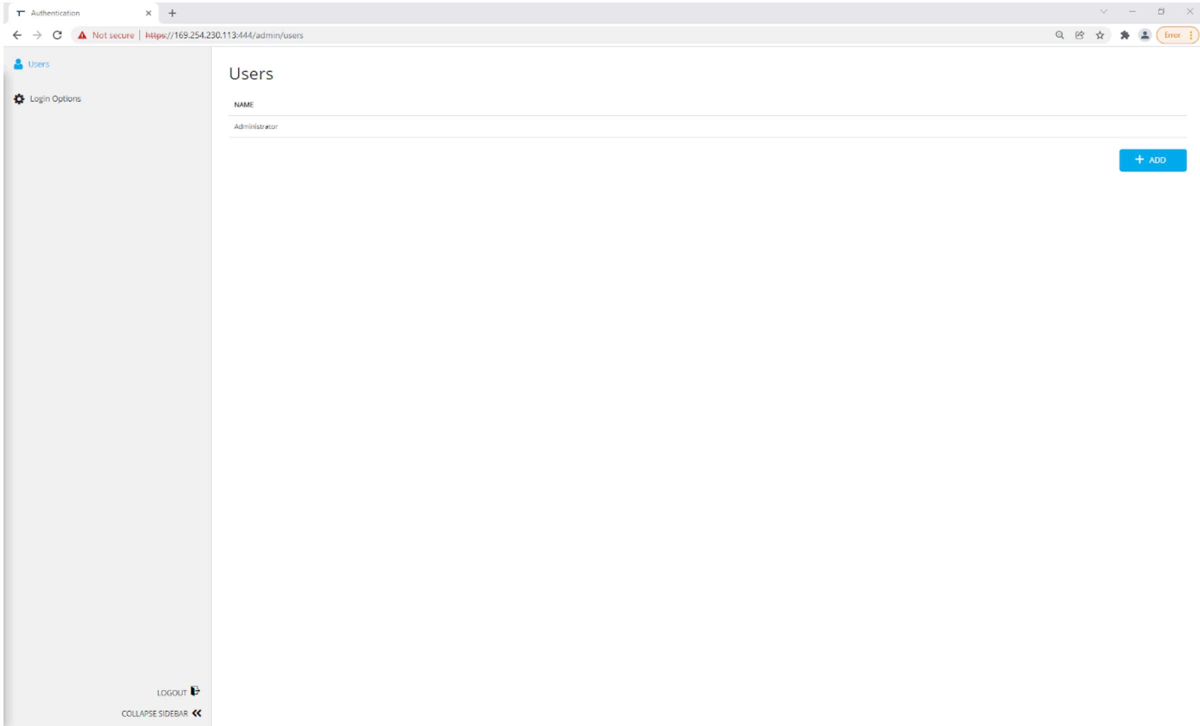
2. Enter the Administrator user login details and click **LOGIN**.

Figure 9-474. Logging In



Upon successful authentication, the **Users** tab of the authentication module is displayed.

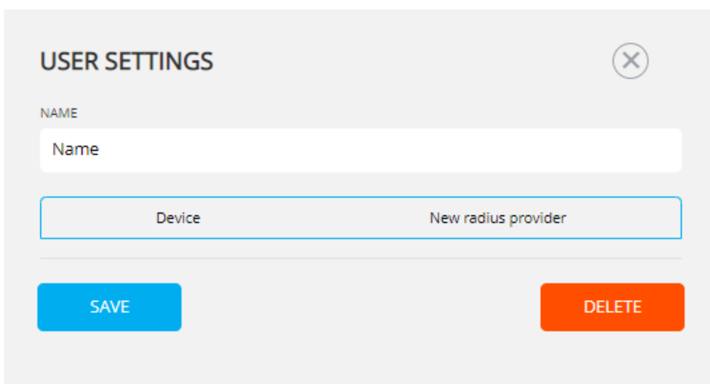
Figure 9-475. Authentication Module-Users Tab



Note: Unless previously modified, only the 'Administrator' user should be present as per the GridTime 3000's default settings.

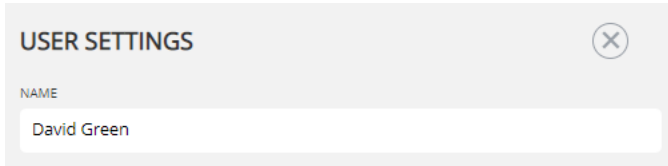
3. To add a new RADIUS user, click **+ADD**. The user settings window is displayed on the right pane.

Figure 9-476. User Settings Window



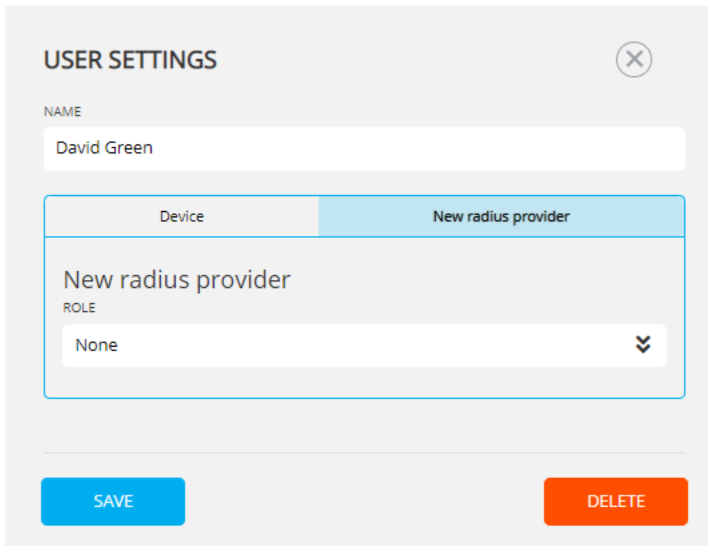
4. **Enter Name**
   Type a name for the user in the **NAME** text box.
   Note: This is not the username used by the user during login; this is simply a name used to identify the user in the Users Configuration Module.

Figure 9-477. Example User Name Entry



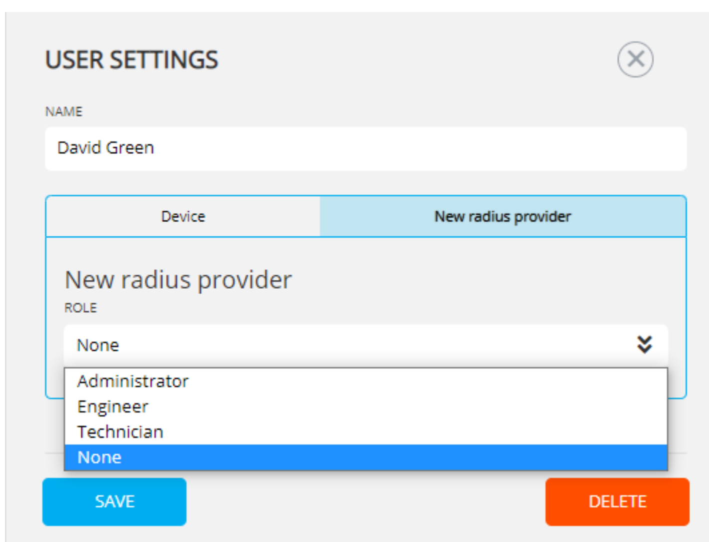
5. **Select Device Provider**
   Select the RADIUS provider (server) that the user belongs to. If the RADIUS provider needs to be set up, see Provisioning RADIUS.

Figure 9-478. New RADIUS User Configuration



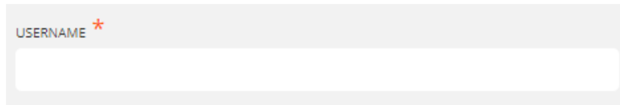
6. **Select Role Mapped to User**
   Select the role mapped to the user from the **ROLE** drop-down list. This displays additional user settings.
   If the role still needs to be set up, see Provisioning Roles.

Figure 9-479. Set User Role



7. **Enter Username**
   Enter the login user name used by the user into the **USERNAME** field.

   Figure 9-480. Enter Username

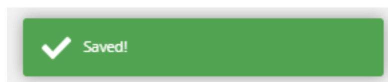
   

   Note: This username must match the username of the user on the RADIUS server.

8. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.

   A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

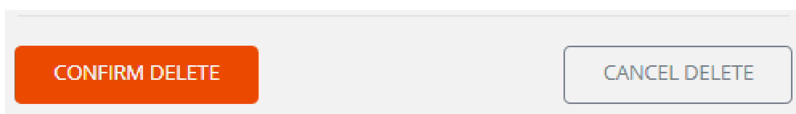
   Figure 9-481. Settings Saved Notification

9. **Repeat Across All Required Users**
   Repeat the steps above until all required users are added.

   Note: To delete a user, bring up the user settings using steps 1, 2 and 3, and click **DELETE**. You will then be prompted to either confirm or cancel the deletion.

   Figure 9-482. Confirm Deletion

   Note: The login username, password, and other details for the default 'Administrator' user can be changed, but the user cannot be deleted.

9.14.3 Provisioning Users - LDAP

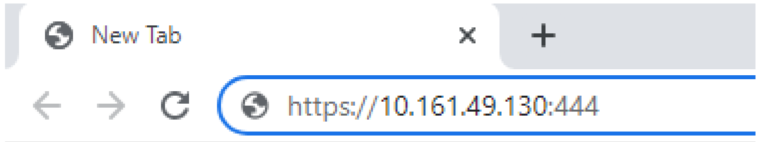
This section describes how to provision users for the GridTime 3000 when using LDAP.

Note: By default, GridTime 3000 only allows the 'Administrator' role to have read and write access to all settings and advanced configuration menus. To set up additional roles, follow the instructions in Provisioning Roles.
By default, it also has a single Administrator user with the Administrator role mapped to it. The username for the Administrator user is 'Administrator', and the password will be what was entered during the first time login to CMT.

Important: Only a user with the role of 'Administrator' can provision users on the GridTime 3000.

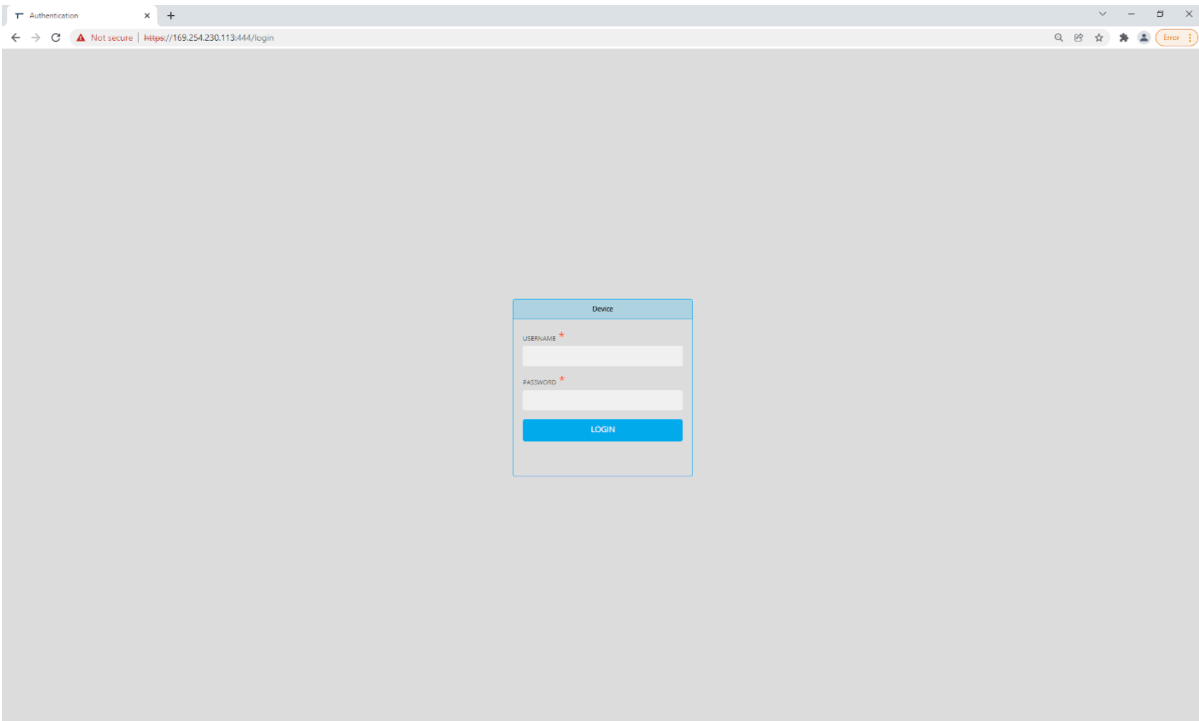
1. To navigate to the CMT authentication module, in your browser's address bar, type the IP address you normally use to access the CMT and then add **:444** to the end of the address.

Figure 9-483. CMT Authentication Module



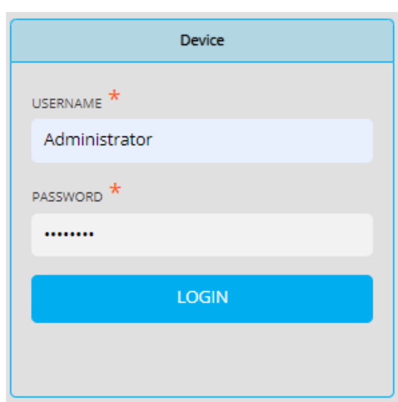
This brings up a new login screen for the authentication module.

Figure 9-484. CMT Authentication Module Login Screen



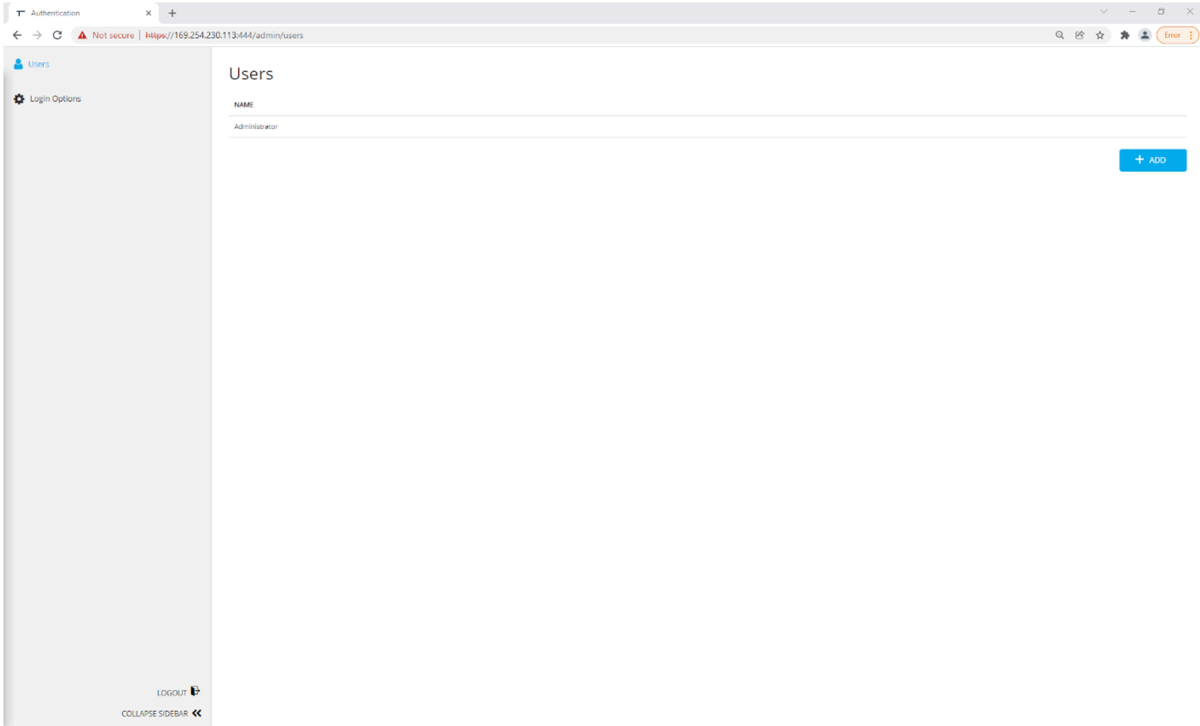
2. Enter the Administrator user login details and click **LOGIN**

Figure 9-485. Logging In



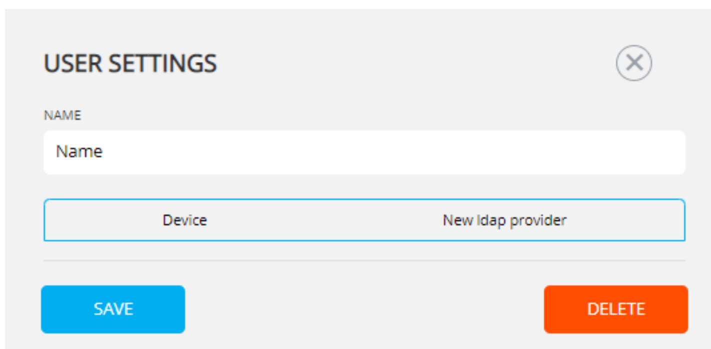
Upon successful authentication, the **Users** tab of the authentication module is displayed.

Figure 9-486. Authentication Module-Users Tab



Unless previously modified, only the 'Administrator' user should be present as per the GridTime 3000's default settings.

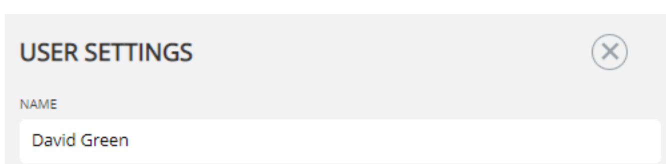
3. To add a new user, click **+ADD**. This displays the user settings window on the right pane.



4. **Enter Name**

   Type the name of the user in the **NAME** text box.
   Note: This is not the username used by the user during login, this is simply a name used to identify the user in the Users Configuration Module.

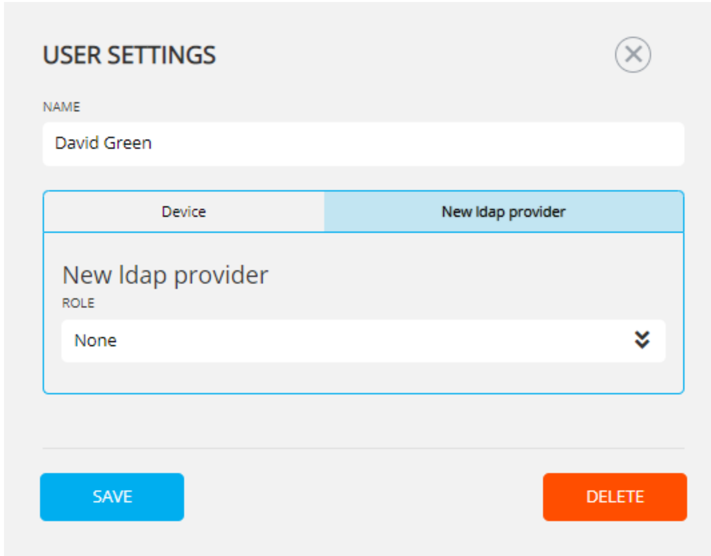
Figure 9-487. Example User Name Entry



5. **Select Device Provider**

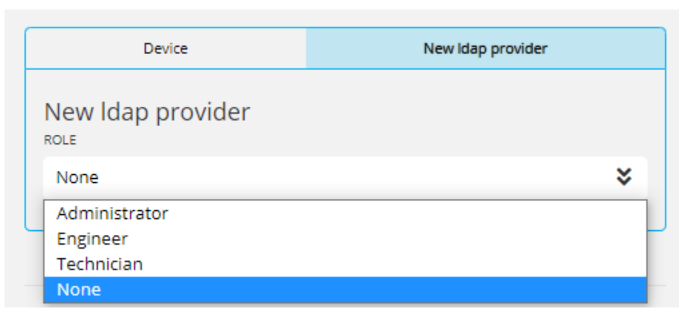
Select the LDAP provider (server) that the user belongs to. If the LDAP provider needs to be set up, see Provisioning LDAP.

Figure 9-488. New LDAP User Configuration



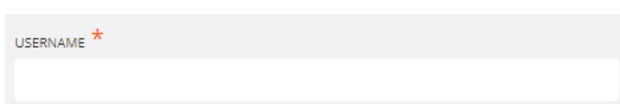
6. **Select Role Mapped to User**
   Select the role mapped to the user from the **ROLE** drop-down list. This displays additional user settings.
   If the role still needs to be set up, see Provisioning Roles.

Figure 9-489. Set User Role



7. **Enter Username**
   Enter the login user name used by the user into the **USERNAME** field.

Figure 9-490. Enter Username



Note: This username must match the username of the user on the LDAP server.

8. **Save Settings**
   To write the settings to the GridTime 3000, click **SAVE**.
   A **Saved!** notification appears in the bottom right corner of the page indicating that the settings have successfully been written to the GridTime 3000.

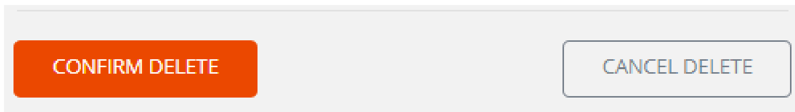
Figure 9-491. Settings Saved Notification

9. **Repeat Across All Required Users**

   Repeat the steps above until all required users are added.

   Note: To delete a user, bring up the user settings using steps 1, 2 and 3, and click **DELETE**. You will then be prompted to either confirm or cancel the deletion.

Figure 9-492. Confirm Deletion



Note: The login username, password, and other details for the default 'Administrator' user can be changed, but the user cannot be deleted.

9.15 Provisioning Logs

These logs provide a comprehensive overview of system activities, and are essential for troubleshooting, maintaining security, and ensuring the smooth operation of the system. The format for these logs follow the recommendations outlined in RFC-5424, with optional encryption.

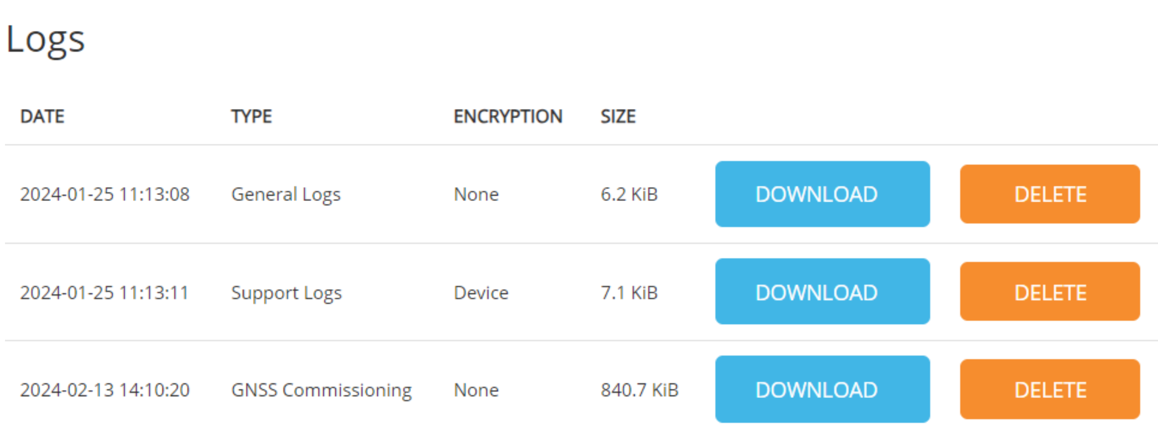
Logs are categorized as :

- General Logs
- Support Logs
- GNSS Commissioning Logs

Once the logs are generated, the user can download the logs. The user will be able to see the logs file ready to download on the front panel screen of the device.

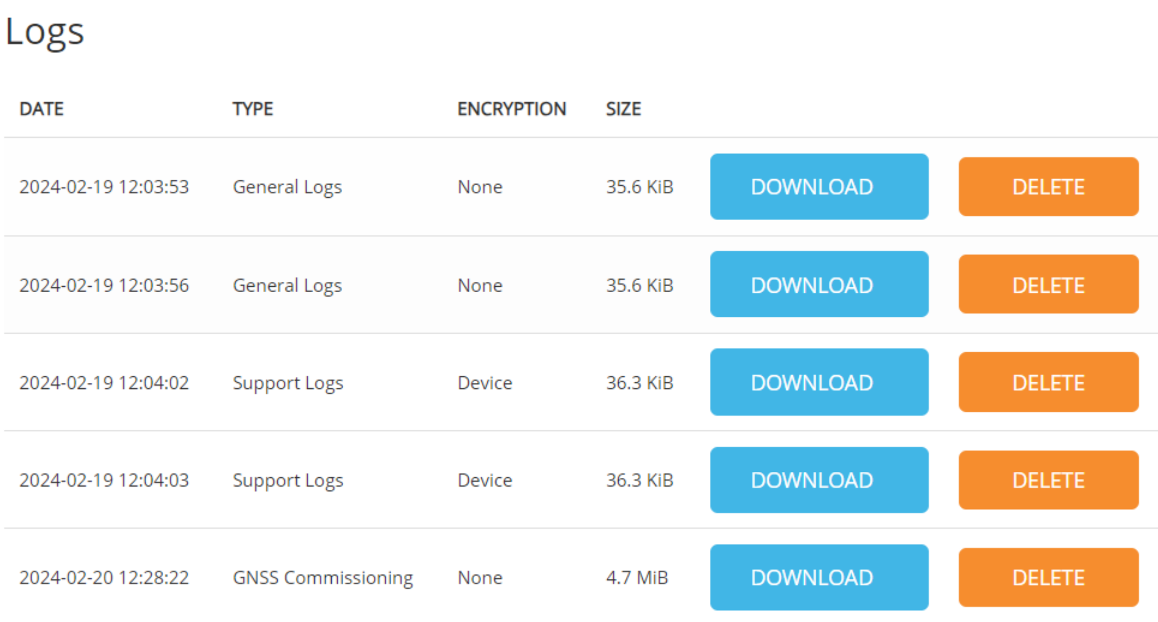
- To download the logs file, click **DOWNLOAD**.
- To delete the logs file, click **DELETE**.

Figure 9-493. Log Files Window



User can generate multiple log files with the same or different types of logs, as shown in the following figure.

Figure 9-494. Generating Multiple Log Files


Logs

DATE	TYPE	ENCRYPTION	SIZE		
2024-02-19 12:03:53	General Logs	None	35.6 KiB	DOWNLOAD	DELETE
2024-02-19 12:03:56	General Logs	None	35.6 KiB	DOWNLOAD	DELETE
2024-02-19 12:04:02	Support Logs	Device	36.3 KiB	DOWNLOAD	DELETE
2024-02-19 12:04:03	Support Logs	Device	36.3 KiB	DOWNLOAD	DELETE
2024-02-20 12:28:22	GNSS Commissioning	None	4.7 MiB	DOWNLOAD	DELETE

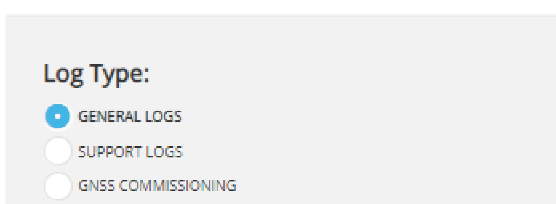
Notes:
1. The ability to Download all **Logging** functionalities are restricted to Administrator users only.
2. Logs can survive power cycle and firmware upgrade.
3. Logs can be wiped off by performing the factory reset on GridTime 3000.
4. This process manages the logs, keeping a maximum of 40 files. Each day, the current log is copied to a new file and then reset. If more than 40 copies exist, the oldest ones are deleted as long as the clock is turned on at least once per day and allowed to sync, so it knows the day has changed.

9.15.1 Provisioning General Logs

General logs encompass a variety of log events organized into distinct high-level categories such as Alarms, Configuration Changes, Logger Events, System, Licensing, Authentication, Time of Day, Network, and Pulse. Upon retrieval, the log file is downloaded as a compressed zip file (`.ezp` format) to either the default download folder or the location specified in the browser settings.

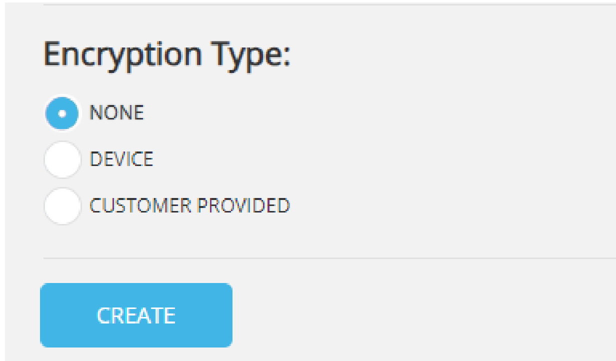
1. On the left navigation pane of the Dashboard screen, select **Settings > Logs**. The Logs configuration window is displayed.
2. On the right pane, under the **Log Type**, select the **GENERAL LOGS** radio button.

Figure 9-495. Selecting the Log Type



3. On the right pane, under the **Encryption Type**, select an option.

Figure 9-496. Select the Encryption Type



- By default, it is set to **NONE**, meaning no encryption logs file.
- If the encryption type is set to **DEVICE**, the system logs file undergoes encryption using Microchip provided public key.
  Note: Microchip private key is required to decrypt the system logs file.
- If the encryption type is **CUSTOMER PROVIDED**, the system logs file undergoes encryption using Microchip provided public key and private key provided by the customer.

  Note: A Microchip private key and customer provided public key is required to decode the system logs file.

4. To generate the log file, click **CREATE**.
5. A **Saved!** notification appears on the bottom right corner of the page indicating that the configuration settings are successfully written to the GridTime 3000.

Figure 9-497. Successful Save Notification

Note: To understand the role of **Encryption**, **Public key**, and **Private Key**, see Functions of Encryption, Public Key and Private Key .

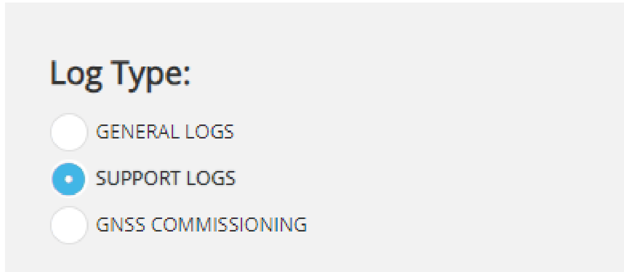
Note: A list of all log events and trigger conditions can be found here:

9.15.2 Provisioning Support Logs

Support logs encompass a variety of log events organized into distinct high-level categories such as Alarms, Configuration Changes, Logger Events, System, Licensing, Authentication, Time of Day, Network, and Pulse. Support logs, with finer diagnostic details, are exclusively for customer support, not accessible to users, addressing cases needing extensive system diagnostics alongside General logs entries.. Upon retrieval, the log file is downloaded as a compressed zip file (`.ezp` format) to either the default download folder or the location specified in the browser settings.

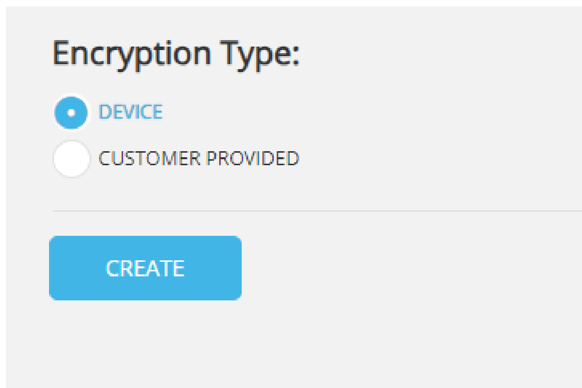
1. On the left navigation pane of the Dashboard screen, select **Settings > Logs**. The Logs configuration window is displayed.
2. On the right pane, under the **Log Type**, select the **SUPPORT LOGS** radio button.

Figure 9-498. Selecting the Log Type



3. On the right pane, under the **Encryption Type**, select an option.

Figure 9-499. Select the Encryption Type



   – If the encryption type is set to **DEVICE**, the system logs file undergoes encryption using Microchip provided public key.
   – If the encryption type is **CUSTOMER PROVIDED**, the system logs file undergoes encryption using Microchip provided public key and private key provided by the customer.

   Note: A Microchip private key and a customer provided public key is required to decode the support logs file.
4. To generate the log file, click **CREATE**.
5. A **Saved!** notification appears on the bottom right corner of the page indicating that the configuration settings are successfully written to the GridTime 3000.

Figure 9-500. Successful Save Notification

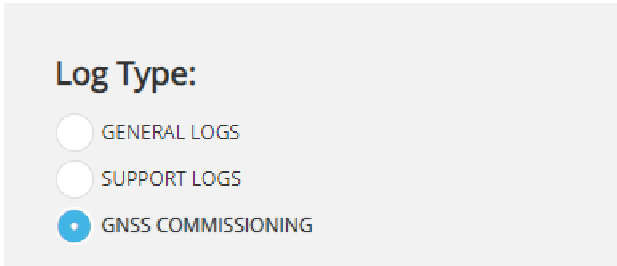
Note: To understand the role of **Encryption**, **Public key**, and **Private Key**, see Functions of Encryption, Public Key and Private Key .

9.15.3 Provisioning GNSS Commissioning Logs

GNSS commissioning logs provide a comprehensive record, capturing a snapshot of the GNSS subsystem every second. Each entry details the receiver's state, time of day, and location, while also offering metadata for every tracked satellite in the constellation, including altitude, latitude, longitude, signal strength, azimuth, and elevation angles. This continuous 24-hour log facilitates the identification of visibility gaps and potential antenna location issues within the system.

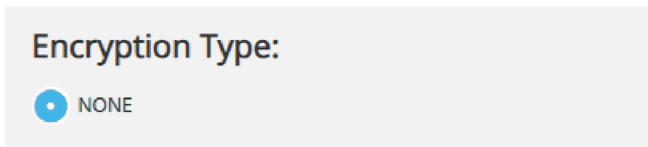
1. On the left navigation pane of the Dashboard screen, select **Settings > Logs**. The Logs configuration window is displayed.
2. On the right pane, under the **Log Type**, select the **GNSS COMMISSIONING** radio button.

Figure 9-501. Selecting the Log Type



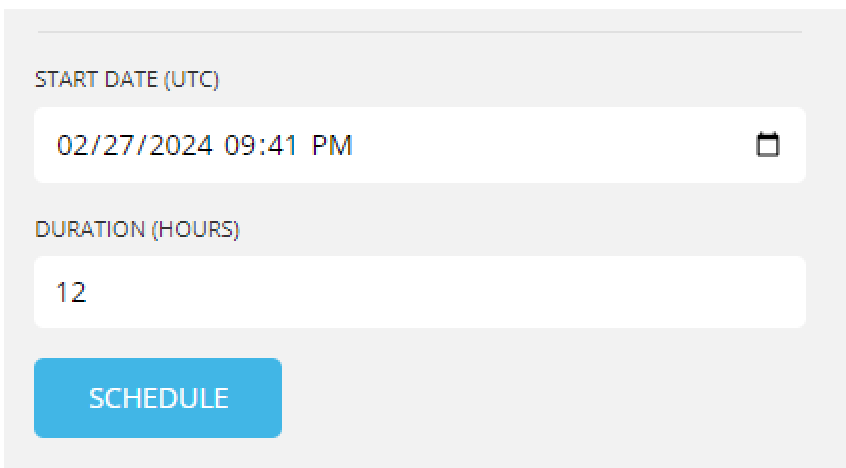
3. Select the **Encryption Type**. No encryption is available for GNSS Commissioning logs.

Figure 9-502. Selecting the Encryption Type



4. Select the **START DATE (UTC)**.

Figure 9-503. Setting the Start Date and Duration



Note: The displayed time is in UTC, you will need to convert your local time into UTC time when scheduling this in the future.

5. The specified time duration is in 12- hour format.
6. Click **SCHEDULE** to start.
7. A **Saved!** notification appears in the bottom right corner of the page indicating that the configuration settings are successfully written to GridTime 3000.

Figure 9-504. Successful Save Notification

The user can click **CANCEL** to cancel the logs before they get scheduled to download.

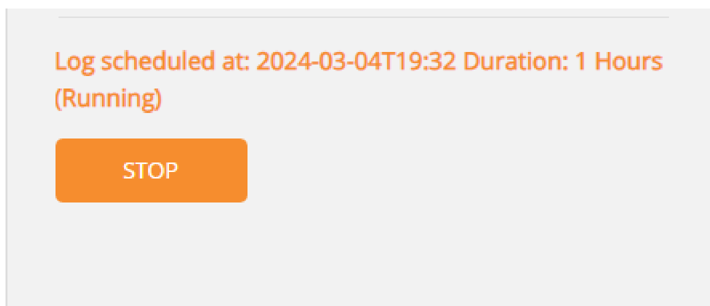
Figure 9-505. Canceling the Log Downloads

Upon reaching the scheduled time, the screen displays the scheduled date and time in the 24-hour format with total duration set for log capture, accompanied by a status indication stating that the process is currently running.

After completion of the specified time duration for log capture, the log file will automatically be presented on the front panel for the user to either download or delete, as outlined in the Provisioning Logs section.

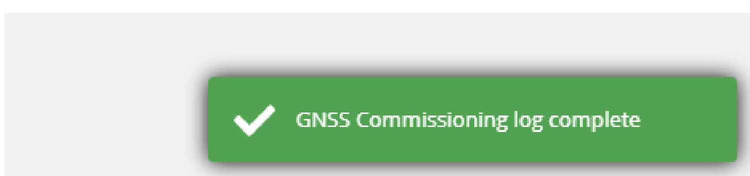
The user has the option to forcefully stop the log capture process by terminating it manually. Upon activating the force stop button, the log file will capture data until the moment the force stop button is clicked.

Figure 9-506. Stopping the Log Capture



8. A **GNSS Commissioning log complete** notification appears in the bottom right corner of the page indicating that the GNSS commissioning logs file has been successfully completed and ready for download..

Figure 9-507. GNSS Commissioning Log Completion Notification



Note: To understand the role of **Public** and **Private key**, see Functions of Encryption, Public Key and Private Key

9.16 Provisioning Certificate

A certificate is a special file that binds identity information to a public key using a digital signature and is used to establish secure connections through TLS. Trusted Certificate Authorities (CA) digitally sign certificates to prevent crafting or modification of the certificates and browsers trust certificates signed by pre-loaded CAs like VeriSign, Comodo, and GoDaddy. The GridTime 3000 uses a self-signed certificate by default, leading to security warnings, but users can upload their own trusted certificates for secure, warning-free connections within their networks. This allows organizations to use their own private keys and act as their own CA, ensuring control over their encryption and certificate trust.

Certificate and Key File Requirements

To ensure secure communications, the GridTime 3000 requires the use of specific certificate and key files, which must be generated using OpenSSL. The device's web interface (CMT) is accessible through a secure HTTPS connection, hosted by an nginx web server using TLSv1.2 encryption. Consequently, the certificates and keys must comply with TLSv1.2 requirements.

Requirements:

1. Format and Bit Length:
    a. Must use RSA format
    b. Minimum key length: 2048 bits (>= 2048)
2. Digital Signature Hashing Algorithms:
    a. **SHA-2**: SHA-224, SHA-256, SHA-384, SHA-512, SHA512-224, SHA512-256
    b. **SHA-3**: SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256

Note: Users can upload a certificate that passes validation, but does not meet TLSv1.2 requirements. If this happens, the user will be locked out of the GridTime 3000 after restarting.

9.16.1 Generating a Key and a Self-Signed Certificate

Generate the Key

1. Run OpenSSL through the command line
    a. If using Windows®, users can use a tool like GitBash or Windows Subsystem for Linux (WSL).
2. To store or save the certificate and key files, navigate to the desired folder location using the following command.`cd 'C:/Users/Documents/Certificates'`
3. To generate a key, enter the following command. Upon pressing the enter key, the key file will be automatically created at the specified file path `openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 > myprivatekey.key`
    Note: The command below generates a private key using RSA with a key size of 2048 bits

Note: The sections highlighted in bold in the key generation command can be modified:`openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:`**2048** > **myprivatekey.key**

Generate the Certificate

1. Run OpenSSL through a command line
    a. If using Windows, user can use tools like GitBash or Windows Subsystem for Linux (WSL).
2. To store or save the certificate and key files, navigate to the desired folder location using the following command.`cd 'C:/Users/Documents/Certificates'`
3. To generate a certificate using a specific hashing algorithm,enter the following command and then press enter:`openssl req -new -x509 -nodes -sha256 -days 365 -key 'myprivatekey.key' -out 'mycert.crt'`
4. Press the Enter key to continue past the prompts (as displayed in the image below).

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

5. Once all the questions are asked, the key file is created automatically in the specified file path.

Note: For the certificate generation command, the bolded sections are user input fields:
`openssl req -new -x509 -nodes -`**<hash_alg>** `-days` **<num>** `-key` '**<key_filename>**' `-out` '**<cert_filename>**'

- hash_alg = sha224, sha256, sha3-224, sha3-256, sha3-384, sha3-512, sha384, sha512, sha512-224, sha12-256, shak3128, shake256
- num = Number of days for the certificate to be valid for
- key_filename = Name of key file, for example, myprivatekey.key
- cert_filename = Name of cert file, for example, mycert.crt

View certificate

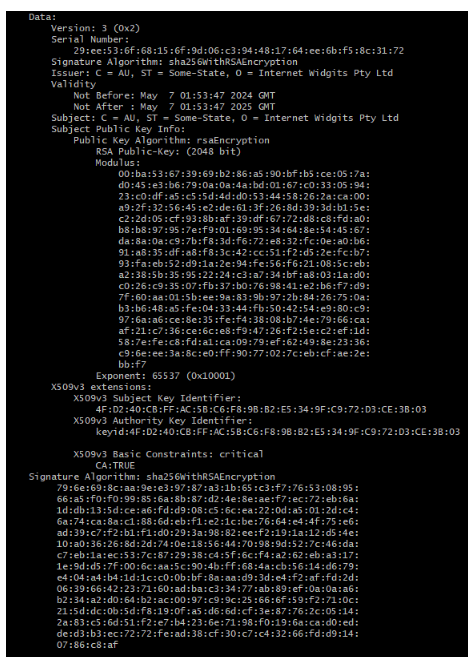
Once the certificate has been successfully generated, it can be viewed in OpenSSL. Enter the following command to view the certificate:

`openssl x509 -in` **<cert_filename>** `-text -noout`

- cert_filename = Name of cert file, for example `mycert.crt`

The certificate should appear as shown in the following image:

Figure 9-508. Sample Certificate



9.16.2 Loading and Applying the Certificate

The process described in the following section can be used to upload new custom certificates .

1. On the **Certificate** page, click **Choose File**, then select the generated key file, and upload it to the device. The **KEY FILE** indicator will highlight to confirm the file has been successfully loaded.

Figure 9-509. KEY FILE Indicator

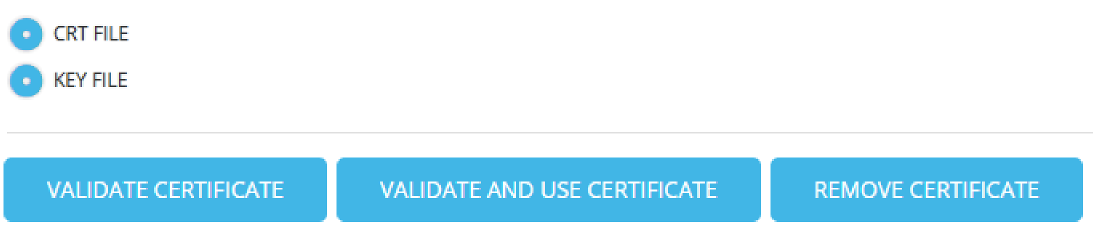
2. On the **Certificate** page, click **Choose File**, then select the generated key file, and upload it to the device. The **CRT FILE** indicator will highlight to confirm the file has been successfully loaded.

Figure 9-510. CRT File Indicator

3. Click **VALIDATE CERTIFICATE** to ensure that the certificate and key files uploaded to the clock are valid.
   Note: The key and certificate files must be generated together. (that is they must match). This validation step will not apply the new certificate to the device.
4. Click **VALIDATE AND USE CERTIFICATE** to verify the validity of the certificate and key files uploaded to the device.
   Note: The certificate will not be applied until the device is restarted. You can restart the device using any restart mechanism, such as the front panel, CMT, or a physical power cycle.

   Note: To view the Validate and Validate and Use buttons, both a valid certificate and a valid key file must be uploaded to the device. Additionally, the device must be restarted for the certificate to be applied.

Figure 9-511. Validate Certificate Options



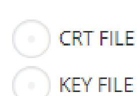
9.16.3 Change and Reset the Certificate

Change the certificate

There are two options to change the certificate:

1. To clear the CRT and KEY indicators in the CMT, click **Remove Certificate**.

Figure 9-512. CRT and KEY Indicators



2. Follow the file uploading process outlined in the Loading and Applying the Certificate section.

Note: Utilizing this method overwrites the previously loaded files, provided that the **Validate and Use Certificate** button is used.

Reset Certificate

To restore the default certificate, click **Reset to Default Certificate**, and then restart the clock.

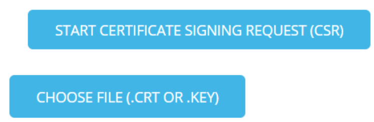
9.16.4 Certificate Signing Request (CSR)

This feature enables the clock to generate its own certificate and private key and then provide the certificate to user as a Certificate Signing Request (CSR). A user can then sign the CSR with a Certificate Authority (CA) certificate and upload it back to the clock. This method is both convenient and secure, as the private key never leaves the clock and cannot be intercepted.

Steps to create Certificate Signing Request (CSR)

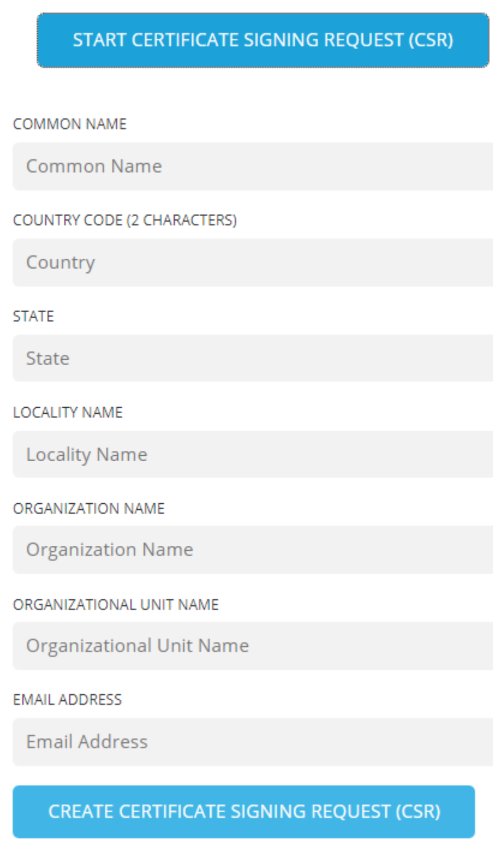
1. On the **Certificate** page, ensure any previous certificate is removed. Once cleared, to proceed further, click **START CERTIFICATE SIGNING REQUEST (CSR)**.

Figure 9-513. Certificate Signing Request



2. A form appears. Fill out the form with the appropriate details. Ensure the country code field contains exactly two characters.

Figure 9-514. Certificate Signing Request Form



3. Click **CREATE CERTIFICATE SIGNING REQUEST (CSR)** button at the bottom of the form.

A certificate signing request appears below the button and appears between the **-----BEGIN CERTIFICATE REQUEST-----** and **-----END CERTIFICATE REQUEST-----** tags.

Figure 9-515. Certificate Signing Request


```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCAboCAQAwgYwxCzAJBgNVBAYTAk5aMRMwEQYDVQQIDApXZWxsaW5ndG9u
MRIwEAYDVQQKDAlNSWNyb2NoaXAxEjAQBgNVBAcMCUxvd2VyaHV0dDEOMAwGA1UE
AwwFQ2FsYW0xETAPBgNVBAsMCE5aaW50MTIzMR0wGwYJKoZIhvcNAQkBFg4xMjM0
QGdtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK9c1PGz
0sIFXTAef23YXA16aOOq2LrakodEngvomYd6sGDtIL4/F2DdsQshd+9x+CxrLXIz
98NzXkI/n75aUmP9zDKBa/CjfWKFJ4szD5JHT03ZBA5PM6VDY/zpDajzyCmPUC56
g2QLmEI6TLSZOHZIIdX3GvQj9Q2Q8iQVCf6I3NB/TxDipcALmPN+gKmNadmA/nZ6
2so2cRBgUfL52WsJsP3K0BjCBYbZ92+PtVhCbozzft3W0F85d5Sx60OuwG7cumRq
BfsomRsmnRwx/O31eAsq+lrQzAgLJC2mtePcQKJ2IWRTKZC5mKUEpwcpvF82waor
S8MLX2PfdhXkVt0CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQANPHurK3dn6Veg
0uNrud+czMsvlKP7tnmpY0wyXXQaLDkjezIPoEyu82IJL4Y0Qa3BnVKUJ5hmWoTI
5ge4faEDKt8sd4hUECCPVXT/oS5UP7F3jgx3mSCFBISA/yp5r/0OKTYsUq8m4KsM
BOjdecUSlY7BeGUyb2krd/z95RRHuCd0cdTU5vZxr0mQGXspAPLP4DuzQ3mAscEg
1O6MTFwRShWdXQw8mJqaz+nRm1wDpGK3Y9NKVvtSFyMu8i9v1BSR/GB789ORB3U4
1vbpyquIIoQcdaz3IxQCUjqgWxlS9+0If/GT5tn0IW3rrmMpR7/xlXc66FB4/HBF
cNMkSy3+
-----END CERTIFICATE REQUEST-----
```


4. Copy and paste the entire certificate request, including the begin and end tags with dashes, into a new text file. Save this file with a `.csr` extension (for example `my_gt3k.csr`) into a folder.

Figure 9-516. Sample Certificate File Saved

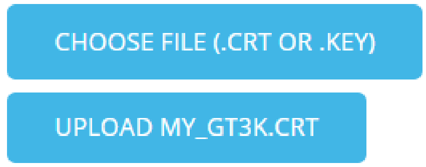
Certficiates.csr	✓	21/05/2024 1:48 pm	CSR File	2 KB

5. Open Git Bash and navigate to the folder containing the certificate request by using the `cd` command, For example, `cd D:/Development/Certificates`.
6. If a user does not already have a CA certificate and private key, follow these steps to create one:
   a. Create the private key by using the following command:
      `winpty openssl genrsa -aes256 -out my_ca.key 4096`

      Note: This step will require to enter a passphrase twice to protect the private key.
   b. Create the CA certificateby using the following command:
      `winpty openssl req -new -key my_ca.key -x509 -out my_ca.crt -days 3650`

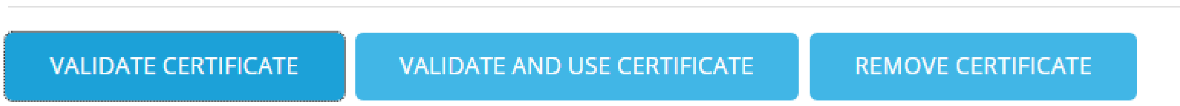
      Note: This command will first prompt user for the passphrase created in the preceding step to protect the private key. Afterward, it will ask for certificate details. User can enter made-up details at this stage.
7. Sign the CSR with the CS certificate by using the following command:
   `winpty openssl x509 -req -in my_gt3k.csr -CA my_ca.crt -CAkey my_ca.key -CAcreateserial -out my_gt3k.crt -days 3650 -sha256`

   Note: User will be prompted for the passphrase for the private key.
8. Click the Choose File button on the Certificate page. Select the `.crt` file created in the preceding step (for example, `my_gt3k.crt`) from your file explorer. Once selected, click the upload button to proceed.



9. Click **VALIDATE AND USE CERTIFICATE**.

Figure 9-517. Validate and Use Certificate

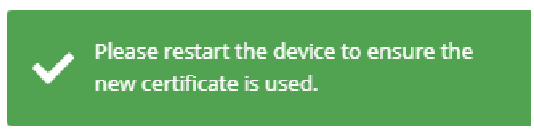


10. **The certificate is valid** notification appears in the bottom right corner of the page.

Figure 9-518. Valid Certificate Notification Message

11. The notification, **Please restart the device to ensure the new certificate is used** appears in the bottom right corner of the page, to restart the unit.

Figure 9-519. Restart Device Notification



12. Restart the unit by navigating to the Restart page in the CMT (Clock Management Tool). For more information, see Restarting the Device
13. After the unit has restarted, view the CMT in any web browser (any page, including the login page is fine) and observe the certificate by clicking the small padlock icon or similar next to the browser's URL field.
14. The details in the certificate should contain both the details the user entered into the form in step 2 (as the "Subject") and the details entered when creating the CA certificate in step 7 (as the "Issuer").

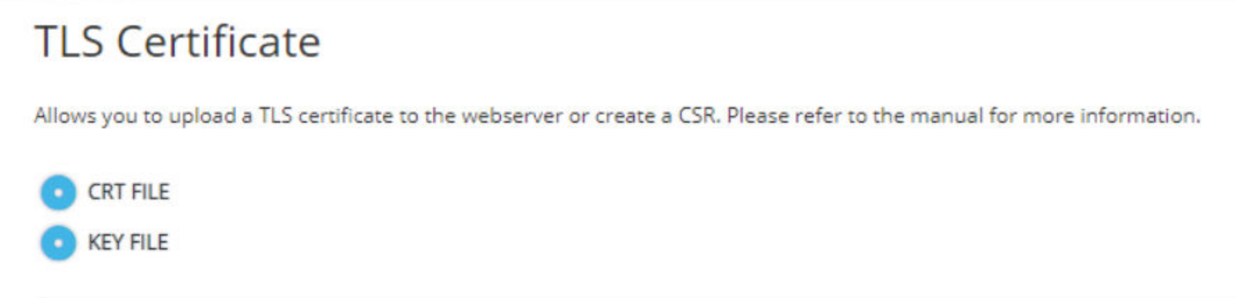
9.16.5 Behavior of Certificates in Different Scenarios

This section describes the behavior of the loaded self-signed certificates in different use cases.

Factory Reset: When a Factory Reset is performed on the GridTime 3000, any custom certificate used by the clock will be removed, and the clock's certificate will revert to the default 'GT3000' certificate.
Note: No power cycle is required to see the change in the applied certificate in the browser.

Firmware Upgrade:When the GridTime 3000 is using a self-signed certificate, the user can view the certificate used by the clock in the browser. The CMT Certificates page shows that the **CRT FILE** and **KEY FILE** indicators are highlighted, as shown in the following image. This indicates that there is a valid `.crt` and `.key` file stored in the internal file system.

Figure 9-520. CMT Certificates Page



When a firmware upgrade is performed, the clock will continue to use the same custom certificate, but the CMT Certificates page will show the**CRT FILE** and **KEY FILE** indicators as empty or not highlighted. This indicates that the valid `.crt` and `.key` files have been removed from the internal file system, but the certificate is still being used by the clock.

Figure 9-521. CMT Certificates Page

Certificate Expiry

All SSL/TLS certificates include a validity period.
Note: When the SSL/TLS certificate used by the clock expires, the clock will continue to use the expired certificate. It is up to the user to monitor and update the certificates.

Alternate Partitions

If the clock boots from the alternate partition and is using a custom certificate, it will continue to use the same custom certificate regardless of the partition it has booted from.

10. Operating

This chapter provides the GridTime 3000 operating guidelines.

10.1 Determining Status

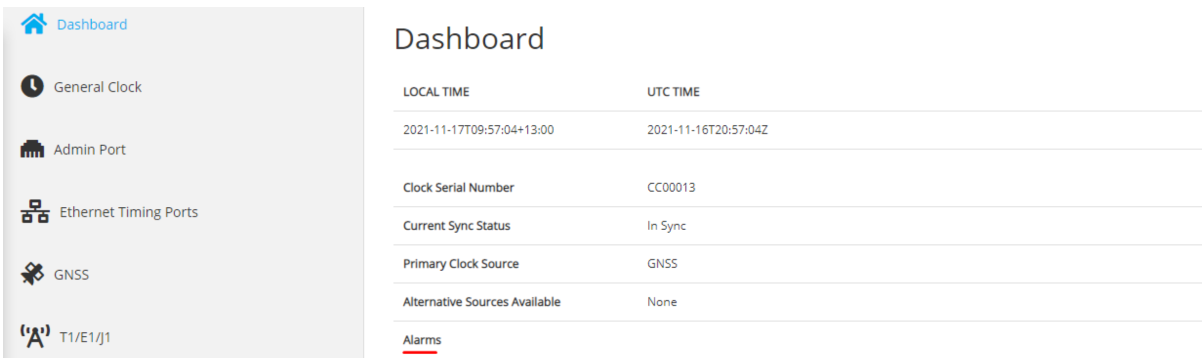
This section describes how to determine the status of the GridTime 3000.

The status of the GridTime 3000 can be monitored by observing what alarms are currently active, and by observing the current sync status.

The GridTime 3000's alarms can be monitored through the following methods:

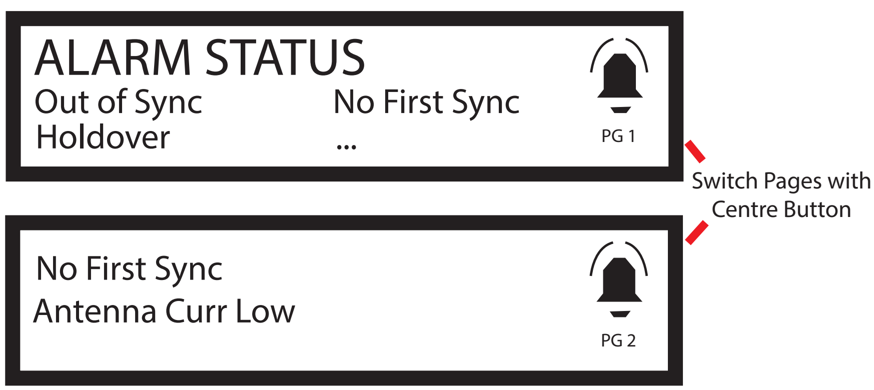
- Monitoring SNMP traps/notifications— SNMP subscriptions must have previously been set up
- Viewing the alarms section of the CMT dashboard for a list of active alarms

Figure 10-1. Dashboard-Active Alarms



- Viewing the LCD alarms tab

Figure 10-2. LCD Alarms Tab



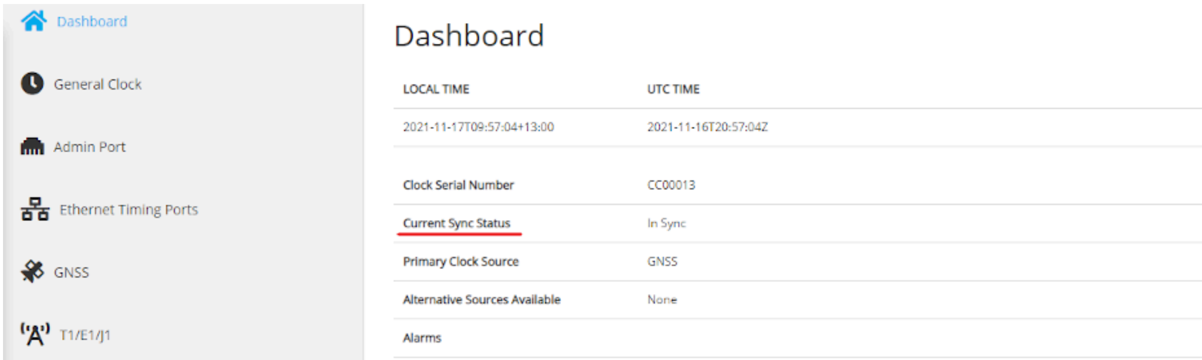
- Monitoring the alarm relays — alarm relays must have previously had alarms mapped to them

For more information on how to monitor the GridTime 3000 alarms and alarm specifications, see Alarms.

The sync status of the GridTime 3000 can be determined through the following methods:

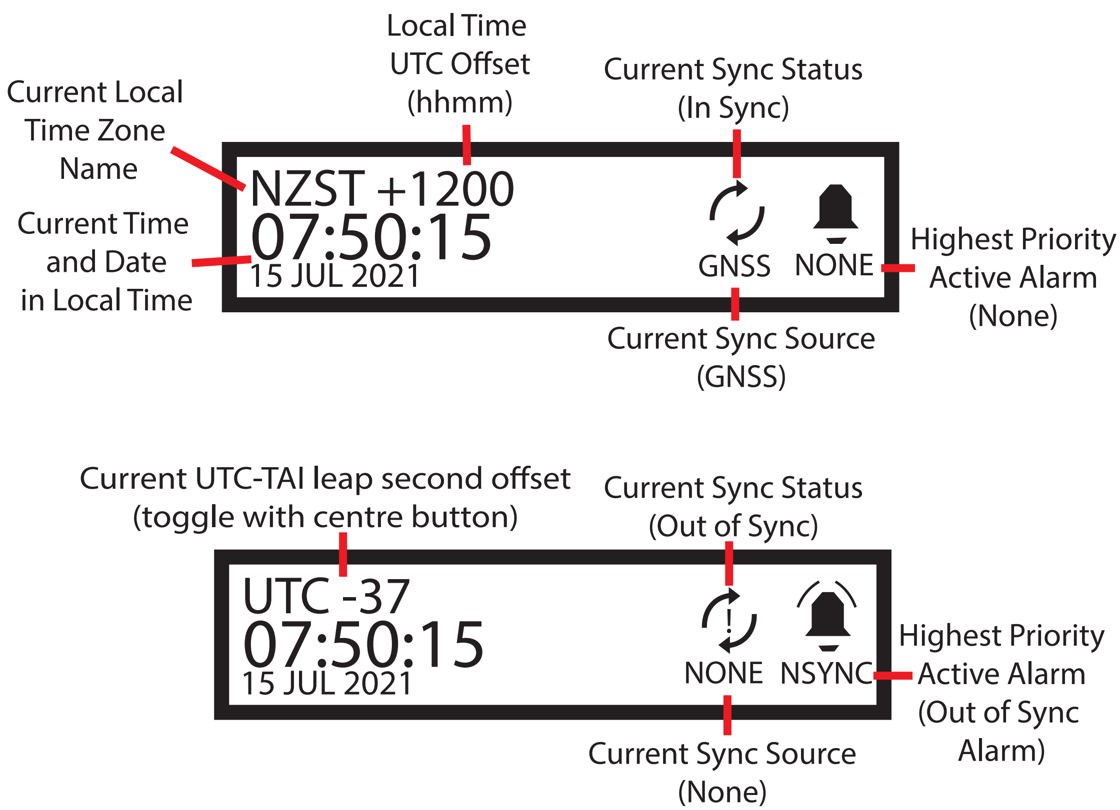
- Viewing the sync status section of the CMT dashboard

Figure 10-3. Dashboard–Current Sync Status



- Viewing the LCD main screen

Figure 10-4. LCD–Current Sync Status



- Performing a SNMP 'get' on the current sync status object (OID .1.3.6.1.4.1.34689.7.1.1.1.1.6)
- Determine if any sync alarms are active — if none are active the unit is in sync

10.1.1 Time Source Status and Availability

The status on the dashboard shows an overview of available time sources being tracked by the time-server. This table is an essential tool for overseeing and ensuring the precision and reliability of the time-server's synchronization sources, maintaining accurate and consistent timekeeping for all connected systems. Each source instance is listed separately.

Figure 10-5. Time Source Status

AVAILABLE SOURCES

SOURCE	PORT NUM	AVAILABILITY	INACCURACY	OFFSET	ORIGIN
GNSS	1	Selected	±30ns	0ns	
PTP	2	Available for selection	±140ns	50ns	GM[00:1D:7F:FF:FE:A2:79:36]
NTP	1	Out of range	±280ns	-2us	Server[192.168.95.116]

Column fields are defined as follows

SOURCE: The common name of the source type.

PORT NUM: The port number through which the service is provided. For protocols like PTP or NTP, this will be the network port number.

AVAILABILITY: The availability status of the source as determined by the time-server.

The possible values are:-

- **Selected:** The time-server is currently synchronized to this source.
- **Available for selection:** This source is ready for synchronization if needed.
- **Tentative availability:** This source can be synchronized if no other options are available. For example, GNSS is considered tentative before its position is stable, and NTP is always tentative.
- **Out of range:** The time provided by this source is outside the acceptable offset range. For a synchronized time-server, the acceptable range is currently 1 microsecond (1 μs).

INACCURACY: This measures the inaccuracy of the source's reported time, combined with observed inaccuracy (one sigma of the magnitude of reported errors). For example, a source might advertise a time 2 days ahead but with an inaccuracy of +/- 50 nanoseconds (50 ns).

OFFSET: The average offset reported by this source compared to the time-server's current time.

ORIGIN: The origin of the time provided by this source. For instance, PTP sources will provide the Grandmaster Identity, and NTP sources will provide the server's IP address.

Note: The **IGNORE INACCURACY IN SOURCE SELECTION** does not allow sources reporting as "out of range" or "tentative availability" to override other available sources.

Note: For the device to change from the current sync source to an alternate sync source with a higher priority, the relative time between each of the sync sources must be less than one microsecond, otherwise the alternate sync source will be ignored.

10.2 Test Mode

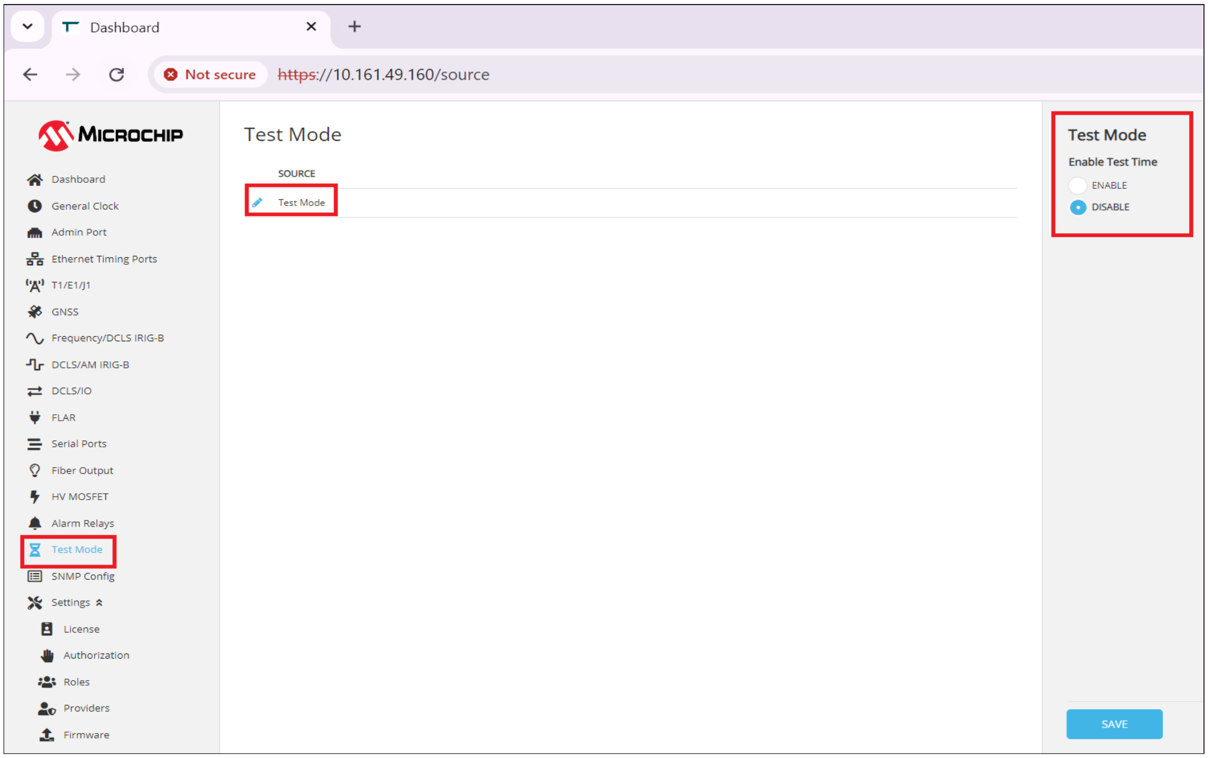
This section describes how to set the GridTime3000 into test mode, and how to change the time to one selected by the user.

The Test Mode behaves like an additional sync source, which overrides all other synchronization sources, reports perfect time accuracy, and can be set to a time specified by the user. While in test mode, the other behavior of the GridTime 3000 remains the same. For example, GNSS associated alarms will still trigger based on the physical inputs to the clock.

Test Mode will be disabled when the GridTime 3000 is power cycled.

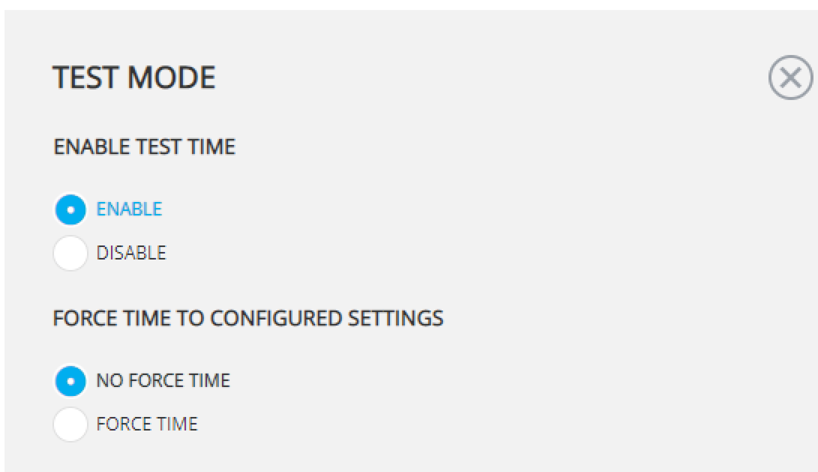
1. Load up the CMT dashboard — see Logging In and Out
2. On the left navigation pane, click **Test Mode** and then click **Test Mode** on the center of the screen. The **Test Mode** settings tab is displayed on the right pane.

Figure 10-6. Dashboard–Test Mode



3. Under **ENABLE TEST TIME** radio buttons, select **ENABLE**.

Figure 10-7. Test Mode Settings

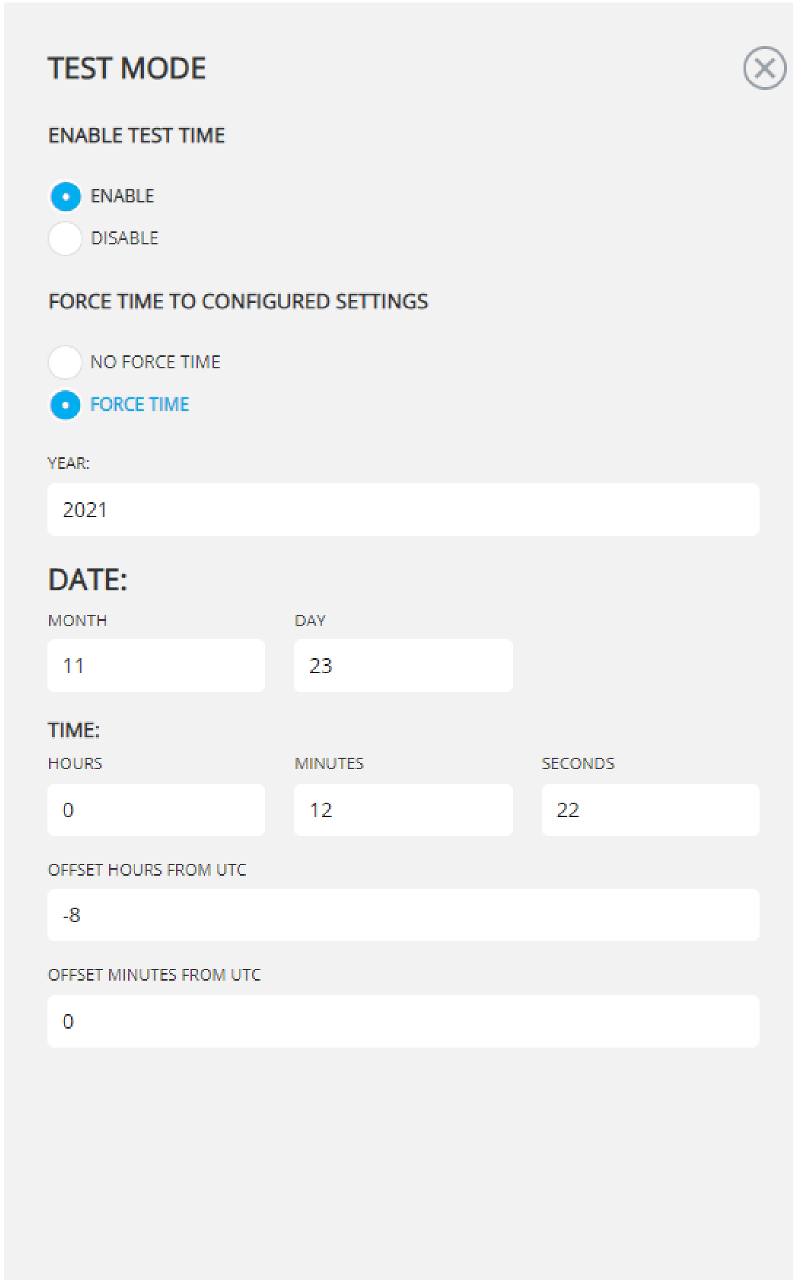


Note: Test Mode will be automatically disabled when then the GridTime 3000 is power cycled.

4. To change the test mode time, first, under the **FORCE TIME TO CONFIGURED SETTINGS** section, select the **FORCE TIME** radio button. Then, enter the desired date, local time, and offset from UTC.

   The **OFFSET HOURS FROM UTC** and **OFFSET MINUTES FROM UTC** should be entered as the offset between local time and UTC. Test Mode automatically compensates for the offset and compute UTC for its internal time.

Figure 10-8. Force Time to Configured Settings



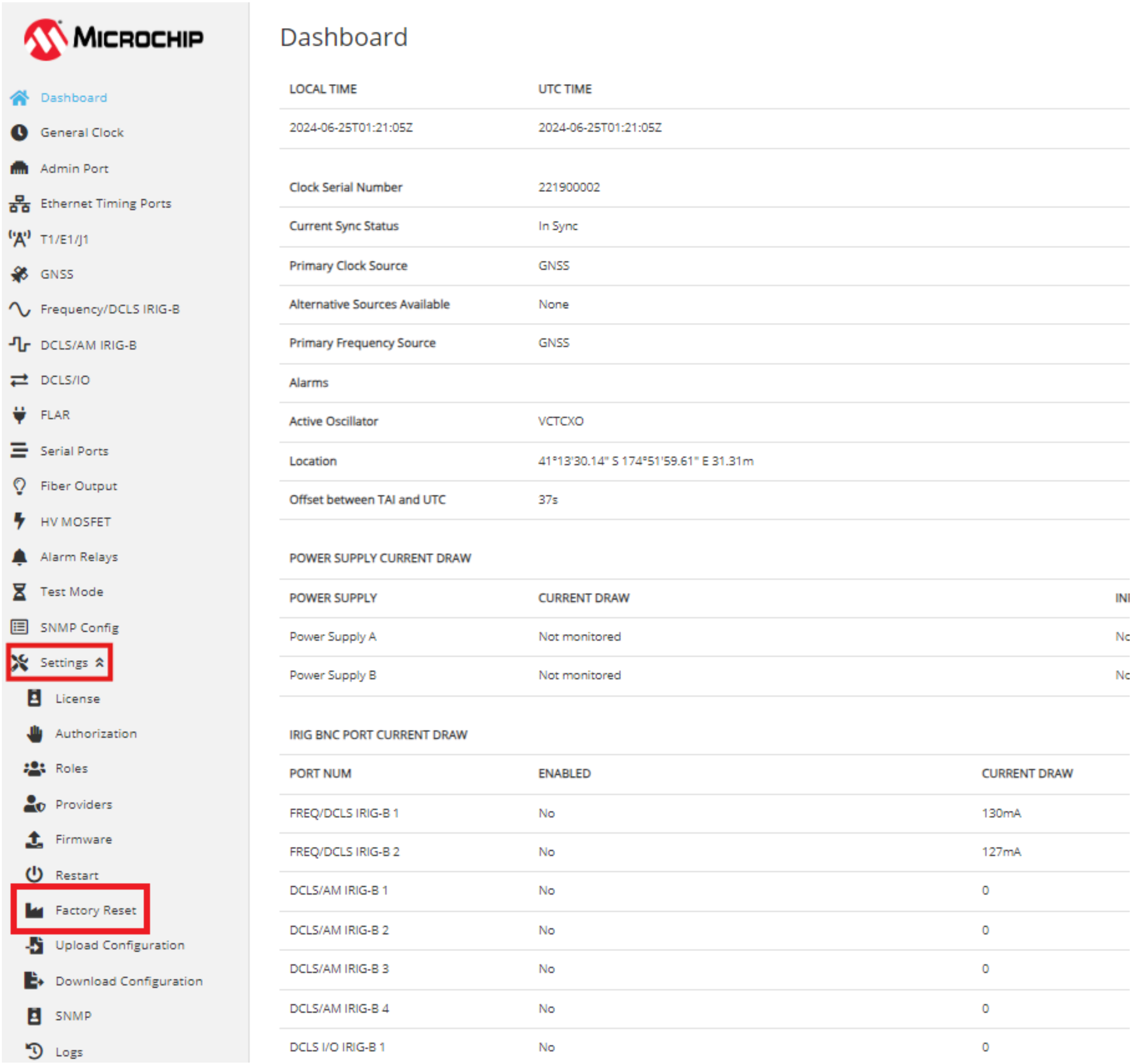
10.3 Factory Reset

This section describes how to factory reset the GridTime 3000 to its default settings.

Note: Only an administrator user can factory reset the GridTime 3000.

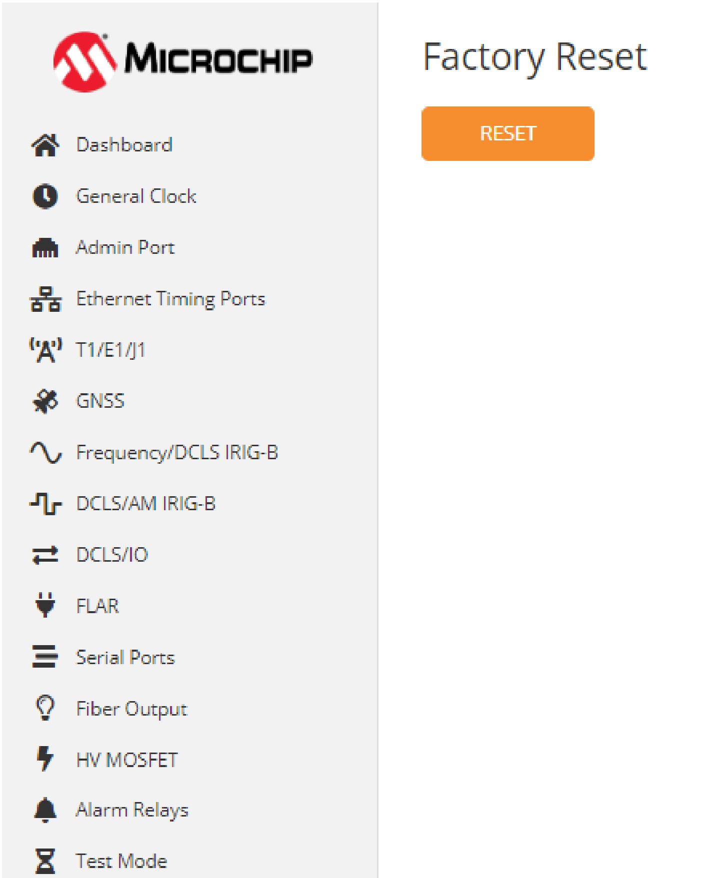
1. Load up the CMT dashboard — see Logging In and Out
2. On the left navigation pane, click **Settings** and then click **Factory Reset**. This brings up the **Factory Reset** window.

Figure 10-9. Dashboard–Factory Reset



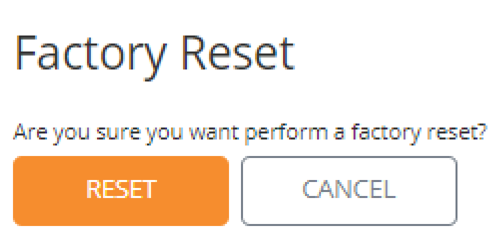
3. On the center of the screen, click the **RESET** button.

Figure 10-10. Factory Reset Window



4. A confirmation message, **Are you sure you want to perform a factory reset?** is displayed. Click **RESET** again to perform the reset.

Figure 10-11. Factory Reset Confirmation Window

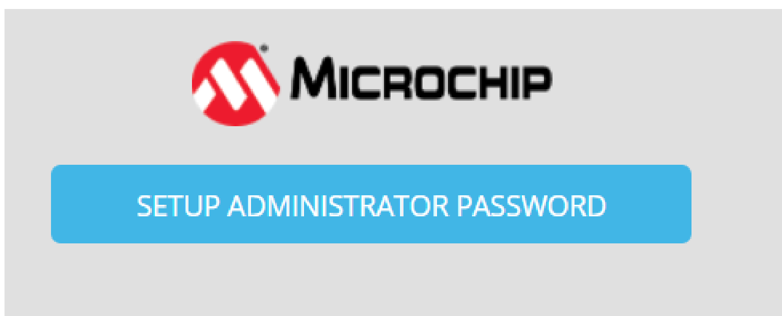


5. If successful, on the bottom right corner of the screen, the message, **Device will perform a factory reset**appears, and then you are taken to the CMT initial login screen where you will be prompted to set the administrator.

Figure 10-12. Message–Device Performing a Factory Reset

When reset, all the users apart from the Administrator are deleted, and the Administrator password is cleared and needs to be set using the following screen.

Figure 10-13. Setting up Administrator Password

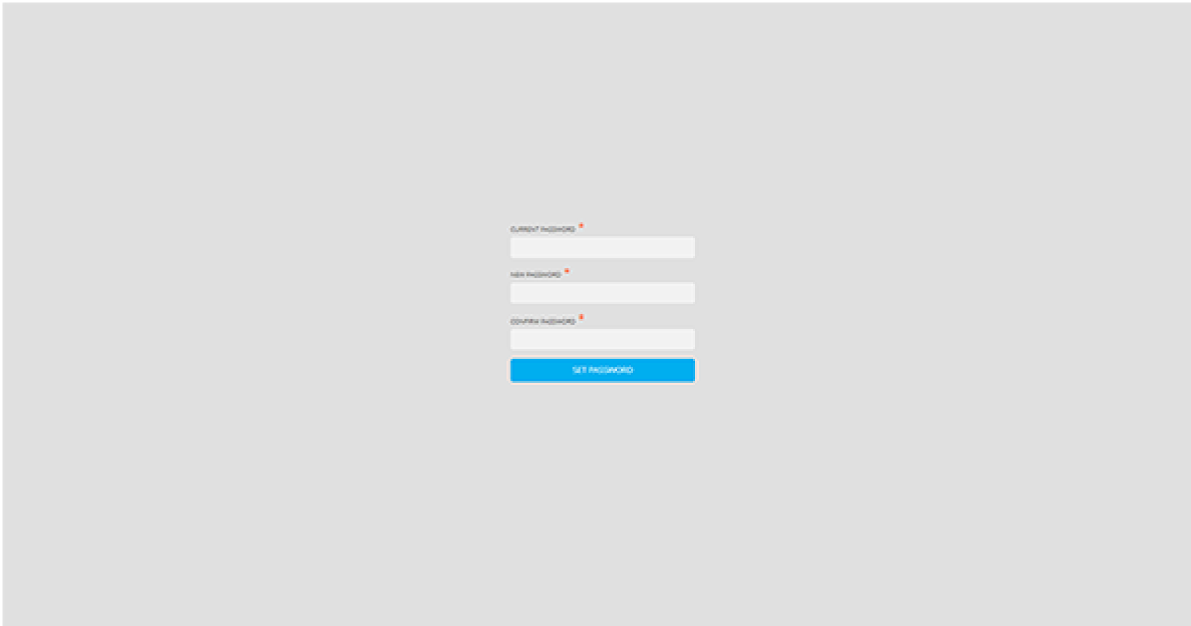


The device is now reset to factory defaults. For a specification of the default settings, see the Factory Default Settings section.

10.4 Changing Password

This section describes how a non-administrator user can change their password on the GridTime 3000

1. Log in to the CMT dashboard —see Logging In and Out
2. On the left navigation pane, scroll down and click **Change Password**.
3. In the CURRENT PASSWORD text box, enter the current user's password. In the **NEW PASSWORD** text box and in the **CONFIRM PASSWORD** text box, enter the new password.
   Note: If the user's current password is not known, an administrator can reset the password by following the steps found here: Changing a User's Password (Admin Only)



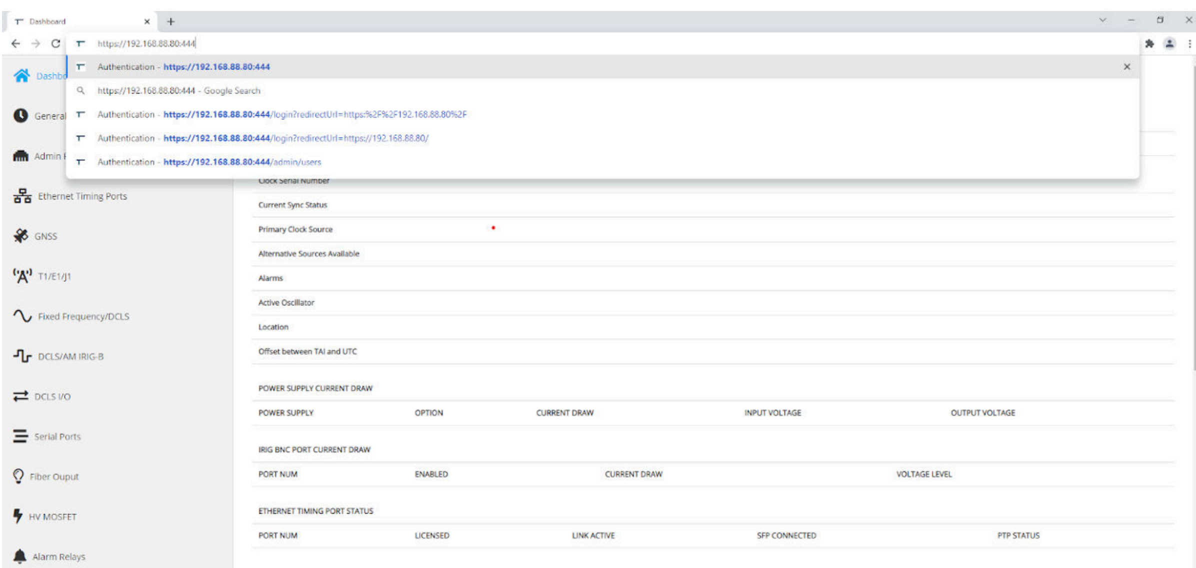
4. To confirm the password change, click **SET PASSWORD**.

10.5 Changing a User's Password (Admin Only)

This section describes how to change the GridTime 3000 user passwords.

1. To modify a password for a GridTime 3000 user, navigate to the CMT authentication module by adding **:444** to the end of the IP address that you normally use to access the CMT in your browser's URL text box.

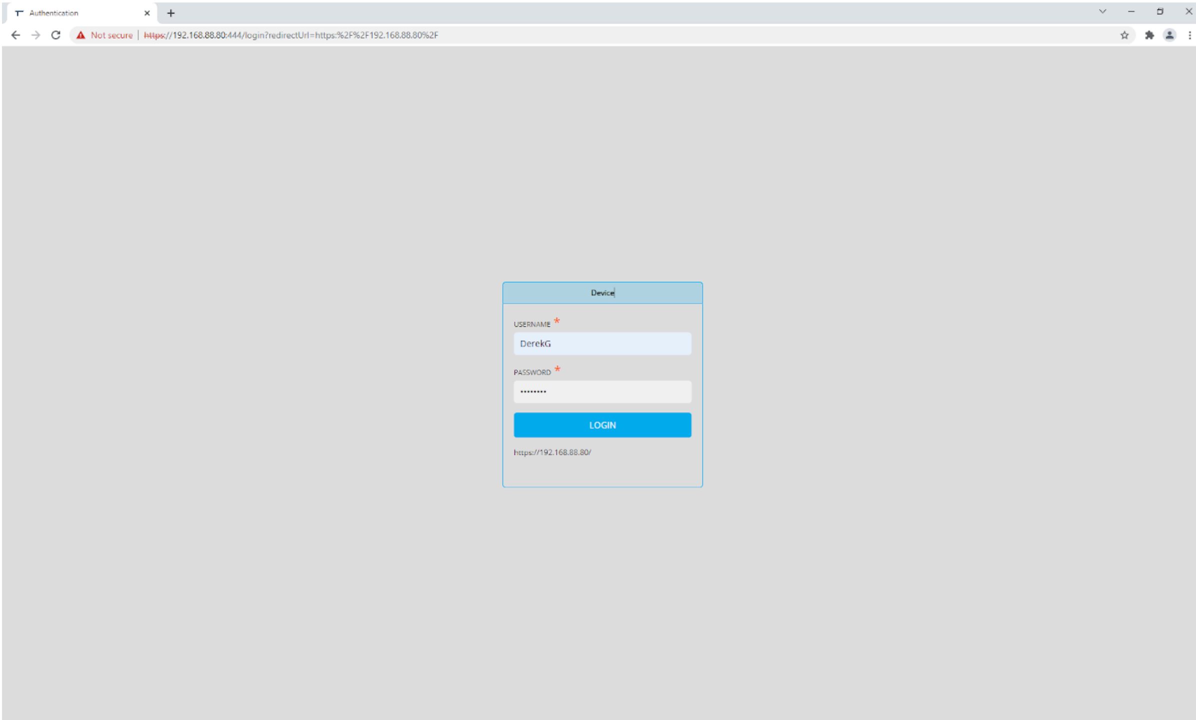
Figure 10-14. Modifying Password Using CMT Authentication Module



The new authentication module login screen is displayed.

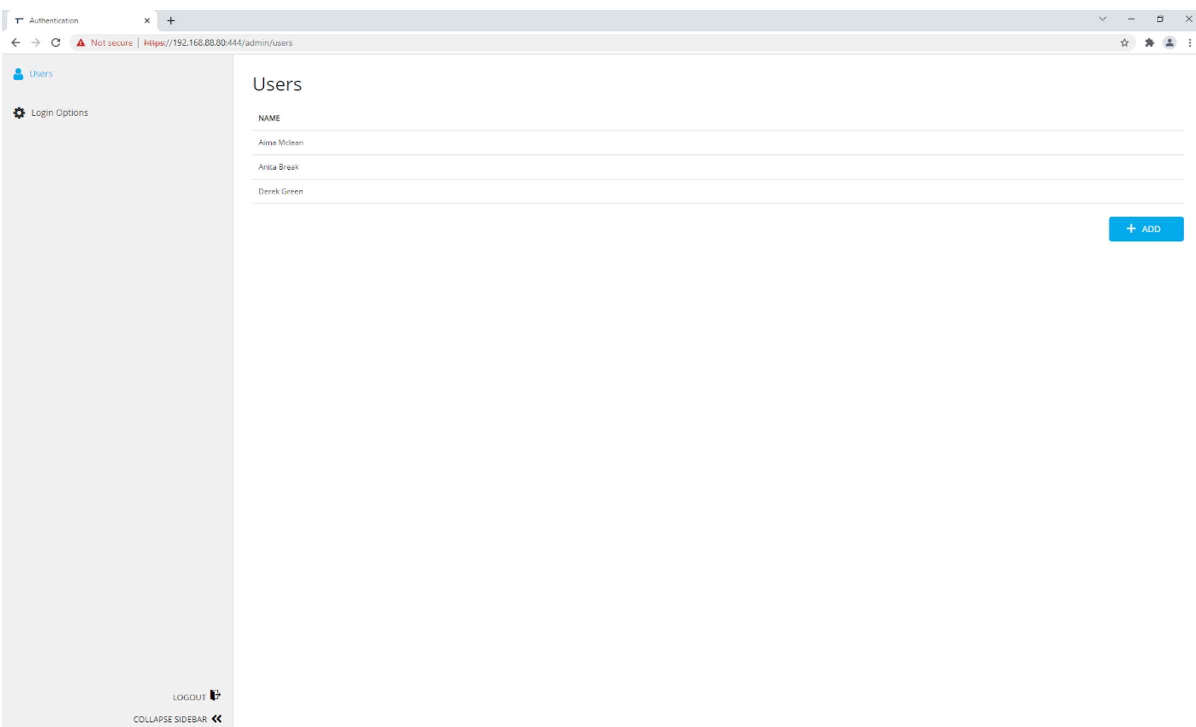
2. Enter the login details for an administrator user and click **LOGIN**.

Figure 10-15. Login Screen



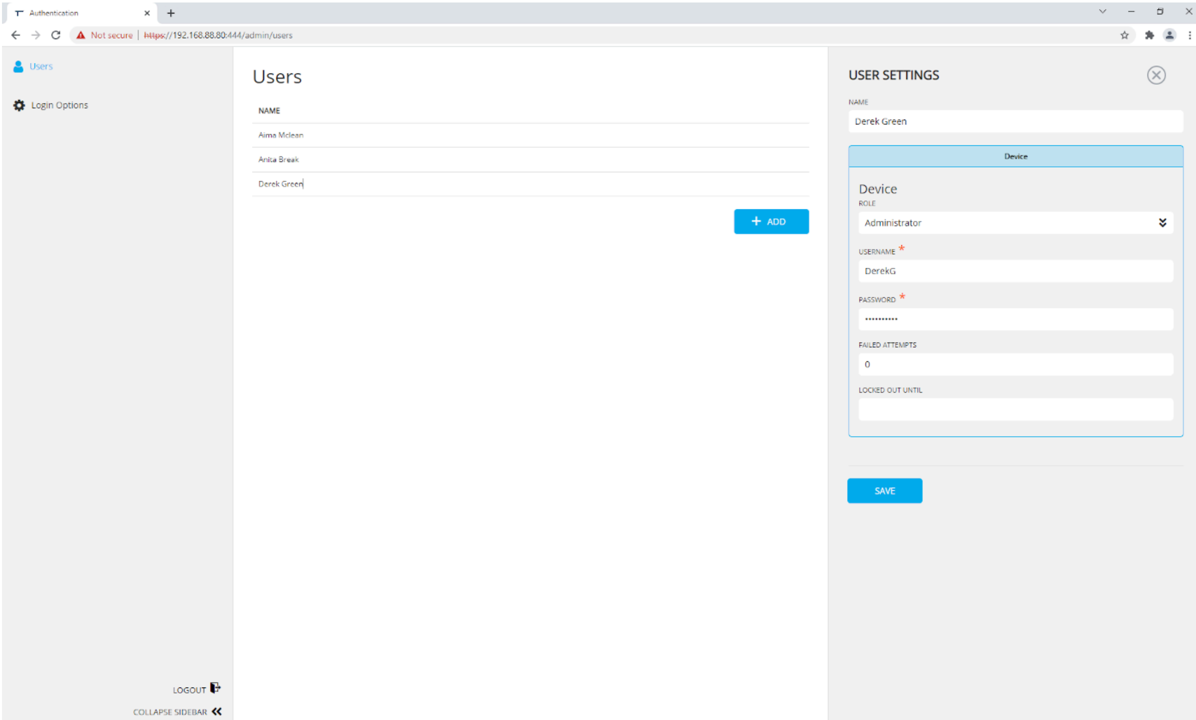
3. Upon successful login, the Users tab of the authentication module is displayed.

Figure 10-16. Users Tab



4. To modify the login settings for a particular user, click on a user's name. The **USER SETTINGS** tab is displayed on the right pane. Click **Device** to show all user login settings.

Figure 10-17. Modify User Settings



5. Modify the password setting as required, and click **SAVE**, when finished.

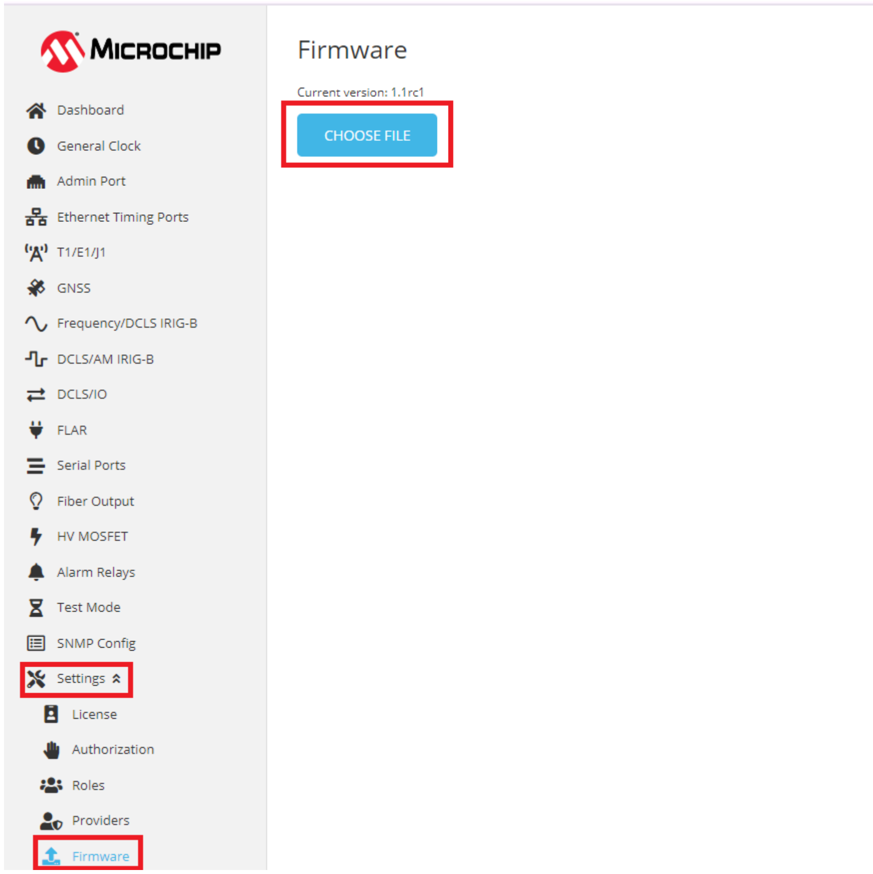
10.6 Upgrading the Firmware

This section describes how to upgrade the GridTime 3000's firmware.

Note: Only an administrator user can upgrade the GridTime 3000's firmware.

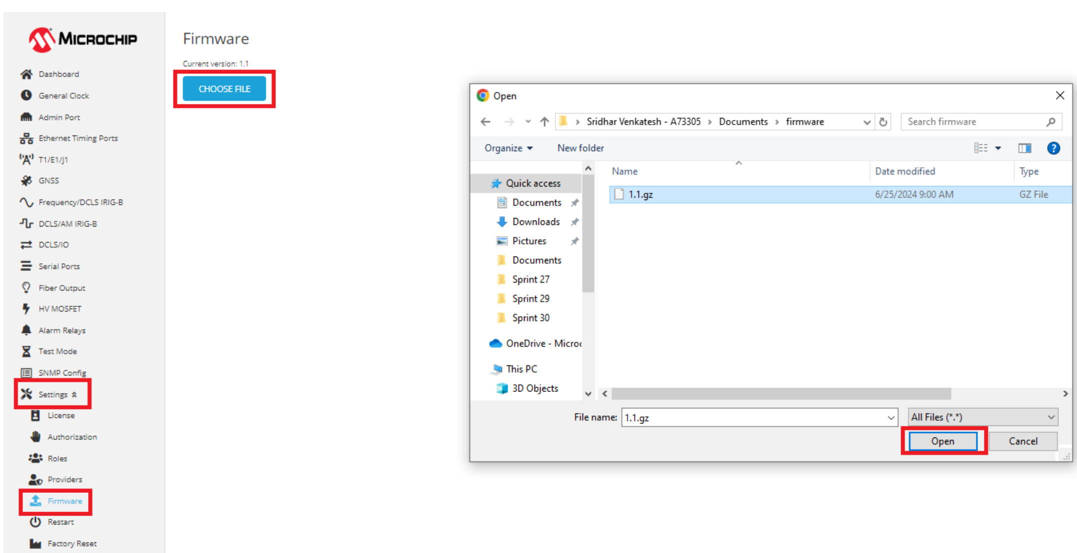
1. Load up the CMT dashboard — see Logging In and Out.
2. On the left navigation pane, click **Settings** and then click **Firmware**. This brings up the Firmware window.

Figure 10-18. Firmware Window



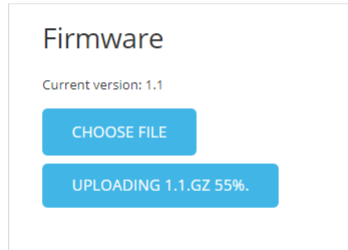
3. To select the new firmware image, click **CHOOSE FILE**. The **Open** dialog box appears. Locate the firmware image on your PC, click on the image, and click the **Open** button.

Figure 10-19. Selecting the New Firmware



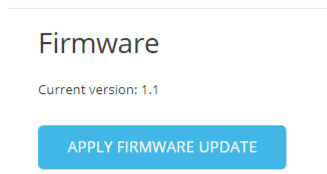
4. An **UPLOAD [Firmware Image]** button appears. Click this button to upload the new firmware image to the device. A percentage is displayed that tracks the upload of the image to the device.

Figure 10-20. Upload Firmware Settings



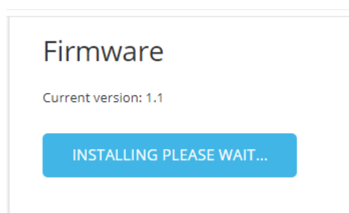
5. Once the percentage reaches 100%, an **APPLY FIRMWARE UPDATE** button appears. Click this button to upload the device's firmware.

Figure 10-21. Apply Firmware Settings



6. An **INSTALLING PLEASE WAIT ...** message appears, and the device will reboot.

Figure 10-22. Installing Firmware Message



7. If the upgrade is successful, the device shows the new firmware on its LCD during boot up, and the new firmware version is shown on screen and in the firmware tab of its CMT once you log out and log back in.
   If the firmware version remains the same, this indicates a potential upgrade failure. If the upgrade failure persists, contact Microchip Support. See Contacting Technical Support.

10.7 Firmware partitions

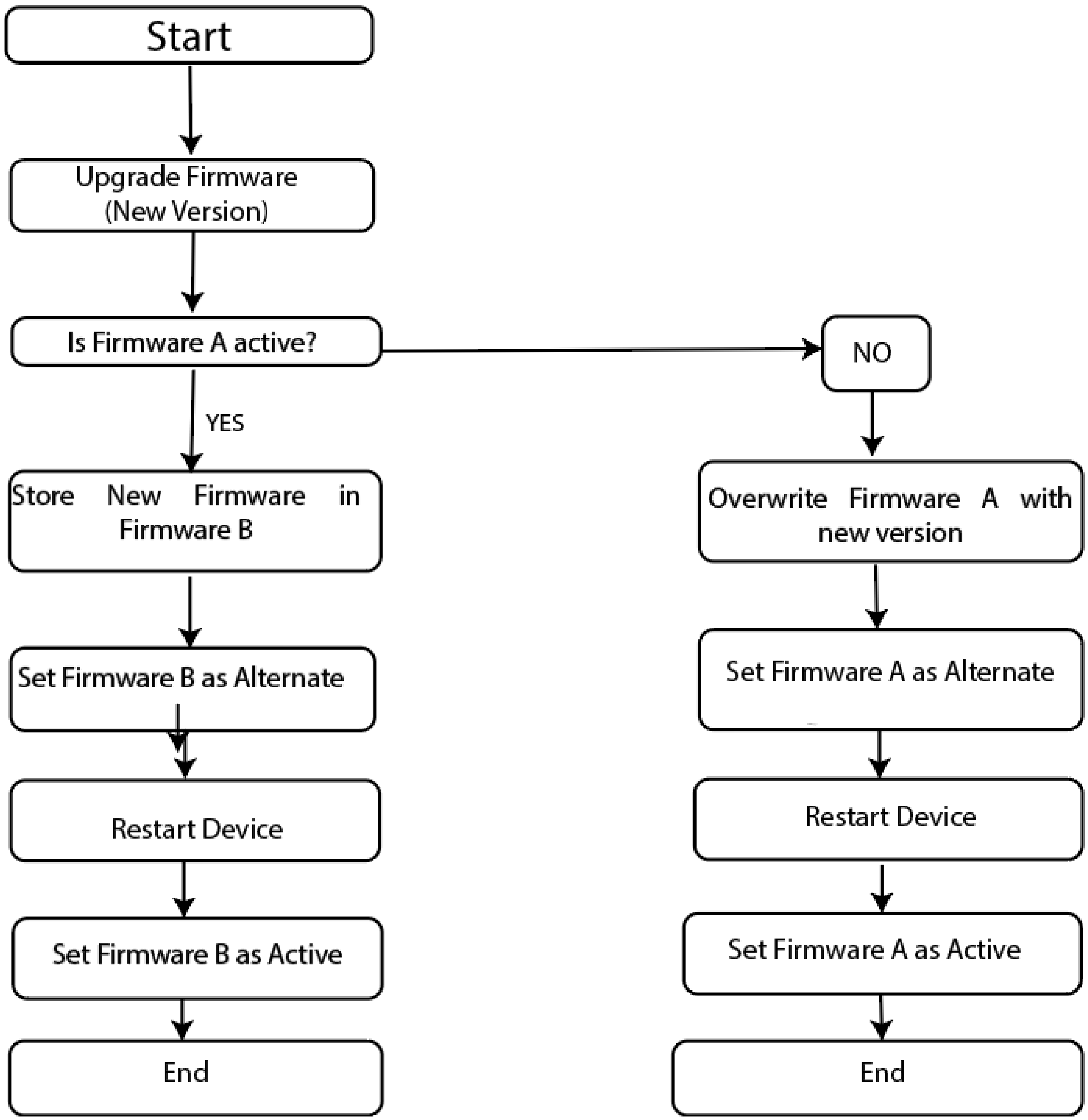
Storage Partitions

The GridTime 3000 operates with three persistent storage areas known as 'Firmware A', 'Firmware B' and 'Settings'. Firmware A and B contain an active and alternate firmware image. This dual image setup ensures reliability and continuity of operation by providing 'Firmware B' as an alternative image if the primary image ('Firmware A') becomes corrupted.

During a firmware upgrade, the new firmware version is stored in the last unused storage partition. Upon completion of the upgrade, the device seamlessly transitions to the updated firmware partition upon restart.

For example: If you have Firmware A with version 1.0 upgraded on 1st May and Firmware B with version 1.1 upgraded on 2nd May, Firmware B will be the active firmware version. When you attempt to upgrade to a new firmware, Firmware A will be overwritten and will become the active firmware version and Firmware B will become the alternate.

Figure 10-23. Firmware Upgrade Flow Chart



Fallback to the Alternate Partition:

In the event of firmware issue or if the bootloader detects corruption on the active image, it will switch to the alternate firmware partition.

For example, if an issue is detected on Firmware A then it will boot onto Firmware B instead.

Manually Booting the Alternate Partition:

Users can manually initiate the use of the alternate image partition by holding down the left hand front panel button when the clock is powering on.

Note: Manual booting will only last until the next reboot, but is useful for reverting to an earlier firmware that can then be used to retry an upgrade.

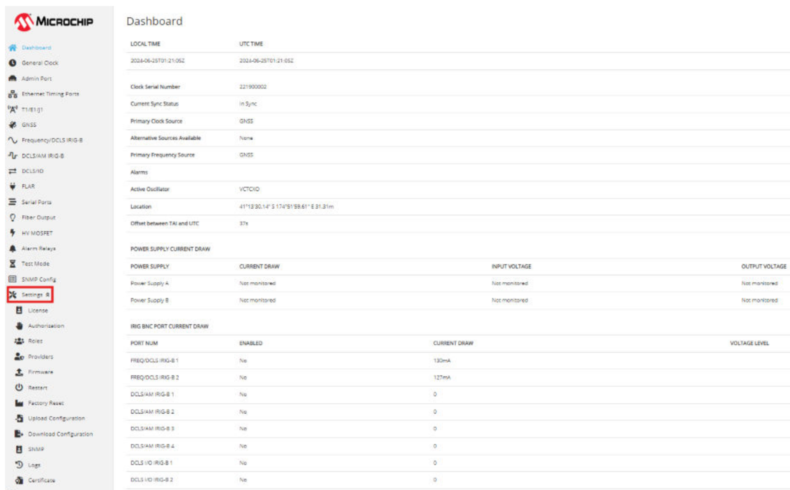
10.8 Adding new Licenses

This section describes how to add a new license key to the GridTime 3000 to enable new licensed features.

Note: Only an administrator user can add new licenses.

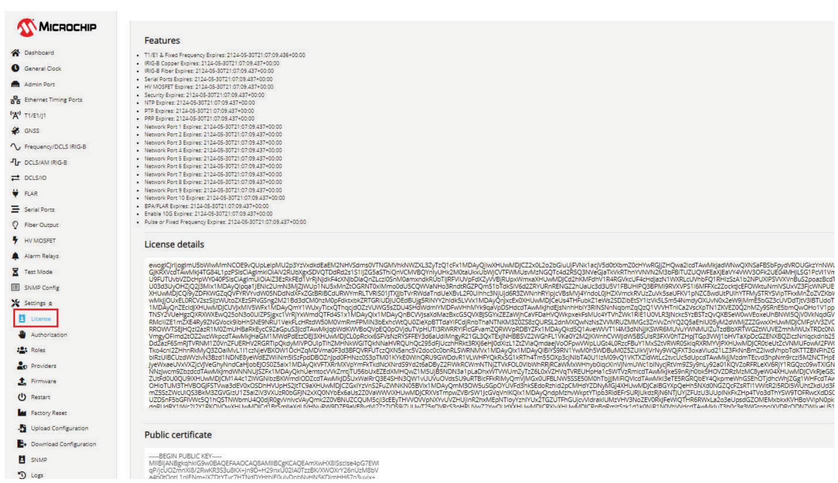
1. Log in to the CMT dashboard —see Logging In and Out.
2. On the left navigation pane of the CMT Dashboard screen, click **Settings**.

Figure 10-24. CMT Dashboard



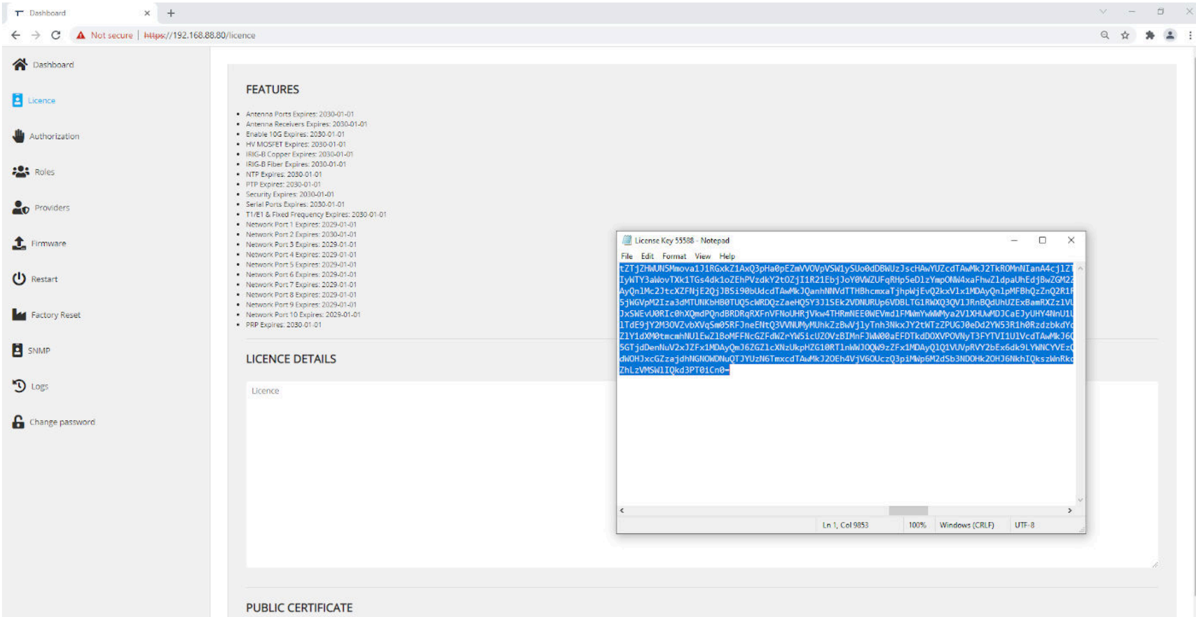
3. Click **License** icon to bring up the license window.

Figure 10-25. License Window



4. Delete all text in the **LICENSE DETAILS** text box as this is the existing license key. Once this is done, the text box should appear empty.
5. Open the license key text file sent to you by Microchip, and copy all text from the file into the **LICENSE DETAILS** text box.

Figure 10-26. New License Details



6. To store the license to the device, scroll down to the bottom of the license window in the CMT and click **SAVE**. If successful, a **Saved!** notification appears on the bottom right corner of the web page, and the page will refresh.

Figure 10-27. Successful Save Notification

The features you activated with the new license key should now be available. Test the functionality activated by the license key to validate that it was successfully enabled. If the newly licensed functionality is not working, contact technical support Contacting Technical Support

10.9 Restarting the Device

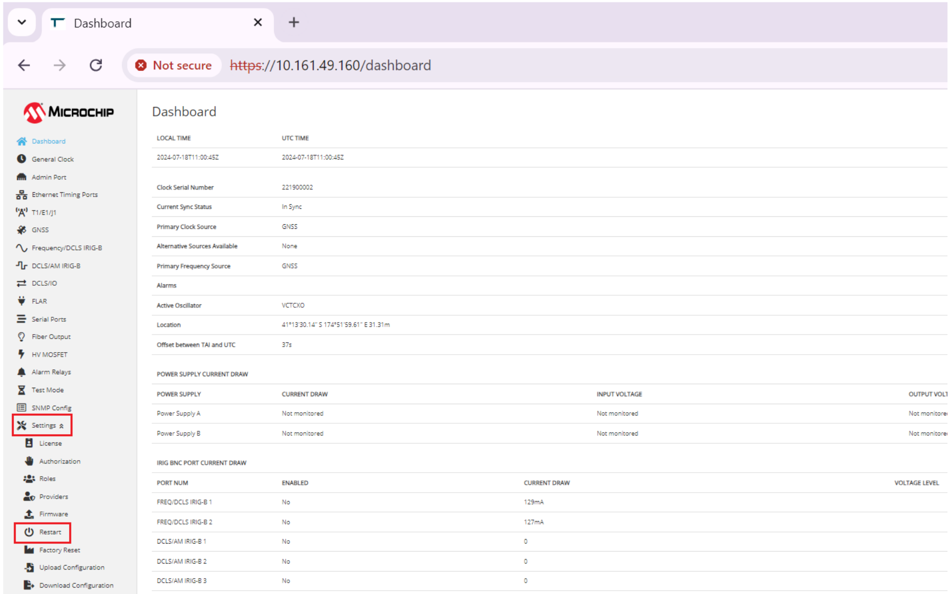
This section describes how to restart the GridTime 3000.

The GridTime 3000 can be restarted through its CMT, its front panel buttons, or by removing and reconnecting power.

CMT Method

1. Load up the CMT dashboard — see Logging In and Out
2. On the left navigation pane, click **Settings** and then click **Restart**. This brings up the **Restart** window.

Figure 10-28. CMT Dashboard



3. Click **RESTART DEVICE**. The confirmation message, **Are you sure you want to restart the device?** appears. Click **RESTART** to trigger the restart.

Figure 10-29. Restart Window

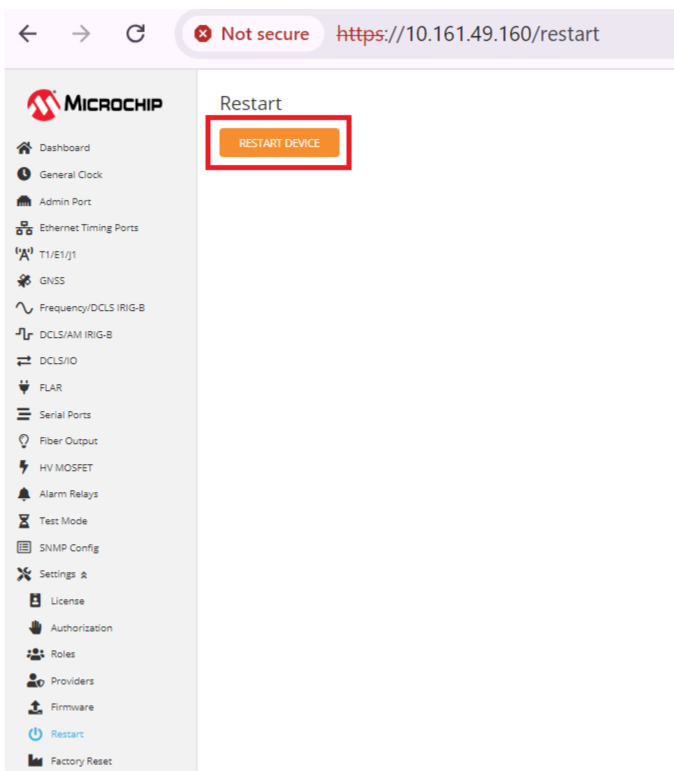
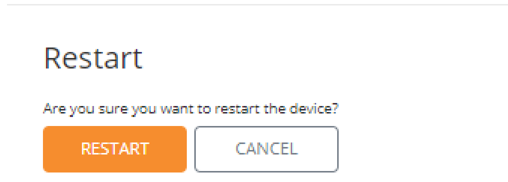
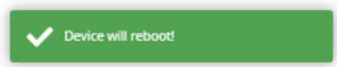


Figure 10-30. Restart Confirmation Message



4. A notification message with the text **Device will reboot!** appears on the bottom right corner of the web page, and the restart initiates.

Figure 10-31. Reboot Notification Message



Front Panel Buttons Method

1. To navigate to the clock power screen, press and hold the center front panel button for 5 seconds.
2. Once the clock power screen appears, press the left-hand front panel button to initiate the restart. The word **Reboot** should appear on the left-hand side of the LCD to show the mapping to this button.
3. A **Goodbye** graphic will show on the LCD, indicating that the restart has begun.

Disconnecting and Reconnecting Power Method

Switch off and on the GridTime 3000's power supply using a switch controlled power source , or disconnect and reconnect its power cable(s) to perform a restart.

10.10 Configuration Management

Follow these steps to upload or download the configuration files.

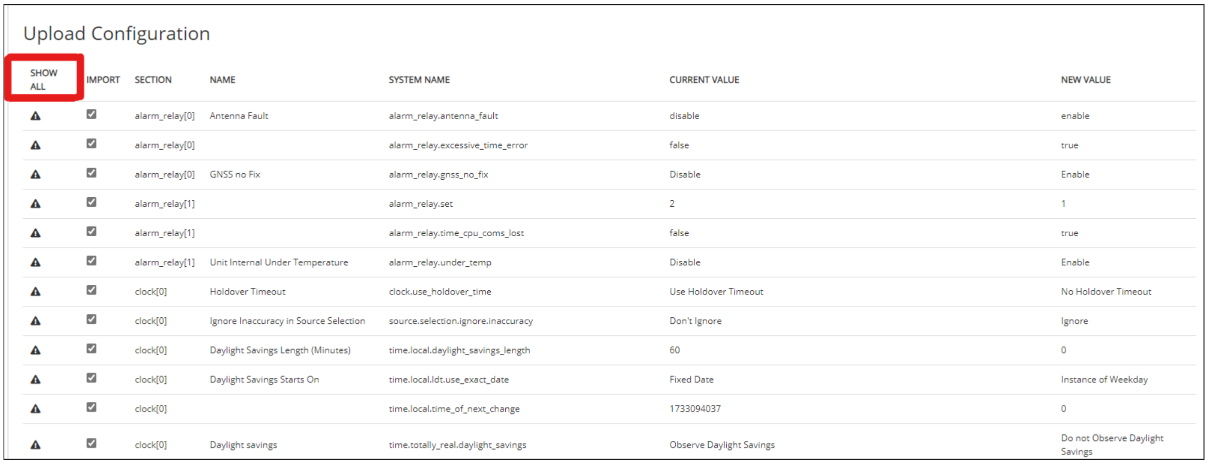
1. On the left navigation pane of the Dashboard, click **Settings.**
2. To upload a configuration file to GridTime 3000, click **Upload Configuration** and follow the steps listed in the Upload Configuration section.
   Likewise, to download a configuration file from GridTime 3000, click **Download Configuration**, and follow the steps listed in the Download Configuration section.

Note: Only Administrator level users can upload or download the configuration files

10.10.1 Upload Configuration

1. To upload a new configuration file, under the Settings menu, click **Upload Configuration**.
2. Click **CHOOSE FILE**. The Open dialog box is displayed.
3. Use the file browser to select the configuration file (JSON File) to upload.
4. Press **Open**, to upload the configuration file (JSON File).
5. Select **SHOW ALL** to display all variables including both those that have been changed and unchanged.

Figure 10-32. Show All Variables

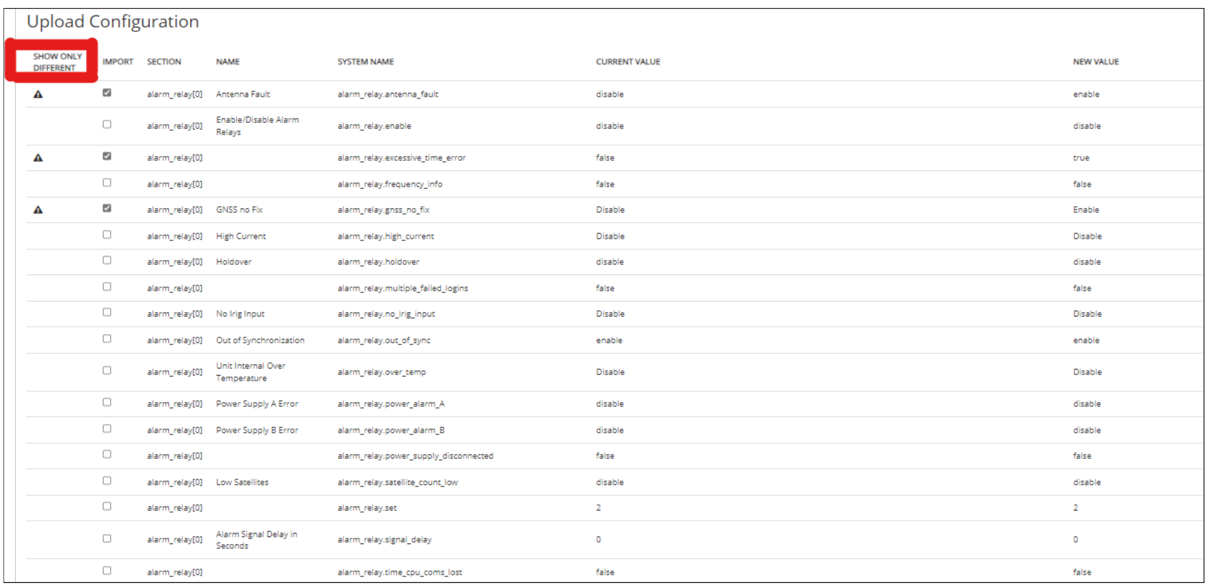


Upload Configuration

SHOW ALL	IMPORT	SECTION	NAME	SYSTEM NAME	CURRENT VALUE	NEW VALUE
⚠	☑	alarm_relay[0]	Antenna Fault	alarm_relay.antenna_fault	disable	enable
⚠	☑	alarm_relay[0]		alarm_relay.excessive_time_error	false	true
⚠	☑	alarm_relay[0]	GNSS no Fix	alarm_relay.gnss_no_fix	Disable	Enable
⚠	☑	alarm_relay[1]		alarm_relay.set	2	1
⚠	☑	alarm_relay[1]		alarm_relay.time_cpu_coms_lost	false	true
⚠	☑	alarm_relay[1]	Unit Internal Under Temperature	alarm_relay.under_temp	Disable	Enable
⚠	☑	clock[0]	Holdover Timeout	clock.use_holdover_time	Use Holdover Timeout	No Holdover Timeout
⚠	☑	clock[0]	Ignore Inaccuracy in Source Selection	source.selection.ignore.inaccuracy	Don't Ignore	Ignore
⚠	☑	clock[0]	Daylight Savings Length (Minutes)	time.local.daylight_savings_length	60	0
⚠	☑	clock[0]	Daylight Savings Starts On	time.local.ldt.use_exact_date	Fixed Date	Instance of Weekday
⚠	☑	clock[0]		time.local.time_of_next_change	1733094037	0
⚠	☑	clock[0]	Daylight savings	time.totally_real.daylight_savings	Observe Daylight Savings	Do not Observe Daylight Savings

6. Select **SHOW ONLY DIFFERENT** option, to display only the variables that have changed. This will show the current and new value which will change when the file is uploaded.

Figure 10-33. Show Only Different Variables



Upload Configuration

SHOW ONLY DIFFERENT	IMPORT	SECTION	NAME	SYSTEM NAME	CURRENT VALUE	NEW VALUE
⚠	☑	alarm_relay[0]	Antenna Fault	alarm_relay.antenna_fault	disable	enable
	☐	alarm_relay[0]	Enable/Disable Alarm Relays	alarm_relay.enable	disable	disable
⚠	☑	alarm_relay[0]		alarm_relay.excessive_time_error	false	true
	☐	alarm_relay[0]		alarm_relay.frequency_info	false	false
⚠	☑	alarm_relay[0]	GNSS no Fix	alarm_relay.gnss_no_fix	Disable	Enable
	☐	alarm_relay[0]	High Current	alarm_relay.high_current	Disable	Disable
	☐	alarm_relay[0]	Holdover	alarm_relay.holdover	disable	disable
	☐	alarm_relay[0]		alarm_relay.multiple_failed_logins	false	false
	☐	alarm_relay[0]	No Irig Input	alarm_relay.no_irig_input	Disable	Disable
	☐	alarm_relay[0]	Out of Synchronization	alarm_relay.out_of_sync	enable	enable
	☐	alarm_relay[0]	Unit Internal Over Temperature	alarm_relay.over_temp	Disable	Disable
	☐	alarm_relay[0]	Power Supply A Error	alarm_relay.power_alarm_A	disable	disable
	☐	alarm_relay[0]	Power Supply B Error	alarm_relay.power_alarm_B	disable	disable
	☐	alarm_relay[0]		alarm_relay.power_supply_disconnected	false	false
	☐	alarm_relay[0]	Low Satellites	alarm_relay.satellite_count_low	disable	disable
	☐	alarm_relay[0]		alarm_relay.set	2	2
	☐	alarm_relay[0]	Alarm Signal Delay in Seconds	alarm_relay.signal_delay	0	0
	☐	alarm_relay[0]		alarm_relay.time_cpu_coms_lost	false	false

7. Under the **IMPORT** column, select the individual check box for those settings that are required to be uploaded to the GridTime 3000.
8. To upload the configuration file to GridTime 3000, click **SUBMIT**.
9. A **Saved!** notification appears on the bottom right corner of the page indicating that the configuration settings have been successfully written to the GridTime 3000.

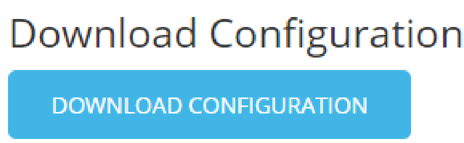
Figure 10-34. Successful Save Notification

10.10.2 Download Configuration

1. To download the configuration file, in the CMT dashboard, under the Settings menu, click **Download Configuration**.

A **DOWNLOAD CONFIGURATION** button appears in the center of the screen as shown in the following figure.

Figure 10-35. Download Configuration



2. Click the **DOWNLOAD CONFIGURATION** button, and your web browser will download the file (JSON). Check the web browser for the download location.

11. Maintenance and Troubleshooting

This chapter describes maintenance and troubleshooting procedures for the GridTime 3000.

11.1 Preventative Maintenance

This section describes how to perform preventative maintenance on the GridTime 3000 to help reduce the chance of future faults.

The GridTime 3000 requires minimal preventive maintenance. Ensure the unit is not exposed to hazards such as direct sunlight, open windows, water, or extreme heat. See Environmental Requirements, for electromagnetic compatibility conditions that may cause damage.

CAUTION To avoid electromagnetic discharge damage to the circuitry, never attempt to vacuum the GridTime 3000.

CAUTION To avoid damage, under no circumstances should the interior chassis of the GridTime 3000 be allowed to come in contact with water.

The following table lists preventive maintenance measures to be performed periodically. Do not disassemble components just for the purpose of inspection.

Table 11-1. Preventive Maintenance

Item	Inspection	Corrective Action	Interval
Chassis	Inspect for dirt or foreign material	Clean the exterior of chassis with a soft dry cloth	Periodically (Once a year)
Cables	Inspect for pinched, worn or damaged cable(s)	Replace pinched, worn or damaged cable at the first opportunity	Periodically (Once a year)
Connectors	Inspect for loose or damaged connector(s)	Tighten loose connectors. If damaged, replace the connector and/or cable at the first opportunity	Periodically (Once a year)

11.2 Safety Considerations

Follow industry or company-specific safety guidelines and policies when working on or around live equipment.

11.3 ESD Considerations

Maintenance personnel should wear ESD (electrostatic discharge) wrist straps when installing or working on all GridTime 3000 equipment and modules. Plug the user-supplied wrist strap onto the ground nut of the GridTime 3000.

11.4 Troubleshooting

This section describes how to troubleshoot issues with the GridTime 3000.

The following table presents troubleshooting information for the GridTime 3000 based on symptoms.

For a detailed description of the trigger and clearance conditions for each of the GridTime 3000's alarms, see Alarm Monitoring

Table 11-2. Troubleshooting Common Symptoms

Symptom	Probable Cause	Troubleshooting Procedure / Corrective Action
No LED lit on any port	No power to unit	Check power supply to ensure that the Uninterruptible Power Supply (UPS) (if applicable) is operating correctly.
	Power supply fuse(s) are blown	Remove and replace fuse(s) . See Power Supply Fuse Replacement.
	Loss of ground connection	Reattach the ground wires. See Making Ground and Power Connections.
	Loose power cabling to unit	Check that the unit's external power cables are securely fastened.
No Ethernet Traffic (PTP or NTP) between GridTime 3000 timeTransmitter/Server and timeReceiver/client(s) (If ACT LED for port is OFF)	Cable connections	Check that cables and SFP transceivers are securely connected to the device. Verify that the SFP transceiver model in use is supported Table 6-4.
	Ethernet auto-negotiation not enabled on a device between timeTransmitter/Server and timeReceiver/client	Check that Ethernet auto-negotiation is enabled on all connected network elements.
No Ethernet Traffic (PTP or NTP) between GridTime 3000 timeTransmitter/Server and timeReceiver/client(s) (If ACT LED for port is ON)	Incorrect virtual LAN (VLAN) configuration	Verify that VLAN configuration is enabled correct in the **VLAN Settings** tab of the Ethernet Timing Ports window in the CMT. See Provisioning VLAN Settings
	Incorrect IP address configuration	Verify that the timeTransmitter/server IP configuration is correct in the Ethernet Timing Port Basic settings window in the CMT Provisioning the Ethernet Ports, and ensure it is on the same subnet as the timeReceiver/client(s).
	timeReceiver/Client configuration for timeTransmitter/server is incorrect	Verify that the timeReceiver/client settings match the timeTransmitter/server's settings.
	PTP domain setting for timeTransmitter do not match timeReceiver/client's domain	Verify the domain setting for each timeTransmitter matches the domain setting for the timeReceiver. This setting can be found in the PTP Tab of the Ethernet Timing Ports Configure Default Domain
Upgrading firmware failed	Internal memory has failed	Retry the upgrade. If upgrade fails again, Contact Microchip technical support. Contacting Technical Support
	Corrupt firmware package	Redownload the latest firmware package from my.microsemi.com and retry the upgrade
GridTime 3000 in Holdover No GNSS position fix	No visible satellites	Check if GNSS Antenna Installation has a clear view of the sky. See Installing the GNSS Antenna for additional information
	Wrong antenna type, cable length, or power level into GNSS Antenna port	Check that the antenna installation (including cables, arrestors, amplifiers, and splitters) delivers sufficient gain into the antenna port, and that the antenna in use is compatible with the antenna port's current and voltage specification as per: GNSS Receiver Specification. The GNSS receiver requires a gain at the antenna connector input to be between 17 dB and 50 dB, and the noise figure to be <4dB.

11.4.1 Alarm Conditions and Correction Actions

This section describes the trigger and clearance conditions, and the recommended corrective user action for the GridTime 3000's alarms.

Each alarm has unique trigger and clearance conditions based on system observables. Hence, each alarm requires unique corrective action when triggered.

For guidance on how to monitor the GridTime 3000's alarms, see Alarm Monitoring.

Table 11-3. Alarm Trigger and Clearance Conditions Table

Alarm Name	Trigger Condition	Clearance Condition	Recommended Corrective Action
No Fix	Device lacks reception of enough usable[1] GNSS satellites to calculate an estimate of its position.	Device has reception of enough usable [1] GNSS satellites to calculate an estimate of its position.	If alarm is recurring, validate the antenna installation using Antenna Installation Troubleshooting. Ensure the antenna has a full sky view.
Satellite Count Low	Number of usable satellites detected by the device drops below the minimum satellites setting. The minimum satellites setting can be modified in the CMT. See Provisioning GNSS	Number of usable satellites detected by the device reaches the minimum satellites setting.	If alarm is recurring, ensure that the minimum satellites setting is not too large (>10). If it is not too large, validate the antenna installation using Antenna Installation Troubleshooting. Ensure the antenna has a full sky view.
Antenna Current High	Current through the antenna port increases above 60 mA.	Current through the antenna port drops below 58 mA.	Electrically test the antenna installation according to How to Check for a short in an Antenna Installation guide.
Antenna Current Low	Current through the antenna port drops below 3 mA.	Current through the antenna port increases above 5 mA.	Electrically test the antenna installation using Antenna Installation Troubleshooting.
Holdover	Device was synchronized to a time source, but has lost all time sources it can synchronize to, causing a transition from 'in sync' to 'holdover'.	Device regains synchronization to a time source, becoming 'in sync'. Device becomes 'out of sync' by exceeding an inaccuracy threshold or going through holdover timeout.[2]	If alarm is recurring, ensure that the device's primary time source is consistently available.
Out of Sync	Device entered 'holdover' then became 'out of sync' by exceeding the maximum internal time inaccuracy threshold, or through holdover timeout.[2]	Device is 'in sync' again through synchronization to an external time source.	Ensure device has a reliable external time source available.
No First Sync	Device has not synchronized to a time source since powering up.	Device has synchronized to a time source since powering up.	Ensure device has external time sources available. If sources are available, wait a few minutes to allow the device to gain synchronization.
No IRIG In	IRIG-B input signal previously sensed on at least one active IRIG-In port is no longer being sensed.	IRIG-B signal sensed on at least one IRIG input again.	If alarm is recurring, check if IRIG signal is present on the device's input with an IRIG-B Analyzer or oscilloscope.
No Valid IRIG In	IRIG-B input signal has been detected on input. Signal does not meet IRIG synchronization input requirements .[3]	IRIG-B input signal that meets synchronization input requirements detected.	If alarm is recurring, check the input signal meets IRIG-B input requirements.

...........continued			
Alarm Name	**Trigger Condition**	**Clearance Condition**	**Recommended Corrective Action**
Power Supply {A|B} (dual power supply units only)	Power supply A or B has failed.	Power supply A or B is operational again.	Contact Microchip technical support. Contacting Technical Support
No Frequency Info	Frequency adjustment information is no longer being generated from the internal oscillator due to a failure.	Frequency adjustment information is being generated again.	Contact Microchip technical support. Contacting Technical Support
Internal Loss of Comms	An internal communications failure has occurred.	Normal internal communications resumes.	Contact Microchip technical support.Contacting Technical Support
Over Temperature	Currently not implemented	—	—
Under Temperature	Currently not implemented	—	—
High Current	Currently not implemented	—	—

1 – For a satellite to be considered usable as a time source it must:

- be a GNSS satellite
- be in an enabled constellation (configurable)
- have a Signal to Noise Ratio (SNR) exceeding the SNR threshold (configurable)
- be positioned in the sky within the mask angle (configurable).

2 – Maximum inaccuracy thresholding and holdover timeout are both configurable. By default, no maximum inaccuracy thresholding and a 60s holdover timeout are used.

3 – IRIG input signal requirements:

- TTL signal over copper
- 0V logic low (±0.4V) to 5V logic high (±1V)
- DCLS IRIG-B
- Includes C37.118.1 Extensions.

Note: If any alarm persists after corrective action, contact Microchip technical support. Contacting Technical Support

11.5 Antenna Installation Troubleshooting

This section describes how to troubleshoot issues with the GridTime 3000's antenna installation.

To troubleshoot an antenna installation perform the following steps:

1. Check that the antenna has a good view of the sky.
2. Check the antenna installation for a short circuit. This can be done by following the steps found in this article.
3. Ensure the antenna installation is compatible with the GNSS Receiver Specification.
4. If none of these steps resolve the issue, contact Microchip technical support. Contacting Technical Support

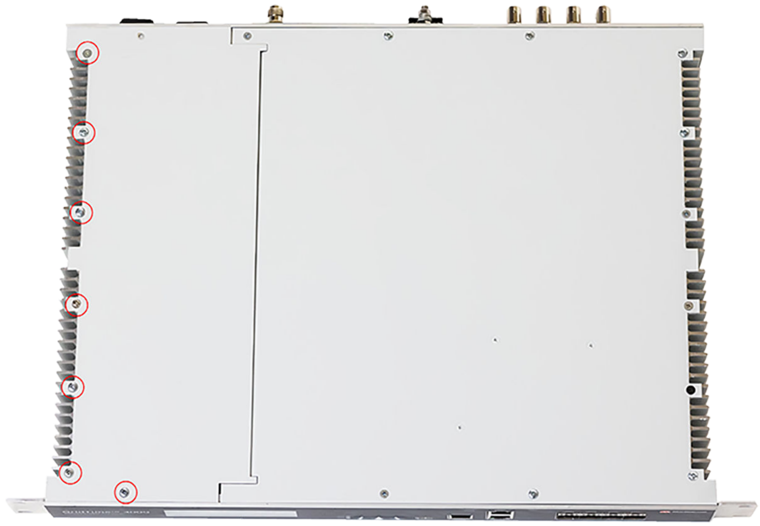
11.6 Power Supply Fuse Replacement

This section describes how to replace the fuse on a GridTime 3000 power supply.

DANGER Remove power to all of the GridTime 3000's power supplies, wait a few minutes for the power supply capacitors to discharge fully

1. Remove the power supply bay lid compartment screws highlighted in the following image.

Figure 11-1. Bay Lid Compartment Screws

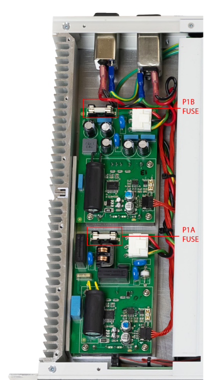


2. Remove the power supply bay lid compartment, as shown in the following image.

Figure 11-2. Removing the Bay Lid Compartment

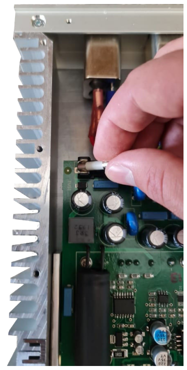
3. Locate the faulty fuse(s) in the power supply's fuse holder as shown in the following image.

Figure 11-3. Power Supply Fuse Holder



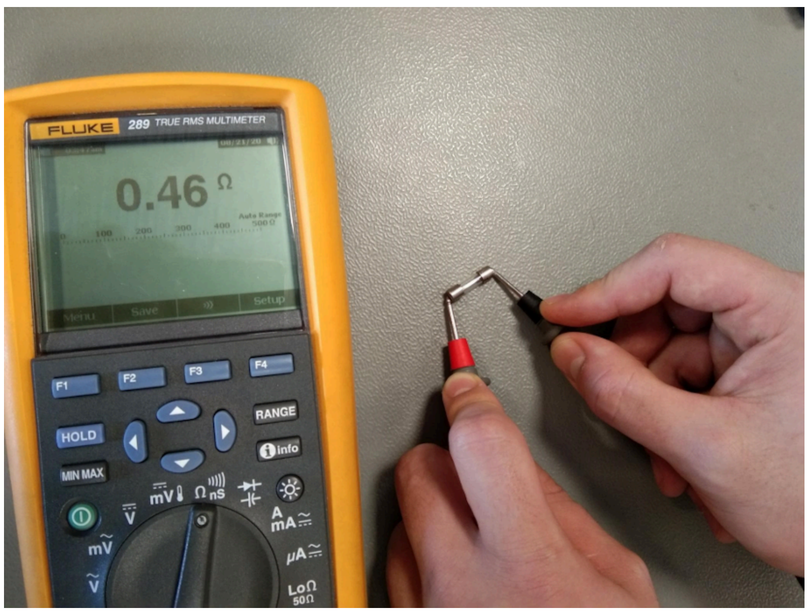
4. Remove the faulty fuse carefully from its holder as shown in the following image.

Figure 11-4. Removing the Faulty Fuse



5. Before inserting the replacement fuse into the fuse holder on the power supply, probe it with a multimeter on a resistance measurement setting to verify that it is not faulty. The resistance should be ~1Ω or less. The following image shows how to probe the fuse appropriately.

Figure 11-5. Probing the Replacement Fuse



6. Once it has been confirmed that the replacement fuse is not faulty, insert it into the power supply fuse holder where the original fuse was.
7. Replace the lid for the power supply bay compartment, and reinsert the screws.
8. Verify that the fuse replacement was successful by powering the GridTime 3000 through the applicable power supply only, and verify that it has started by checking that the front panel LCD has lit up.

11.7 Power Supply Replacement

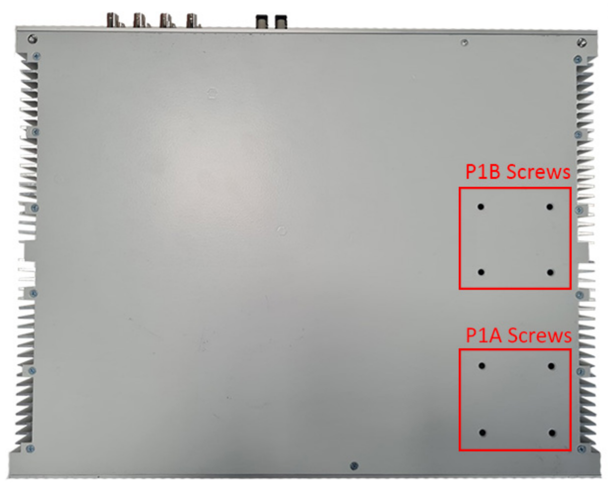
This section describes how to replace a GridTime 3000 power supply.

DANGER Remove power to all of the GridTime 3000's power supplies and wait a few minutes for the power supply capacitors to discharge fully

CAUTION Power supplies should only be replaced with the same equivalent power supply module.

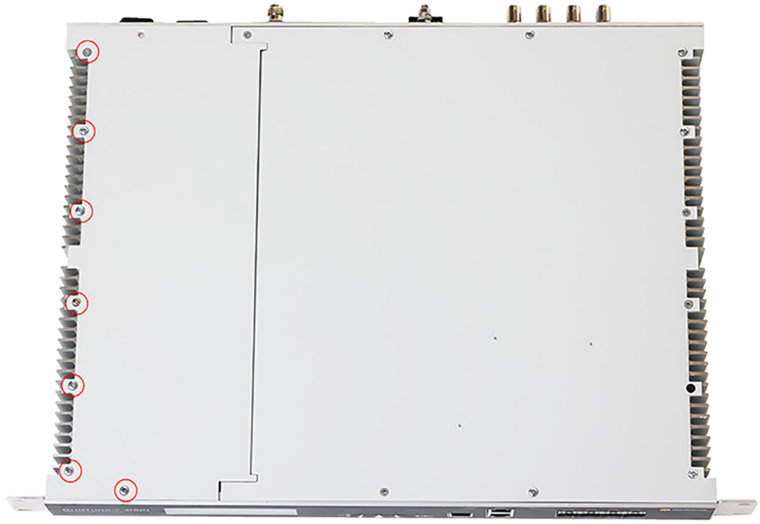
1. Remove all other cables connected to the GridTime 3000 and if rack mounted, remove it from the rack.
   Note: If both supplies are to be replaced, replace them one at a time so that the heat sink remains bolted to the chassis at all times during the operation.
2. Flip the GridTime 3000 upside down and remove the power supply screws, as shown in the following image.

Figure 11-6. Power Supply Screws



3. Once the screws are removed for the relevant power supply(s), flip the GridTime 3000 upright again.
4. Remove the power supply bay lid compartment screws as highlighted in the following figure.

Figure 11-7. Bay Lid Compartment Screws

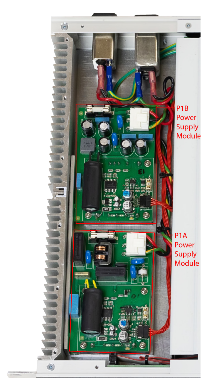


5. Remove the power supply bay lid compartment.

Figure 11-8. Removing the Bay Lid Compartment

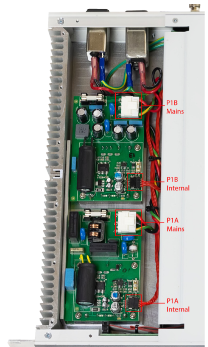
6. Identify the power supply(s) you wish to replace.

Figure 11-9. Power Supply



7. Remove the cables for the mains and internal cabling connectors to the power supply you wish to replace.

Figure 11-10. Removing the Cables and Cabling Connectors



8. Remove the old PSU module, and connect the mains and internal cabling connectors to the new PSU module in the same position and orientation as when you removed them.

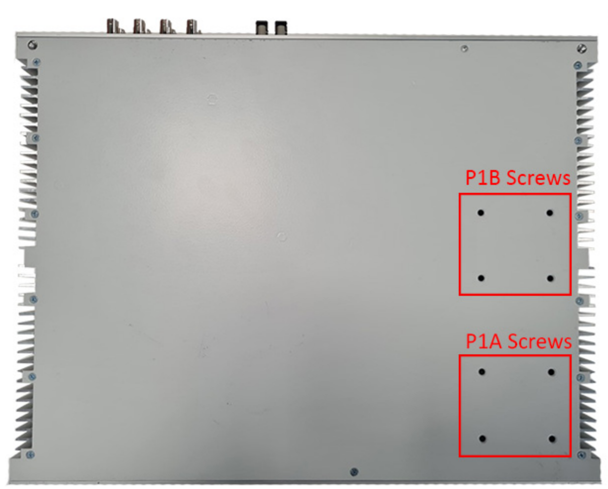
DANGER If cables are damaged before or during the replacement of the power supplies, do not connect power. Contact Microchip technical support Contacting Technical Support

---

Note: Ensure that the internal cable connector is oriented so the bevel is on the top, before inserting the connector.

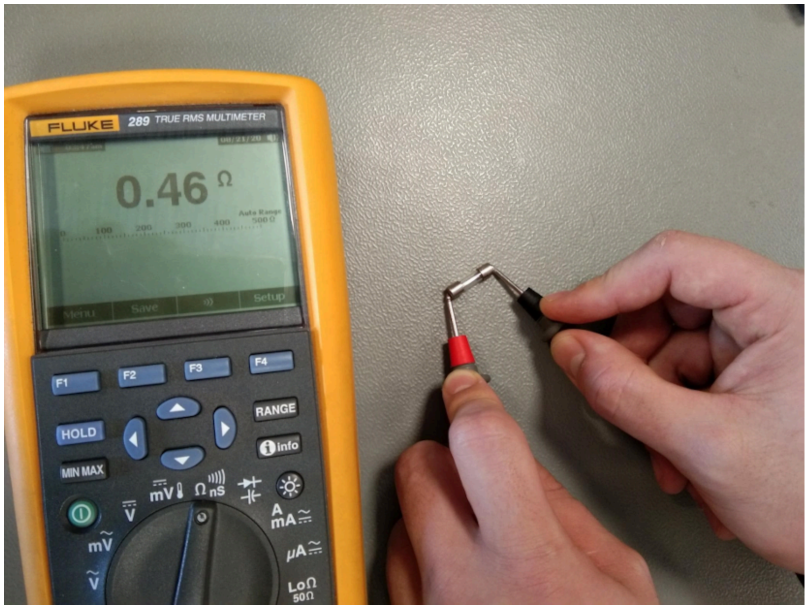
9. Hold the new PSU module in place, and carefully flip over the GridTime 3000 unit. Replace the screws holding the PSU module in place.

Figure 11-11. Power Suppy Screws



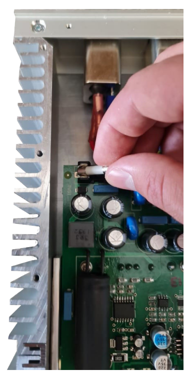
10. Flip the GridTime 3000 unit back over.
11. Retrieve a new ceramic fuse for the power supply and test it for continuity. If the fuse has a resistance of open circuit, it is faulty and a different fuse should be used, if it has a low resistance (< 1Ω) it is suitable.

Figure 11-12. Testing the New Fuse



12. Carefully place the new fuse into the power supply.

Figure 11-13. Placing the New Fuse



13. Replace the lid for the power supply bay compartment, and reinsert the screws.
14. Verify that the power supply replacement is successful by powering the GridTime 3000 through the applicable power supply, verify that it has started by checking if the front panel LCD has lit up.

11.8 Returning the GridTime 3000

This section describes under what conditions the GridTime 3000 should be returned.

You should return the equipment to Microchip only after you have exhausted the troubleshooting procedures described earlier in this chapter, or Microchip Support has advised you to return the unit.

Important: Please retain the original packaging for re-shipping the product. If the original packaging is not available, contact Microchip Support for assistance.

11.9 Manual Updates

The updated version of this manual is available for download from the Microchip web site. Manuals are provided in PDF format for ease of use. After downloading, you can view the manual on a computer or print it using Adobe Acrobat Reader.

Updated manuals are available at: microchip.com/gridtime3000.

11.10 Contacting Technical Support

This section describes how to contact Microchip technical support.

To order any accessory, contact the Microchip Sales Department. If you encounter any difficulties installing or using the product, contact Microchip Frequency and Time Systems (FTS) Services and Support:

Table 11-4. Contacting Technical Support

Region	Address	Contact Information
North and South America	Microchip, Inc. Frequency and Time Division 3870 N First Street San Jose, CA 95134-1702	• Toll-free in North America: 888-367-7966, Option 1 • Telephone: 408-428-7907 • Fax: 408-428-7998 • E-mail: SJO-FTD.Support@microchip.com OR nzp-support@microchip.com • Website: microchip.my.site.com/s/
Europe, Middle East, and Africa (EMEA)	Microchip FTD Services and Support EMEA Altlaufstrasse 42 85635 Hoehenkirchen-Siegertsbrunn Germany	• Telephone: +49 700 3288 6435 • Fax: +49 8102 8961 533 • E-mail: – SJO-FTD.Support@microchip.com OR nzp-support@microchip.com
Australia and New Zealand	Tekron International Ltd Level 1, 47 The Esplanade Lower Hutt, 5022 New Zealand	• Telephone: +64 566 7722 • Toll-free in Australia: 1 800 506 311 • E-mail: nzp-support@microchip.com

12. Appendix A: Specifications

This appendix provides specifications for the GridTime 3000 and its accessories.

12.1 Factory Hardware Options

This section specifies the hardware options the GridTime 3000 can be ordered with.

Product Code	Product Description
C-V-SG-HV	1 x GridTime 3000 , VCTCXO, Single GNSS, 1 x HV PSU
C-V-SG-HV-HV	1 x GridTime 3000 , VCTCXO, Single GNSS, 2 x HV PSU
C-V-SG-HV-LV	1 x GridTime 3000 , VCTCXO, Single GNSS, 1 x HV PSU and 1 x LV PSU
C-V-SG-LV-LV	1 x GridTime 3000 , VCTCXO, Single GNSS, 2 x LV PSU
C-V-SG-LV	1 x GridTime 3000 , VCTCXO, Single GNSS, 1 x LV PSU
C-O-SG-HV	1 x GridTime 3000 , OCXO, Single GNSS, 1 x HV PSU
C-O-SG-HV-HV	1 x GridTime 3000 , OCXO, Single GNSS, 2 x HV PSU
C-O-SG-HV-LV	1 x GridTime 3000 , OCXO, Single GNSS, 1 x HV PSU and 1 x LV PSU
C-O-SG-LV-LV	1 x GridTime 3000 , OCXO, Single GNSS, 2 x LV PSU
C-O-SG-LV	1 x GridTime 3000 , OCXO, Single GNSS, 1 x LV PSU
C-R-SG-HV	1 x GridTime 3000 , Rubidium, Single GNSS, 1 x HV PSU
C-R-SG-HV-HV	1 x GridTime 3000 , Rubidium, Single GNSS, 2 x HV PSU
C-R-SG-HV-LV	1 x GridTime 3000 , Rubidium, Single GNSS, 1 x HV PSU and 1 x LV PSU
C-R-SG-LV-LV	1 x GridTime 3000 , Rubidium, Single GNSS, 2 x LV PSU
C-R-SG-LV	1 x GridTime 3000 , Rubidium, Single GNSS, 1 x LV PSU

12.2 Software License Options

This section specifies the available software license options for the GridTime 3000.

Table 12-1. Available Software License Options

Part Number	Description
LIC-GT3K-T	GridTime 3000 2x T1/E1/J1 & 2x Fixed Frequency License
LIC-GT3K-J	GridTime 3000 8x BNC, IRIG-B, Programmable pulse, DCF-77 License
LIC-GT3K-F	GridTime 3000 2x ST Fibre IRIG-B License
LIC-GT3K-S	GridTime 3000 1x RS232, 1x RS422 Serial String License
LIC-GT3K-M	GridTime 3000 1x HV MOSFET License
LIC-GT3K-C1	GridTime 3000 1x Copper Ethernet License
LIC-GT3K-C2	GridTime 3000 2x Copper Ethernet License
LIC-GT3K-SF1	GridTim e3000 1x SFP Ethernet (1GB) License
LIC-GT3K-SF2	GridTime 3000 2x SFP Ethernet (1GB) License
LIC-GT3K-SF3	GridTime 3000 3x SFP Ethernet (1GB) License
LIC-GT3K-SF4	GridTime 3000 4x SFP Ethernet (1GB) License
LIC-GT3K-SF5	GridTime 3000 5x SFP Ethernet (1GB) License
LIC-GT3K-SF6	GridTime 3000 6x SFP Ethernet (1GB) License
LIC-GT3K-SF7	GridTime 3000 7x SFP Ethernet (1GB) License
LIC-GT3K-SF8	GridTime 3000 8x SFP Ethernet (1GB) License
LIC-GT3K-SG	GridTime 3000 10Gb License

...........continued	
Part Number	**Description**
LIC-GT3K-NTP	GridTime 3000 NTP/SNTP License
LIC-GT3K-PTP	GridTime 3000 PTP License
LIC-GT3K-PRP	GridTime 3000 PRP License
LIC-GT3K-SYNCE	GridTime 3000 SyncE License
LIC-GT3K-AUTH	GridTime 3000 Authentication License (RADIUS/LDAP)

12.3 Power Supply and Electrical Protection

This section describes the electrical specifications of the GridTime 3000's power supplies.

Table 12-2. Power Supply Electrical Specifications

Power Supply Type	Input Range		Frequency	Maximum Power Consumption
	Min	Max		
High Voltage (DC)	120VDC	250VDC	N/A	60W
High Voltage (AC)	100VAC	240VAC	50Hz/60Hz	60W
Low Voltage	24VDC	120VDC	N/A	60W

Table 12-3. Protection and Isolation Specifications

Type	Specification	
Protection	Safety earth, fuse, surge and transient suppression	
Isolation	HV Power Supply:	2.0 kV Input to Ground 3.0 kV Input to Output
	LV Power Supply:	3.0 kV Input to Ground 3.0 kV Input to Output

12.4 Mechanical Specifications

This section describes the mechanical specifications of the GridTime 3000.

Table 12-4. Mechanical Specifications

Type		Specification
External Dimensions (standard 1U case)	**Width**	430 mm (481 mm across front/rear mounts)
	Depth	330 mm
	Height	44 mm
Weight		3.76 kg
Ingress Protection		IP40
Enclosure		Aluminum, Painted and anodized
LCD Display		80x15 mm

12.5 Factory Default Settings

This section describes the factory default settings.

Table 12-5. Factory Default Settings

Port	Description	Function
LCD Screen	Real-time clock status	• Clock information and time • Alarm states • Sync states • Firmware version

...........continued		
Port	**Description**	**Function**
Alarm LED Indicator	Alarm condition	• Red LED for alarm condition
Sync LED Indicator	Sync state	• Green LED for sync state
Navigation Buttons	Screen navigation and safe shutdown of unit	• Left/Right buttons to scroll LCD screen • Centre button for safe shutdown/reboot
Ethernet Administration Port	GridTime 3000 configuration and administration	• DHCP enabled • SNMP disabled by default • RADIUS disabled by default • LDAP disabled by default
USB Administration Port	GridTime 3000 configuration and administration	• DHCP enabled (Will act as DHCP Server) • RADIUS disabled by default • LDAP disabled by default
RJ-45 Ethernet Timing Ports	Eth 1:	• DHCP enabled • NTP — Disabled by default • PTP — Disabled by default • SyncE — Disabled by default
	Eth 2:	• DHCP enabled • NTP — Disabled by default • PTP — Disabled by default • SyncE — Disabled by default
SFP Ethernet Transceiver Sockets	Eth 3:	• DHCP enabled • NTP — Disabled by default • PTP — Disabled by default • SyncE — Disabled by default
	Eth 4:	• DHCP enabled • NTP — Disabled by default • PTP — Disabled by default • SyncE — Disabled by default
	Eth 5:	• DHCP enabled • NTP — Disabled by default • PTP — Disabled by default • SyncE — Disabled by default

..........continued		
Port	**Description**	**Function**
	Eth 6:	• DHCP enabled • NTP — Disabled by default • PTP - Disabled by default • SyncE — Disabled by default
	Eth 7:	• DHCP enabled • NTP — Disabled by default • PTP — Disabled by default • SyncE — Disabled by default
	Eth 8:	• DHCP enabled • NTP — Disabled by default • PTP — Disabled by default • SyncE — Disabled by default
	Eth 9:	• DHCP enabled • NTP — Disabled by default • PTP — Disabled by default • SyncE — Disabled by default
	Eth 10:	• DHCP enabled • NTP — Disabled by default • PTP — Disabled by default • SyncE — Disabled by default
RJ-48 (T1/E1/J1)	Port 1 Port 2	• Disabled by default
BNC (Freq/DCLS IRIG-B)	Port 3	• Disabled by default
BNC (Freq/ DCLS IRIG-B)	Port 4	• Disabled by default
BNC (DCLS/AM IRIG-B)	Port 5	• Disabled by default
BNC (DCLS/AM IRIG-B)	Port 6	• Disabled by default
BNC (DCLS/AM IRIG-B)	Port 7	• Disabled by default
BNC (DCLS/AM IRIG-B)	Port 8	• Disabled by default
BNC (DCLS I/O)	Port 9	• Disabled by default
BNC (DCLS I/O)	Port 10	• Disabled by default
Serial String	Port 11 (RS422) Port 12 (RS232)	• Disabled by default
ST Optical Fibre	Port 13 Port 14	• Disabled by default
HV MOSFET	Port 15	• Disabled by default
Alarm Relay Terminal Block	Port 16 Port 17	• Alarm relays disabled by default

...........continued		
Port	**Description**	**Function**
GNSS Antenna Socket	TNC antenna connector	• GPS, GLONASS, Beidou, Galileo enabled • Cable delay 150 ns

12.6 Input and Output Electrical Specifications

This section describes the electrical specifications of the GridTime 3000's ports.

Table 12-6. Input and Output Specifications

Circuit	Connector	Voltage	Current Rating	Isolation
T1 (at 75Ω)	RJ-48	2.4V	110 mA	1.5 kV
E1 (at 75Ω)	RJ-48	2.37V	110 mA	1.5 kV
J1 (at 75Ω)	RJ-48	2.4V	110 mA	1.5 kV
1.544 MHz square wave (at 75Ω)	BNC	1.3V	17 mA	2.5 kV
1.544 MHz sinusoidal wave (at 75Ω)	BNC	1.3V	17 mA	2.5 kV
2.048 MHz square wave (at 75Ω)	BNC	1.3 V	17 mA	2.5 kV
2.048 MHz sinusoidal wave (at 75Ω)	BNC	1.3V	17 mA	2.5 kV
10 MHz square wave (at 50Ω)	BNC	1V	20 mA	2.5 kV
10 MHz sinusoidal wave (at 50Ω)	BNC	800 mV	16 mA	2.5 kV
AM IRIG-B (Modulated)	BNC	8 V	80mA	2.5 kV
DCLS IRIG-B/Pulse output	BNC	5.5 V	150 mA	2.5 kV
DCLS IRIG-B input	BNC	5 V	5 mA	2.5 kV
RS232 String	RJ-12	±3 V - ±15 V	10 mA	2.5 kV
RS422 String	RJ-12	±5 V	35 mA	2.5 kV
HV Switching	Green screw terminal—2pin	250 Vdc max	1A	3 kV
Alarm relay	Green screw terminal—6pin	250 Vdc max	100 mA	3.75 kV
Fiber	ST Fiber (multi-mode 820nm)	n/a	n/a	n/a
Administration port	RJ-45	n/a	n/a	1.5 kV
Timing ports ETH1, ETH2	RJ-45	n/a	n/a	1.5 kV

12.7 Time String Specifications

This section outlines the specifications for the GridTime 3000's time strings.

The GridTime 3000 supports 12 different time strings, which can be outputted from either its RS232 serial port (Port 12) or its RS422 serial port (Port 11).

The on-time point of each serial string is accurate to within ±50 μs of UTC.

The specifications for both serial ports are given in RS422 and RS232 Port Specifications.

Table 12-7. RS422 and RS232 Port Specifications

Port	Connector	Voltage	Current Rating	Isolation
RS422 Port	RJ-12	±5 V	35 mA	2.5 kV
RS232 Port	RJ-12	±3 V-±15 V	10 mA	2.5 kV

The content specifications for each time string are given below.

NGTS Time Code

Transmitted once per minute. Sent during the last second before the minute rollover to which the data in the string refers.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
TyyMMDDwhhmmx<CR><LF>
```

Table 12-8. NGTS Time Code Content Specification

Placeholder	Content
T	ASCII "T"
yy	Last two digits of the year: For example, "12" = the year 2012 ASCII
MM	Month: "00" = January ... "12" = December ASCII
DD	Day of month: 01 ... 31 ASCII
w	Day of week: "1" = Monday ... "7" = Sunday ASCII
hh	Two digit hour ASCII
mm	Two digit minute ASCII
x	Time mode: "0" = Local time, "1" = UTC time ASCII
<CR>	Carriage return (HEX 0D)
<LF>	Line feed (HEX 0A)

Example:

```
T020422112340<CR><LF>
```

Monday 22 April 2002 - 12:34 local time

IRIG J-17 Time Code

This code is compatible with IRIG Standard 212-00.

Transmitted once every second. The leading edge of the "start" bit of the first character <SOH> is exactly on the second that the message describes.

Default settings: 9600bps, 7-bit ASCII, odd parity.

Definition:

```
<SOH>ddd:hh:mm:ss<CR><LF>
```

Table 12-9. IRIG J-17 Time Code Content Specification

Placeholder	Content
<SOH>	Start of heading (HEX 01)
ddd	Day of year: range "001"-"366" ASCII
:	HEX 3A (colon)
hh	Hour: "00"-"23" ASCII
mm	Minute: "00"-"59" ASCII

...........continued

Placeholder	Content
ss	Second: "00"-"59" ASCII
<CR>	Carriage return (HEX 0D)
<LF>	Line feed (HEX 0A)

Example:

```
<SOH>112:12:34:36<CR><LF>
```

Day 112, time 12:34:36

String-A Time Code

This code is very similar in data content to the IRIG J-17 code, but adds a two-character field containing the year, and uses 8-bit ASCII, no parity data format.

Transmitted once per second. The leading edge of the "start" bit of the first character <SOH> is exactly on the second that the message describes.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
<SOH>ddd:hh:mm:ss:yy<CR><LF>
```

Table 12-10. String-A Content Specification

Placeholder	Content
<SOH>	Start of heading (HEX 01)
ddd	Day of year: range "001"-"366" ASCII
:	HEX 3A (colon)
hh	Hour: "00"-"23" ASCII
mm	Minute: "00"-"59" ASCII
ss	Second: "00"-"59" ASCII
yy	Year: "00"-"99" representing the last two digits of the year
<CR>	Carriage return (HEX 0D)
<LF>	Line feed (HEX 0A)

Example:

```
<SOH>112:12:34:36:10<CR><LF>
```

Day 112, time 12:34:36, year 2010

String-B Time Code

This code substitutes a "Quality" indicator byte for the year field, but otherwise is identical in form, function and timing to String-A.

Transmitted once every second. The leading edge of the "start" bit of the first character <SOH> is exactly on the second that the message describes.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
<SOH>DDD:hh:mm:ssQ<CR><LF>
```

Table 12-11. String-B Content Specification

<table>
<tr><th>Placeholder</th><th>Content</th></tr>
<tr><td><SOH></td><td>Start of heading (HEX 01)</td></tr>
<tr><td>ddd</td><td>Day of year: range "001"-"366" ASCII</td></tr>
<tr><td>:</td><td>HEX 3A (colon)</td></tr>
<tr><td>hh</td><td>Hour: "00"-"23" ASCII</td></tr>
<tr><td>mm</td><td>Minute: "00"-"59" ASCII</td></tr>
<tr><td>ss</td><td>Second: "00"-"59" ASCII</td></tr>
<tr><td>Q</td><td>
<table>
<tr><th colspan="2">Character</th><th>Meaning</th></tr>
<tr><td>HEX</td><td>ASCII</td><td></td></tr>
<tr><td>20</td><td>" " (space)</td><td>Clock in sync, timing accuracy is better then 60 ns</td></tr>
<tr><td>2E</td><td>"." (full stop)</td><td>Clock is accurate to 1 µs</td></tr>
<tr><td>2A</td><td>"*" (asterisk)</td><td>Clock is accurate to 10 µs</td></tr>
<tr><td>23</td><td>"#" (hash)</td><td>Clock is accurate to 100 µs</td></tr>
<tr><td>3F</td><td>"?" (question)</td><td>Clock accuracy may be worse than 100 µs</td></tr>
</table>
</td></tr>
<tr><td><CR></td><td>Carriage return (HEX 0D)</td></tr>
<tr><td><LF></td><td>Line feed (HEX 0A)</td></tr>
</table>

Example:

```
<SOH>112:12:34:36?<CR><LF>
```

Day 112, time 12:34:36, >100 µs sync error

String-C Time Code

This code is effectively a combination of String-A and String-B. It provides both year information and a sync indicator field.

Transmitted once every second. The leading edge of the "start" bit of the first character <CR> is exactly on the second to which the message data refers.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
<CR><LF>Q<SPACE>yy<SPACE>ddd<SPACE>hh:mm:ss.000<SPACE><SPACE><SPACE>
```

Table 12-12. String-C Content Specification

Placeholder	Content
<CR>	Carriage return (HEX 0D)
<LF>	Line feed (HEX 0A)
Q	Quality indicator: " " (space) = in sync, "?" = out of sync
<SPACE>	HEX 20
yy	Year: "00"-"99" ASCII representing the last two digits of the year
ddd	Day of year: range "001"-"366" ASCII
hh	Hour: "00"-"23" ASCII

...........continued

Placeholder	Content
mm	Minute: "00"-"59" ASCII
ss	Second: "00"-"59" ASCII
.	ASCII "." (full stop)
0	ASCII "0" (zero)

Example:

```
<CR><LF>? 02 112 12:34:36.000
```

Day 112 of year 2002, time 12:34:36, out of sync

String-D Time Code

String-D is **identical** in content to String-B, but the second mark is at the leading edge of the "start" bit of the <CR>.

Transmitted once every second. The leading edge of the "start" bit of the character <CR> is exactly on the second to which the message data refers.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
<SOH>DDD:hh:mm:ssQ<CR><LF>
```

Table 12-13. String-D Content Specification

<table>
<tr><th>Placeholder</th><th>Content</th></tr>
<tr><td><SOH></td><td>Start of heading (HEX 01)</td></tr>
<tr><td>ddd</td><td>Day of year: range "001" - "366" ASCII</td></tr>
<tr><td>:</td><td>HEX 3A (colon)</td></tr>
<tr><td>hh</td><td>Hour: "00"-"23" ASCII</td></tr>
<tr><td>mm</td><td>Minute: "00"-"59" ASCII</td></tr>
<tr><td>ss</td><td>Second: "00"-"59" ASCII</td></tr>
<tr><td>Q</td><td>
<table>
<tr><th colspan="2">Character</th><th>Meaning</th></tr>
<tr><td>HEX</td><td>ASCII</td><td></td></tr>
<tr><td>20</td><td>" " (space)</td><td>Clock in sync, timing accuracy is better then 60 ns</td></tr>
<tr><td>2E</td><td>"." (full stop)</td><td>Clock is accurate to 1 µs</td></tr>
<tr><td>2A</td><td>"*" (asterisk)</td><td>Clock is accurate to 10 µs</td></tr>
<tr><td>23</td><td>"#" (hash)</td><td>Clock is accurate to 100 µs</td></tr>
<tr><td>3F</td><td>"?" (question)</td><td>Clock accuracy may be worse than 100 µs</td></tr>
</table>
</td></tr>
<tr><td><CR></td><td>Carriage return (HEX 0D)</td></tr>
<tr><td><LF></td><td>Line feed (HEX 0A)</td></tr>
</table>

Example:

```
<SOH>112:12:34:36?<CR><LF>
```

Day 112, time 12:34:36, >100 µs sync error

String-E Time Code

This provides the time, year information, and a sync indicator field.

The string is transmitted once every second, with the leading edge of the "start" bit of the first character <SOH> exactly on the second to which the message data refers.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
<SOH>YYYY:ddd:hh:mm:ssQ<CR><LF>
```

Table 12-14. String-E Content Specification

<table>
<tr><th>Placeholder</th><th>Content</th></tr>
<tr><td><SOH></td><td>Start of heading (HEX 01)</td></tr>
<tr><td>YYYY</td><td>4-digit year</td></tr>
<tr><td>:</td><td>HEX 3A (colon)</td></tr>
<tr><td>ddd</td><td>Day of year: range "001"-"366" ASCII</td></tr>
<tr><td>hh</td><td>Hour: "00"-"23" ASCII</td></tr>
<tr><td>mm</td><td>Minute: "00"-"59" ASCII</td></tr>
<tr><td>ss</td><td>Second: "00"-"59" ASCII</td></tr>
<tr><td>Q</td><td>
<table>
<tr><th colspan="2">Character</th><th>Meaning</th></tr>
<tr><td>HEX</td><td>ASCII</td><td></td></tr>
<tr><td>20</td><td>" " (space)</td><td>Clock in sync, timing accuracy is better then 60 ns</td></tr>
<tr><td>2E</td><td>"." (full stop)</td><td>Clock is accurate to 1 µs</td></tr>
<tr><td>2A</td><td>"*" (asterisk)</td><td>Clock is accurate to 10 µs</td></tr>
<tr><td>23</td><td>"#" (hash)</td><td>Clock is accurate to 100 µs</td></tr>
<tr><td>3F</td><td>"?" (question)</td><td>Clock accuracy may be worse than 100 µs</td></tr>
</table>
</td></tr>
<tr><td><CR></td><td>Carriage return (HEX 0D)</td></tr>
<tr><td><LF></td><td>Line feed (HEX 0A)</td></tr>
</table>

Example:

```
<SOH>2004:112:12:34:36?<CR><LF>
```

Year 2004, day 112, time 12:34:36, >100 µs sync error

String-F Time Code

This string complies with the protocol required to drive Vorne type Time Displays.

The string is transmitted once every second, with the leading edge of the "start" bit of the last <BEL> character exactly on the second.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
<CR><LF>1100<CR><LF>44hhmmss<CR><LF>54ddd<CR><LF>45HHMMss<CR><LF>55DDD<CR><LF><BEL>
```

Table 12-15. String-F Content Specification

Placeholder	Content
<CR>	Carriage return (HEX 0D)
<LF>	Line feed (HEX 0A)
1	ASCII "1" (one)
0	ASCII "0" (zero)
4	ASCII "4" (four)
hh	Local hour: "00"-"23" ASCII
mm	Local minute: "00"-"59" ASCII
ss	Second: "00"-"59" ASCII
5	ASCII "5" (five)
ddd	Local day of year: "001"-"365" ASCII
HH	UTC hour: "00"-"23" ASCII
MM	UTC minute: "00"-"59" ASCII
DDD	UTC day of year: "001"-"365" ASCII
<BEL>	Bell (HEX 07)

Example:

1100

44123456

54112

45003456

55111

Local time 12:34:56, local day 112, UTC time 00:34:56, UTC day 111

String-G Time Code

This general time string is used predominantly in Europe.

The string is transmitted once every second, with the leading edge of the "start" bit of the last <ETX> exactly on the second.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
<STX>swhhmmssddMMyy<LF><CR><ETX>
```

Table 12-16. String-G Content Specification

Placeholder	Content
<STX>	Start of text (HEX 02)

<table>
<tr><th colspan="2">...........continued</th></tr>
<tr><th>Placeholder</th><th>Content</th></tr>
<tr><td>s</td><td>The "Clock Status" is an ASCII character in the range 0-9, A-F representing a single hex digit.
To interpret the value, the Hex digit should be converted to a Nibble (half a byte) and referenced against the state chart below which contains the bit position and subsequent definition ("x" is a place holder).
<table>
<tr><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Bit 0</th><th>Definition</th></tr>
<tr><td>x</td><td>x</td><td>x</td><td>0</td><td>No announcement for time change</td></tr>
<tr><td>x</td><td>x</td><td>x</td><td>1</td><td>Announcement for time change - active for an hour before</td></tr>
<tr><td>x</td><td>x</td><td>0</td><td>x</td><td>Local Standard Time (LST)</td></tr>
<tr><td>x</td><td>x</td><td>1</td><td>x</td><td>Daylight Saving Time (DST)</td></tr>
<tr><td>0</td><td>0</td><td>x</td><td>x</td><td>Time/date invalid/unknown</td></tr>
<tr><td>0</td><td>1</td><td>x</td><td>x</td><td>Time is known but clock running on oscillator - not synced</td></tr>
<tr><td>1</td><td>0</td><td>x</td><td>x</td><td>Clock is synced</td></tr>
<tr><td>1</td><td>1</td><td>x</td><td>x</td><td>Clock is synced, high accuracy</td></tr>
</table></td></tr>
<tr><td>w</td><td>The "Day of Week" is an ASCII character in the range 0-9, A-F representing a single hex digit.
To interpret the value, the Hex digit should be converted to a Nibble (half a byte) and referenced against the state chart below which contains the bit position and subsequent definition ("x" is a place holder).
<table>
<tr><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Bit 0</th><th>Definition</th></tr>
<tr><td>1</td><td>x</td><td>x</td><td>x</td><td>UTC time</td></tr>
<tr><td>x</td><td>0</td><td>0</td><td>1</td><td>Monday</td></tr>
<tr><td>x</td><td>0</td><td>1</td><td>0</td><td>Tuesday</td></tr>
<tr><td>x</td><td>0</td><td>1</td><td>1</td><td>Wednesday</td></tr>
<tr><td>x</td><td>1</td><td>0</td><td>0</td><td>Thursday</td></tr>
<tr><td>x</td><td>1</td><td>0</td><td>1</td><td>Friday</td></tr>
<tr><td>x</td><td>1</td><td>1</td><td>0</td><td>Saturday</td></tr>
<tr><td>x</td><td>1</td><td>1</td><td>1</td><td>Sunday</td></tr>
</table></td></tr>
<tr><td>hh</td><td>Hour: "00"-"23" ASCII</td></tr>
<tr><td>mm</td><td>Minute: "00" - "59" ASCII</td></tr>
<tr><td>ss</td><td>Second: "00" - "59" ASCII</td></tr>
<tr><td>dd</td><td>Day of month: "01" - "31" ASCII</td></tr>
<tr><td>mm</td><td>Month of year: "01"-"12" ASCII</td></tr>
<tr><td>yy</td><td>Year: "10"-"99" representing the last two digits of the year</td></tr>
<tr><td><LF></td><td>Line feed (HEX 0A)</td></tr>
<tr><td><CR></td><td>Carriage return (HEX 0D)</td></tr>
<tr><td><ETX></td><td>End of text (HEX 03)</td></tr>
</table>

Example:

```
<STX>E3123456170410<LF><CR><ETX>
```

Synced high accuracy, DST, no announcement, Wednesday, time 12:34:56, date 17/04/2010

String-H Time Code

Transmitted once every second. The leading edge of the "start" bit of the first character <STX> is exactly on the second that the message describes.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
<STX>D:dd.MM.yy;T:w;U:hh.mm.ss;uvxy<ETX>
```

Table 12-17. String-H Content Specification

Placeholder	Content
<STX>	Start of text (HEX 02)
D	ASCII "D"
:	HEX 3A (colon)
dd	Day of month: "01"-"31" ASCII
.	HEX 2E (full stop)
MM	Month of year: "01"-"12" ASCII
yy	Year: "10"-"99" ASCII
;	HEX 3B (semicolon)
T	ASCII "T"
w	Day of week: "1"-"7", "1" = Monday ASCII
U	ASCII "U"
hh	Hour: "00"-"23" ASCII
mm	Minute: "00"-"59" ASCII
ss	Second: "00"-"59" ASCII
u	ASCII "#" (hash) if not synchronized since last reset, or space (HEX 20) if synchronized since last reset
v	ASCII "*" (asterisk) if clock is running on local oscillator, or space (HEX 20) if clock is currently synchronized
x	ASCII "U" if UTC time, or ASCII "S" if DST, or space (HEX 20) if standard time
y	ASCII "!" (exclamation) if DST change pending, or ASCII "A" if leap second pending, or space (HEX 20) otherwise
<ETX>	End of text (HEX 03)

Example:

```
<STX>D:17.04.10;T:6;U:12.34.56;#*S!<ETX>
```

17/04/2010, Saturday, 12:34:56, out of sync, DST, DST change pending

NMEA ZDA Time Code

This string is in accordance with NMEA-0183 standard in content, but is transmitted at 9600bps by default.

Transmission is once per second. The leading edge of the "start" bit of the "$" character is exactly on the second.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
$GPZDA,hhmmss.00,dd,MM,yyyy,s,xx,YY*CC<CR><LF>
```

Table 12-18. NMEA ZDA Time Code Content Specification

Placeholder	Content
$GPZDA	ASCII "$GPZDA"
,	ASCII "," (comma)
hh	UTC hour: "00"-"23" ASCII
mm	UTC minute: "00"-"59" ASCII
ss	UTC second: "00"-"59" ASCII

...........continued	
Placeholder	Content
.00	ASCII ".00" (fullstop zero zero)
dd	UTC day of month: "01"-"31" ASCII
MM	UTC month: "01"-"12", "01" = January ASCII
yyyy	UTC year, 4 digits
s	Local time zone offset sign (positive means local time leads UTC)
xx	Local time zone offset from UTC in hours
YY	Local time zone offset from UTC in minutes
*	ASCII "*" (asterisk)
CC	2-digit hex representation of the result of XORing the 8 data bits of each character between, but not including, the "$" and "*". ("00"-"FF")
<CR>	Carriage return (HEX 0D)
<LF>	Line feed (HEX 0A)

Example:

```
$GPZDA,123456.00,23,04,2010,+,12,00* <CR><LF>
```

UTC time 12:34:56, UTC date 23 April 2010, local time offset is +12:00

NMEA RMC Time Code

This string is compatible with and defined by the NMEA-0183 standard.

Transmission is once every second. The leading edge of the "start" bit of the "$" character is exactly on the second.

Default settings: 9600bps, 8-bit ASCII, no parity.

Definition:

```
$GPRMC,hhmmss.00,a,tttt.tttt,N,ggggg.gggg,W,0.0,0.0,DDMMYY,0.0,E*CC<CR><LF>
```

Table 12-19. NMEA RMC Time Code Content Specification

Placeholder	Content
$GPRMC	ASCII "$GPRMC"
,	ASCII "," (comma)
hh	UTC hour
mm	UTC minute
ss	UTC second
.	ASCII "." (full stop)
0	ASCII "0" (zero)
a	Status: ASCII "A" = valid, ASCII "V" = invalid
tttt.tttt	Latitude (degrees, minutes): "0000.0000" - "8959.9999" ASCII
N	Latitude (north/south): ASCII "N" = north, ASCII "S" = south
ggggg.gggg	Longitude (degrees, minutes): "00000.0000" - "35959.9999" ASCII
W	Longitude (east/west): ASCII "E" = east, ASCII "W" = west
DD	UTC day of month, ASCII
MM	UTC month, ASCII
YY	UTC year: 2 digits representing the last two digits of the year, ASCII
E*	ASCII "E*" (E asterisk)

...........continued	
Placeholder	**Content**
CC	2-digit hex representation of the result of XORing the 8 data bits of each character between, but not including the "$" and "*". ("00"-"FF")
<CR>	Carriage return (HEX 0D)
<LF>	Line feed (HEX 0A)

Example:

```
$GPRMC,123456.00,A,1234.5678,S,12345.6789,E,0.0,0.0,230410,0.0,E* <CR><LF>
```

UTC time 12:34:56, valid, latitude 1234.5678 degrees south, longitude 12345.6789 degrees east, UTC date 23 April 2010

12.8 GNSS Receiver Specification

This section gives the specifications of the GNSS receiver connected to the GridTime 3000's antenna port.

Table 12-20. Supported Constellations

GPS	GLONASS	BeiDou	Galileo
L2C (1227.60 Mhz)	L2OF (1246 MHz + k×437.5kHz, k = –7,..., 5, 6)	B2I (1207.140 Mhz)	E5 b/Q (1207.140 Mhz)
L1C/A (1575.42 MHz)	L1OF (1602 MHz + k×562.5kHz, k = –7,..., 5, 6)	B1I (1561.098 MHz)	E1-B/C (1575.42 MHz)

Position Accuracy	**Horizontal**	2m
	Altitude	<18 m
Timing	**Accuracy**	<5 ns to UTC (1-sigma, clear sky)
	Jitter	±4ns, 2.5ns using dual receivers
Acquisition	**Reacquisition**	<2 s
	Hot Start	<2 s
	Cold Start	<30 s
Sensitivity	**Tracking**	-167 dBm
	Re-acquisition	-160 dBm
	Hot start	-157 dBm
	Cold start	-148 dBm
Antenna supply voltage		5 V
Antenna supply current		Typical 10-30mA (current limited to 80mA)

13. Accessories

This appendix describes the accessories and kits that you can order with GridTime 3000.

The appendix consists of the following sections:

- Antenna Kits
  - Dual Band GNSS Antenna Specification
  - Antenna Coaxial Cable Specifications
- Lightning Arrestor Kits
  - Lightning Arrestor
- In Line Amplifier

13.1 Antenna Kits

This section gives specification of the Microchip Antenna Kits.

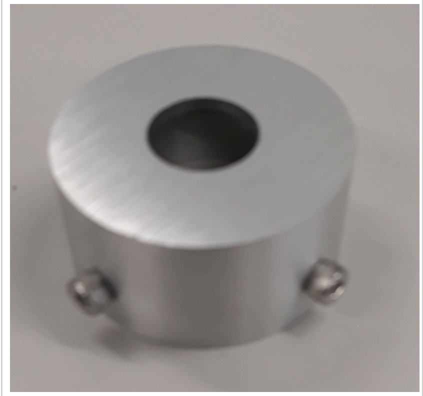
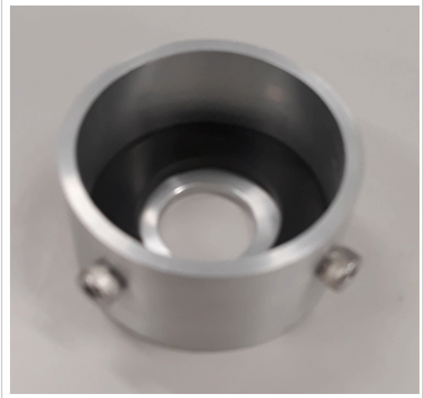
All Microchip Antenna kits include a GPS/GLONASS/Beidou/Galileo L1/L2 Antenna, a pipe mounting bracket, and a length CNT-240 cable.

The CNT-240 (LMR-240) low-loss coaxial cable in the kits comes in predefined lengths of 15m, 30m and 60m (49 ft, 98 ft, 196 ft). The L1 signal loss on a CNT-240 cable is 0.321 dB/meter and the signal loss from the available surge arrestor is less than 0.1 dB.

For a full list of the parts in the Microchip Antenna Kits, see the following table.

Table 13-1. Microchip Antenna Kit Components

Item	Details	Image
Antenna Cable CNT-240	TNC to TNC coaxial cable. Length can be 15m, 30m, 60m corresponding to each Kit.	
Antenna	Dual band GNSS antenna	

...........continued		
Item	**Details**	**Image**
Pipe Mount	Used to sit the antenna on top of the pipe	 
Antenna mount	Adjustable pipe to mount the antenna	

Each of the three Microchip Antenna Kits consists of the same components, but a different length of coaxial cable. The three different Microchip Antenna Kits are specified in the following table.

Table 13-2. Microchip Antenna Kits

Antenna Kits	Description	Order Code
Microchip 15m Antenna Kit	Dual-band timing antenna, 15m coaxial cable, adjustable mounting bracket	KIT2-ANT-15M
Microchip 30m Antenna Kit	Dual-band timing antenna, 30m coaxial cable, adjustable mounting bracket	KIT2-ANT-30M
Microchip 60m Antenna Kit	Dual-band timing antenna, 60m coaxial cable, adjustable mounting bracket	KIT2-ANT-60M

13.1.1 Dual Band GNSS Antenna Specification

This section explains the dual band GNSS antenna specifications of the Microchip antenna kits.

Table 13-3. Antenna Specification

Characteristic	Specification	
Mechanical		
Diameter	66.5 mm	
Height	47.7 mm (76.3 mm with connector)	
Weight	185g	
Form Factor	Conical Radome	
Environmental		
Operating Temperature	−40 °C to +85 °C (−40 °F to 185 °F)	
Ingress Protection	IP67	
Compliance	CE, RoHS, REACH and RED	
Shock	Vertical axis: 50G, other axes 30G	
Vibration	3 axis, sweep= 15 min, 10 to 200 Hz sweep 3G	
Salt fog / Spray	MIL-STD-810F Section 509.4	
Electrical		
Bandwidth	L2: 1213MHz-1261MHz L1: 1557MHz-1606MHz	
Overall LNA Gain	35 dB typ, 32 dB min, each of L1 and L2 Bands	
Gain Variance	3 dB max over operational temperature range	
LNA Noise Figure	2.5 dB typ at 25 °C	
VSWR	<1.5:1 typ. 1.8:1 max	
Supply Voltage Range	+2.5 to 16VDC nominal, up to 50 mV p-p ripple	
EMI Immunity	50V/meter excepting L1+/- 100 MHz and L2 +/- 100 MHz	
Supply Current	24 mA typ. At 25 °C, 25 mA max at 75 °C	
ESD Circuit protection	15 KV air discharge	
Out of Band rejection	L1 <1450 MHz >40 dB <1520 MHz >30 dB <1650 MHz >35 dB	L2 <1050 MHz >50 dB <1100 MHz >40 dB <1350 MHz >50 dB

13.1.2 Antenna Coaxial Cable Specifications

This section gives the specification of the coaxial antenna cables in the Microchip antenna kits.

Table 13-4. Antenna Cable Specifications

Characteristic	Specification
Size	AWG #16
Length	15m, 30m, 60m
Connector type	TNC
Impedance	50± 10Ω
Cable weight	50.1 Kg/Km
Installation/Operating Temperature	−40 °C ~ 85 °C (−40 °F ~ 185 °F)
UV Rating	300 Hr, ΔE ≤:3.0

13.2 Lightning Arrestor Kits

This section gives a specification for the Microchip lightning arrestor kits.

Microchip supplies two lightning arrestor kits to offer protection against lightning strikes - the Simple Lightning Protection Kit and the Lightning Protection Kit.

Both kits include a lightning arrestor and the N-type mating connectors for connecting the antenna cable to the arrestor. The Simple Lightning Protection Kit just includes these base components, whereas the Lightning Protection Kit includes additional equipment to assist with the splitting and termination of the antenna cable on either side of the arrestor. These additional components include a crimping tool and self amalgamating tape.

For a specification of each kit, see the following table.

Table 13-5. Lightning Arrestor Kits Specification

Kit	Description	Order Code
Lightning Protection Kit	Crimp tool, Lightning arrestor, N Type mating connectors and Self amalgamating tape	KIT-LPK1-COAX240
Simple Lightning Protection Kit	Lightning arrestor, N Type mating connectors	KIT-LPK2-COAX240

For a detailed specification of the lightning arrestor in each kit, see Lightning Arrestor.

13.2.1 Lightning Arrestor

This section gives the specification of the lightning arrestor in the Microchip lightning arrestor kits.

Figure 13-1. Lightning Arrestor

Table 13-6. Lightning Arrestor Specification

Characteristic	Specification
Mechanical	
Diameter	30.5 mm
Height	90 mm
Weight	104g
Type	DC Pass
Mount Type	Bulkhead Mounting
Connector Type	N-Type (Ingress and Egress)

...........continued				
Characteristic	**Specification**			
Environmental				
Temperature Range	−50 °C to +90 °C (−58 °F to 194 °F)			
Salt Fog	MIL-STD-202 Method 101D / Condition B (35 °C/48 hrs)			
Immersion	MIL-STD-202 Method 104A / Condition A (65 °C to 25 C w/NaCL – 2 cycles)			
Moisture Resistance	MIL-STD-202 Method106E (65 °C/98% RH condensing/240 hours)			
Temperature Shock	MIL-STD-202 Method107D / Condition B-1 (25 cycles -65 °C to 125 °C)			
Life	MIL-STD-202 Method 108A / Condition A (96 hours at 100 °C)			
Dust and Waterproof rating	IEC 529 – IP68			
Vibration	MIL-STD-202 Method 204D / Condition D (10Hz-2kHz 0.06” DA/20g)			
Mechanical Shock	MIL-STD-202 Method / Condition A (50g/11ms~24”)			
RF Specification				
Frequency	1.10-1.70 GHz			
VSWR	1.10 typ.			
Insertion Loss (dB)	0.10 dB typ.			
Nominal Impedance	50Ω			
Through Current	2.5A			
DC Thru Resistance	150 mΩ typ.			
RF Power	5W			
Transient Specification				
Response Time	10 ns			
Maximum Transient (IMAX)	30 kA 1x			
Multiple Strike (IN)	20 kA 10x			
Let-Through	Nominal Voltage	Maximum Voltage	Let Through Voltage	Voltage Code
	+5V	+6.7V	+8V	P05
	+12V	+15V	+18V	P12
	+24V	+30V	+39V	P24
	+48V	+55V	+80V	P48
	−48V	−64V	−90V	N48

13.3 In Line Amplifier

This section gives the specification of the In Line Amplifier, an optional accessory.

The In Line Amplifier provided by Microchip is a Tallysman TW125. This amplifier is intended to be powered by the internal power supply provided by the GNSS receiver within the GridTime 3000.

Table 13-7. In Line Amplifier Specification

Characteristic	Specification
Mechanical	
Diameter	20.0 mm
Height	59 mm
Weight	104g
Mount Type	Bulkhead Mounting
Connector Type	SMA or TNC
Environmental	

...........continued

Characteristic	Specification
Temperature Range	−40 °C to +85 °C (−40 °F to 185 °F)
Dust and Waterproof rating	IEC 529 – IP67
Electrical Specification	
Nominal Gain	25 dB +4/-0 dB typ.
Frequency	1.20-1.80 GHz
Passband Ripple	+/- 2 dB
Input VSWR	1.5 typ. / 2 max.
Output VSWR	1.5 typ. / 2 max.
Reverse Isolation	35 dB min
Noise Figure	1.5 dB max
Output 1dB	-10 dB
Output IP3	+5 dBm
Nominal Impedance	50Ω
Supply Voltage	3-10V DC
Supply Current	25 mA typ.

14. Appendix B: Third Party Software Licenses

This appendix provides the third party software licenses used by the GridTime 3000.

This product contains licensed third party software, including software available under the GPL licensing scheme. You can obtain these licenses and the open-source software by contacting Microchip Technical support at the following numbers:

- Worldwide (Main Number): 1-408-428-7907
- USA, Canada, Latin America including Caribbean, Pacific Rim including Asia, Australia and New Zealand: 1-408-428-7907
- USA toll-free: 1-888-367-7966
- Europe, Middle East & Africa: 49 700 32886435

An administrative fee may be charged to obtain the source code. By using the GridTime 3000, the user agrees to the terms of these licenses.

The licenses can be obtained using the following URL:

- www.gnu.org/licenses
- www.opensource.org/licenses/BSD-3-Clause
- www.opensource.org/licenses/BSD-2-Clause
- www.opensource.org/licenses/MIT
- www.spdx.org/licenses/bzip2-1.0.6.html
- spdx.org/licenses/ICU.html
- www.openssl.org/source/license.html
- www.openldap.org/software/release/license.html
- www.opensource.org/licenses/Artistic-1.0
- www.opensource.org/licenses/Artistic-2.0
- creativecommons.org/publicdomain/mark/1.0/
- www.zlib.net/zlib_license.html

14.1 Third Party Software

The following is a list of third-party software applications provided with the GridTime 3000

- PACKAGE NAME: base-files
  PACKAGE VERSION: 3.0.14
  RECIPE NAME: base-files
  LICENSE: GPLv2
- PACKAGE NAME: base-passwd
  PACKAGE VERSION: 3.5.29
  RECIPE NAME: base-passwd
  LICENSE: GPLv2+
- PACKAGE NAME: bash
  PACKAGE VERSION: 4.4.18
  RECIPE NAME: bash
  LICENSE: GPLv3+
- PACKAGE NAME: busybox
  PACKAGE VERSION: 1.30.1

RECIPE NAME: busybox
LICENSE: GPLv2 & bzip2

- PACKAGE NAME: busybox-hwclock
PACKAGE VERSION: 1.30.1
RECIPE NAME: busybox
LICENSE: GPLv2 & bzip2
- PACKAGE NAME: busybox-syslog
PACKAGE VERSION: 1.30.1
RECIPE NAME: busybox
LICENSE: GPLv2 & bzip2
- PACKAGE NAME: busybox-udhcpc
PACKAGE VERSION: 1.30.1
RECIPE NAME: busybox
LICENSE: GPLv2 & bzip2
- PACKAGE NAME: cryptsetup
PACKAGE VERSION: 2.1.0
RECIPE NAME: cryptsetup
LICENSE: GPL-2.0-with-OpenSSL-exception
- PACKAGE NAME: dropbear
PACKAGE VERSION: 2019.78
RECIPE NAME: dropbear
LICENSE: MIT & BSD-3-Clause & BSD-2-Clause & PD
- PACKAGE NAME: e2fsprogs-e2fsck
PACKAGE VERSION: 1.44.5
RECIPE NAME: e2fsprogs
LICENSE: GPLv2
- PACKAGE NAME: eudev
PACKAGE VERSION: 3.2.7
RECIPE NAME: eudev
LICENSE: GPLv2.0+ & LGPL-2.1+
- PACKAGE NAME: eudev-hwdb
PACKAGE VERSION: 3.2.7
RECIPE NAME: eudev
LICENSE: GPLv2.0+ & LGPL-2.1+
- PACKAGE NAME: expat
PACKAGE VERSION: 2.2.6
RECIPE NAME: expat
LICENSE: MIT
- PACKAGE NAME: firmware-imx-brcm
PACKAGE VERSION: 7.8
RECIPE NAME: firmware-imx
LICENSE: Proprietary
- PACKAGE NAME: firmware-imx-epdc

PACKAGE VERSION: 7.8
RECIPE NAME: firmware-imx
LICENSE: Proprietary

- PACKAGE NAME: glibc
  PACKAGE VERSION: 2.29
  RECIPE NAME: glibc
  LICENSE: GPLv2 & LGPLv2.1
- PACKAGE NAME: glibc-locale-en-gb
  PACKAGE VERSION: 2.29
  RECIPE NAME: glibc-locale
  LICENSE: GPLv2 & LGPLv2.1
- PACKAGE NAME: gmp
  PACKAGE VERSION: 6.1.2
  RECIPE NAME: gmp
  LICENSE: GPLv2+ | LGPLv3+
- PACKAGE NAME: gnutls
  PACKAGE VERSION: 3.6.8
  RECIPE NAME: gnutls
  LICENSE: LGPLv2.1+
- PACKAGE NAME: init-ifupdown
  PACKAGE VERSION: 1.0
  RECIPE NAME: init-ifupdown
  LICENSE: GPLv2
- PACKAGE NAME: iproute2
  PACKAGE VERSION: 4.19.0
  RECIPE NAME: iproute2
  LICENSE: GPLv2+
- PACKAGE NAME: iptables
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ebt-802-3
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ebt-ip
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ebt-log
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ebt-mark-m
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-ah
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-dnat
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-dnpt
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-dst
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-eui64
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-frag
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-hbh
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-hl
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-icmp6
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-ipv6header
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables

LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ip6t-log
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-masquerade
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-mh
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-netmap
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-redirect
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-reject
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-rt
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-snat
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-snpt
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ip6t-srh
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-ah
  PACKAGE VERSION: 1.6.2

RECIPE NAME: iptables
LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-clusterip
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-dnat
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-ecn
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-icmp
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-log
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-masquerade
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-netmap
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-realm
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-redirect
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-reject
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-snat

PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-ipt-ttl
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-ipt-ulog
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-addrtype
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-audit
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-bpf
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-cgroup
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-checksum
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-classify
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-cluster
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-comment
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-connbytes
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-connlimit
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-connmark
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-connsecmark
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-conntrack
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-cpu
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-ct
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-dccp
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-devgroup
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-dscp
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-ecn
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables

LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-esp
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-hashlimit
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-helper
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-hmark
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-idletimer
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-ipcomp
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-iprange
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-ipvs
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-led
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-length
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-limit
  PACKAGE VERSION: 1.6.2

RECIPE NAME: iptables
LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-mac
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-mangle
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-mark
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-multiport
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-nfacct
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-nflog
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-nfqueue
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-notrack
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-osf
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-owner
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-physdev

PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-pkttype
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-policy
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-quota
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-rateest
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-recent
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-rpfilter
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-sctp
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-secmark
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-set
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-socket
PACKAGE VERSION: 1.6.2
RECIPE NAME: iptables
LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-standard
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-state
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-statistic
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-string
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-synproxy
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-tcp
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-tcpmss
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-tcpoptstrip
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-tee
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-time
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-tos
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables

LICENSE: GPLv2+

- PACKAGE NAME: iptables-module-xt-tproxy
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-trace
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-u32
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-module-xt-udp
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: iptables-modules
  PACKAGE VERSION: 1.6.2
  RECIPE NAME: iptables
  LICENSE: GPLv2+
- PACKAGE NAME: json-c
  PACKAGE VERSION: 0.13.1
  RECIPE NAME: json-c
  LICENSE: MIT
- PACKAGE NAME: kernel-base
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-image
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-image-fitimage
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-image-zimage
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-8021q-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9

RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-ah4-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ah6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-arp-tables-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-arpt-mangle-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-arptable-filter-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-binfmt-misc-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-br-netfilter-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-bridge-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-bsd-comp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-can-bcm-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-can-gw-4.9.67-fslc+g953c6e30c970

PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-can-raw-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2
- PACKAGE NAME: kernel-module-crc-ccitt-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2
- PACKAGE NAME: kernel-module-crc-itu-t-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2
- PACKAGE NAME: kernel-module-crc7-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2
- PACKAGE NAME: kernel-module-echainiv-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2
- PACKAGE NAME: kernel-module-esp4-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2
- PACKAGE NAME: kernel-module-esp6-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2
- PACKAGE NAME: kernel-module-flexcan-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2
- PACKAGE NAME: kernel-module-fou-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2
- PACKAGE NAME: kernel-module-fou6-4.9.67-fslc+g953c6e30c970
PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-g-acm-ms-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-g-cdc-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-g-ether-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-g-mass-storage-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-g-ncm-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-g-serial-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-g-zero-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-gadgetfs-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-garp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-geneve-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-gre-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx

LICENSE: GPLv2

- PACKAGE NAME: kernel-module-i2c-algo-pca-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-i2c-algo-pcf-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip-gre-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip-tables-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip-vti-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6-gre-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6-tables-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6-tunnel-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6-udp-tunnel-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6-vti-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-ah-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9

RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-ip6t-eui64-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-frag-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-hbh-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-ipv6header-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-masquerade-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-mh-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-npt-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-reject-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-rpfilter-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-rt-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6t-synproxy-4.9.67-fslc+g953c6e30c970

PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-ip6table-filter-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6table-mangle-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6table-nat-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6table-raw-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ip6table-security-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ipcomp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ipcomp6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ipip-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ipt-ah-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ipt-clusterip-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2

- PACKAGE NAME: kernel-module-ipt-ecn-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ipt-masquerade-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ipt-reject-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ipt-rpfilter-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-iptable-filter-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-iptable-mangle-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-iptable-nat-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-iptable-raw-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-iptable-security-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-libcomposite-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-libcrc32c-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx

LICENSE: GPLv2

- PACKAGE NAME: kernel-module-llc-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-md5-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-mip6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-mrp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-msdos-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-mxc-mipi-csi2-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-conntrack-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-conntrack-ftp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-conntrack-ipv4-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-conntrack-ipv6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-conntrack-tftp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9

RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-nf-defrag-ipv4-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-defrag-ipv6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-dup-ipv4-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-dup-ipv6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-log-common-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-log-ipv4-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-log-ipv6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-nat-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-nat-ftp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-nat-ipv4-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-nat-ipv6-4.9.67-fslc+g953c6e30c970

PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-nf-nat-masquerade-ipv4-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-nat-masquerade-ipv6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-nat-redirect-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-nat-tftp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-reject-ipv6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nf-synproxy-core-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nfnetlink-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nfnetlink-acct-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nfnetlink-log-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-nfnetlink-queue-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2

- PACKAGE NAME: kernel-module-nls-iso8859-15-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-p8022-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ppp-async-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ppp-deflate-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ppp-generic-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ppp-synctty-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-psnap-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-sctp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-sctp-diag-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-slhc-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-spi-ad568x-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx

LICENSE: GPLv2

- PACKAGE NAME: kernel-module-spi-idt82p2282-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-spi-st7920-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-spidev-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-stp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ts-bm-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ts-fsm-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-ts-kmp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-tun-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-tunnel6-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-u-ether-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-u-serial-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9

RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-udp-tunnel-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-uio-jaguar2-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-usb-f-acm-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-usb-f-ecm-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-usb-f-ecm-subset-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-usb-f-eem-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-usb-f-fs-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-usb-f-mass-storage-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-usb-f-ncm-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2\
- PACKAGE NAME: kernel-module-usb-f-obex-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-usb-f-rndis-4.9.67-fslc+g953c6e30c970

PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-usb-f-serial-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-usb-f-ss-lb-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-userspace-consumer-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-w1-gpio-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-w1-max31826-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-wire-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xfrm-algo-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xfrm-ipcomp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xfrm-user-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xfrm4-mode-beet-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2

- PACKAGE NAME: kernel-module-xfrm4-mode-transport-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xfrm4-mode-tunnel-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xfrm4-tunnel-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xfrm6-mode-ro-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xfrm6-tunnel-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-addrtype-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-bpf-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-cgroup-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-checksum-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-classify-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-cluster-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx

LICENSE: GPLv2

- PACKAGE NAME: kernel-module-xt-comment-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-connbytes-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-connlabel-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-connlimit-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-connmark-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-conntrack-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-cpu-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-ct-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-dccp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-devgroup-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-dscp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9

RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-xt-ecn-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-esp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-hashlimit-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-helper-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-hl-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-hmark-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-idletimer-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-ipcomp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-iprange-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-l2tp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-led-4.9.67-fslc+g953c6e30c970

PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-xt-length-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-limit-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-log-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-mac-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-mark-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-multiport-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-nat-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-netmap-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-nfacct-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-nflog-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2

- PACKAGE NAME: kernel-module-xt-nfqueue-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-osf-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-owner-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-physdev-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-pkttype-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-policy-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-quota-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-rateest-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-realm-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-recent-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-redirect-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx

LICENSE: GPLv2

- PACKAGE NAME: kernel-module-xt-sctp-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-socket-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-state-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-statistic-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-string-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-tcpmss-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-tcpoptstrip-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-tee-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-time-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-tproxy-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-module-xt-trace-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9

RECIPE NAME: linux-fslc-imx
LICENSE: GPLv2

- PACKAGE NAME: kernel-module-xt-u32-4.9.67-fslc+g953c6e30c970
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: kernel-modules
  PACKAGE VERSION: 4.9-1.0.x+gitAUTOINC+953c6e30c9
  RECIPE NAME: linux-fslc-imx
  LICENSE: GPLv2
- PACKAGE NAME: keyutils
  PACKAGE VERSION: 1.5.9
  RECIPE NAME: keyutils
  LICENSE: GPLv2
- PACKAGE NAME: kmod
  PACKAGE VERSION: 26
  RECIPE NAME: kmod
  LICENSE: GPL-2.0+ & LGPL-2.1+
- PACKAGE NAME: libacl
  PACKAGE VERSION: 2.2.52
  RECIPE NAME: acl
  LICENSE: LGPLv2.1+
- PACKAGE NAME: libaio
  PACKAGE VERSION: 0.3.111
  RECIPE NAME: libaio
  LICENSE: LGPLv2.1+
- PACKAGE NAME: libattr
  PACKAGE VERSION: 2.4.47
  RECIPE NAME: attr
  LICENSE: LGPLv2.1+
- PACKAGE NAME: libcap
  PACKAGE VERSION: 2.26
  RECIPE NAME: libcap
  LICENSE: BSD | GPLv2
- PACKAGE NAME: libcomerr
  PACKAGE VERSION: 1.44.5
  RECIPE NAME: e2fsprogs
  LICENSE: GPLv2 & LGPLv2 & BSD & MIT
- PACKAGE NAME: libcrypto
  PACKAGE VERSION: 1.1.1g
  RECIPE NAME: openssl
  LICENSE: openssl
- PACKAGE NAME: libdevmapper

PACKAGE VERSION: 2.03.02
RECIPE NAME: libdevmapper
LICENSE: GPLv2 & LGPLv2.1

- PACKAGE NAME: libe2p
PACKAGE VERSION: 1.44.5
RECIPE NAME: e2fsprogs
LICENSE: GPLv2 & LGPLv2 & BSD & MIT
- PACKAGE NAME: libelf
PACKAGE VERSION: 0.176
RECIPE NAME: elfutils
LICENSE: GPLv2 | LGPLv3+
- PACKAGE NAME: libext2fs
PACKAGE VERSION: 1.44.5
RECIPE NAME: e2fsprogs
LICENSE: GPLv2 & LGPLv2 & BSD & MIT
- PACKAGE NAME: libgcc
PACKAGE VERSION: 8.3.0
RECIPE NAME: libgcc
LICENSE: GPL-3.0-with-GCC-exception
- PACKAGE NAME: libgcrypt
PACKAGE VERSION: 1.8.4
RECIPE NAME: libgcrypt
LICENSE: LGPLv2.1+
- PACKAGE NAME: libgpg-error
PACKAGE VERSION: 1.35
RECIPE NAME: libgpg-error
LICENSE: GPLv2+ & LGPLv2.1+
- PACKAGE NAME: libgpiod
PACKAGE VERSION: 1.3
RECIPE NAME: libgpiod
LICENSE: LGPLv2.1+
- PACKAGE NAME: libgpiod-tools
PACKAGE VERSION: 1.3
RECIPE NAME: libgpiod
LICENSE: LGPLv2.1+
- PACKAGE NAME: libicudata
PACKAGE VERSION: 63.1
RECIPE NAME: icu
LICENSE: ICU
- PACKAGE NAME: libicui18n
PACKAGE VERSION: 63.1
RECIPE NAME: icu
LICENSE: ICU

- PACKAGE NAME: libicuuc
  PACKAGE VERSION: 63.1
  RECIPE NAME: icu
  LICENSE: ICU
- PACKAGE NAME: libidn2
  PACKAGE VERSION: 2.0.5
  RECIPE NAME: libidn2
  LICENSE: (GPLv2+ | LGPLv3)
- PACKAGE NAME: libkmod
  PACKAGE VERSION: 26
  RECIPE NAME: kmod
  LICENSE: LGPL-2.1+
- PACKAGE NAME: libmnl
  PACKAGE VERSION: 1.0.4
  RECIPE NAME: libmnl
  LICENSE: LGPLv2.1+
- PACKAGE NAME: libpcre
  PACKAGE VERSION: 8.43
  RECIPE NAME: libpcre
  LICENSE: BSD
- PACKAGE NAME: libssl
  PACKAGE VERSION: 1.1.1g
  RECIPE NAME: openssl
  LICENSE: openssl
- PACKAGE NAME: libstdc++
  PACKAGE VERSION: 8.3.0
  RECIPE NAME: gcc-runtime
  LICENSE: GPL-3.0-with-GCC-exception
- PACKAGE NAME: libudev
  PACKAGE VERSION: 3.2.7
  RECIPE NAME: eudev
  LICENSE: LGPL-2.1+
- PACKAGE NAME: libunistring
  PACKAGE VERSION: 0.9.10
  RECIPE NAME: libunistring
  LICENSE: LGPLv3+ | GPLv2
- PACKAGE NAME: libusb1
  PACKAGE VERSION: 1.0.22
  RECIPE NAME: libusb1
  LICENSE: LGPLv2.1+
- PACKAGE NAME: libxcrypt
  PACKAGE VERSION: 4.4.2
  RECIPE NAME: libxcrypt

LICENSE: LGPLv2.1

- PACKAGE NAME: linux-firmware-imx-sdma-imx7d
  PACKAGE VERSION: 20190815
  RECIPE NAME: linux-firmware
  LICENSE: Firmware-imx-sdma_firmware
- PACKAGE NAME: linux-firmware-imx-sdma-license
  PACKAGE VERSION: 20190815
  RECIPE NAME: linux-firmware
  LICENSE: Firmware-imx-sdma_firmware
- PACKAGE NAME: locale-base-en-gb
  PACKAGE VERSION: 2.29
  RECIPE NAME: glibc-locale
  LICENSE: GPLv2 & LGPLv2.1
- PACKAGE NAME: locale-base-en-us
  PACKAGE VERSION: 2.29
  RECIPE NAME: glibc-locale
  LICENSE: GPLv2 & LGPLv2.1
- PACKAGE NAME: logrotate
  PACKAGE VERSION: 3.15.0
  RECIPE NAME: logrotate
  LICENSE: GPLv2
- PACKAGE NAME: lrzsz
  PACKAGE VERSION: 0.12.20
  RECIPE NAME: lrzsz
  LICENSE: GPLv2+
- PACKAGE NAME: lsof
  PACKAGE VERSION: 4.91
  RECIPE NAME: lsof
  LICENSE: BSD
- PACKAGE NAME: lvm2
  PACKAGE VERSION: 2.03.02
  RECIPE NAME: lvm2
  LICENSE: GPLv2 & LGPLv2.1
- PACKAGE NAME: lvm2-scripts
  PACKAGE VERSION: 2.03.02
  RECIPE NAME: lvm2
  LICENSE: GPLv2 & LGPLv2.1
- PACKAGE NAME: lvm2-udevrules
  PACKAGE VERSION: 2.03.02
  RECIPE NAME: lvm2
  LICENSE: GPLv2 & LGPLv2.1
- PACKAGE NAME: modutils-initscripts
  PACKAGE VERSION: 1.0

RECIPE NAME: modutils-initscripts
LICENSE: PD

- PACKAGE NAME: ncurses-libncurses
PACKAGE VERSION: 6.1+20181013
RECIPE NAME: ncurses
LICENSE: MIT
- PACKAGE NAME: ncurses-libtinfo
PACKAGE VERSION: 6.1+20181013
RECIPE NAME: ncurses
LICENSE: MIT
- PACKAGE NAME: ncurses-terminfo-base
PACKAGE VERSION: 6.1+20181013
RECIPE NAME: ncurses
LICENSE: MIT
- PACKAGE NAME: netbase
PACKAGE VERSION: 5.6
RECIPE NAME: netbase
LICENSE: GPLv2
- PACKAGE NAME: nettle
PACKAGE VERSION: 3.4.1
RECIPE NAME: nettle
LICENSE: LGPLv3+ | GPLv2+
- PACKAGE NAME: nginx
PACKAGE VERSION: 1.15.7
RECIPE NAME: nginx
LICENSE: CLOSED
- PACKAGE NAME: nodejs
PACKAGE VERSION: 10.15.3
RECIPE NAME: nodejs
LICENSE: MIT & BSD & Artistic-2.0
- PACKAGE NAME: ntpdate
PACKAGE VERSION: 4.2.8p13
RECIPE NAME: ntp
LICENSE: NTP
- PACKAGE NAME: openldap
PACKAGE VERSION: 2.4.47
RECIPE NAME: openldap
LICENSE: OpenLDAP
- PACKAGE NAME: openldap-bin
PACKAGE VERSION: 2.4.47
RECIPE NAME: openldap
LICENSE: OpenLDAP
- PACKAGE NAME: openssl-bin

PACKAGE VERSION: 1.1.1g
RECIPE NAME: openssl
LICENSE: openssl

- PACKAGE NAME: openssl-conf
PACKAGE VERSION: 1.1.1g
RECIPE NAME: openssl
LICENSE: openssl
- PACKAGE NAME: packagegroup-base
PACKAGE VERSION: 1.0
RECIPE NAME: packagegroup-base
LICENSE: MIT
- PACKAGE NAME: packagegroup-base-ipv6
PACKAGE VERSION: 1.0
RECIPE NAME: packagegroup-base
LICENSE: MIT
- PACKAGE NAME: packagegroup-base-usbgadget
PACKAGE VERSION: 1.0
RECIPE NAME: packagegroup-base
LICENSE: MIT
- PACKAGE NAME: packagegroup-base-usbhost
PACKAGE VERSION: 1.0
RECIPE NAME: packagegroup-base
LICENSE: MIT
- PACKAGE NAME: packagegroup-core-boot
PACKAGE VERSION: 1.0
RECIPE NAME: packagegroup-core-boot
LICENSE: MIT
- PACKAGE NAME: packagegroup-core-ssh-dropbear
PACKAGE VERSION: 1.0
RECIPE NAME: packagegroup-core-ssh-dropbear
LICENSE: MIT
- PACKAGE NAME: packagegroup-distro-base
PACKAGE VERSION: 1.0
RECIPE NAME: packagegroup-base
LICENSE: MIT
- PACKAGE NAME: packagegroup-machine-base
PACKAGE VERSION: 1.0
RECIPE NAME: packagegroup-base
LICENSE: MIT
- PACKAGE NAME: perl
PACKAGE VERSION: 5.28.1
RECIPE NAME: perl
LICENSE: Artistic-1.0 | GPL-1.0+

- PACKAGE NAME: perl-module-config-heavy
  PACKAGE VERSION: 5.28.1
  RECIPE NAME: perl
  LICENSE: Artistic-1.0 | GPL-1.0+
- PACKAGE NAME: popt
  PACKAGE VERSION: 1.16
  RECIPE NAME: popt
  LICENSE: MIT
- PACKAGE NAME: procps
  PACKAGE VERSION: 3.3.15
  RECIPE NAME: procps
  LICENSE: GPLv2+ & LGPLv2+
- PACKAGE NAME: pv
  PACKAGE VERSION: 1.6.6
  RECIPE NAME: pv
  LICENSE: Artistic-2.0
- PACKAGE NAME: run-postinsts
  PACKAGE VERSION: 1.0
  RECIPE NAME: run-postinsts
  LICENSE: MIT
- PACKAGE NAME: shadow
  PACKAGE VERSION: 4.6
  RECIPE NAME: shadow
  LICENSE: BSD | Artistic-1.0
- PACKAGE NAME: shadow-base
  PACKAGE VERSION: 4.6
  RECIPE NAME: shadow
  LICENSE: BSD | Artistic-1.0
- PACKAGE NAME: shadow-securetty
  PACKAGE VERSION: 4.6
  RECIPE NAME: shadow-securetty
  LICENSE: MIT
- PACKAGE NAME: sysvinit
  PACKAGE VERSION: 2.88dsf
  RECIPE NAME: sysvinit
  LICENSE: GPLv2+
- PACKAGE NAME: sysvinit-inittab
  PACKAGE VERSION: 2.88dsf
  RECIPE NAME: sysvinit-inittab
  LICENSE: GPLv2
- PACKAGE NAME: sysvinit-pidof
  PACKAGE VERSION: 2.88dsf
  RECIPE NAME: sysvinit

LICENSE: GPLv2+

- PACKAGE NAME: thin-provisioning-tools
PACKAGE VERSION: 0.7.6
RECIPE NAME: thin-provisioning-tools
LICENSE: GPLv3
- PACKAGE NAME: tzdata
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-africa
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-americas
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-antarctica
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-arctic
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-asia
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-atlantic
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-australia
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-core
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-europe
PACKAGE VERSION: 2019c

RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause

- PACKAGE NAME: tzdata-misc
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-pacific
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-posix
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: tzdata-right
PACKAGE VERSION: 2019c
RECIPE NAME: tzdata
LICENSE: PD & BSD & BSD-3-Clause
- PACKAGE NAME: u-boot-fslc
PACKAGE VERSION: v2019.07+gitAUTOINC+ca0ab15271
RECIPE NAME: u-boot-fslc
LICENSE: GPLv2+
- PACKAGE NAME: udev-rules-imx
PACKAGE VERSION: 1.0
RECIPE NAME: udev-rules-imx
LICENSE: MIT
- PACKAGE NAME: update-alternatives-opkg
PACKAGE VERSION: 0.4.0
RECIPE NAME: opkg-utils
LICENSE: GPLv2+
- PACKAGE NAME: update-rc.d
PACKAGE VERSION: 0.8
RECIPE NAME: update-rc.d
LICENSE: GPLv2+
- PACKAGE NAME: usbutils
PACKAGE VERSION: 010
RECIPE NAME: usbutils
LICENSE: GPLv2+
- PACKAGE NAME: util-linux-libblkid
PACKAGE VERSION: 2.32.1
RECIPE NAME: util-linux
LICENSE: GPLv2+ & LGPLv2.1+ & BSD
- PACKAGE NAME: util-linux-libuuid

PACKAGE VERSION: 2.32.1
RECIPE NAME: util-linux
LICENSE: GPLv2+ & LGPLv2.1+ & BSD

- PACKAGE NAME: util-linux-sulogin
  PACKAGE VERSION: 2.32.1
  RECIPE NAME: util-linux
  LICENSE: GPLv2+ & LGPLv2.1+ & BSD
- PACKAGE NAME: zlib
  PACKAGE VERSION: 1.2.11
  RECIPE NAME: zlib
  LICENSE: Zlib

15. Appendix C: Crimping Connectors

This appendix describes how to crimp connectors for the cables used by the GridTime 3000.

15.1 Crimping the DC Connector

This section describes how to crimp a cable with the connector for the GridTime 3000's low voltage power supply.

1. Strip the wire exposing 8 mm of copper.
2. Place the crimp into the crimping tool die in the correct orientation, with the crimping tool jaws open.
3. Ensure the insulation crimp and wire crimps are located in the die correctly and the rest of the crimp terminal will clear the die when the jaw is closed.
4. Close the crimp tool so it holds the crimp in place, and no further.
5. Fit the crimped wire into the crimp. Make sure the wires are pointing straight and the insulation does not exceed past the insulation clamp.
6. Squeeze the tool to start the crimping process, and check the wire is sitting straight in the tool.
7. Complete the process by applying pressure to the tool and closing the crimp.
8. Remove the completed crimp and test it is securely fastened. You should be able to hold the end of the crimped terminal and the wire, and be unable to pull it apart. It should not move or break the wire.

Figure 15-1. Alignment Of the Wire in the Crimp

9. Push the completed crimped wire into the housing.
10. Check that it is securely fitted by holding the housing and the wire and try to pull it apart. It should not move or break the wire.

15.2 Crimping the AC Connector

This section describes how to crimp a cable with the connector for the GridTime 3000's high voltage power supply.

1. Strip the wire exposing 8 mm of copper.
2. Lie the copper wire under the screw of the crimp.
3. Tighten the screw of the crimp so it is held fast. You should be able to hold the end of the crimped terminal and the wire and try to pull it apart. It should not move or break the wire.

Figure 15-2. Screw Holding Copper in Place

4. Insert the crimp into socket and press firmly into place.
5. Repeat steps 1 through 3 for the other two wires.
6. Add the wire clamp, fastening the two screws.

Figure 15-3. Wire Clamp Added to Hold Wires in Place

7. Add rubber strain relief.

Figure 15-4. Rubber Strain Relief

8. Clip the second half of the housing in place and fasten the screw.

Figure 15-5. Assembled Connector

16. Appendix D: Protocol Implementation Conformance Statement (PICS)

16.1 IEEE C37.238-2017 PICS

The capabilities and options supported by GridTime 3000 for IEC C37.238-2017 profile under PTP configuration settings.

Conventions:

- The **Base** column reflects the definitions and specifications in the base standard.
- The **Functional Specification (F/S)** column refers to IEEE Std C37.238. Each entry in this column is chosen from the following list:
  - **mandatory (m)**: the base standard mandates this capability and it is implemented
  - **optional (o)**: the base standard leaves this capability optional, but it is implemented
  - **Out-of-scope (i)**: Indicates that the specification is not applicable

PICS Proforma Reference	Capability	Base	F/S	Support
CLOCK_TYPE_OC	Clock is OC according to this base	AtLeastOne(1)	AtLeastOne(1)	True
CLOCK_TYPE_TC	Clock is TC according to this base	AtLeastOne(1)	AtLeastOne(1)	False
CLOCK_TYPE_BC	Clock is BC according to this base	AtLeastOne(1)	AtLeastOne(1)	True
TIMERECEIVER_ONLY	Clock is ordinary clock that is not grandmaster capable	AtLeastOne(1)	AtLeastOne(1)	False
REDBOX_DATC	Redbox is TC	AtLeastOne(1)	AtLeastOne(1)	False
REDBOX_DABC	Redbox is BC	AtLeastOne(1)	AtLeastOne(1)	False
AtLeastOne(1): at least one shall be supported				

Table 16-1. PICS for Ordinary Clocks

PICS Proforma Reference	Capability	Base	F/S	Support
NR_PORTS	Number of clock ports (total)	integer>0	1	10
PORTS_STEP.1	All ports support 1-step on egress	OnlyOne(1)	OnlyOne(1)	False
PORTS_STEP.2	All ports support 2-step on egress	OnlyOne(1)	OnlyOne(1)	False
PORTS_STEP.3	All ports support 1-step and 2-step on egress	OnlyOne(1)	OnlyOne(1)	True
TIME_TRACEABLE	Connectable to a time reference outside of PTP (Example: GPS)	o	m	True
FREQ_TRACEABLE	Connectable to a frequency reference outside of PTP (Example: GPS)	o	m	True
ATOI	Supports ATOI TLV as specified in IEC 61588:2009 | IEEEE std 1588-2008, 16.3	o	m	True

...........continued				
PICS Proforma Reference	**Capability**	**Base**	**F/S**	**Support**
PPS	Clock has a 1 PPS output	o	o	True
ACCURACY	Design value of clockAccuracy. Specified in nanoseconds	o	o	100 ns
238_TLV_GMID	238 TLV: GMID	i	o	True
238_TLV_TI	238 TLV: Total time inaccuracy	i	m	True
PDELAY_SUPPORT	Pdelay support for downstream IEDs	i	m	True
PDELAY_DOMAIN	Indicates if the implementation accepts a Pdelay_Req with any Domain Number	i	o	False
TIMETRANSMITTER_ONLY	TimeReceiver not supported	i	o	False
MAX_DEVICE_INACCURACY	Maximum device inaccuracy. Shall be specified in nanoseconds	m	m	100 ns
Management Information Support				
MIB_SNMP	Supports MIB of IEC 62439-3:2016, Annex E	o	AtLeastOne(2)	False
MIB_61850	Supports IEC TR 61859-90-4 Clock Objects	o	AtLeastOne(2)	False
MIB_OTHER	Clock supports fixed values or a mechanism defined by the manufacturer (if True, this list is appended to this PICS)	o	AtLeastOne(2)	True
IEC 62439-3 Support				
DAC	Doubly attached	o	o	True
PORTS_PAIRED	Paired clock ports for redundancy ((Example: {3-4}). Must specify the list of paired ports	o	o	True
OnlyOne(1): only one shall be supported. At least one shall be supported.				
AtLeastOne(2): at least one shall be implemented				

Table 16-2. PICS for Boundary Clocks

PICS Proforma Reference	Capability	Base	F/S	Support
NR_PORTS	Number of clock ports (total)	integer>0	integer>=2	10
PORTS_STEP.1	All ports support 1-step on egress	OnlyOne(1)	OnlyOne(1)	False
PORTS_STEP.2	All ports support 2-step on egress	OnlyOne(1)	OnlyOne(1)	False
PORTS_STEP.3	All ports support 1-step and 2-step on egress	OnlyOne(1)	OnlyOne(1)	True

...........continued

PICS Proforma Reference	Capability	Base	F/S	Support
TIME_TRACEABLE	Connectable to a time reference outside of PTP (Example: GPS)	o	m	True
FREQ_TRACEABLE	Connectable to a frequency reference outside of PTP (Example: GPS)	o	m	True
ATOI	Supports ATOI TLV as specified in IEC 61588:2009 | IEEE std 1588-2008, 16.3	o	m	True
PPS	Clock has a1 PPS output	o	o	True
ACCURACY	Design value of clockAccuracy. Specified in nanoseconds.	o	o	100 ns
238_TLV_GMID	237 TLV: gmID	i	o	True
238_TLV_TI	238 TLV: Total time inaccuracy	i	m	True
PDELAY_SUPPORT	Pdelay support for downstream IEDs	i	m	True
PDELAY_DOMAIN	Indicates if the implementation accepts a Pdelay_Req with any Domain Number	i	o	False
TIMETRANSMITTER_ONLY	TimeReceiver not supported	i	o	False
MAX_DEVICE_INACCURACY	Maximum device inaccuracy. Shall be specified in nanoseconds.	m	m	100 ns
Management Information Support				
MIB_SNMP	Supports MIB of IEC 62439-3:2016, Annex E	o	AtLeastOne(2)	False
MIB_61850	Supports IEC TR 61859-90-4 Clock Objects	o	AtLeastOne(2)	False
MIB_OTHER	Clock supports fixed values or a mechanism defined by the manufacturer (if True, this list is appended to this PICS)	o	AtLeastOne(2)	True
IEC 62439-3 Support				
DAC	Doubly attached	o	o	True
PORTS_PAIRED	Paired clock ports for redundancy ((Example: {3-4}). Must specify the list of paired ports	o	o	True

OnlyOne(1): only one shall be supported. At least one shall be supported.

AtLeastOne(2): at least one shall be implemented

...........continued				
PICS Proforma Reference	Capability	Base	F/S	Support
Following notes are for Ordinary clock **(OC)** and Boundary clock **(BC)**				
Note: ***NR_PORTS*** - Port functionality is determined by the number of licenses purchased, with a maximum of 10 Ethernet timing ports available for use. Each port require individual license.				
Note: ***DAC*** - Configuration allows for up to 5 pairs, requiring a PRP license for base functionality and 2 port licenses for each pair.				
Note: ***PORTS_PAIRED* -** Configuration allows for up to 5 pairs, requiring a PRP license for base functionality and 2 port licenses for each pair.				
Note: ***MIB_OTHER* -** Support mechanism is defined by the manufacturer provided Management Information Base (MIB).				
Note: ***PPS* -** Supported rear panel ports can be configured to deliver 1PPS output				
Note: 6:need to be investigated				

16.2 IEC/IEEE 61850-9-3:2016 PICS

The capabilities and options supported by GridTime 3000 for IEC 61850-9-3 profile under PTP configuration settings.

Conventions:

- The **Base** column reflects the definitions and specifications in the base standard. Each entry in this column is chosen from the following list:
  - **mandatory (m)**: the base standard mandates this capability and it is implemented;
  - **optional (o)**: the base standard leaves this capability optional, but it is implemented.
- The **Condition** column reflects the condition(s) for the capability. Each entry in this column is chosen from the following list:
  - **conditionally supported (c)**: this capability is supported under the conditions specified at the end of the table.
  - **unconditionally supported (–)**: this capability is not constrained.

PICS Proforma reference	Capability	Value Range	Base	Condition	Support
CLOCK_TYPE_OC	Clock is OC according to this base	True, False	m	c.1	True
CLOCK_TYPE_TC	Clock is TC according to this base	True, False	m	c.1	False
CLOCK_TYPE_BC	Clock is BC according to this base	True, False	m	c.1	True
NR_PORTS	Number of clock ports (total)	integer > 0	m	—	10
PORTS_STEP	1: All ports support 1-step on egress 2: All ports support 2-step on egress 3: All ports support both 1-step and 2-step	1...3	m	—	{3}
TIMRECEIVER_ONLY	All ports of the clock are timeReceiver-only	True, False	m	c.2	False

...........continued

PICS Proforma reference	Capability	Value Range	Base	Condition	Support
TIME_TRACEABLE	Connectable to a time reference outside of PTP (Example: GPS)	True, False	m	c.3	True
FREQ_TRACEABLE	Connectable to a frequency reference outside of PTP (Example: GPS)	True, False	m	c.3	True
DAC	double attached OC	True, False	o	—	True
PORTS_PAIRED	Paired clock ports for redundancy (Example: {3-4})	identifier pair	o	c.4	5
REDBOX_DATC	Redbox as TC	True, False	o	c.5	N/A
REDBOX_SLTC	Redbox as stateless TC	True, False	o	c.5	N/A
REDBOX_TWBC	Redbox as three-way BC	True, False	o	c.6	N/A
REDBOX_DABC	Redbox as DAC BC	True, False	o	c.6	N/A
MIB_SNMP	Support MIB of IEC 62439-3:2016, Annex E	True, False	m	c.7	False
MIB_61850	Support IEC TR 61850-90-4 Clock Objects	True, False	m	c.7	False
MIB_OTHER	Clock supports fixed values or a mechanism defined by the manufacturer (if True, this list is appended to this PICS)	True, False	m	c.7	True
ATOI	Supports ATOI TLV as specified in IEC 61588:2009 | IEEE Std 1588-2008, 16.3	True, False	o	—	True
PPS	Clock has a 1 PPS output	True, False	o	—	True
ACCURACY	Design value of clockAccuracy	nanoseconds	o	—	100 ns

...........continued

PICS Proforma reference	Capability	Value Range	Base	Condition	Support

c.1: at least one shall be supported (CLOCK_TYPE_OC and CLOCK_TYPE_ TC may be both True)

c.2: only if CLOCK_TYPE_OC = True

c.3: only if TIMERECEIVER_ONLY = False

c.4: shall be “m” (>1) if DAC = True

c.5: support shall only be declared if CLOCK_TYPE_TC = True and DAC=True

c.6: support shall only be declared if CLOCK_TYPE_BC = True and DAC=True

c.7:at least one shall be supported

Note: ***NR_PORTS*** - Port functionality is determined by the number of licenses purchased, with a maximum of 10 Ethernet timing ports available for use. Each port require individual license.

Note: ***DAC*** - Configuration allows for up to 5 pairs, requiring a PRP license for base functionality and 2 port licenses for each pair.

Note: ***PORTS_PAIRED*** **-** Configuration allows for up to 5 pairs, requiring a PRP license for base functionality and 2 port licenses for each pair.

Note: ***MIB_OTHER*** **-** Support mechanism is defined by the manufacturer provided Management Information Base (MIB).

Note: ***PPS*** **-** Supported rear panel ports can be configured to deliver 1PPS output

Note: 6:need to be investigated

16.3 IEC 62439-3:2016 Clock Profile Conformance Statement

The capabilities and options supported by GridTime 3000 for IEC 62439-3 profile under PTP configuration settings.

PICS Reference	Capability	Supported
PRP_MRP	Ability to perform as an MRP bridge element (timeReceiver or timeTransmitter)	Not supported
PRP_RSTP	Ability to perform as an RSTP bridge element with designated port role	Not supported
PRP_SRP	Ability to perform as non-bridging node with no PRP	Supported
HSR_H	Ability to support HSR Mode H (default)	Not supported
HSR_M	Ability to support HSR Mode M (mixed forwarding)	Not supported
HSR_N	ability to support HSR Mode N (no forwarding)	Not supported
HSR_T	Ability to support HSR Mode T (transparent forwarding)	Not supported
HSR_U	Ability to support HSR Mode U (forwarding also when unique destination)	Not supported
HSR_X	Ability to support HSR Mode X (no forwarding on counter-duplicate)	Not supported
SNMP_MIB	Ability to support the SNMP MIB	Not Supported
NTAB_SIZ	Number of entries in the NodesTable (0 = no NodesTable)	Supported **Note:** Number of entries = 10
RBX_PNT	Number of entries in the ProxyNodeTable	Not Supported.
PRIO_QTY	Number of supported priorities	Supported **Note:** Number of entries = 7
VLAN_QTY	Number of supported VLANS	Supported. **Note:** Number of supported VLANS = 10
QBX_HSR	QuadBox integrating two RedBoxes	Not supported
RBX_HSR	RedBox with HSR ports	Not supported
RBX_PRP	RedBox with PRP ports	Not supported
CLK_1588	Support of IEC 61588 synchronization	Supported

...........continued

PICS Reference	Capability	Supported
Note: ***VLAN_QTY*** - Ethernet timing ports are individually assigned to VLANs, with support for a maximum of 10 simultaneous VLANs with 0 or 1 VLAN per port.		

17. Log Events and Triggers

The following tables outline how each of the 'General' log events are triggered and an example log message.

Table 17-1. Priority Values Used

Priority Value	Severity Level	Severity Level	Description
128	0	Emergency	Only used for an unexpected shutdown.
129	1	Alert	Not in use
130	2	Critical	Used for interupptions such as going out of sync or restarting
131	3	Error	Used for important, but unexpected events. Including going into holdover, high current and PSU faults.
132	4	Warning	Used for events that are unexpected by do not directly affect operation, Including failed logins, input lost.
133	5	Notice	Used for most events, error/warning clearing and configuration changes.
134	6	Informational	Used to inform users of a change.

Each log entry will be assigned a priority value. This is derived from a facility number multiplied by eight, plus a severity number. For all entries the facility number will always be 16, and the severity number will vary depending on the event. To determine the sevrity level of an event look for the number surronded by "<" and ">" at the start of the log entry, and then subtract 128.

17.1 'ACCESS' Trigger Conditions

All log entries related to accessing the device.

Table 17-2. 'ACCESS' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Security Login Successful CMT	5	A user has successfully logged into the CMT using the basic authentication	[User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"]Login Successful
Security Login Successful RADIUS	5	A user has successfully logged into the CMT using RADIUS	[User@34689 username="Administrator" context="RADIUS" identifier="Administrator" role="Administrator"]Login Successful - RADIUS
Security Login Successful LDAP	5	A user has successfully logged into the CMT using LDAP	[User@34689 username="Administrator" context="LDAP" identifier="Administrator" role="Administrator"]]Login Succesful
Security No Response RADIUS	4	The clock fails to get a response from a RADIUS server	No Response from RADIUS Server
Security No Response LDAP	4	The clock fails to get a response from a LDAP server	No Response from LDAP Server
Security Logout	5	A user has logged out of their account	[IPAddress@34689 addressType="IPv4" address="192.168.42.244"] Logout Successful
Security User Lock Out	3	A user has attempted to log in too many times and has been locked out	[IPAddress@34689 addressType ="IPv4", Address = 192.168.2.125]Login Attempt Limit Reached - User locked out

...........continued

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Security Login Failed Incorrect Username	4	A user has entered an invalid username	[IPAddress@34689 addressType ="IPv4", Address = 192.168.2.125]Login Attempt Failed
Security Login Failed Incorrect Password	4	A user has entered an incorrect password	[IPAddress@34689 addressType ="IPv4", Address = 192.168.2.125]Login Attempt Failed
Security Login Failed RADIUS	4	A user has failed to login using RADIUS	[IPAddress@34689 addressType ="IPv4", Address = 192.168.2.125]Login Attempt Failed
Security Login Failed LDAP	4	A user has failed to login using LDAP	[IPAddress@34689 addressType ="IPv4", Address = 192.168.2.125]Login Attempt Failed
Security Connection Test RADIUS	5	A user has attempted to connect a RADIUS server and test the connection	[IPAddress@34689 addressType ="IPv4", Address = 192.168.2.125]Connection Test - RADIUS
Security Connection Test LDAP	5	A user has attempted to connect a LDAP server and test the connection	[IPAddress@34689 addressType ="IPv4", Address = 192.168.2.125]Connection Test - LDAP

17.2 'BOOT' Trigger Conditions

All log entries related to the start up and shutdown procedure.

Table 17-3. 'BOOT' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
System Ready	5	The device system is ready to operate	[alarmInfo@34689 alarmName="system.ready"] Indicates that all modules are started and running
Unit Unexpected Shutdown	0	The device has unexpectedly shutdown	[alarmInfo@34689 alarmName="system.unit.died_unexpectedly"] Unit died indicator
Security Unit Shutdown	3	The device has been intentionally shutdown	[ActionOrigin@34689 Origin=LCD] Device Shutdown
Security Unit Restart	2	The device has been intentionally restarted	[User@34689 username="Administrator"] [ActionOrigin@34689 origin="CMT"] Device restart
Security Unit Startup	5	The device has started	[alarmInfo@34689 alarmName="first_power"] Indicates that the clocks has been successfully powered

17.3 'CONFIG' Trigger Conditions

All log entries related to changing of configuration

Table 17-4. 'CONFIG' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Configuration changed via CMT	various	Indicates when a value has changed and that change has orignated from CMT	[User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"][configChange@34689 variable="gnss[0\],gnss.enable" valueBefore="true" valueAfter="false"] 'Administrator' changed variable 'gnss[0],gnss.enable' via CMT
Configuration changed via SNMP	various	Indicates when a value has changed and that change has orignated from SNMP	[User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"][configChange@34689 variable="gnss[0\],gnss.enable" valueBefore="true" valueAfter="false"] 'Administrator' changed variable 'gnss[0],gnss.enable' via SNMP

...........continued			
Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Configuration changed via the configuration file	various	Indicates when a value has changed and that change has orignated from the configuration file	[User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"][configChange@34689 variable="serial.baud_rate" valueBefore="9600" valueAfter="2400"] Setting changed from configuration file upload

17.4 'DST' Trigger Conditions

All log entries related to changing of daylight savings.

Table 17-5. 'DST' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Pending Daylight Savings Entry	5	The device is expecting to enter daylight savings	[TimeDiscontinuity@34689 dateTime="2024-09-28T15:00:00.000Z" amount="+01:00:00"] Pending daylight savings entry
Pending Daylight Savings Exit	5	The device is expecting to exit daylight savings	[TimeDiscontinuity@34689 dateTime="2024-09-28T15:00:00.000Z" amount="+01:00:00"] Pending daylight savings exit
Daylight Savings Entry	5	The device has entered daylight savings	[dateTime=2023-09-05T:02:00:00.000000Z, Amount= +01:00:00] Daylight Savings Entry
Daylight Savings Exit	5	The device has exited daylight savings	[TimeDiscontinuity@34689 dateTime="2024-09-28T15:00:00.000Z" amount="+01:00:00"] Daylight savings exit

17.5 'FILE' Trigger Conditions

All log entries related to the upload or download of a configuration file.

Table 17-6. 'FILE' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Config File Download Generated	5	The generation of a configuration file was successful	[User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Indicates that a configuration file download attempt has been made
Config File Uploaded (just uploaded, not applied)	5	Configuration file was uploaded to the device, but was not applied	[User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Indicates that a configuration file upload attempt has been made

17.6 'FIRMWARE' Trigger Conditions

All log entries related to the upload of a firmware image.

Table 17-7. 'FIRMWARE' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Security Firmware Upgraded	5	Firmware upgrade process has been completed successfully	[User@34689 username="Administrator"] [FirmwareChange@34689 newVersion="1.1rc1" oldVersion="1.1b16.08" activePartition="1" result="Success"] Security system firmware upgraded

...........continued			
Trigger Condition/Test Team Mapping	**Severity**	**Trigger Condition**	**Example Entry**
Security Firmware Upgrade Failed	4	Firmware upgrade process has failed	[User@34689 username="Administrator"] [FirmwareChange@34689 newVersion="1.1rc1" oldVersion="1.1b16.08" activePartition="0" result="Failure"] Security system firmware, unrecognised target
Security Firmware Backup Partition Boot	4	The back up partition has succesfully changed it's firmware	[User@34689 username="Administrator"] [FirmwareChange@34689 newVersion="1.1rc1" oldVersion="1.1b16.08" activePartition="1" result="Success"] Security system firmware upgraded
Security Firmware Uploaded	5	A firmware image has been uploaded to the device via the CMT	[User@34689 username="Administrator"] Administrator is uploading new firmware.

17.7 'GNSS' Trigger Conditions

All log entries related to GNSS

Table 17-8. 'GNSS' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
GNSS Receiver Time Jump	3	The device has detected that it's GNSS receiver has had a jump in it's time of day	[timeDiscontinuity@34689 dateTime="2024-06-11T03:28:58Z" amount="-00:00:01.786"] GNSS Time Jump Detected
Antenna Current Ok	5	The current on the antenna is no longer too high or too low	[alarmInfo@34689 alarmName="gnns_antenna_current_fine_from_low"] Gnns antenna is no longer under current state
GNSS Status - Fix Acquired	5	The GNSS receiver has managed to gain synchronization using GNSS satellites	[alarmInfo@34689 alarmName="fix_available"] GNSS fix available
GNSS Satellite Count Ok	5	The device has detemined that there are now enough satellites to synchronize to	[alarmInfo@34689 alarmName="satellite_count_fine"] Sufficient satellites for fix available
GNSS Commissioning Log Cleared	5	GNSS Commissioning log successfully cleared	[logAction@34689 logAction="delete" dateCreated="2024-06-19T23:38:50.520Z" fileType="GNSS" encryption="None" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Log deletion (name_of_file.csv)
GNSS Commissioning Log Generated	5	GNSS Commissioning log successfully downloaded	[logAction@34689 logAction="download" dateCreated="2024-06-20T00:49:57.670Z" fileType="GNSS" encryption="None" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Log download (name_of_file.csv)

...........continued

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
GNSS Commissioning Log Generation Failed	4	GNSS commissioning log failed to be downloaded	[logAction@34689 logAction="download" dateCreated="2024-06-20T00:49:57.670Z" fileType="-" encryption="None" result="failure"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Log download (name_of_file.csv)
GNSS Commissioning Log Scheduled	5	A GNSS commissioning log has succesfully been scheduled	[logAction@34689 logAction="scheduled" dateCreated="2024-05-17T17:55:42.977Z" fileType="GNSS" encryption="None" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] GNSS log generation scheduled
GNSS Commissioning Log Started	5	A GNSS commissioning log has succesfully been started	[logAction@34689 logAction="created" dateCreated="2024-06-19T23:38" fileType="GNSS" encryption="None" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] GNSS log generation started
GNSS Commissioning Scheduled Log Cancelled	5	A GNSS commissioning log has succesfully been cancelled	[logAction@34689 logAction="cancel" dateCreated="-" fileType="GNSS" encryption="none" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] GNSS log generation cancelled
GNSS Commissioning Log Interrupted	5	A GNSS commissioning log has been interupted	[logAction@34689 logAction="cancel" dateCreated="2024-06-19T23:38" fileType="GNSS" encryption="None" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] GNSS log generation interrupted
GNSS Status - No Fix	4	Device cannot fix to a GNSS signal	[alarmInfo@34689 alarmName="no_fix_available"] GNSS no fix available
GNSS Satellite Count Low	4	Device is reporting that there are not enough satellites to synchronize to	[alarmInfo@34689 alarmName="gnns_satellite_count_low"] Insufficient satellites for fix
Antenna Current High	3	The current on the antenna connector is too high	[alarmInfo@34689 alarmName="gnns_antenna_current_high"] A gnss antenna over current state
Antenna Current Low	3	The current on the antenna connector is too low	[alarmInfo@34689 alarmName="gnns_antenna_current_low"] A gnss antenna under current state
Antenna Current fine from high	5	The current on the antenna is no longer too high	[alarmInfo@34689 alarmName="gnss_antenna_current_fine_from_high"] GNSS antenna is no longer over current state

...........continued

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Antenna Current fine from low		The current on the antenna is no longer too low	[alarmInfo@34689 alarmName="gnss_antenna_current_fine_from_low"] GNSS antenna is no longer under current state

17.8 'IRIG' Trigger Conditions

All log entries related to the input and output of IRIG-B

Table 17-9. 'IRIG' Trigger Conditions

Trigger Condition/ Test Team Mapping	Severity	Trigger Condition	Example Entry
Output Started	5	An IRIG-B output has been started	[irigInfo@34689 port="1" quality="100" CTQ="5" valid="valid"] Output Started
Output Stopped	4	An IRIG-B output has been stopped	[irigInfo@34689 port="1" quality="100" CTQ="5" valid="valid"] Output Stopped
Valid IRIG-B Input	5	A valid IRIG-B signal has been discovered on the IRIG-B input	[irigInfo@34689 port="1" quality="100" CTQ="5" valid="valid"][sourceIdentifier@34689 usedFor="Synchronization" event="AVAILABLE" SourceType="IRIG-B" SourceIndex="1"] Valid IRIG-B Input Detected
Invalid IRIG-B Input	4	An invalid IRIG-B signal has been discovered on the IRIG-B input	[irigInfo@34689 port="1" quality="100" CTQ="5" valid="invalid"] Invalid IRIG-B Input Detected
IRIG-B Input Lost	4	The IRIG-B input ports are configured but do not detect any IRIG-B	[irigInfo@34689 port="1" quality="100" CTQ="5" valid="valid"] IRIG-B Input Lost
IRIG-B Quality Changed Output	5	The quality bit on an outgoing IRIG-B output has changed	[irigInfo@34689 port="10" quality="1000" CTQ="2" valid="valid"] Quality Changed
IRIG-B Quality Changed Input	5	The quality bit on an incoming IRIG-B input has changed	[irigInfo@34689 port="10" quality="1000" CTQ="2" valid="valid"] IRIG-B Input Quality Changed

17.9 'LEAP' Trigger Conditions

All log entries related to the application of a leap second.

Table 17-10. 'LEAP' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Time Leap Second Pending	5	The device is expecting a leap second to be added	[dateTime=2023-09-05T:02:00:00.000000Z, Amount= -00:00:02] Pending Leap Second addition
Time Leap Second Pending	5	The device is expecting a leap second to be removed	[dateTime=2023-09-05T:02:00:00.000000Z, Amount= -00:00:12] Pending Leap Second subtraction
Time Leap Second Applied	5	The device has applied a leap second	[dateTime=2023-09-05T:02:00:00.000000Z, Amount= -00:00:02] Leap Second addition
Time Leap Second Removed	5	The device has removed a leap second	[dateTime=2023-09-05T:02:00:00.000000Z, Amount= -00:00:12] Leap Second subtraction

17.10 'LICENSE' Trigger Conditions

All log entries related to the adding and expiry of licenses

Table 17-11. 'LICENSE' Trigger Conditions

Trigger Condition/ Test Team Mapping	Severity	Trigger Condition	Example Entry
License Added	5	A license has been added	[User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"][LicenseInfo@34689 featureName="xyz" expiryDate=2099-01-01T00:00:00.000000Z] License for <feature> added
License Expired	4	A license has expired	[User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"][LicenseInfo@34689 featureName="<feature>" expiryDate=2099-01-01T00:00:00.000000Z] License for <feature> has expired

17.11 'LOG ' Trigger Conditions

All log entries for the downloading and creation of the logs files.

Table 17-12. 'LOG ' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
General Log Downloaded	5	General log successfully downloaded	[logAction@34689 logAction="download" dateCreated="2024-06-20T00:49:57.670Z" fileType="General" encryption="None" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Log download (name_of_file.zip)
Support Log Downloaded	5	Support log successfully downloaded	[logAction@34689 logAction="download" dateCreated="2024-06-20T00:49:57.670Z" fileType="Support" encryption="None" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Log download (name_of_file.zip)
General Log Download Failed	4	General log failed to be downloaded	[logAction@34689 logAction="download" dateCreated="2024-06-20T00:49:57.670Z" fileType="-" encryption="None" result="failure"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Log download (name_of_file.zip)
Support Log Download Failed	4	Support log failed to be downloaded	[logAction@34689 logAction="download" dateCreated="2024-06-20T00:49:57.670Z" fileType="-" encryption="None" result="failure"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Log download (name_of_file.zip)

...........continued

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
General Log Deleted	5	System Log Download Cleared	[logAction@34689 logAction="delete" dateCreated="2024-05-17T17:47:58.218Z" fileType="General" encryption="None" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Log deletion (name_of_file.zip)
Support Log Deleted	5	Support Log Download Cleared	[logAction@34689 logAction="delete" dateCreated="2024-05-17T17:47:58.218Z" fileType="Support" encryption="Device" result="success"][User@34689 username="Administrator" context="basic" identifier="Administrator" role="Administrator"] Log deletion (name_of_file.zip)

17.12 'NET' Trigger Conditions

All log entries related to the setting of IP addresses or changes in SFP state

Table 17-13. 'NET' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
IP Address Collision Detected Event	4	The device has detected that one of it's IP addresses has collided with another device on the network	[alarmInfo@34689 alarmName="address_collision"] Indicates that the port has fallen back to link local due to a detected address collision
Network SFP Connected	5	A SFP has been connected	[networkTimingPort@34689 physical="3" virtual="2" interface="SFP" vlanID="0"] [sfpInfo@34689 manufacturer="OEM" model="HLY23C0619014" autoNegotiation="false" supported="false"] SFP Connected
Network Ethernet Link Up	5	An Ethernet port is now sending and receiving traffic.	[networkTimingPort@34689 physical="0" virtual="0" interface="RJ45" vlanID="0"] [netPortConfig@34689 speed="100M" autoNegotiation="false" fullDuplex="true"] Link established
Network Ethernet Link Down	4	An Ethernet port is no longer sending and receiving traffic.	[networkTimingPort@34689 physical="9" virtual="9" interface="SFP+" vlanID="0"] Link lost
IP Address Assigned	5	An IP address has been assigned to an Ethernet port	[networkTimingPort@34689 physical="0" virtual="0" interface="RJ45" vlanID="0"] [ipAddress@34689 addressType="IPV4" address="192.168.89.10"] IP Address assigned

17.13 'NTP' Trigger Conditions

All log entries related to Network Time Protocol

Table 17-14. 'NTP' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Network NTP Stratum Changed Output	5	The stratum level for the NTP outputs has changed	[networkTimingPort@34689 physical="1" virtual="1" interface="RJ45"][IPAddress@34689 addressType="IPV4" address="192.168.89.11"] Network NTP Stratum Changed Output (1)
Network NTP Stratum Changed Input	5	The stratum level on an incoming NTP signal has changed	[networkTimingPort@34689 physical="1" virtual="1" interface="RJ45"][IPAddress@34689 addressType="IPV4" address="192.168.89.11"] Network NTP Stratum Changed Input (1)
NTP Server Time Jump	4	The device has detected that a time jump has occurred on an incoming NTP input	[networkTimingPort@34689 physical="1" virtual="1" interface="RJ45"][IPAddress@34689 addressType="IPV4" address="192.168.89.11"] NTP Server Time Jump

17.14 'OUTPUT' Trigger Conditions

All log entries related to outputs

Table 17-15. 'OUTPUT' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Output Signal Suppressed	5	A port has its output suppressed	[irigInfo@34689 port="1" quality="100" CTQ="5" valid="valid"] Output Suppressed

17.15 'POWER' Trigger Conditions

All log entries related to the monitoring of the power supplies.

Table 17-16. 'POWER' Trigger Conditions

Trigger Condition/ Test Team Mapping	Severity	Trigger Condition	Example Entry
Power Supply A External Fault	3	Power Supply A has a fault between the power source and the power supply	[alarmInfo@34689 alarmName="state_power_supplyA_down"] Indicates that the power cable A has been disconnected
Power Supply B External Fault	3	Power Supply B has a fault between the power source and the power supply	[alarmInfo@34689 alarmName="state_power_supplyB_down"] Indicates that the power cable B has been disconnected
Power Supply A Ok	5	Power supply A is no longer indicating a fault	[alarmInfo@34689 alarmName="state_power_supplyA_up"] Indicates that the power cable A has been re-connected
Power Supply B Ok	5	Power supply B is no longer indicating a fault	[alarmInfo@34689 alarmName="state_power_supplyB_up"] Indicates that the power cable B has been re-connected

17.16 'PRP' Trigger Conditions

All log entries related to PRP.

Table 17-17. 'PRP' Trigger Conditions

Trigger Condition/ Test Team Mapping	Severity	Trigger Condition	Example Entry
PRP Link A Up	4	Port A of a PRP pair is now sending and receiving traffic.	[networkTimingPort@34689 physical="3" virtual="2" interface="SFP" vlanID="0"][netPortConfig@34689 speed="100M" autoNegotiation="false" fullDuplex="true"] PRP Link A up

...........continued			
Trigger Condition/ Test Team Mapping	**Severity**	**Trigger Condition**	**Example Entry**
PRP Link B Up	4	Port B of a PRP pair is now sending and receiving traffic.	[networkTimingPort@34689 physical="3" virtual="2" interface="SFP" vlanID="0"][netPortConfig@34689 speed="100M" autoNegotiation="false" fullDuplex="true"] PRP Link B up
PRP Link A Down	4	Port A of a PRP pair is no longer sending and receiving traffic.	[alarmInfo@34689 alarmName="prp_link_a_down"] PRP Link A is down
PRP Link B Down	4	Port B of a PRP pair is no longer sending and receiving traffic.	[alarmInfo@34689 alarmName="prp_link_b_down"] PRP Link B is down

17.17 'PTP' Trigger Conditions

All log entries related to PTP.

Table 17-18. 'PTP' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Network PTP Port State Change	5	A PTP port has transitioned from one state to another (eg from TimeTransmitter to TimeReceiver)	[ipAddress@34689 addressType="IPV4" address="192.168.89.10"][ptpInfo@34689 port="1" clockId="0" clockClass="255" portState="UNCALIBRATED" GMClockID="00:b0:ae:ff:fe:07:f9:a6" clockAccuracy="36" domain="4" parentID="00:b0:ae:ff:fe:07:f9:a6"] Port state change
Network PTP Clock Class Change Output	5	The clock class on a PTP output has changed	[networkTimingPort@34689 physical="0" virtual="0" interface="RJ45" vlanID="0"][ipAddress@34689 addressType="IPV4" address="192.168.89.10"][ptpInfo@34689 port="1" clockId="0" clockClass="110" portState="LISTENING" GMClockID="00:1d:7f:ff:fe:03:03:ff" clockAccuracy="38" domain="4" parentID="00:1d:7f:ff:fe:03:03:ff"] Output clock class change
Network PTP Clock Class Change Input	5	The clock class on an incoming PTP input has changed	[networkTimingPort@34689 physical="0" virtual="0" interface="RJ45" vlanID="0"][ipAddress@34689 addressType="IPV4" address="192.168.89.10"][ptpInfo@34689 port="1" clockId="0" clockClass="90" portState="TIME_RECEIVER" GMClockID="00:b0:ae:ff:fe:07:f9:a6" clockAccuracy="34" domain="4" parentID="00:b0:ae:ff:fe:07:f9:a6"] Input clock class change
PTP Change in Grandmaster	5	When the grandmaster used when synchronizing to PTP has changed	[networkTimingPort@34689 physical="0" virtual="0" interface="RJ45" vlanID="0"][ipAddress@34689 addressType="IPV4" address="192.168.89.10"][ptpInfo@34689 port="1" clockId="0" clockClass="84" portState="LISTENING" GMClockID="00:b0:ae:ff:fe:07:f9:a6" clockAccuracy="33" domain="4" parentID="00:b0:ae:ff:fe:07:f9:a6"] Grandmaster change

...........continued

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
PTP timeTransmitter Time Jump	4	The device has detected that a time jump has occurred on an incoming PTP input	[networkTimingPort@34689 physical="0" virtual="0" interface="RJ45" vlanID="0"] [ipAddress@34689 addressType="IPV4" address="192.168.89.10"][ptpInfo@34689 port="1" clockId="0" clockClass="84" portState="UNCALIBRATED" GMClockID="00:b0:ae:ff:fe:07:f9:a6" clockAccuracy="33" domain="4" parentID="00:b0:ae:ff:fe:07:f9:a6"] [timeDiscontinuity@34689 dateTime="2024-06-05T23:42:02Z" amount="00:01:58.376"]
PTP Offset From timeTransmitter Limit Exceeded	4	The offset from a PTP timetransmitter has exceeded the allowable threshold	[networkTimingPort@34689 physical="0" virtual="0" interface="RJ45" vlanID="0"] [ipAddress@34689 addressType="IPV4" address="192.168.89.10"][ptpInfo@34689 port="1" clockId="0" clockClass="255" portState="UNCALIBRATED" GMClockID="00:b0:ae:ff:fe:07:f9:a6" clockAccuracy="33" domain="4" parentID="00:b0:ae:ff:fe:07:f9:a6"] Offset from grandmaster exceeds limit

17.18 'ROLL' Trigger Conditions

All log entries related to expected time rollover events (Unix Rollover, Week Number Rollover etc.)

Table 17-19. 'ROLL' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Time Rollover Pending NTP	5	The device is expecting a NTP rollover event	[Rollover@34689 dateTime = "2024-09-28T15:00:00.000Z" type="NTP"] Rollover pending
Time Rollover Pending GNSS	5	The device is expecting a GNSS rollover event	[Rollover@34689 dateTime = "2024-09-28T15:00:00.000Z" type="GNSS"] Rollover pending
Time Rollover Event NTP	5	The device has had a NTP rollover event	[Rollover@34689 dateTime = "2024-09-28T15:00:00.000Z" type="NTP"] Rollover occurred
Time Rollover Event GNSS	5	The device has had a GNSS rollover event	[Rollover@34689 dateTime = "2024-09-28T15:00:00.000Z" type="GNSS"] Rollover occurred

17.19 'SECURITY' Trigger Conditions

Log entries related to security

Table 17-20. 'SECURITY' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
{username} is resetting the certificate to use factory default.	5	Remove Certificate or Reset to Default Certificate have been selected in CMT	[User@34689 username="Administrator"] Administrator is resetting the certificate to use factory default.
{username} is uploading new certificate.	5	Uploading certificate data key or cert or crt	[User@34689 username="Administrator"] Administrator is uploading new certificate.

...........continued			
Trigger Condition/Test Team Mapping	**Severity**	**Trigger Condition**	**Example Entry**
Upload complete for file 'custom-cert.{type}' {size} bytes received.	5	Completed upload of certificate data	[User@34689 username="Administrator"] Upload complete for file 'custom-cert.crt' 2118 bytes received.
{username} is generatingrequesting a CSR	5	Begin generating a CSR (after clicking Create Certificate Signing Request (CSR))	[User@34689 username="Administrator"] Administrator is generating a CSR.
{username} has failed to generate a CSR (Invalid data).	4	CSR generation failed (posibly problems with data submitted)	[User@34689 username="Administrator"] Administrator has failed to generate a CSR (Invalid data).
{username} has successfully generated a CSR.	5	CSR generation succeeeded	[User@34689 username="Administrator"] Administrator has successfully generated a CSR.
{username} has successfully validated newly uploaded certificate.	5	Validation of uploaded certificate/key is successful	[User@34689 username="Administrator"] Administrator has successfully validated newly uploaded certificate.
Validation of newly uploaded certificate has failed for {username}.	4	Validation of uploaded certificate/key is unsuccessful	[User@34689 username="Administrator"] Validation of newly uploaded certificate has failed for Administrator.
{username} has applied the newly uploaded certificate.	5	Application of uploaded certificate/key was successful	[User@34689 username="Administrator"] Administrator has applied the newly uploaded certificate.
{username} failed applying the newly uploaded certificate as it is not valid.	5	Application of uploaded certificate/key was unsuccessful	[User@34689 username="Administrator"] Administrator failed applying the newly uploaded certificate as it is not valid.

17.20 'SOURCE' Trigger Conditions

All entries related to the gaining, losing and changing of synchronization sources

Table 17-21. 'SOURCE' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Sync Source Changed - Unknown	5	All sync source's have been lost	[alarmInfo@34689 alarmName="primary_source_change"] Primary Source Change GNSS[0] => UNKNOWN[0]
Sync Source Changed - GNSS	5	The primary sync source has changed to GNSS	[alarmInfo@34689 alarmName="primary_source_change"] Primary Source Change UNKNOWN[0] => GNSS[0]
Sync Source Changed - PTP	5	The primary sync source has changed to PTP	[alarmInfo@34689 alarmName="primary_source_change"] Primary Source Change UNKNOWN[0] => PTP[0]
Sync Source Changed - NTP	5	The primary sync source has changed to NTP	[alarmInfo@34689 alarmName="primary_source_change"] Primary Source Change UNKNOWN[0] => NTP[0]
Sync Source Changed - IRIG-B	5	The primary sync source has changed to IRIG-B	[alarmInfo@34689 alarmName="primary_source_change"] Primary Source Change UNKNOWN[0] => IRIGB[0]

...........continued

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
Sync Source Changed - Test	5	The primary sync source has changed to test mode	[alarmInfo@34689 alarmName="primary_source_change"] Primary Source Change UNKNOWN[0] => TEST[0]

17.21 'SYNC' Trigger Conditions

All log entries related to changes of synchronization state.

Table 17-22. 'SYNC' Trigger Conditions

Trigger Condition/ Test Team Mapping	Severity	Trigger Condition	Example Entry
Holdover	2	Device enters the holdover state	[alarmInfo@34689 alarmName="state_holdover"] Indicates the clock is in the holdover state
Out of Sync (Non-Holdover)	2	Device transitions from holdover to out of sync	[alarmInfo@34689 alarmName="clock_state_change"] Clock state change HOLDOVER=>OUT_OF_SYNC_NON_HOLDOVER
Out of Sync (Startup)	2	Device has been turned on and is reporting out of sync	[alarmInfo@34689 alarmName="clock_state_change"] Clock state change OUT_OF_SYNC_NON_HOLDOVER=>OUT_OF_SYNC_STARTUP
Synchronization Achieved	5	Device has gained sync	[alarmInfo@34689 alarmName="firstSyncAchieved"] Indicates that the clocks first sync has been achieved

17.22 'TEMP' Trigger Conditions

All log entries related to temperature changes.

Table 17-23. 'TEMP' Trigger Conditions

Trigger Condition/Test Team Mapping	Severity	Trigger Condition	Example Entry
SFP Over Temperature	3	A SFP has exceeded its max temperature threshold	[temperature@34689 source="SFP" degrees_c="29.597"] Indicates that the SFP Over Temperature alarm has been raised
Unit Temperature Ok	5	The device has reached a suitable temperature	[alarmInfo@34689 alarmName="subsystem_temp_fine"] Indicates the subsystem is no long in an over temperature state
Unit Over Temperature	3	The device has registered that the temperature is too high	[alarmInfo@34689 alarmName="subsystem_over_temp"] Indicates that the subsystem is in an over temperature state
Unit Under Temperature	3	The device has registered that the temperature is too low	[alarmInfo@34689 alarmName="subsytem_under_temp"] Indicates that the subsystem is in an under temperature state

18. Functions of Encryption, Public Key and Private Key

Purpose of Encryption: Encrypting these logs ensures they remain unreadable to unauthorized parties, bolstering data privacy and security. Encrypted logs can be sent through email to our technical support team who can decrypt them and review the information. The "customer provided" option provides a two-tier encryption approach that provides an additional layer of control, as customers must grant permission by providing the decryption key, ensuring that only the authorized parties can access the data.

Public and Private keys are essential components of asymmetric cryptography, a cryptographic system that uses a pair of keys for secure communication. The two keys are mathematically related, but have distinct purposes.

Public Key: Public key is shared openly and can be distributed widely. It is a long string of numbers and letters.

The public key is used to encrypt data that only the corresponding private key can decrypt.

Public key must be used to verify signatures made with the private key.

Private Key: Private key is a long string of numbers and letters that is generated randomly and is meant to be kept confidential and should only be known to the owner.

Private key is used to decrypt data that has been encrypted with the corresponding public key. It can also be used to sign data, which can be then be verified by others using the public key.

How They Work Together:

In a typical use case, such as sending an encrypted file, the device uses its own generated public key to encrypt the log file. Once encrypted, the log file can only be decrypted by the recipient private key.

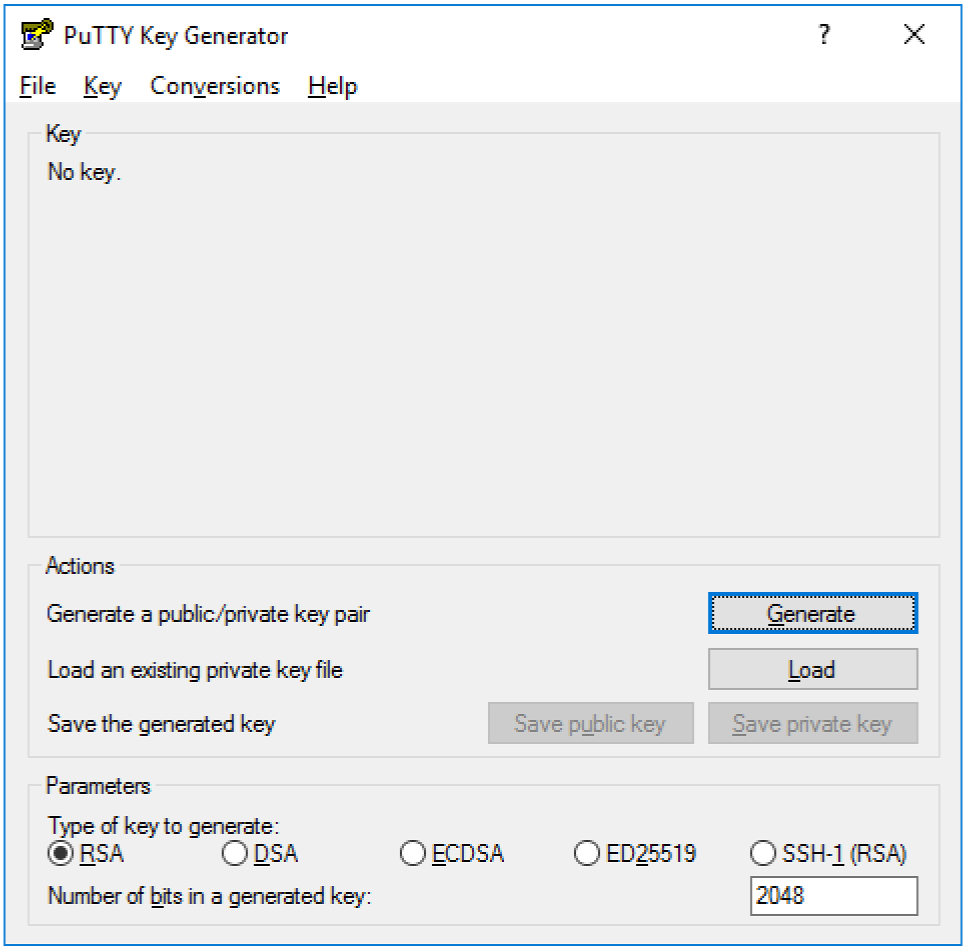
If a user wants to prove their identity or ensure that the file has not been altered, the user can sign the encrypted log file with their private key. The signature can then be verified by the recipient who has access the corresponding public key.

18.1 Creating a New Key Pair for Log Encryption

This guide shows you how to generate a "customer provided" key pair for use on the general logs.

1. Download a key generation tool such as PuTTYgen.
2. In the **PuTTY Key Generator** dialog box, perform the following:
   a. Under **Type of key to generate:**, select **RSA**.

Figure 18-1. PuTTY Key Generator

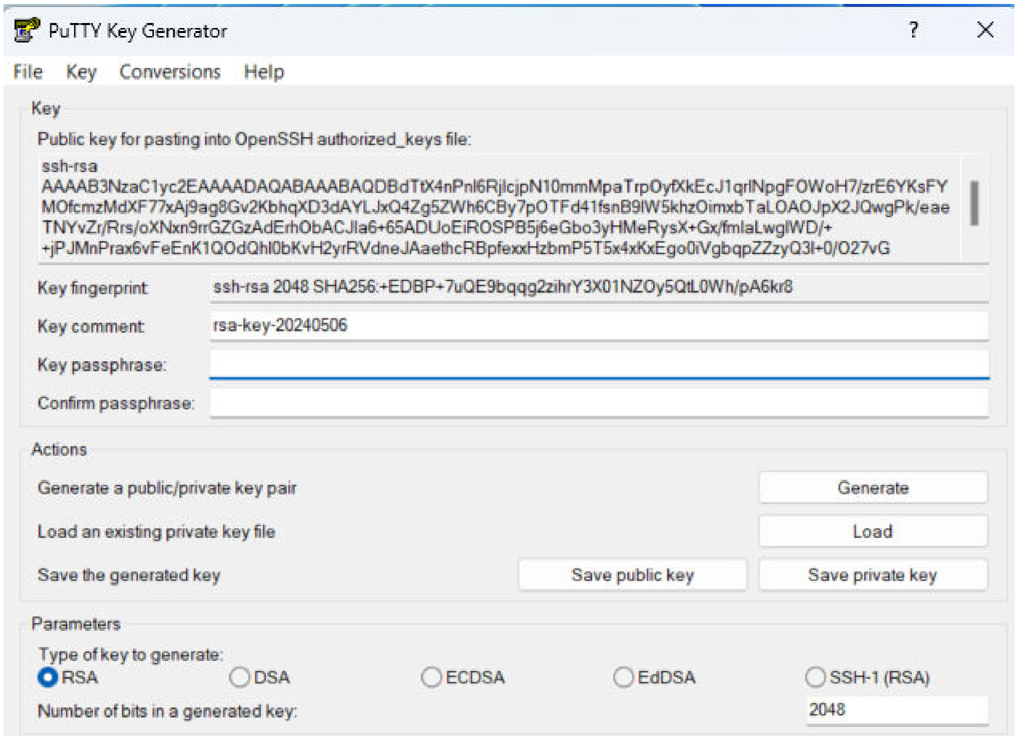


b. Click **Generate**.

c. You will be prompted to move your mouse around to create randomness.

d. Enter your desired passphrase.

Figure 18-2. Entering the PassPhrase



e. Click **Save public key** and **Save private key** and name each file something you can remember.

3. Open the private key file with a text editor, such as notepad.
4. Copy the section "Private-Lines"

Figure 18-3. Sample

```
PuTTY-User-Key-File-3: ssh-rsa
Encryption: aes256-cbc
Comment: rsa-key-20240506
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAABAQDBdTtX4nPnI6RjlcjpN10mmMpaTrpOyfXk
EcJ1qrlNpgFOWoH7/zrE6YKsFYMOfcmzMdXF77xAj9ag8Gv2KbhqXD3dAYLJxQ4Z
g5ZWh6CBy7pOTFd41fsnB9IW5khzOimxbTaLOAOJpX2JQwgPk/eaeTNYvZr/Rrs/
oXNxn9rrGZGzAdErhObACJla6+65ADUoEiROSPB5j6eGbo3yHMeRysX+Gx/fmlaL
wglWD/++jPJMnPrax6vFeEnK1QOdQhI0bKvH2yrRVdneJAaethcRBpfexxHzbmP5
T5x4xKxEgo0iVgbqpZZzyQ3I+0/O27vG+u0ndMp3Sad++D6kXg57
Key-Derivation: Argon2id
Argon2-Memory: 8192
Argon2-Passes: 34
Argon2-Parallelism: 1
Argon2-Salt: 90059e80354f8786f74bbf9ef983f9d9
Private-Lines: 14
4L9P6kUkJzBnO+C8c6kOorlWEJDp7a4CvOzhD4yIvam3lmmWEel8ElBH/lSFuddB
U7T4FDhBQAWpnbs28Q+BOc2Z80u2XBdp5t+Ze1MDWcEdtOOY8nMgxcthdNVX3RWH
NnEFttdgwvlk+lP/3gNz4Srv2Q2APxu4LunEFrcsZIExwOB/qjQ4nBPKmMnAE2jO
G9eB3OU2NOZJq3gKtG2mFCRfiUEpnNzfmchfwo5BOpG4fvsGoSkcdO5akxplkqMa
pwr0XIqEv2OEN6mejCJLmJ2DgeZkZVmWD/IbEHGWkIWeqKQ5fjE2/D0UFBJ6xcBs
NwNgy7+XFtbGnCxZQnKJzPjJ6VUZhyc6XxWhlANehMGbE/b1/K+L9fB3rK0Y1U5P
Wx6HklpzdcS2CLeCwnDKePXkhkluIH53JbdfzSdg35JkLrM9+/VOLuWIzU9nBUUW
Lfna+cEaDirXdUfBuEgfF4s5VMwzrELEu6Ph2DBSuxPMVCH39BwytXMO+7xK4G0A
Qyi7l4ylu3Kg4HH1XLEjMjZcKeaO+ZnQCPzydqg09lda4rdX12vSzlKgTDBZSAev
AEC2RWyTTXq0VBlM+s0x0lMvQZnzMsrHoIgMSUfb30LUoz+BObDOX6KfTai8hUoB
hUkdtQ2ppE5ZVqAwQJP3+q7WlqB+Gi/Qk21t1Yu8diIj5t5UjUAV3/nZpb0rib4u
PpJKh2E83hw+hy64efLUwQfzAWbJ8y04tvEYVWpGKjJ3U6XrNj9CXh51oWm2aI2h
y1xE+HTfH7qlbf6QSR3c4j1iaAwsNQx7Bf7+iL6zTev6vU/9TVd7I1j5kL8sXTTv
gz8nvU07M3v6h71MUs+vvjk9gz2/rglbVqFy+QXHFVaHTfFMlecevJW6DmXpFquF
Private-MAC: e35f2b84ef371037f1b4eb1602628005a69c95796cf2f17490a9c710ceae8894
```

5. Paste in the text box provided under "Customer Provided".
6. Click **Download**.

Note: The private key entered here is stored in a secure portion of the device's memory and is not shared with any other subsystem and is only used to generate the log. When the log is deleted, so is the private key information. This functionality is intended only to be used to provide an extra layer of security. By using this feature, you ensure that only the individual Microchip employee you have provided the public key to will be able to decrypt the log file. By using the device's key instead only those with the device's public key will be able to decrypt (including Microchip Technical Support).

19. Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Table 19-1. Revision History

Revision Level	Date	Description
D	01/2025	Following are the list of changes made in this revision: • Added the Management Functionality feature to Provisioning the Ethernet Ports section. • Updated the following sections: – Static IP Address – DHCP IP Address – Link Local IP Address – Provisioning RADIUS – Provisioning LDAP • Added the Respond to Peer Delay Requests From Other Domains feature to the Peer to Peer Default Profile Auto Mode section • Updated Figure 9-427 • Added Figure 9-433 and Figure 9-434
C	08/2024	Following are the list of changes made in this revision: • Added the following sections: – Provisioning Logs – Provisioning Certificate – Factory Reset – Firmware partitions – Restarting the Device – Configuration Management – Accessories – Appendix D: Protocol Implementation Conformance Statement (PICS) – Log Events and Triggers – Functions of Encryption, Public Key and Private Key
B	9/2022	Addition of RADIUS and LDAP provisioning
A	7/2022	Initial version

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at https://www.microchip.com/en-us/about/legal-information/microchip-trademarks.

ISBN: 979-8-3371-0465-2

Legal Notice

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip products are strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.