PROTEMPIS THUNDERBOLT GM330

IEEE-1588 (PTP) GRANDMASTER CLOCK / NTP TIME SERVER

USER GUIDE

For use with: Thunderbolt GM330 Time server (P/N 100836-xx)

Version 2.00.00
Revision B
July
2025
P/N: 100836-xx

Legal Notices

Corporate Office

Protempis USA
www.protempis.com
Email: support@protempis.com

Release Notice

This is the October 2024 release (Revision A) of the GM/ documentation.

The Australian Consumer Law

Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.
Protempis' warranty(set out below) is in addition to any mandatory rights and remedies that you may have under the Australian Consumer Law.

LIMITED WARRANTY TERMS AND CONDITIONS

Product Limited Warranty

Subject to the following terms and conditions, Protempis Inc. (“Protempis”) warrants that for a period of one (1) year from the date of purchase this Protempis product (the “Product”) will substantially conform to Protempis' publicly available specifications for the Product and that the hardware and any storage media components of the Product will be substantially free from defects in materials and workmanship.

Product Software

Product software, whether built into hardware circuitry as firmware, provided as a standalone computer software product, embedded in flash memory, or stored on magnetic or other media, is licensed solely for use with or as an integral part of the Product and is not sold. If accompanied by a separate end-user license agreement (“EULA”), use of any such software will be subject to the terms of such end-user license agreement (including any differing limited warranty terms, exclusions, and limitations), which shall control the terms and conditions set forth herein.
Except for the limited license rights expressly provided herein, Protempis and its suppliers have and will retain all rights, title, and interest (including, without limitation, all patent, copyright, trademark, trade secret, and other intellectual property rights) in and to the Product Software and all copies, modifications and derivative works thereof (including any changes which incorporate any of your ideas, feedback or suggestions). You shall not (and shall not allow any third party to): (a) decompile, disassemble, or otherwise reverse engineer the Product Software or attempt to reconstruct or discover any source code, underlying ideas, algorithms, file formats or programming interfaces of the Product Software by any means whatsoever (except and only to the extent that applicable law prohibits or restricts reverse engineering restrictions); (b) distribute, sell, sublicense, rent, lease, or use the Product Software (or any portion thereof) for time sharing, hosting, service provider, or like purposes; (c) remove any product identification, proprietary, copyright, or other notices contained in the Product Software; (d) modify any part of the Product Software, create a derivative work of any part of the Product Software, or incorporate the Product Software into or with other software, except to the extent expressly authorized in writing by Protempis; (e) attempt to circumvent or disable the security key mechanism that protects the Product Software against unauthorized use (except and only to the extent that applicable law prohibits or restricts such restrictions); or (f) publicly disseminate performance information or analysis(including, without limitation, benchmarks) from any source relating to the Product Software. If the Product Software has been provided to you as embedded in any hardware device, you are not licensed to separate the Product Software from the hardware device. If the Product Software has been provided to you separately from a hardware device but is intended to be loaded onto a hardware device specified by Protempis (such as a firmware update), your license is limited to loading the Product Software on the device specified by Protempis, and for no other use.

Software Fixes

During the limited warranty period, you will be entitled to receive such Fixes to the Product software that Protempis releases and makes commercially available and for which it does not charge separately, subject to the procedures for delivery to purchasers of Protempis products generally. If you have purchased the Product from a Protempis authorized dealer rather than from Protempis directly, Protempis may, at its option, forward the software Fix to the Protempis authorized dealer for final distribution to you. Minor Updates, Major Upgrades, new products, or substantially new software releases, as identified by Protempis, are expressly excluded from this update process and limited warranty. Receipt of software Fixes or other enhancements shall not serve to extend the limited warranty period. For purposes of this warrant, the following definitions shall apply: (1) “Fix(es)” means an error correction or other update created to fix a previous software version that does not substantially conform to its Protempis specifications; (2) “Minor Update” occurs when enhancements are made to current features in a software program, and (3) “Major Upgrade” occurs when significant new features are added to the software, or when a new product containing new features places the further development of a current product line. Protempis reserves the right to determine, in its sole discretion, what constitutes a Fix, Minor Update, or Major Upgrade.

Warranty Remedies

If the Protempis Product fails during the warranty period for reasons covered by this limited warranty and you notify Protempis of such failure during the warranty period, Protempis will repair OR replace the nonconforming Product with new, equivalent to new, or reconditioned parts or Product, OR refund the Product purchase price paid by you, at Protempis’ option, upon your return of the Product in accordance with Protempis' product return procedures then in effect.

How to Obtain Warranty Service

To obtain warranty service for the Product, please contact your local Protempis authorized dealer. Alternatively, you may contact Protempis to request warranty service by sending an email to support@protempis.com. Please prepare to provide:

–your name, address, and telephone numbers –proof of purchase –a copy of this Protempis warranty –a description of the nonconforming Product including the model number – an explanation of the problem.
The customer service representative may need additional information from you depending on the nature of the problem. Any expenses incurred in the making of a claim under this warranty will be borne by you.

Warranty Exclusions and Disclaimer

This Product limited warranty shall only apply in the event and to the extent that: (a) the Product is properly and correctly installed, configured, interfaced, maintained, stored, and operated in accordance with Protempis' applicable operator's manual and specifications, and; (b) the Product is not modified or misused.
This Product limited warranty shall not apply to, and Protempis shall not be responsible for, defects or performance problems resulting from (i) the combination or utilization of the Product with hardware or software products, information, data, systems, interfaces, or devices not made, supplied, or specified by Protempis;
(ii) the operation of the Product under any specification other than, or in addition to, Protempis' standard specifications for its products; (iii) the unauthorized installation, modification, or use of the Product; (iv) damage caused by: accident, lightning or other electrical discharge, fresh or salt water immersion or spray(outside of Product specifications), or exposure to environmental conditions for which the Product is not intended; (v) normal wear and tear on consumable parts (e.g., batteries); or (vi) cosmetic damage. Protempis does not warrant or guarantee the results obtained through the use of the Product, or that software components will operate error-free.
NOTICE REGARDING PRODUCTS EQUIPPED WITH TECHNOLOGY CAPABLE OF TRACKING SATELLITE SIGNALS FROM SATELLITE-BASED AUGMENTATION SYSTEMS (SBAS) (WAAS/EGNOS, AND MSAS), OMNISTAR, GPS, MODERNIZED GPS OR GLONASS SATELLITES, OR FROM IALA BEACON SOURCES: PROTEMPIS IS NOT RESPONSIBLE FOR THE OPERATION OR FAILURE OF OPERATION OF ANY SATELLITE-BASED POSITIONING SYSTEM OR THE AVAILABILITY OF ANY SATELLITE-BASED POSITIONING SIGNALS.
THE FOREGOING LIMITED WARRANTY TERMS STATE PROTEMPIS' ENTIRE LIABILITY, AND YOUR EXCLUSIVE REMEDIES, RELATING TO THE PROTEMPIS PRODUCT UNDER THIS LIMITED WARRANTY. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED HEREIN, THE PRODUCT, AND ACCOMPANYING DOCUMENTATION AND MATERIALS ARE PROVIDED "AS-IS" AND WITHOUT EXPRESS OR IMPLIED WARRANTY OF ANY KIND, BY EITHER PROTEMPIS OR ANYONE WHO HAS BEEN INVOLVED IN ITS CREATION, PRODUCTION, INSTALLATION, OR DISTRIBUTION, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR GUARANTEES OF MERCHANTABILITY, ACCEPT ABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NONINFRINGEMENT. THE STATED EXPRESS WARRANTIES ARE IN LIEU OF ALL OBLIGATIONS OR
LIABILITIES ON THE PART OF PROTEMPIS ARISING OUT OF, OR IN CONNECTION WITH, ANY PRODUCT. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON DURATION OR THE EXCLUSION OF AN IMPLIED WARRANTY, THE ABOVE LIMITATION MAY NOT APPLY OR FULLY APPLY TO YOU.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, Protempis' ENTIRE LIABILITY UNDER ANY PROVISION HEREIN SHALL BE LIMITED TO THE AMOUNT PAID BY YOU FOR THE PRODUCT AND IN NO EVENT SHALL Protempis OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGE WHAT SO EVER UNDER ANY CIRCUMSTANCE OR LEGAL THEORY RELATING IN ANYWAY TO THE PRODUCTS, SOFTWARE AND ACCOMPANYING DOCUMENTATION AND MATERIALS, (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY OTHER PECUNIARY LOSS), REGARDLESS OF WHETHER Protempis HAS BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH LOSS AND REGARDLESS OF THE COURSE OF DEALING WHICH DEVELOPSOR HAS DEVELOPED BETWEEN YOU AND Protempis. BECAUSE SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY OR FULLY APPLY TO YOU.
PLEASE NOTE: THE ABOVE Protempis LIMITED WARRANTY PROVISIONS WILL NOT APPLY TO PRODUCTS PURCHASED IN THOSE JURISDICTIONS (E.G., MEMBER STATES OF THE EUROPEAN ECONOMIC AREA) IN WHICH PRODUCT WARRANTIES ARE THE RESPONSIBILITY OF THE LOCAL Protempis AUTHORIZED DEALER FROM WHOM THE PRODUCTS ARE ACQUIRED. IN SUCH A CASE, PLEASE CONTACT YOUR LOCAL PROTEMPIS AUTHORIZED DEALER FOR APPLICABLE WARRANTY INFORMATION.

Official Language

THE OFFICIAL LANGUAGE OF THESE TERMS AND CONDITIONS IS ENGLISH. IN THE EVENT OF A CONFLICT BETWEEN ENGLISH AND OTHER LANGUAGE VERSIONS, THE ENGLISH LANGUAGE SHALL CONTROL.

Notices

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

-Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

Changes and modifications not expressly approved by the manufacturer or registrant of this equipment can void your authority to operate this equipment under Federal Communications Commission rules.

Canada

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the radio interference regulations of the Canadian Department of Communications, ICES-003.

Le présent appareilnumérique n'émet pasde bruits radioélectriquesdépassant leslimitesapplicablesaux appareilsnumériquesde Classe Bprescritesdansle règlement sur le brouillage radioélectrique édicté par le Ministère desCommunicationsdu Canada, ICES-003.

Europe

This product has been tested and found to comply with the requirements for a device pursuant to European Council Directive 89/336/EEC on EMC, thereby satisfying the requirements for CE Marking and sale within the European Economic Area (EEA). These requirements are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential or commercial environment.

CE

Notice to Our European Union Customers

At Protempis, we recognize the importance of minimizing the environmental impacts of our products. We endeavor to meet your needs, not only when you purchase and use our products, but also when you are ready to dispose of them. That is why Protempis is actively pursuing and will continue to pursue, the expanded use of environmentally-friendly materials in all its products, and why we have established a convenient and environmentally friendly recycling program. As Protempis makes additional recycling facilities available for your use, we will post their locations and contact information to our website.

Recycling in Europe:

To recycle **Protempis WEEE:**

Spectra Precision GmbH C/O RCL EHV

Ekkersrijt 2066, 5692 BA Son, Netherlands

For product recycling instructions and more information, go to www.protempis.com/Compliance.

Declaration of Conformity

We, Protempis, LLC, based in the United States of America, declare under sole responsibility that the product: GM/ time server complies with Part 15B of FCC Rules.

Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

VCCI Class A

Declaration of VCCI Conformity

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

ＶＣＣＩ－Ａ

If you would like to obtain the source code of the OSS used in our products, please contact us using the inquiry form below.
＜Contact Us and Talk Success with Industry Innovators (support@protempis.com)＞

EMI 甲類警語

警告：為避免電磁干擾，本產品不應安裝或使用於住宅環境。

EMI 甲類警語	EMI Category A Warning
警告：為避免電磁干擾，本產品不應安裝或使用於住宅環境。	WARNING: To avoid electromagnetic interference, this product should not be installed or used in a residential environment.

Document History

Version	Date	Author	Changes
A	05/05/2025	FAE	Initial Release
B	07/08/2025	FAE	Added Get Time & Set Time, Cert .csr & .crt need the same name, .crt PEM (X509) format required

List of Abbreviations

A-GPS	Assisted GPS
APTS	Assisted Partial Timing Support
BC or T-BC	Boundary Clock or Telecom Boundary Clock
C/No	Carrier-to-Noise power ratio
DC	Direct Current
DOP	Dilution of Precision
EGNOS	European Geostationary Navigation Overlay Service
ESD	Electrostatic Discharge
GLONASS	Globalnaya Navigatsionnaya Sputnikovaya Sistema
GND	Ground
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
LNA	Low Noise Amplifier
NMEA	National Marine Electronics Association
NTP	Network Time Protocol. Common time distribution over networks
OCXO	Oven Controlled Crystal Oscillator
OD mode	Over-determined clock mode
PoE	Power over Ethernet
PCB	Printed Circuit Board
PDOP	Position Dilution of Precision
PPS	Pulse per Second
PTP	Precision Time Protocol (IEEE-1588)
QZSS	Quasi-Zenith Satellite System
RF	Radio Frequency
SyncE	Synchronous Ethernet
SFP	Small Form-factor Pluggable
ToD	Time of Day
T-RAIM	Timing Receiver Autonomous Integrity Monitoring
VCC	Voltage at the Common Collector; positive supply voltage
VSWR	Voltage Standing Wave Ratio
ZTP	Zero-Touch Provisioning

Safety Information

Warnings and Cautions

Always follow the instructions that accompany a Warning or Caution. The information it provides is intended to minimize the risk of personal injury and/or property damage. In particular, observe safety instructions that are presented in the following format:

WARNING - This alert warns of a potential hazard that, if not avoided, could result in severe injury or even death.

CAUTION - This alert warns of a potential hazard or unsafe practice that, if not avoided, could result in injury property damage, or irretrievable data loss.

CAUTION - Electrical hazard - the risk of damage to equipment. Make sure all electrostatic energy is dissipated before installing or removing components from the device. An electrostatic discharge (ESD) can cause serious damage to the component once it is outside the chassis.

This system can become extremely hot and cause burns. To reduce the risk of injury from a hot system, allow the surface to cool before touching it.

Operation and storage

WARNING - Operating or storing the Thunderbolt GM330 Time server outside the specified temperature range can damage it. For more information, see the product specifications on the data sheet.

WARNING - The Thunderbolt GM330 Time server is only to be used in a restricted access location.

WARNING - Short-circuit (overcurrent) protection device required. The Thunderbolt GM330Time server relies on the building installation for short-circuit

(overcurrent) protection. Check that the protective device is listed and rated not greater than 10 A.

Routing any cable

CAUTION - Be careful not to damage the cable. Take care to avoid sharp bends or kinks in the cable, hot surfaces (for example, exhaust manifolds or stacks), rotating or reciprocating equipment, sharp or abrasive surfaces, door and window jambs, and corrosive fluids or gases.

Contents

1. Introduction

The Precision Time Protocol (PTP) is one of the most important packet timing protocols for next-generation network synchronization. Other packet-based protocols include the Network Time Protocol (NTP). However, PTP offers much better accuracy and often at an accuracy of <100 nanoseconds.

PTP is a packet-based two-way communications protocol specifically designed to precisely synchronize distributed clocks to sub-microsecond resolution, typically on an Ethernet or IP-based network. Defined byIEEE1588standards, PTP provides real-time applications with precise time-of-day (ToD) information and time-stamped inputs, as well as scheduled and/or synchronized outputs for a variety of systems in different industry-specific networks, ranging from LTE/5G-based mobile networks, industrial automation, audio-visual networks, smart grid to transportation, automotive and Industrial Internet of Things (IoT) networking.

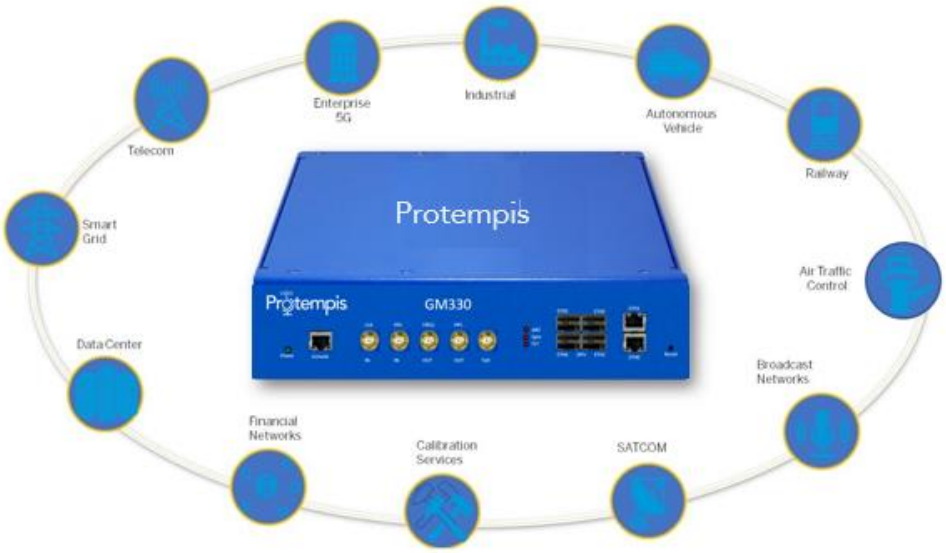
The Protempis® Thunderbolt® GM330 Time server offers PTP and NTP enabling backward compatibility with existing network sync infrastructure for the deployments in different vertical industries. It is the industry's most cost-effective grandmaster solution available today. The Thunderbolt GM330 Time server is widely deployed in the following industries:

- Smart Grids & Power Utilities: Synchronization is critical to the control and management of power utilities, specifically the smart grid infrastructure. The GM330 Time server is used in many power utility infrastructures around the globe to provide a highly accurate sync plane for power substations.
- Telecom: The telecommunication infrastructure is undergoing significant changes due to increased packetization and penetration of 5G-led virtualized RAN and software-defined network virtualization. The GM330 Time server has been a product of choice for many service providers to augment their existing LTE-A sync planes and provide a highly precise sync plane for 5G-based edge infrastructure.
- Enterprise 5G: With many countries auctioning unlicensed and licensed 5G spectrum for commercial use, several new generation service providers have taken the opportunity to offer highly reliable 5G wireless infrastructure for enterprises, which solves many pressing issues such as reliable communications in the healthcare industry and logistics

and broadband services for all enterprises. In the USA, the Citizen Band Radio Service (CBRS) is becoming a common choice for enterprise 5G solutions. The GM330 Time server is widely deployed in CBRS and similar enterprise 5G use cases in many countries.

- Industrial Networks & Industrial Automation: Much of the industrial networks deterministic meaning high accuracy and reliability of transport are standard. Industrial networks serve as the fundamental conduit to build connectivity infrastructure for industrial and factory automation. A highly precise sync plane is an integral part of a deterministic industrial network and is now the overall transport solution for industrial and factory automation. The GM330 Time server has been a product of choice for building highly accurate industrial networks in many countries.
- Autonomous Vehicles: Many elements within autonomous vehicle interconnects require a highly precise sync plane including sensors and LiDAR cameras. The GM330 Time server is a product of choice for autonomous vehicle sync plane deployments globally.
- Railways: The signaling and control of high-speed railways require a new type of network known as Communication-based Train Control (CBTC). Time Sensitive Networking (TSN) is the choice of a sync plane solution for CBTC and for this reason, the GM330 Time server has been deployed in many countries to enable a TSN solution for high-speed railways.
- Air Traffic Control: Airports and Air Traffic Control systems need accurate timing to manage airport operations from ticketing systems to clearing airspace and assisting flight landings and departures. Less accurate clocks may provide disastrous consequences for air traffic management and perhaps the overall operations of the airport. When it comes to a cost-effective reliable clocking solution, airports and air traffic control systems rely on the GM330 Time server. The product has been widely deployed around the world.
- Broadcast Networks: Synchronization is critical to broadcast systems whether it is a mobile or stationary network system. The GM330 Time server is deployed in many sports broadcast networks as the sole source for a clock in head-end systems.
- SATCOM: A highly precise sync plane is essential for control and command centers for satellite communications. The GM330 Time server provides unparalleled performance for the SATCOM sync plane and is trusted by many customers.
- Calibration Services: Providing a single source for a reliable clock that is both cost-effective and essential in calibration and testing services. When it comes to reliability and performance, the GM330 Time server provides the best cost-performance choice for a reliable clock in testing services and hence, is widely deployed in many calibration services use cases for this purpose.
- Financial Networks: A highly accurate clock is standard in high-performance trading, computing, and many other financial services systems. The GM330 Time server meets stringent MiFID standards as a highly accurate clock source for financial networks.
- Data Center: Many applications including distributed database systems need highly

accurate clocks that are difficult to obtain through NTP-based time distribution. Thus, many data centers choose application-centric sync clusters to provide a highly accurate clock where it is needed. The GM330 Time server is both a cost-effective and highly reliable clock source for application-centric point of delivery (POD). Additionally, the GM330 Time server is a profile-rich device that provides appropriate PTP profiles for different use cases of distributed data centers in various industry verticals.



Today's mission-critical infrastructure relies on a highly accurate clock for various clusters within the network infrastructure. The GM330 Time server meets and exceeds the performance requirements of many industry verticals as edge grand master.

Its price performance is ideal for highly distributed sync plane design. Additionally, the GM330 Time server offers holdover capabilities and thus guarantees a highly precise reliable clock source during network anomalies.

1.1 Product Overview

The Protempis Thunderbolt GM330 Time server is a Stratum 1 IEEE-1588 PTP grandmaster clock with an integrated Protempis GNSS receiver (referred to in this document as the timeserver). The Time server is designed and optimized for deployment in wireless service provider networks to meet the stringent time and phase requirements of 4G/5G and small cell networks.
It provides NTP, PTP, and Synchronous Ethernet timing protocols. The Time server uses GNSS (Global Navigation Satellite Systems) signals from GPS, GLONASS, Galileo, Beidou, QZSS, and NavIC as the primary time source for synchronization.

The Time server can use its built-in, disciplined OCXO (oven-controlled crystal oscillator) as an autonomous time base for providing several hours of accurate holdover in case GNSS signals are not available.

Hardware redundancy can be achieved by using two Time servers.

The Time server comes in a rack-mountable enclosure; two units fit side-by-side in a 1RU height 19" rack.

1.2 Key Features

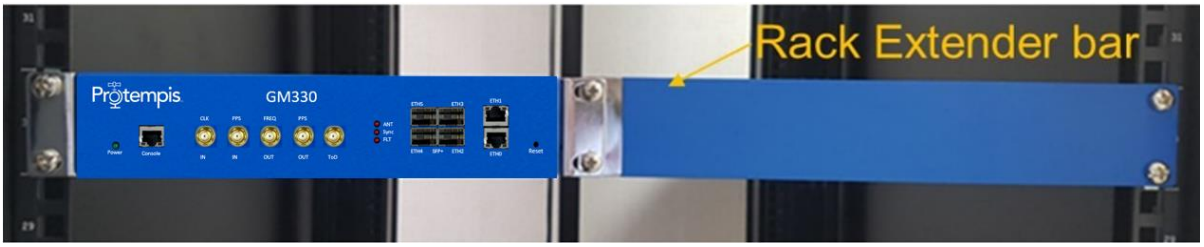
- IEEE-1588 Precision Time Protocol (PTP) grandmaster clock
- Network time server (NTP v4)
- PRTC-B class T-GM
- Holdover ± 1.5us for > 4h @ 25 °C (after seven days locking)
- Single or Dual Frequency (L1 & L5) Option
- Multi-GNSS receiver (GPS, GLONASS, Beidou, Galileo,QZSS and Navic)
- 2 10/100/1000 Base T RJ45 port (NTP/PTP/SyncE) DC and POE+ Eth0 Only
- 4x 1G/10G SFP+ interface (NTP/PTP/SyncE)
- 6 SMA ports (Inputs: GNSS, PPS, CLK) (Outputs: FREQ, PPS, ToD) (In/Out: NTP, PTP, SyncE)
- IPv4, IPv6, and VLAN support
- VLAN-aware layer2 switching
- 1 RJ45 console serial port up to 230K Bits/s
- HTTP, HTTPS, SCP, FTP, TFTP, FTPS, and SFTP
- DC (default) POE+, and AC power options
- Small footprint -½ Rack1U
- Wide operating temperature range, -40 °C to +50 °C
- PTP Freerun mode
- PTP APTS mode
- PTP T-BC mode

1.3 Physical Specifications

1.3.1 ETSI standard 19" rack mounting

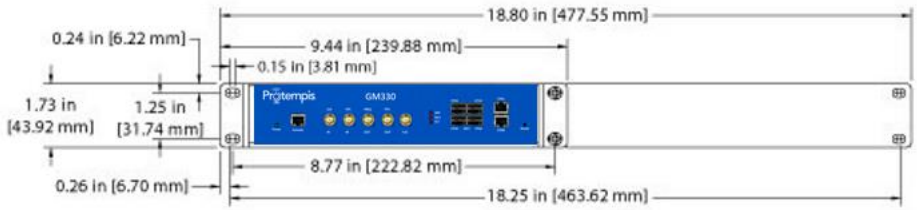
The Time server can be installed in a 19" half rack size mount unit with a 1U form factor.

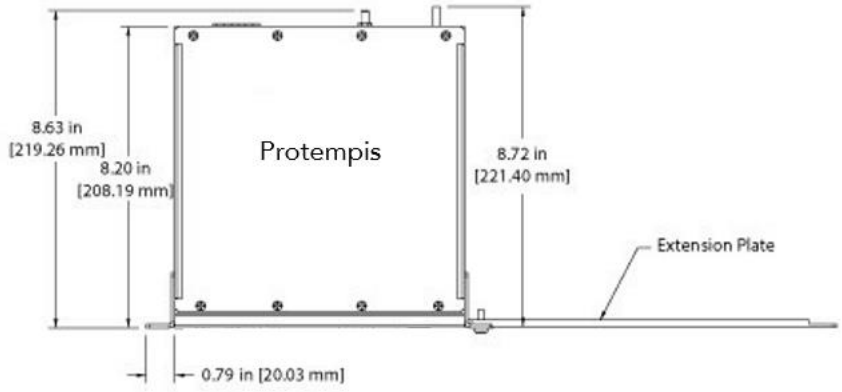
You can install one Time server with a rack-mounting extender (included in the product box in the ETSI standard 19" rack)



or two Time servers, installed side-by-side in a full-rack space for additional redundancy.

1.3.2 Mechanical Specification Diagram





1.5 Front panel elements

The RJ45 console serial port provides an interface with up to 230k bits/sec to the Time serve.

1.5.2 SMA Female/Jack

The Time server has SMA female connectors that provide IN and OUT signals

CLK IN	10MHz, 3.3V, 5V tolerant
PPS IN	1PPS, 3,3V, 5V tolerant
FREQ OUT	Selectable frequency output, 10MHz default, 1.2V into 50 Ω or 3.3V into 1 MΩ square wave
PPS OUT	1PPS, PP2S output, 1.2V into 50 Ω or 3.3V into 1 MΩ

ToD	Various Outputs, DC encoded TOD default, 3.3V

1.5.3 Status LED

Alarm and status information is shown using four LEDs. In a critical alarm condition, the dry contact relay output at the rear of the Time server is closed.

LED	Color	Indication	Meaning
Power	Green	ON	The system is powered on
		OFF	The system does not have power
ANT	Red	ON	GNSS module failed
		Blinking, 1Hz	Reference being acquired/searched. No fixes are available.
		OFF	Reference acquired & Tracking
Sync	Green	ON	Locked
		Blinking, 1 Hz	Halt mode, Recovery mode
		Blinking, 1/2 Hz	Holdover mode
		OFF	Freerun, jamming or re-aquisition
FLT	Red	OFF	No active alarms
		ON	Critical alarm
		Blinking, 1 Hz	Minor alarm condition
		Blinking, 1/2 Hz	Major alarm condition
Port Link Status	Green		
Port Activity	Yellow/Green dual		

1.5.4 Console Port

The Time server has one dedicated management port. The RJ45 port provides serial connectivity. Default: 115,200, N,8,1

1.5.5 Ethernet Port (Eth 0 - Eth 1)

Two RJ45 ethernet port that provides NTP/PTP connectivity to Ethernet networks.

Port Speed	1G
POE+	Only Eth0
SyncE IN	1 primary and 1 secondary
SyncE OUT	All ports
Management	Any port can be used as management when configured with the appropriate VLAN and VIF

1.5.6 SFP+ Port (Eth 2 – Eth5)

The Time server supports one SFP+ port, that provides NTP/PTP connectivity to Ethernet networks.

Port Speed	1G or 10G
POE+	None
SyncE IN	1 primary and 1 secondary
SyncE OUT	All ports
Management	Any port can be used as management when configured with the appropriate VLAN and VIF

The following SFPs have been tested by Protempis for the electrical SFP module:
(For the latest information go to the www.protempis.com web site)

Part number 1G (Copper)	Type	Manufacturer
FCLF8521P2BTL	RJ45	FINISAR
S-RJ01	RJ45	MICROTIC
SFP-GB-GE-T	RJ45	Fiberstore
SFP-1GBT-05	RJ45	Electrical Belfuse
1G (Fiber)		
SFP-1G85-5MDA	LC	Fiberstore

The following specification is for the recommendation of SFP+ modules:

SFP+ module 10G (Copper)	Type	Manufacturer
ASF-10G-T	RJ45	Ipolex
ASF-10G2-T	RJ45	Hi Fiber
ASF-10G-T	RJ45	HiFiber
CAB-10GSFP-P0.5M	RJ45	Hi Fiber
(Fiber)		
TAS-A1NH1-P11	LC	FORMERICAOE
SFP-10G-LR	LC	10Gtek
AXS86-192-M3	LC	Hi Fiber
AXS85-192-M3	LC	10Gtek

1.6 Back panel elements

1.6.1 GNSS antenna connection

The Time server has an SMA connector for the antenna input to the embedded GNSS receiver.

1.6.2 Power Input

The standard input power is -48 V DC, 1A. The Time server provides a 5-pole terminal block to connect dual DC power inputs.

1.6.3 Alarm Relay

The Time server provides a 3.81 mm 3-pin terminal header for the dry relay connection. Both Normally Open (NO) and Normally Closed (NC) connections are available to the user. The relay closure is considered closed in Critical alarm conditions.

1.6.4 Grounding

The frame ground connection on the Time server is available through an M5 grounding terminal stud.

1.7 Use and care

The Time server is a high-precision electronic instrument and should be treated with reasonable care. Typically, it doesn't need any care after the first setup. If you need to clean the unit, use a dry non-static tissue or a light moist tissue to remove dust or stain from the enclosure. Ensure that water does not enter anywhere in the enclosure. Do not use solvents, or aggressive or abrasive cleaning products anywhere on the Time server.

> CAUTION – There are no user-serviceable parts inside the Time server. Any modification to the unit by the user voids the warranty.

1.8 Technical assistance

If you have a problem and cannot find the information you need in the product documentation, contact Protempis technical support at email support@Protempis.com.

2. Installation

2.1 Getting Started

This section explains how to install and configure the Time server.

Unpack and inspect the content of the box. The following items are included in the standard box:

Item	Quantity	Description
Quick reference guide	1	Simple description
Time server	1	Thunderbolt GM330
Mounting brackets	2	Rack mounting brackets and installation accessories for 19" standard rack
Dummy plate	1	Extender bar for a single unit installation in a 19" standard rack

2.2 Mounting the device to a rack

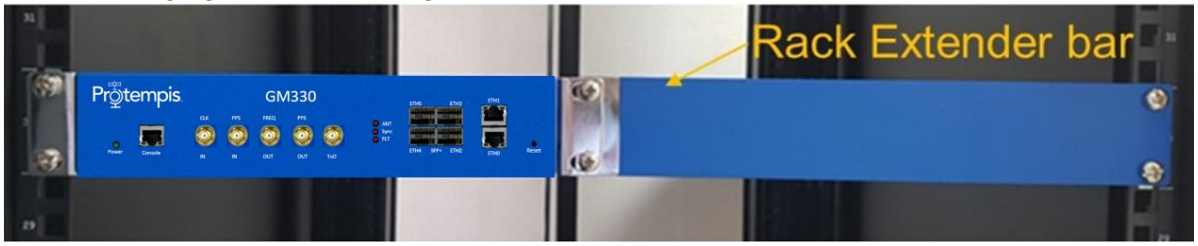
The Time server should be installed indoors or outdoors in an environmentally controlled cabinet.

ETSI Standard 19 Inch Rack Mounting

The Time server supports a 19” half-rack size with a 1U form factor.

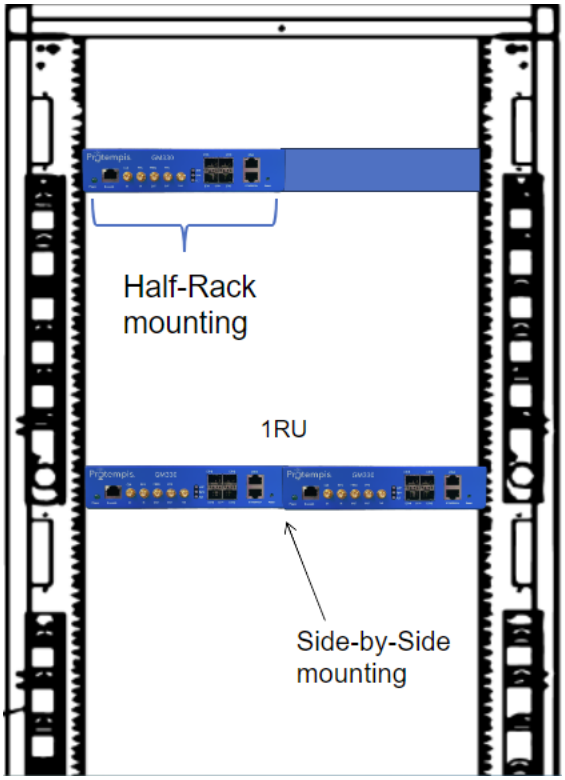
You can install one Time server with a rack-mounting extender, included in the product box in the ETSI standard 19” rack, or you can install two Time servers side by side.

The following figure shows a single-time server installation.



The following figure shows a rack-mounting extender (included in the box).

The following figure shows a dual-time server installation.



2.3 Connecting Power

The Time server supports single- or dual-redundant DC power supplies. The standard option is 48 V DC. The unit can operate from -36 V DC to -72 V DC.

The DC input is reverse polarity protected. Reversing polarity with 48 V DC options will not damage the unit and the unit will operate normally. RJ45 Eth0 POE+ only accepts +48V DC.

NOTE – The power cable should be routed separately from the data (signal) cables.

Except Eth0

The table below shows the DC power interface information:

Item	Description	Note
Interface name	DC power	
Connector type	RJ45 Eth0 only	Powered Device(PD) +48V DC
Connector type	Terminal block	
Number of power inputs	Dual -48 V DC input	
Maximum DC power input range	-36 V DC to -72 V DC	
Overall power consumption	Steady-state default config without any SFPs plugged in: ~13-15W. Fully populated with optical SFPs with normal load: ~20-22W. Fully populated with 10G copper SFPs with apps and data traffic, max: ~26-30W.	

Wiring	Solid wire: 30 AWG~ 12 AWG/ 0.05 to 3.3 MM² Stranded wire: 30 AWG~ 12 AWG / 0.05 to 3.3 MM² Torque for screws: 4.0 lb-In / 0.45 Nm	Wire strip length: 9 mm recommended
Power damage protection	• Overcurrent protection • Overvoltage protection • Reverse power polarity input protection • Power line surge protection	
Related alarms generation	No related alarm generation for DC power interface connection and operation	

The Time server is powered by 48 V DC with the default power input terminal block.

However, if you use a Protempis AC/DC power adapter accessory, you can power the Time server with AC power within 100 A ~ 240 V AC range.

The Time server does not have any alarms related to power input failure or related operations except for the 'Relay' operation.

2.3.1 DC Power Connection

The image below shows how to connect dual-48 V DC.

The Time server supports reverse power polarity input protection, so you can connect -48 V DC and GND cable to "-" and "+" as a pair to each input terminal without considering order.

The unit supports power over ethernet (POE+) on interface Eth0. The GM330 will get power on this port.

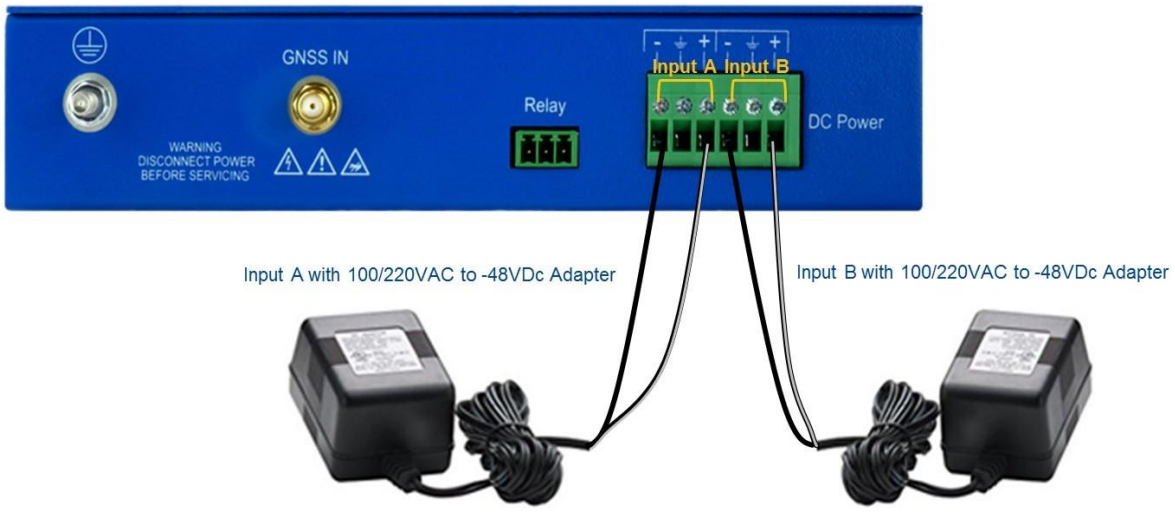
> Note - When switching the power from DC to POE the unit will reset (POE is not "hot standby" power). Switching from POE to DC should be seamless.

2.3.2 AC Power Connection

The image below shows how to connect dual100/220 V AC power.

To supply 100/220 V AC power, you must use the Protempis AC/DC Power Adapter Accessory.

The Time server supports reverse power polarity input protection, so you can connect the two strip lines from the AC/DC adapter to “-“ and “+” as a pair to each input terminal without considering order.



2.3.3 Grounding The Device

The Time server M5 terminal stud on the back panel is used for grounding.

The Time server is suitable for connection to the Central Office and CPE. The grandmaster clock must be in a restricted access location where only craft personnel are allowed access.

The Time server must be grounded via a copper ground conductor. The unit must be installed and connected to the common bonding network (CBN).

All bare grounding connection points to the Time server must be cleaned and coated with an antioxidant solution before connections are made.

All surfaces that are un-plated must be brought to a bright finish and treated with an antioxidant solution before the connection is made.

All non-conductive surfaces must be removed from all threads and connection points to ensure electrical continuity.

The DC power returns must be treated as DC-I (Isolated from Frame Ground).

The Time server requires a ring terminal with a 14-AWG wire that utilizes 15 in-lbs to secure to primary ground.

There are to be no breaks in the outer shield of the GNSS cable.

2.3.4 Powering-Up

After verification of the input power source, switch on the power supply to the Time server. The green power LED should turn ON.

2.4 GNSS Considerations

For a full description of how to choose the correct antenna cable/antenna combination, see the chapter GNSS Antenna

When connected to a GNSS antenna, the Time server can receive GNSS signals without user intervention—the factory default is GPS and GLONASS. You can enable Beidou in place of GLONASS or enable single-constellation mode.

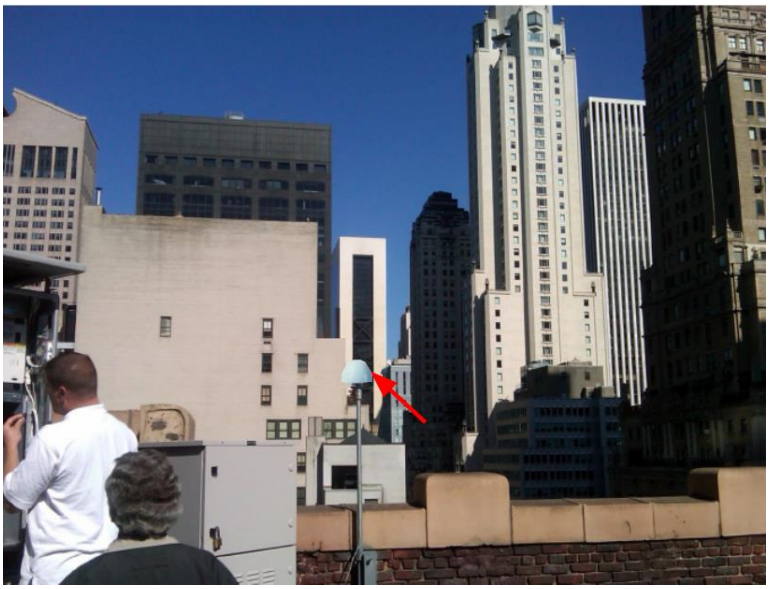
The recommended antenna is the Protempis Bullet 720, which supports GPS, GLONASS, Beidou, Galileo, QZSS, and NavIC

2.4.1 Selecting a site for the GNSS antenna

The GNSS antenna must have the fullest possible view of the sky. In most cases, this means installing the antenna on a high point, such as a rooftop. Avoid overhanging objects such as trees and towers. Also, take care to place the antenna away from low-lying objects such as neighboring buildings that may block a portion of the sky near the horizon. If a full view of the sky is not possible, mount the antenna and aim it toward the Equator to maximize the southern view of the sky (choose a northern view in the Southern Hemisphere).

Use the criteria below to select a good outdoor site for the antenna. The best locations provide:

- Unobstructed views of the sky and horizon.
- Low electromagnetic interference (EMI) and radio frequency interference (RFI) -away from high-power lines, transmitting antennas, and powerful electrical equipment.
- Convenient access for installation and maintenance.
- Reasonable access for the antenna cable to reach the Time server.



2.5 Communication Ports

The Time server has seven communications ports on the front panel:

- Any port can be used for management
- 1 × console serial port (RJ-45)
- 2 × traffic port autosensing ethernet (eth0 , eth1) 10/100/1000 Base-T (RJ-45)
- 4 × traffic port SFP+ (Small Form-Factor Pluggable)

Either the console serial port or ethernet Eth0 - Eth5 (RJ-45) can be used to manage and configure the Time server.

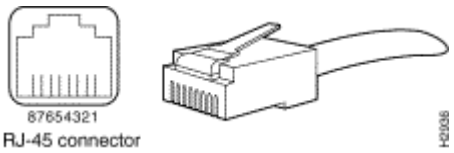
2.5.1 Console Serial Port

A bi-directional console RJ45 serial port is located on the left side of the front panel. The serial port provides access to the command line interface (CLI) for the status and configuration of the Time server.

Use a straight-through cable with the following settings:

Data rate	115,200 baud
Parity	None
Data bits	8
Stop bits	1

Console Serial Port Pin Assignment



Pin	RJ-45 signal	Description of Echo Side
1	NC	No Used
2	NC	Not Used
3	RxD	Data Receive
4	GND	Ground
5	GND	Ground
6	TxD	Data Transmit
7	NC	Not Used
8	NC	Not Used

The table below shows the Console Serial port:

Item	Description	Notes
Interface name	Console	
Connector type	RJ-45	
Required cable	Console cable	
Usage	Local serial console for CLI	
Related software tool	Terminal program	Ex., Tera term, Putty
Serial configuration	Baud rate: 115,200 Parity: None Data bits: 8 Stop bits: 1	
Console ID/PW	protempissuper / super	Supervisor level only

2.5.2 Management /Timing Ethernet Port

The Time server supports two 10/100/1000 Base-T ethernet ports that allow connection to standard CAT-5 / CAT-5e / CAT-6 cables with an RJ-45 male connector. The SFP+ ports

Support 1G/10G copper and Fiber modules.

The ethernet port features an LED that indicates its state. You can use any of these ports to access the web interface (HTTPS) or command line interface (SSH).
As long as the VIF connection allows the device to be reachable.

The factory default settings for the Ethernet network ports are:

Ethernet 0	Ethernet Port RJ-45 (Marked Eth0) Default: DHCP access mode	VLAN 2
Ethernet 1	Ethernet Port RJ-45 (Marked Eth1) Default: Static 192.168.1.250/24	VLAN 1
Ethernet 2	Ethernet Port RJ-45 (Marked Eth2) Default: Static 192.168.1.250/24	VLAN 1
Ethernet 3	Ethernet Port RJ-45 (Marked Eth3) Default: Static 192.168.1.250/24	VLAN 1
Ethernet 4	Ethernet Port RJ-45 (Marked Eth4) Default: Static 192.168.1.250/24	VLAN 1
Ethernet 5	Ethernet Port RJ-45 (Marked Eth5) Default: Static 192.168.1.250/24	VLAN 1

The table below shows the Eth1-RJ45 interface:

Item	Description	Notes
Interface name	Eth1, (Eth0 DHCP)	
Connector type	RJ45	
Initial operating status	Enabled	
Required cable	Recommended UTP CAT-5E or Better	
Specification	10/100/1000Base-T	
Auto-negotiation mode	Supports1000Base-X auto-negotiation mode only	
Item	**Description**	**Notes**
Usage	Management only for remote access	SSH, web interface
Related software tool	Terminal Program, Protempis web interface, and NMS	Ex., Tera term, Putty
Connection information	Default IP address: 192.168.1.250	Netmask: /24
Connection ID / PW	protempissuper / super	Supervisor level
Port LED	Left side LED: Link Right side LED: Act	

NOTE - Time Server default password is "**protempissuper**" and the default password is “Tbolt_SN#”

Example:
Serial Number of the unit = 2246015779
Password: Tbolt_2246015779

2.5.3 PTP/NTP/SyncE electrical ethernet port

The Time server supports two 10/100/1000 Base-T ethernet ports or four SFP+ 1G or 10G ports that allow connection to standard CAT-5 / CAT-5e / CAT-6 cables with RJ-45 male connector or for SFP+ Fiber.

The ethernet port features an LED that indicates the state of the port. For security reasons, this port is not designed for communication purposes. This port is designed to provide NTP/PTP/SyncE.

NOTE - The ethernet interface should not be connected to a cable longer than 100 meters. If a distance greater than 100 meters is required, then the ethernet interface should be connected to a switch.

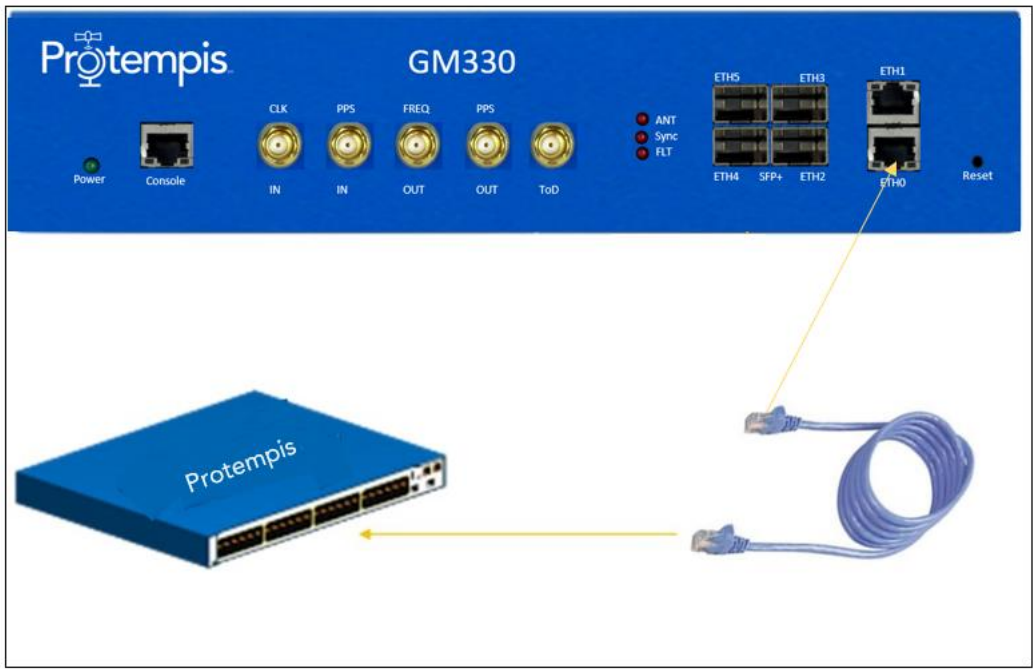
The table below shows the Eth1 or Eth0 -RJ45 interface:

Item	Description	Notes
Interface name	Eth1 or Eth0	
Connector type	RJ45	
Initial operating status	Disabled	
Required cable	Recommended UTP CAT-6 or CAT-6E	
Specification	10/100/1000Base-T	
Auto-negotiation mode	Supports1000Base-X auto-nego mode only	
Usage	Input and Output for PTP, NTP, and SyncE	
PTP accuracy	ITU-T G.8272 PRTC Class B	

Port LED	Left side LED: Link Right side LED: Act

The Eth1 interface is dedicated to synchronization signal input and output to support PTP (IEEE 1588), NTP, and SyncE. It supports 10/100/1000Base-T with Auto-nego mode. It is recommended to use UTP-CAT6 or UTP-CAT6E cable.

When it is linked on, the left-side LED on the RJ45 connector indicators for “Link” connection and the right-side LED indicators for “Act” states. The following illustration shows that the Eth1 interface is connected to a UTP cable and RJ-45 port.



2.5.4 PTP/NTP/SyncE SFP+ ethernet ports (2 to 5)

The Time server supports four 10/100/1000 Base-T ethernet ports that allow connection to standard CAT-5 / CAT-5e / CAT-6 cables with electrical SFP or fiber cables with optical SFP+ 1G or 10G. The ethernet port features an LED that indicates the state of the port.

The table below shows the Eth2 to Eth5 -SFP interfaces:

Item	Description	Notes
Interface name	Ethernet 2 to Ethernet 5	
Connector type	SFP+	
Initial operating status	Disabled	
Required cable	Single-mode or multi-mode optic fiber	

Specification	1000Base-X	
Auto-negotiation mode	Supports1000Base-X auto-nego mode and 1000Base-X forced mode (auto-nego off mode)	No support for Forced mode on the electrical SFP module
Recommended SFP Module	1000Base/10G -SX, LX, BX, and electrical SFP (10/100/1000Base-T SFP)	
Usage	Input and Output for PTP, NTP, and SyncE	To support SyncE with an electrical SFP module, it should be a verified one by Protempis.
PTP accuracy	ITU-T G.8272 PRTC Class B	
Port LED	Left side LED: Link Right side LED: Act	
Related alarms generation	Default: Ignored, no alarm asserted Asserted 'Eth-Port0-Down' when Eth0 Link is off. Asserted 'Eth-Same-Subnet' when ethernet interfaces have the same IP address in subnet class B.	Cleared when the Eth0 link is on. Cleared when ethernet interfaces have different subnets.

Eth 0 to Eth 5 interfaces are dedicated to synchronization signal input and output to support PTP (IEEE 1588), NTP, and SyncE.

Eth 0 to Eth5 supports 1G/10G Base-X with supporting "1G/10G Base-X auto-nego" mode and "1G/10G Base-X forced mode" when the "auto-nego" mode is off based on user configuration.

Also, it supports the Electrical SFP module to support 10/100/1000Base-T auto-nego mode on the SFP+ interface.

2.5.5 Approved and Tested SFP Modules

The following SFPs have been tested by Protempis for the electrical SFP module:

Part number 1G (Copper)	Connector Type	Manufacturer
FCLF8521P2BTL	RJ45	FINISAR
S-RJ01	RJ45	MICROTIC
SFP-GB-GE-T	RJ45	Fiberstore
SFP-1GBT-05	RJ45	Electrical Belfuse
1G (Fiber)		
SFP-1G85-5MDA	LC	Fiberstore

The following specification is for the recommendation of SFP+ modules:

SFP+ module 10G (Copper)	Connector Type	Manufacturer
ASF-10G-T	RJ45	Ipolex
ASF-10G2-T	RJ45	Hi Fiber
ASF-10G-T	RJ45	HiFiber

CAB-10GSFP-P0.5M	RJ45	Hi Fiber
(Fiber)		
TAS-A1NH1-P11	LC	FORMERICAOE
SFP-10G-LR	LC	10Gtek
AXS86-192-M3	LC	Hi Fiber
AXS85-192-M3	LC	10Gtek

Note: Power Consumption. If using 10G connections, consider using 10G SFPs fiber which consumes 0.9W Compared with 10G coppers at 3.5W per port

2.5.6 Port Speed Settings

Port Type	SFP Type	Configured Setting	Operational Setting
RJ45 (ETH0-ETH1)	N/A	Auto-negotiation	Auto-negotiation (10/100/1000)
RJ45 (ETH0-ETH1)	N/A	Manual (Any)	Fixed (10/100/1000)
SFP+ (ETH2-ETH5)	Copper 1G	Auto-negotiation	Auto-negotiation (1G)
SFP+ (ETH2-ETH5)	Copper 10G	Auto-negotiation	Auto-negotiation (10G)
SFP+ (ETH2-ETH5)	Copper 1G	Manual (Any)	Fixed (1G)
SFP+ (ETH2-ETH5)	Copper 10G	Manual (Any)	Fixed (10G)
SFP+ (ETH2-ETH5)	Optical 1G	Auto-negotiation	Fixed (1G)
SFP+ (ETH2-ETH5)	Optical 10G	Auto-negotiation	Fixed (10G)
SFP+ (ETH2-ETH5)	Optical 1G	Manual (Any)	Fixed (1G)
SFP+ (ETH2-ETH5)	Optical 10G	Manual (Any)	Fixed (10G)
SFP+ (ETH2-ETH5)	DAC	Auto-negotiation	Fixed (10G)
SFP+ (ETH2-ETH5)	DAC	Manual (1G / 10G)	Fixed (1G / 10G)

RJ45 ports:
The GM330 supports 2 RJ45 ports (ETH0 and ETH1), which can be operated at speeds of 10M, 100M and 1G. These ports support both auto-negotiation and manual speed and duplexity configuration settings. The default configuration setting is auto-negotiation.

It is recommended that the RJ45 ports and their remote counter parts be configured with the default auto-negotiation settings. If the remote ports do not support auto-negotiation, or if a successful link cannot be established via auto-negotiation, both sides of the connection need to be configured for the correct manual speed and full duplex settings to establish a link and ensure correct port operation. For these ports, the configured and operational values for the port speed settings (auto-negotiation or manual) will always match.

SFP+ ports:
The GM330 supports 4 SFP+ ports (ETH2-ETH5), which can be operated at speeds of 1G or 10G. These ports support both auto-negotiation and manual speed and duplexity configuration settings. The default configuration setting is auto-negotiation.

The SFP+ ports support hot-pluggable SFPs that can be inserted and removed at any time. Auto-negotiation is only supported on copper SFPs. It is not supported on optical or DAC SFPs. The port speed settings are configured at the port level and not per SFP. The GM330 will factor in the configured port settings and the SFP capabilities of the plugged in SFP and apply the port settings accordingly. NOTE: The SFP capabilities (i.e. type and speed) are inferred from reading the SFP EEPROM information. For some SFPs, the correct capabilities may not be programmed in the EEPROM, in which case, the GM330 will try and set default behavior.

It is recommended that the SFP+ ports be configured with the default auto-negotiation settings. With this setting, when a copper SFP is plugged in, the port is set for auto-negotiation. In this case, the configured and operational values for the port speed settings will match and indicate auto-negotiation.

When an optical SFP is plugged in, the advertised maximum SFP speed capability is checked, and the port speed is set to 1G or 10G accordingly, with a duplexity of full-duplex. In this case, the configured port speed setting will indicate auto-negotiation, and the operational value will indicate fixed.
When a DAC SFP is plugged in, the port speed is set to 10G, with a duplexity of full-duplex. In this case, the configured port speed setting will indicate auto-negotiation, and the operational value will indicate fixed.

If a successful link cannot be established via auto-negotiation, both sides of the connection need to be configured for the correct manual speed and full duplex settings, based on the SFP capabilities of both ends, to establish a link and ensure correct port operation. For these ports, the configured and operational values for the port speed settings (both manual) will match.

2.5.7 CLK IN

The following table shows the Sync Out interface:

Item	Description	Notes
Interface name	Sync Out	
Connector type	SMA (Female), 50Ω	Female type
Specification	3.3 V DC CMOS level 5V Tolerant	
Required cable and connector	50Ω coaxial cable with SMA (male) connector for the Time server side	
Usage	10 MHz input	Reference

The CLK IN interface is an SMA (Female) connector with 50 Ω.

The coaxial cable: use 50 Ω cable with RG-58 or above specification cable in a short distance.

2.5.8 PPS IN

The following table shows the PPS IN interface:

Item	Description	Notes
Interface name	PPS IN	
Connector type	SMA (Female), 50Ω	Female type
Specification	3.3 V DC CMOS level 5V Tolerant	
Required cable and connector	50Ω coaxial cable with SMA (male) connector for the Time server side	

Usage	1PPS input	Reference

The PPS IN interface is an SMA (Female) connector with 50 Ω.

The coaxial cable: use 50 Ω cable with RG-58 or above specification cable in a short distance.

2.5.9 FREQ Out

The following table shows the FREQ Out interface:

Item	Description	Notes
Interface name	FREQ Out	
Connector type	SMA (Female)	Female type
Specification	1.2V into 50 Ω or 3.3V into 1 MΩ Square wave	
Required cable and connector	SMA (male) connector for the Time server side	
Usage	Fixed 10 MHz (default) square wave (Selectable option will be provided in a Future Release)	

The Freq Out interface is an SMA (Female) connector

This interface is a selectable frequency output or 10 MHz configured by the user.

Cable: Use a short-distance cable.

2.5.10 PPS Out

The following table shows the PPS Out interface:

Item	Description	Notes
Interface name	PPS Out	
Connector type	SMA (Female)	Female type
Specification	1.2V into 50 Ω or 3.3V into 1 MΩ	
1PPS accuracy	± 5 ns(1-sigma) to GPS time	When the Time server is locked with GNSS
Required cable and connector	SMA (male) connector for the Time server side	
Usage	1PPS output (default) or PP2S output	By user configuration

The PPS Out interface is an SMA (Female) connector.

This interface can output 1PPS or PP2S as configured by the user.

Cable: Use a short-distance cable.

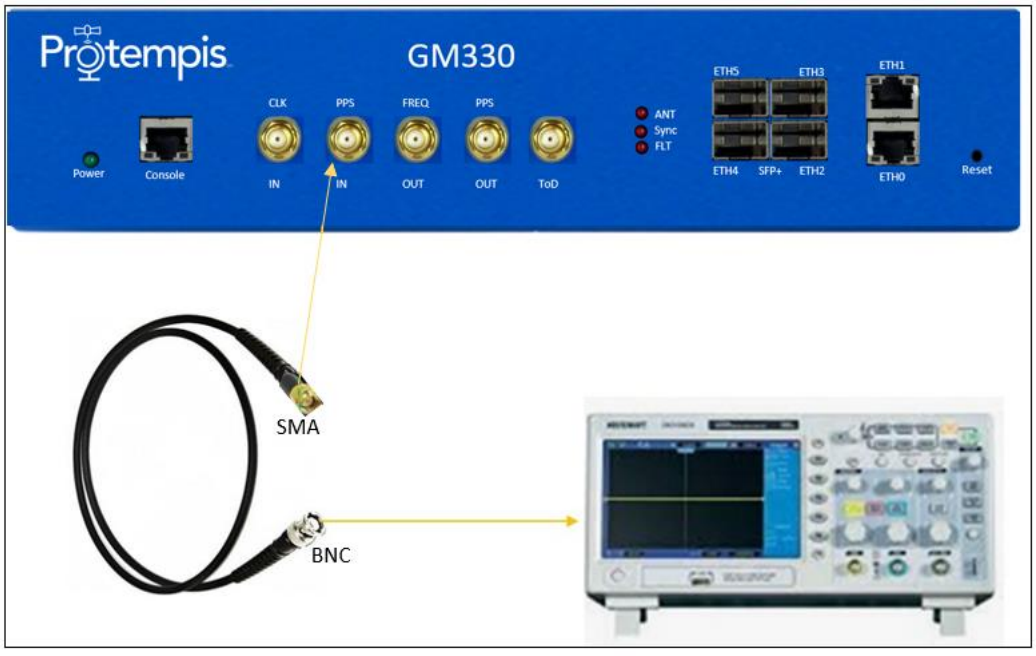
2.5.11 ToD Out

The following table shows the ToD Out interface:

Item	Description	Notes
Interface name	ToD Out	
Connector type	SMA (Female), 50Ω	Female type
Specification	3.3 V DC CMOS level	
Required cable and connector	50Ω coaxial cable with SMA (male) connector for the Time server side	
Usage	Various outputs, DC encoded PTP ToD output (default)	By user configuration
Related alarms generation	No related alarm generation for 'Sync Out' interface connection	

The Sync Out interface is an SMA (Female) connector with 50 Ω.

This interface can output various outputs or DC-encoded PTP ToD as configured by the user. The coaxial cable: use 50 Ω cable with RG-58 or above specification cable in a short distance.



2.5.12 Relay Interface Connection

Relay 'Open' and 'short' (close) operations are directly related to Alarm operation.

The alarm conditions are CRI: Critical, MAJ: Major, MIN: Minor, and IGN: Ignore.

This Relay interface only reacts when a "CRI" alarm occurs or on Power off; it does not react for MAJ, MIN, and IGN alarms. However, when the Time server is in the Holdover mode, the relay reacts as a "CRI" alarm.

Alarm conditions (CRI, MAJ, or MIN) can energize the relay and are programmable through the user interface.

① and ② Pins

- When Power is off or a CRI alarm occurs on the Time server, these pins are CLOSED (shorted) with 0Ω.
- When the Time server is in normal operation (without any CRI alarms), these pins are OPEN with ∞Ω as NO (normally open).

② and ③ Pins

- When Power is off or a CRI alarm occurs on the Time server, these pins are OPEN with ∞Ω.
- When the Time server is in normal operation (without any CRI alarms), these pins are CLOSED (shorted) with 0Ω as NC (normally closed).

3

3. GNSS Antenna

A good GNSS antenna and a good installation site are the keys to getting the best performance from a GNSS receiver.

This chapter explains the requirements for the antenna and provides recommendations for a good installation.

3.1 GNSS antenna requirements

The antenna receives the GNSS satellite signals and passes them to the receiver. The GNSS signals are spread spectrum signals in the 1551 MHz to 1614 MHz range and do not penetrate conductive or opaque surfaces. Therefore, the antenna must be located outdoors with a clear view of the sky. The internal GNSS receiver requires an active antenna with an integrated Low Noise Amplifier (LNA). The received GNSS signals are very low power, approximately -130 dBm, at the surface of the earth. Protempis' active antenna includes a pre-amplifier that filters and amplifies the GNSS signals before delivery to the receiver.

The on-board circuits provide DC supply voltage on the SMA coax connector for the external, active GNSS antenna. The antenna supply voltage is fully protected against short circuits by the onboard Open/Short detection with an integrated current limiter. The Time server has a full antenna monitoring circuit on board.

3.1.1. Antenna power supply on RF output

Make sure that the current draw of the antenna is above the open circuit and below the short circuit detection thresholds below

Voltage:	+5 V DC +/-0.5 V
Current detection:	Open circuit < 10 mA
	Short circuit > 100 mA

3.1.2 Antenna Gain Requirements

The Time server requires an active GNSS antenna with built-in LNA for optimal performance. The antenna LNA amplifies the received satellite signals for two purposes:

a. Compensation of losses on the cable.

b. Lifting the signal amplitude to a suitable range for the receiver front-end.

Task b) requires amplification of at least 15 dB, while 20 dB is optimum for the Time server. This would be the required LNA gain if the antenna was directly attached to the receiver without a cable in between. The cable and connector between the antenna and the receiver cause signal loss. The overhead over the minimum required 15 dB and the actual LNA gain of the antenna is available for task a). So, in the case of a 30 dB LNA gain in the antenna, 15 dB is available for compensating losses.

In other words, the attenuation of all elements (cables and connectors) between the antenna and the receiver can be up to a total of 15 dB with a 30 dB LNA. With a different antenna type, take the difference between 15 dB and the antenna's LNA gain as the available compensation capability. Subtract the insertion losses of all connectors from the 15 dB (or whatever the number is) and the remainder is the maximum loss, which your cable must not exceed.

As the GNSS signals are hidden in the thermal noise floor, the antenna LNA mustn't add more noise than necessary to the system; therefore, a low-noise figure is even more important than absolute amplification.

Protempis does not recommend having more than 35 dB remaining gain (LNA gain minus all cable and connector losses) at the antenna input of the receiver module. The recommended range of remaining LNA gain at the connector of the receiver module is 20 dB to 30 dB, with a minimum of 15 dB and a maximum of 35 dB.

It is not recommended to use additional amplifiers in the RF path. That includes dedicated inline amplifiers, as well as active splitters with built-in amplifiers. Using additional amplifiers adds noise to the system and that may degrade the performance of the GNSS receiver. It also increases the risk of overloading the RF front end of the GNSS receiver if the resulting total gain exceeds the recommended gain range.

As a rule of thumb, the satellite signal strength indicators (C/No values) of the strongest satellite signals—usually seen on satellites at a high elevation—should be at, or near, 48 dBHz, and weaker satellites should be seen at lower C/No values to below 20 dBHz.

If none of the satellite signals is ever stronger than 44 dBHz, then check the antenna installation regarding the antenna placement and the cable attenuation. Likewise, if multiple C/No signals are exceeding 52 dBHz and if there are no values in the range of 20 or less, then check the antenna installation for too much overall gain.

3.1.3 Considering coaxial cable loss and delay

The following table shows cable types appropriate for different cable lengths to ensure proper GNSS signal strength. If the Time server does not receive the appropriate signal

strength, it will not be synchronized with GNSS and it will not provide PTP service for slave devices.

To calculate the cable loss:

RF in Gain in the Time server: GNSS Antenna Gain - (Surge Protector + adapters + Cable Loss) ≥ 20 dB

Example:

Bullet 40dB(40dB) – [Surge Protector(1dB) + adapter(0.5dB) + RG58_30m(19.2dB)] =19.3dB

Typical dB loss values by Cable type:

Cable type	dB / 100ft	dB / 100 meter	Max length for 18 dB loss at 1575 MHz (feet/meter)
RG-6	12	40	150/45
RG8 (and 8/U)	9.6	31	185/58
RG-8X	16.8	55	107/33
RG-58	19.6	64	92/28
RG-59	14.7	48.2	122/37
LMR-400	5.3	17.2	340/105
LMR-600	3.4	11.2	530/161

When you use a long coaxial cable, you must also consider the coaxial cable delay. The typical delay with RG-59 is around 1.24 ns/ft or around 4 ns/1 meter.

You can compensate for the cable delay time by using a CLI command.

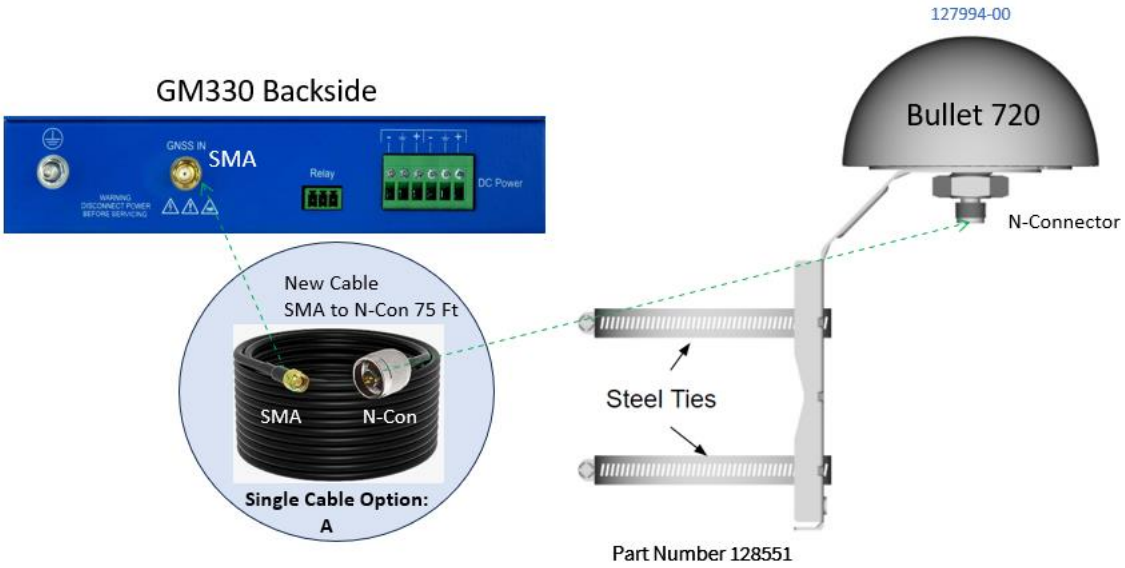
3.2 Antenna Placement

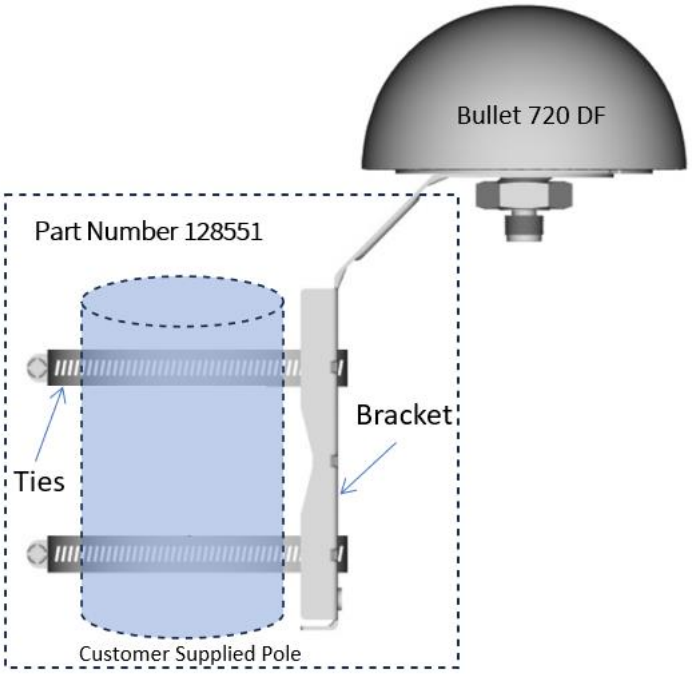
3.2.1 Mounting bracket for GNSS antenna

The mounting bracket installation and part numbers for the Protempis Bullet™ 720 antenna are:

GM330 Kit

100836-90

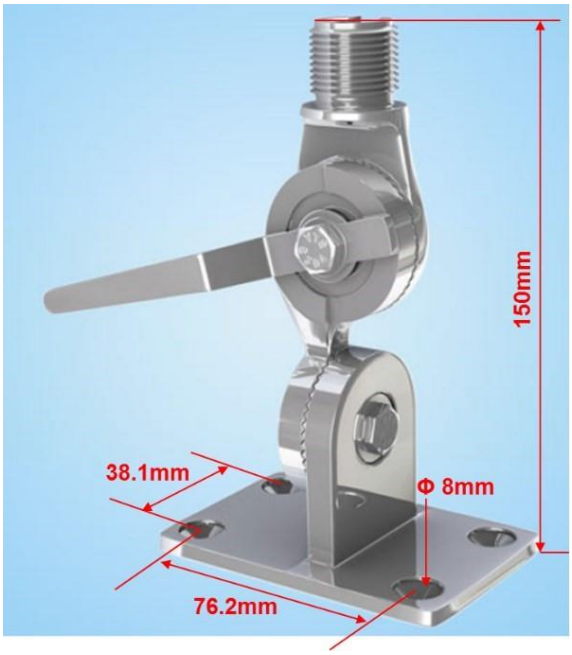




The thread specification of the Bullet antenna is a 3/4" NPT thread, dimensions according to ANSI/ASME B1.20.1. It is also called a 1"-14 marine thread because it has 14 threads per inch.

The Bullet antenna thread should fit both specifications.

In the case of an NPT thread with tapered type, the geometry of the thread shape must meet the standard, but the tolerance of the base diameter can be fairly large without violating the standard, due to the conical shape of the thread.



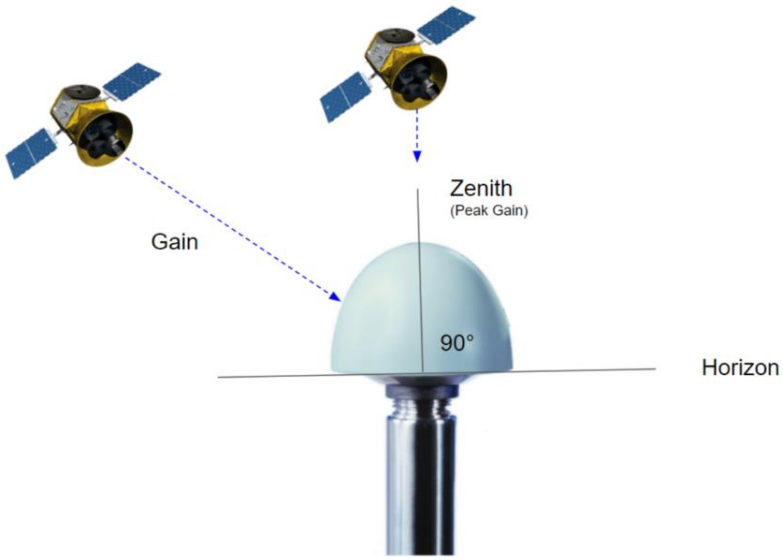
3.2.2 Sky Visibility

GNSS signals can only be received on a direct line of sight between the antenna and the satellite. The antenna should see as much as possible of the total sky.

Seen from the northern hemisphere of the earth, more satellites will be visible in the southern direction rather than in the northern direction. The antenna should therefore have an open view of the southern sky. If there are obstacles at the installation site, the antenna should be preferably placed south of the obstacles to not block the sky-view to the south.

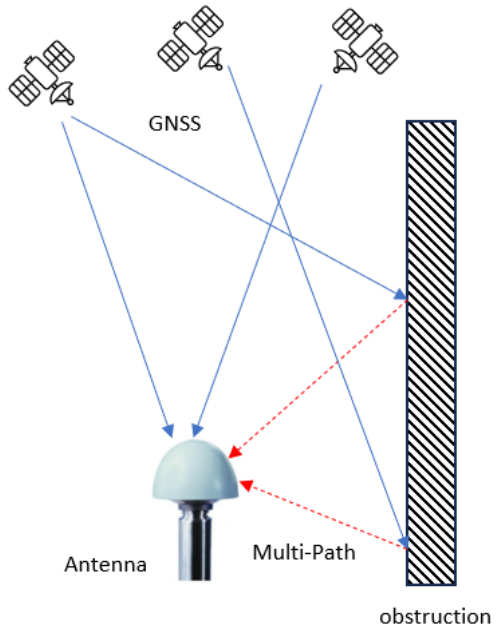
If the installation site is in the southern hemisphere of the earth, then the statements above are reversed–more satellites will be visible in the northern direction. Near to the equator, it doesn't matter.

Partial sky visibility often causes poor Dilution of Precision (DOP) values due to the geometry of the visible satellites in the sky. If the receiver can only see a small area of the sky, the DOP has a high degree of uncertainty and will be worse compared to a condition with a better geometric distribution. A receiver may see six satellites, all close together, and still gets a much worse DOP than a receiver that sees four satellites, but all in different corners of the sky. The receiver's DOP filter rejects fixes with high DOP (high uncertainty); therefore it can take longer to get the first acceptable fix if sky visibility is partly obstructed.



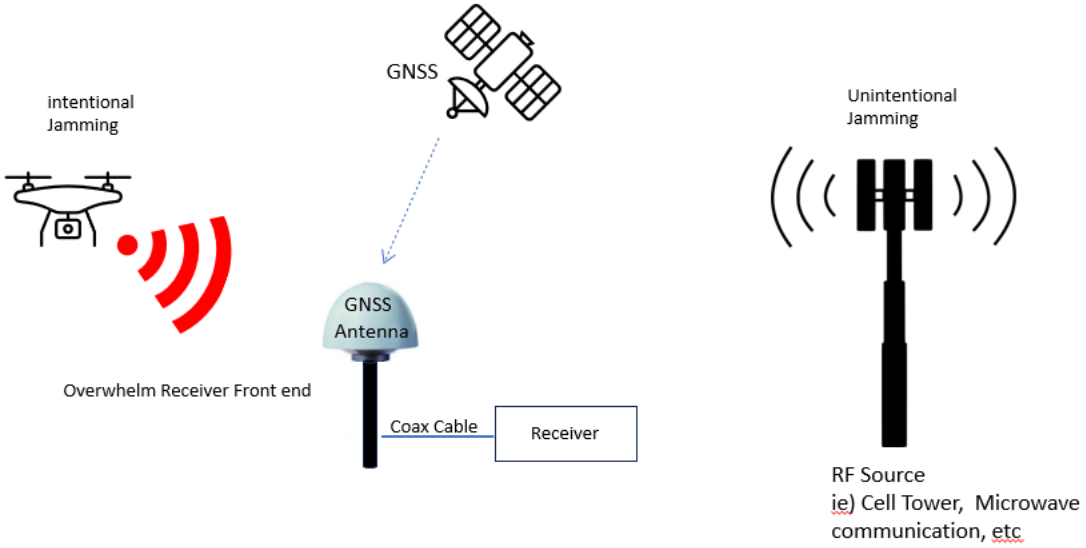
3.2.3 Multipath Reflections

Multipath occurs when the GNSS signals are reflected by objects, such as metallic surfaces, walls, and shielded glass for example. If possible, the antenna should not be placed near a wall, window, or other large vertical objects.



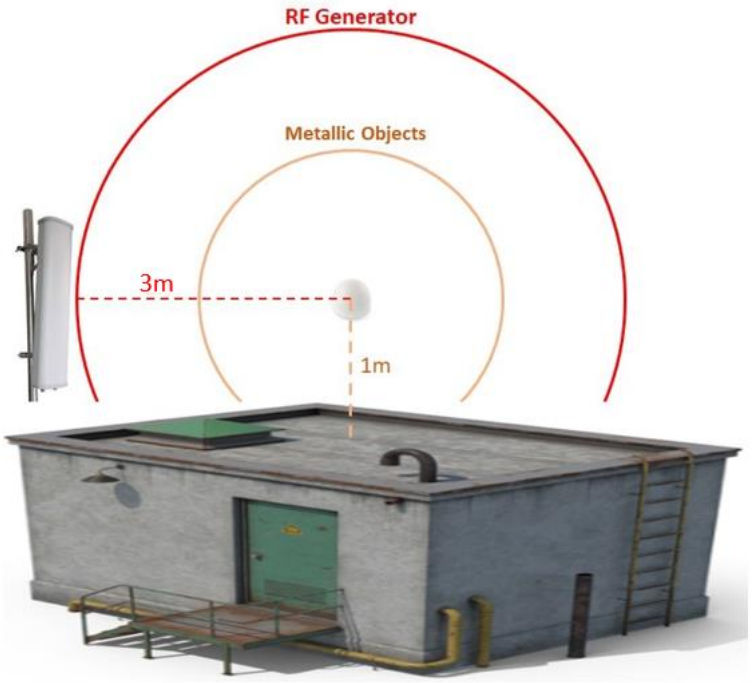
3.2.4 Jamming

Jamming occurs when the receiver function is disturbed by external radio frequency (RF) sources that interfere with GNSS signals or saturate the antenna LNA or receiver front-end. A good indicator to detect jamming is switching off all other equipment except the GNSS. Watch the satellite signal levels in this condition. Then switch on other equipment and see if the signal levels go down. A drop in signal levels indicates interference to GNSS from the other equipment. This method cannot, however, detect all possible kinds of jamming. Spurious events are hard to catch. Low-frequency fields, like 50 Hz, are unlikely to jam the receiver. Broadband sparks are a potential source of spurious jamming. There is no general installation rule or specification though because the effect of jamming highly depends on the nature of the jamming signal and there are countless potential variations, so it is not possible to standardize a test scenario.



3.2.5 Clearance of GNSS antenna location

GNSS antenna should be installed with the conditions below.

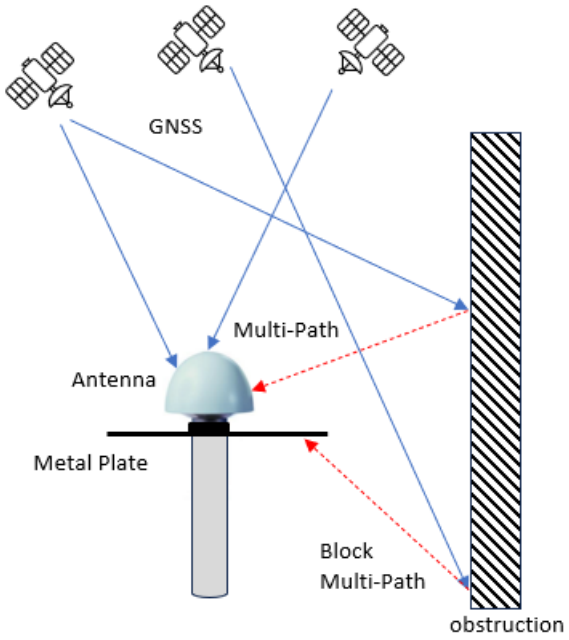


NOTE - GNSS antenna should be at least one meter away from any metallic objects to avoid multipath reflections.

NOTE - GNSS antenna should be at least three meters away from any RF generators to avoid signal interference.

3.2.6 Ground Plane

A metal plate or surface under the antenna can block signal reflections from below. This is a good method to mitigate reflections if the receiver is mounted on high masts or other elevated sites.



3.2.7 GNSS Antenna Cabling

Protempis recommends low-loss coaxial cabling.

Using any length of coaxial cable will add some time delay to the GPS signal, which affects the absolute accuracy of the computed time solution. The time delay is dependent on the type of dielectric material in the cable and ranges from 3.3 to 6.5 ns/meter.

The Antenna Cable Delay advances the Hardware Clock slightly to cancel out the signal delay caused by the length of the GPS antenna cable. To calculate the adjustment, select the signal propagation rate for the appropriate cable type and multiply it by the length of the cable.

For example, the standard RG-59 antenna cable has a propagation rate of 4.07 ns/meter. The delay for a 25-meter cable will be 101.75 ns (25 x4.07 =101.75).

The outer shield on the GNSS cable must be grounded to the chassis via the cable shell to the connector ground on the chassis. The connector ground is tied to the chassis. The chassis is connected to the primary ground, which utilizes a ring terminal with a 14 AWG wire connected to the rack. There are to be no breaks in the outer shield of the GNSS cable. Reference ANSI/NFPA70, the National Electrical Code (NEC), in particular Section 820.93.

> NOTE - The GNSS antenna cable should only be connected when the unit is properly earth-grounded.

3.2.8 Lightning Considerations

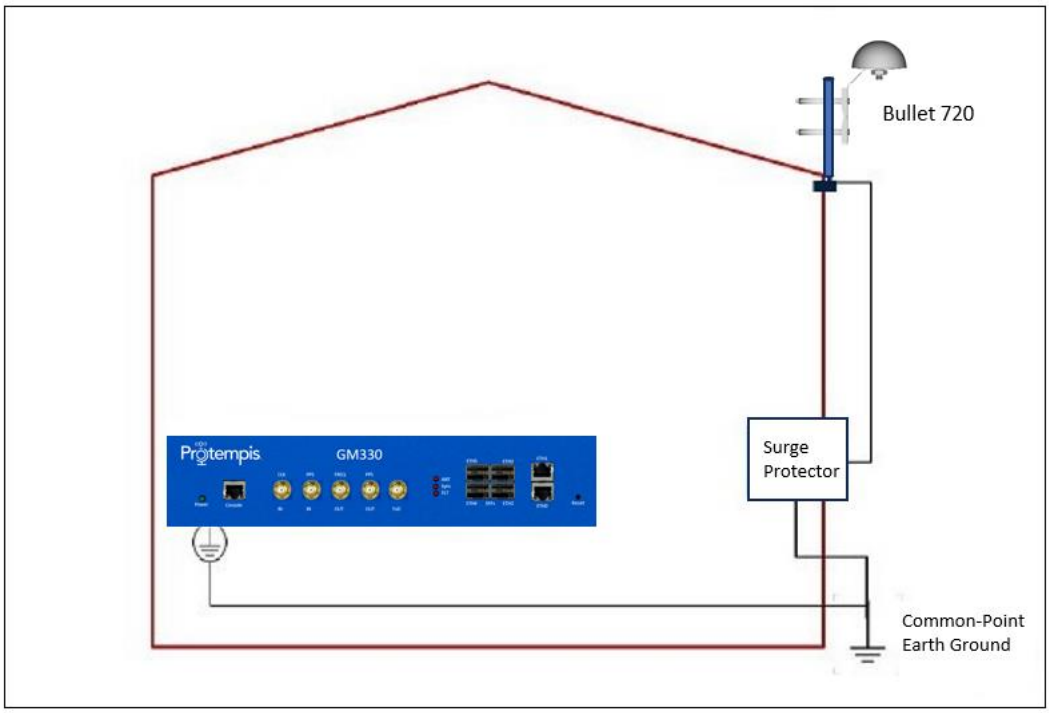
Although you cannot protect the antenna from a direct lightning strike, the connected devices can be protected from secondary effects through protection devices.

Protempis recommends installing an in-line lightning arrestor in the antenna line to protect the receiver and connected devices. In-line lightning arrestors are mounted on a low-impedance ground, between the antenna and the point where the cable enters the building.

3.2.9 Installing Surge Protection

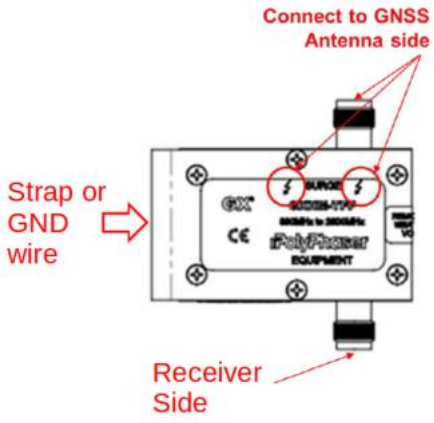
The surge protection must be installed at the cable entrance into the building with a proper earth/ground connection.

The image below shows how to connect and place the surge protector.



It is recommended to use a minimum of 6 AWG (13.3 mm) wire or larger.

NOTE - Refer to local electrical codes.



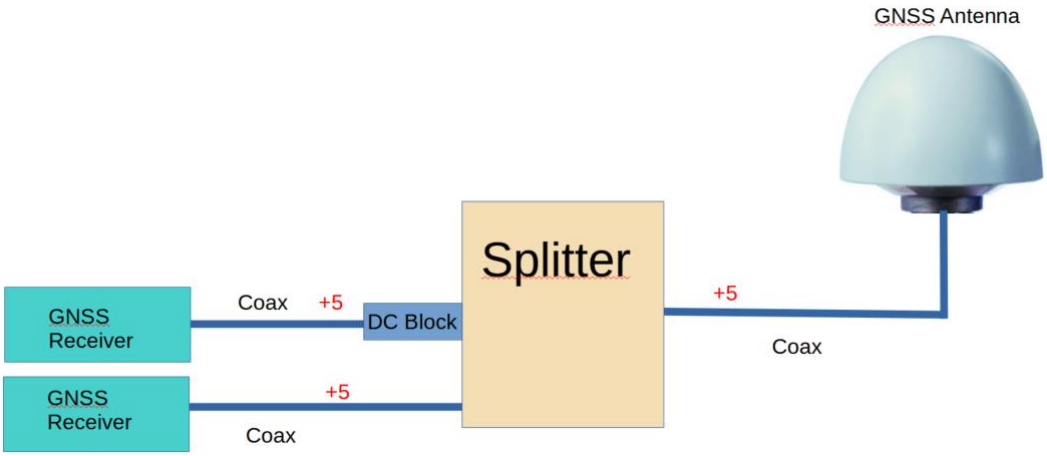
The image below shows the direction of the coaxial cable connection between the GNSS antenna and the Time server.

> NOTE - Frame GND in the surge protector must be connected properly to a building GND to bypass the surge to the earth GND.

3.2.9 Powering the Antenna

GNSS antennas are active, they need power for the internal LNA. Depending on the antenna, you need to supply 3.3 or 5V. Usually, circuitry on the GNSS receiver supplies the LNA power through the coax cable.

If you are using an RF Splitter, make sure only one of the GNSS receivers is powering the GNSS antenna. You can use a DC Block for this.



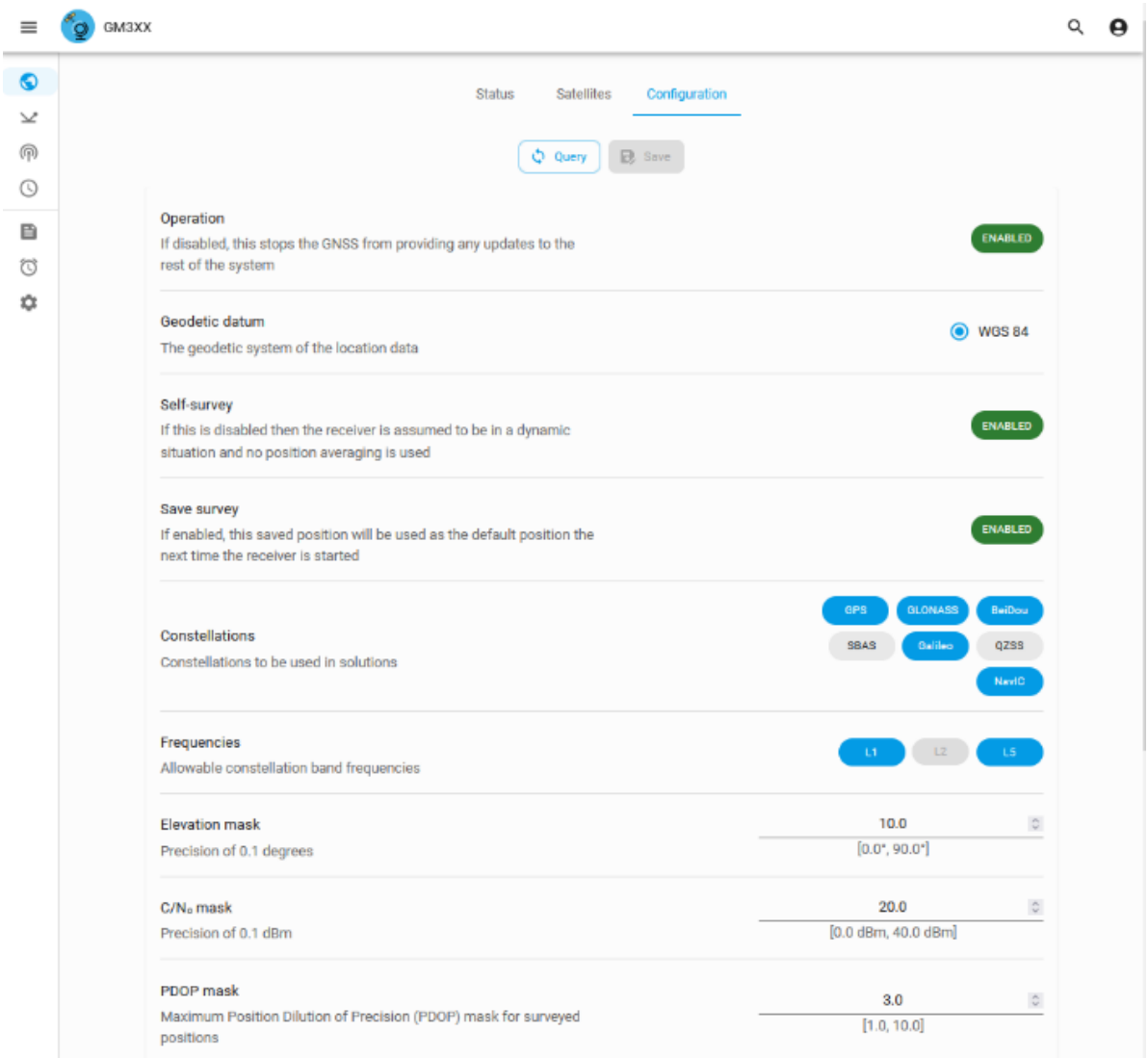
3.3 GNSS tuning settings

The default GNSS settings are suitable for most installations of the Time server. These can include antenna installations with good- or less-than-ideal views of the sky.

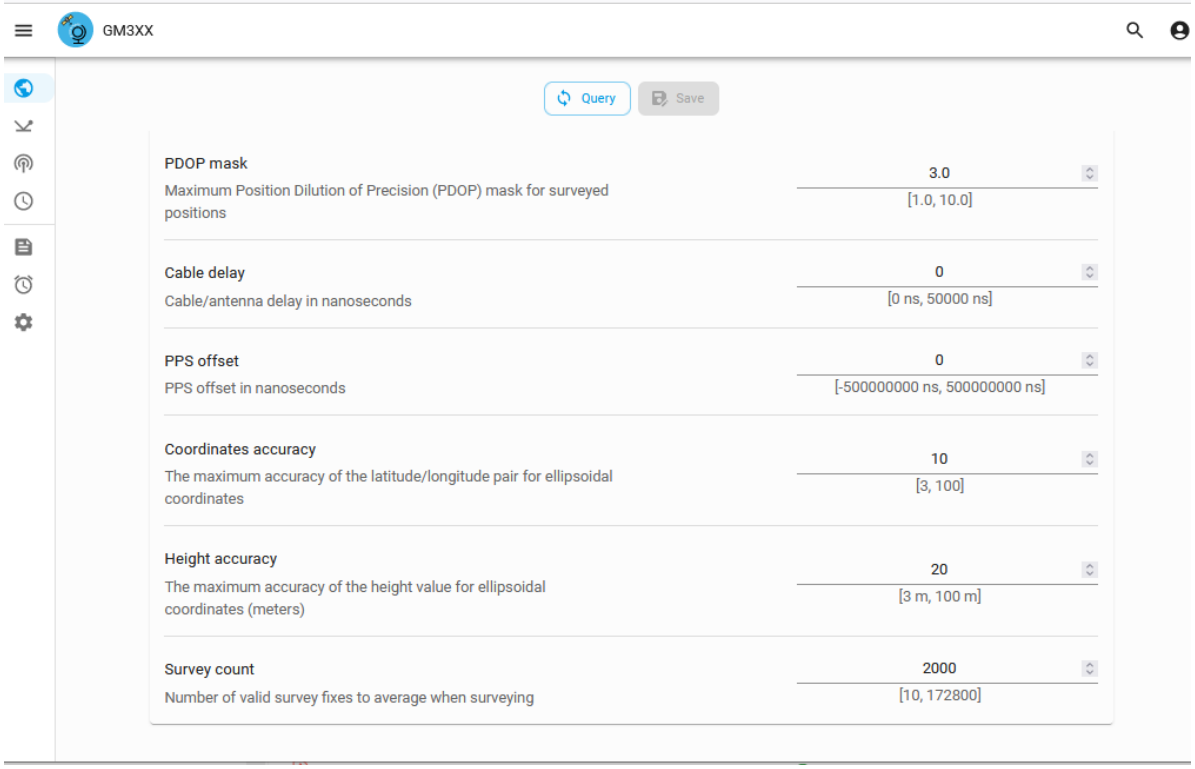
The factory settings should not be changed unless there are specifically identified reception problems or timing issues. Protempis recommends that you first discuss any changes with your local Protempis representative.

> NOTE - The exception is the Antenna Delay setting which must be changed because it needs to be custom to the specific cable length of the installation.

The tuning settings should only be changed once all the antenna position and cabling instructions listed earlier in this chapter have been followed correctly. The settings can be changed either by using the web interface (see GNSS) or using the CLI commands.



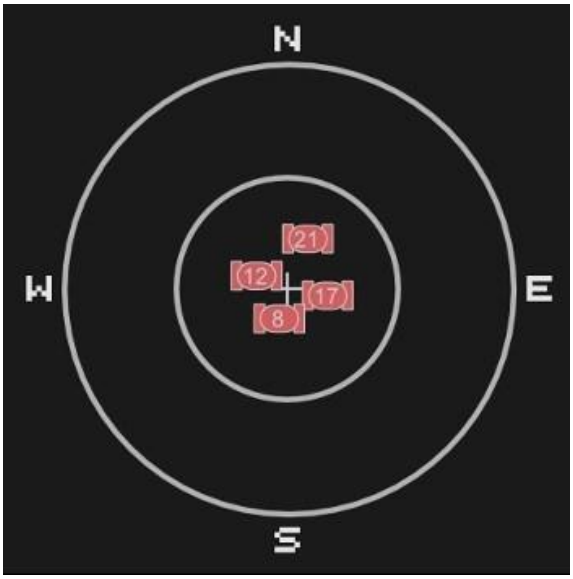
For the following setting descriptions, the GNSS Configuration web page for GNSS is used for demonstration purposes. The CLI commands are also available and are described in the Command Line Interface Reference



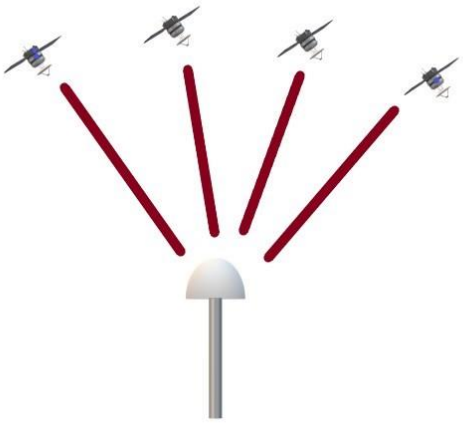
3.3.1 PDOP Mask

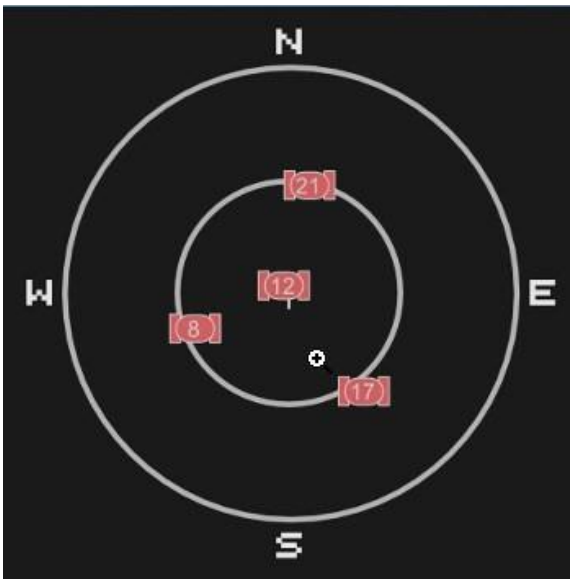
Position Dilution of Precision (PDOP) is a measure of the error caused by the geometric relationship of the satellites used in the position solution. Satellite sets that are tightly clustered together in the sky have a high PDOP and contribute to lower position accuracy. Satellites that, when viewed by the receiver are widely separated, have a low PDOP and contribute to better position accuracy.

Satellites with poor geometry (High DOP):



Satellites with good geometry (Low DOP):





The Dilution of Precision indicates the confidence level of a position fix. Low DOP values indicate a high confidence level, while high DOP values indicate a low confidence level. High DOP values are caused by the poor geometry of the visible satellites. Lowering the DOP mask will exclude fixes with poor (high) DOP and will thereby improve the quality of the reference position by only accepting fixes with high confidence levels. A too-low DOP mask setting may, however, cause extended self-survey times, because fewer position fixes will pass the mask criteria, so it takes longer to collect the amount of position fixes to complete the self-survey. The default DOP mask is 3. It is configurable by the user if needed. For most applications, a PDOP mask of 3 offers a satisfactory trade-off between accuracy and GPS coverage.

Permitted range: 0.0 to 10.0. Default: 3.

NOTE - PDOP is applicable only during self-surveyor whenever the receiver is performing position fixes.

3.3.2 Survey Count

The default value is 2,000 seconds. At power-on, the Time server performs a self-survey by averaging 2,000 position fixes. The number of position fixes until survey completion is configurable. The receiver mode during self-survey is 2D/3D Automatic, where the receiver must obtain a three-dimensional (3-D) position solution. The very first fix in 2D/3D Automatic mode must include five satellites or more. After a successful first fix, only four satellites are required. If fewer than the required number of satellites are visible, the Time server suspends the self-survey. 3D mode may not be achieved when the receiver is subjected to frequent obscuration or when the geometry is poor due to an incomplete constellation.

Once the survey is completed, the receiver automatically moves into over-determined mode, where the average value of the position calculations is saved and used for the timing solution.

Over-determined clock mode is used only in stationary timing applications. This is the default mode for the Time server once a surveyed position is determined. The timing solution is qualified by the T-RAIM algorithm, which automatically detects and rejects faulty satellites from the solution.

To improve the consistency of the time solution, the length of the self-survey can be extended to 14400 seconds (four hours). Four hours allowed for the satellites to move either completely, or halfway, through their trajectory. That should allow the PDOP to be minimized at least sometime during that period if some of the satellites are blocked. This allows the maximum amount of time that the unit can average a position with what will generally be the best PDOP that is going to be available with the current antenna placement.

The self-survey time can be extended to 86,400 seconds (24 hours) which allows the entire constellation to be visible, as well as any diurnal movement due to ionospheric model errors. This will provide a very good position fix average, that will utilize all the satellites that the receiver will observe in the sky over a day. 24 hours to wait for Over Determined mode is much longer than the default 33 minutes (2,000 seconds). This may be a factor in the user application, but otherwise lengthening the self-survey period can potentially improve our solution.

Permitted range: 10 to 172,800. Default: 2,000.

3.3.3 Elevation Mask

Generally, signals from low-elevation satellites are of poorer quality than signals from higher-elevation satellites. These signals travel farther through the ionospheric and tropospheric layers and undergo distortion due to these atmospheric conditions. For

example, an elevation mask of 10° excludes very low satellites from position fix computations and reduces the likelihood of potential errors induced by using those signals.

Permitted range: 0.0 to 90.0. Default: 10.

3.3.4 C/No Mask

The quality of received GNSS satellite signals is reported as a C/No value (Carrier-to-Noise power ratio). Low C/No values can result from low-elevation satellites, partially obscured signals (for example due to dense foliage), or reflected RF signals (multipath).

Multipath can degrade the position and timing solution. Multipath is commonly found in urban environments with many tall buildings and a preponderance of mirrored glass. Reflected signals tend to be weak (low C/No value) since each reflection diminishes the signal.

If the antenna has a clear view of the sky (outdoor antenna placement), a C/No mask of 35 dBHz is recommended for optimal results. However, for indoor use or operation with an obscured view of the sky, the mask must be low enough to allow valid weak signals to be used. For indoor operation, a C/No mask of 0 dB-Hz(zero) is recommended.

Permitted range: 0.0 to 40.0. Default: 20.

3.3.5 GNSS IN Interface

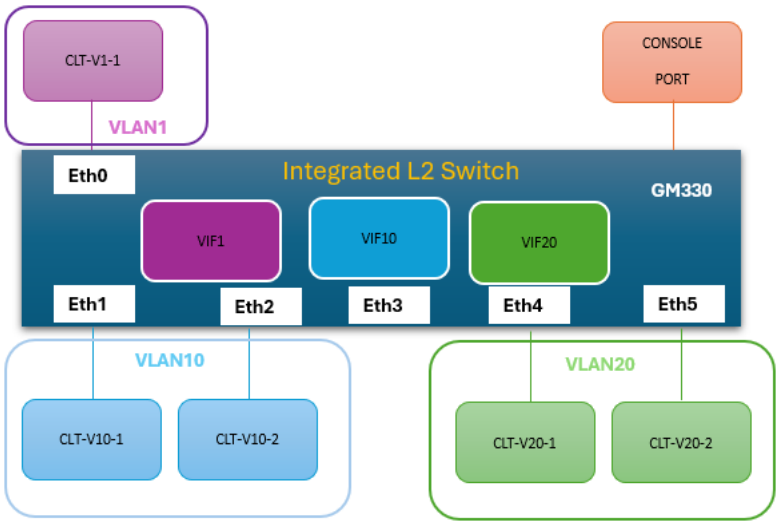
This table shows the possible constellation options you can select.

GPS	Galileo	GLONASS	BeiDou	QZSS	NavIC
√					√
	√				
		√			
			√		
√	√				
√		√			
√			√		
√	√			√	
√		√			
√			√	√	
√				√	
					√

If you select a single constellation, then the PPS and Time alignment is automatically set to the same constellation.

3.4 L2 Switch

The GM330 has an integrated VLAN-aware L2 Switch. This Switch includes layer2 functions, such as line rate layer2 switching, port operation in access and trunk mode, vlan operation in tagged and untagged mode, virtual interfaces for host applications, and dynamic MAC learning and aging.



3.4.1 Port Configuration

The GM330 provides for the management of two types of ports: physical interfaces and virtual interfaces.

Physical interface management

A physical interface represents one of the external physical ports on the device. The GM330 supports six physical interfaces: 2 x 1G RJ45 and 4 x 1/10G SFP+. These interfaces are always present in the device by default and cannot be added, deleted, or renamed.

Configuration parameters

The following configuration parameters are supported for a physical interface: Certain VLAN tagging options will be available in follow-on releases.

Admin state	Down:	Port is administratively down and does not pass any traffic.
	Up:	Port is administratively up and can pass traffic. Factory default: Up
Autoneg	Enable:	Port auto-negotiates speed and duplexity with peer.

	Disable:	Port does not auto-negotiate speed and duplexity with peer
Speed setting	10/100/1000M for 2 x RJ45 ports, 1G/10G for 4 x SFP+ ports. Applicable when autoneg is disabled. Factory default: 1G for 2 x RJ45, 10G for 4 x SFP+	
Duplexity:	Full or half duplex. Applicable when autoneg is disabled. Factory default: full duplex.	

Port mode	Access:	This mode is normally used to connect the port to an end station and not a switch. In this mode, the port is a member of exactly one access VLAN which defaults to VLAN1. An access port can receive untagged and C-tagged frames for its access VLAN. An access port can transmit untagged and C-tagged frames for its access VLAN. An access port does not carry traffic associated with any other VLAN. In access mode, the access VLAN is the port VLAN or PVID associated with the port.
	Trunk:	This mode is normally used to connect the port to another switch port. In this mode, the port can carry traffic for multiple VLANs simultaneously. Each trunk port is a member of multiple VLANs, which are controlled by the allowed VLAN list setting, and default to all configured VLANs. In trunk mode, the native VLAN is the port VLAN or PVID associated with the port. All frames on a trunk port, except those classified with a native VLAN are expected to be C-tagged with their respective VLAN tags on ingress. Frames corresponding to the native VLAN may be untagged on ingress by default. All frames on a trunk port, except those classified with the native VLAN are C-tagged with their respective VLAN tags on egress. Frames corresponding to the native VLAN are not tagged on egress by default. Egress tagging can be changed to tag all frames, in which case, the port will only accept tagged frames on ingress. Factory default: access mode.
Access port VLAN ID	This specifies the single VLAN (between 1 – 4094) associated with the port when configured in access mode. It internally	

	maps to the port VLAN or PVID in access mode. It is not relevant when the port is in trunk mode. The VLAN being assigned must already be created in the system. Factory default: VLAN1	
Trunk port VLAN ID	This specifies the native VLAN associated with the port when configured in trunk mode. It internally maps to the port VLAN or PVID in trunk mode. It is not relevant when the port is in access mode. The VLAN being assigned must already be created in the system. Factory default: VLAN1	
Allowed VLANS IDs	This is a list of VIDs whose frames can be carried simultaneously on a port that is configured as a trunk port. It is not relevant when the port is in access mode. The VLANs being assigned must already be created in the system. Factory default: All configured VLANs in the system.	
Port type	Unaware:	On ingress, all frames, whether they are carrying a VLAN tag or not, are classified to the PVID. VLAN tags are not removed on egress.
	C-Port:	On ingress, frames with a VLAN tag with TPID = 0x8100 are classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the port PVID. If frames must be tagged on egress, then they are tagged with a C-tag. Factory default: Unaware.

Operational parameters including status and statistics

The following operational parameters are supported for a physical interface:

Admin state	Administrative state configured by the user (up or down).
Oper status	Operational state of the port (up or down).
Auto negotiation status	Auto negotiation status as configured by the user and the current speed and duplexity settings.

Port medium type	10/100/1000M RJ45, or 1G/10G Copper SFP+, or 1G/10G Optical SFP+
SFP info	For SFP+ ports only. Shows whether the SFP is plugged in and if so, vendor information about the SFP.
Statistics	Various byte and packet counters for the port, including the following:

Octets (in)/(out)	Rx / Tx Bytes
Unicast packets (in)/(out)	Rx/Tx packets with a unicast destination address
Multicast packets (in)/(out)	Rx/Tx packets with a multicast destination address
Broadcast packets (in)/(out)	Rx/Tx packets with a broadcast destination address
Discards (in)	Rx dropped packets
Discards (out)	Tx dropped packets
Errors (in)	Aggragate of Rx CRC errors, Rx undersize and Rx oversize packets
Errors (out)	Collisions

3.4.2 VLAN and Virtual Interface Configuration

VLAN and VIF management

The GM330 supports VLANs for broadcast domain separation of the layer2 networks. The GM330 also supports virtual interfaces (VIF) associated with corresponding VLANs, that represent a layer2/layer3 network interface in user space, used by the host applications running on the GM330 to communicate with devices on the corresponding VLAN.

VLAN1 and its corresponding VIF1 are always created by default and cannot be deleted. Additional VLANs and corresponding VIFs can be added and deleted in the system. A VLAN must first be created and exist in the system before it is assigned to an access or trunk port. A VIF is managed through its corresponding VLAN configuration and management interface. The corresponding VLAN must exist for its VIF to be present and enabled.

Configuration parameters

The following configuration parameters are supported for a VLAN:

Name	Specified as VLANXX at creation (XX is between 1 – 4094)
VLAN enable	Admin-state of the vlan; enable or disable the vlan within the system. It must be enabled to transport network traffic.
Description	Eighty-character string description (e.g. ORAN timing VLAN) Factory default: Same as VLAN name.
VIF enable	Enable or disable a layer2/layer3 network interface in the user space associated with this VLAN, for host traffic. Factory default: Disable

The following configuration parameters are supported for a VIF (only applicable when VIF enable is set):

IPV4 admin state	Enable:	VIF is enabled, and IPV4 network interface is up. Factory default: Enabled
	Disable:	IPV4 network interface is down.
IPV4 address mode	Static IP assignment or DHCP. Factory default: DHCP	
IPV4 address	IPV4 IP address if mode is static.	
IPV4 netmask	IPV4 netmask if mode is static.	
IPV4 gateway	IPV4 gateway if mode is static.	
IPV6 admin state	Enable:	VIF is enabled, and IPV6 network interface is up. Factory default: Enabled
	Disable:	IPV6 network interface is down.
IPV6 address mode	Static IP assignment or DHCP or SLAAC. Factory default: DHCP	
IPV6 address	IPV6 IP address if mode is static.	
IPV6 prefix	IPV6 prefix is mode is static.	

IPV6 gateway	IPV6 gateway if the mode is static.
ZTP mode	This parameter controls the ZTP configuration option over this VIF interface. Possible values are None, Dual, IPV4, IPV6. Factory default: None.

Operational parameters including status and statistics

The following operational parameters are supported for a VLAN:

Oper state	Operational state of the VLAN (up if at least one member port is oper up, or down if all the member ports are oper down).
Port member list	Listing of all ports (access and trunk) that are members of this VLAN.

The following operational parameters are supported for a VIF:

Admin state	Shows whether the VIF is enabled or disabled by the user.
Oper state	Operational state of the VIF (up or down).
IPV4 address	IPV4 address, netmask, and gateway, based on selected static or DHCP setting.
IPV6 address	IPV6 address, prefix, and gateway, based on selected static, slaac or dhcp settings.
Statistics	Various byte and packet counters for the VIF

3.4.3 MAC Learning and Aging

The GM330 maintains a MAC address table per VLAN domain, including one for default VLAN1. Line rate layer2 switching is based on the MAC address table entries. The GM330 dynamically creates and maintains MAC address table entries that map a destination MAC address (DMAC) to a device port on which the packet will be sent out.

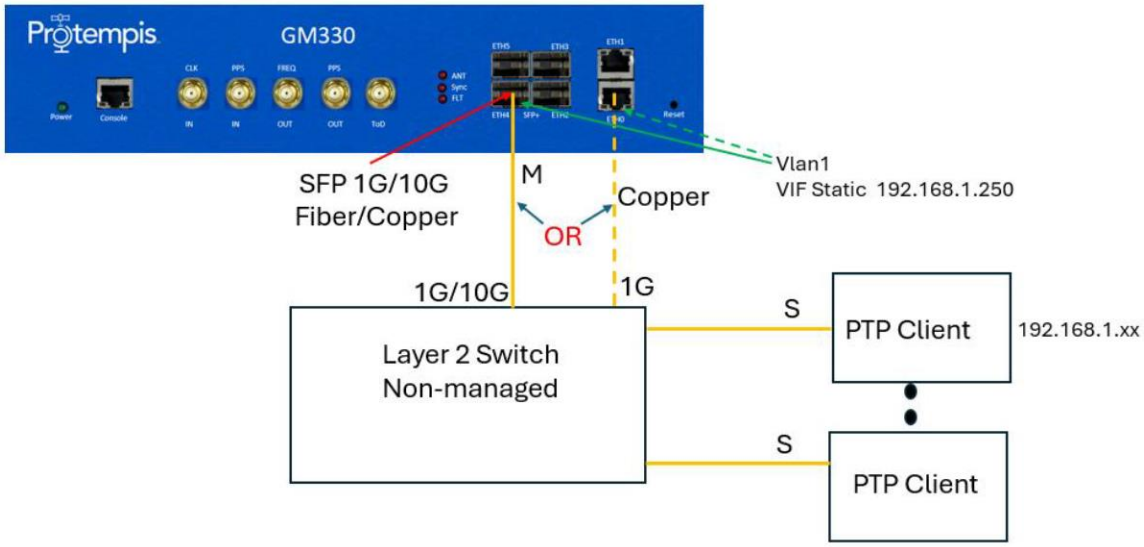
A device port is either an external physical port or the internal CPU host port. Layer2 multicast packets are forwarded per VLAN domain to a set of device ports associated with the multicast address. Layer2 broadcast packets are forwarded per VLAN domain to all the access ports that are part of that VLAN and to all the trunk ports that carry that VLAN.

The MAC address table supports dynamic learning and contains dynamic entries based on the source MAC address (SMAC) seen by the device on an incoming device port. The device supports dynamic aging, whereby a dynamic entry is removed from the table if the corresponding SMAC has not been seen within the default aging time.

Configuration and management of static MAC address table entries and aging times, along with the ability to display the MAC address table entries per VLAN will be supported in a future release.

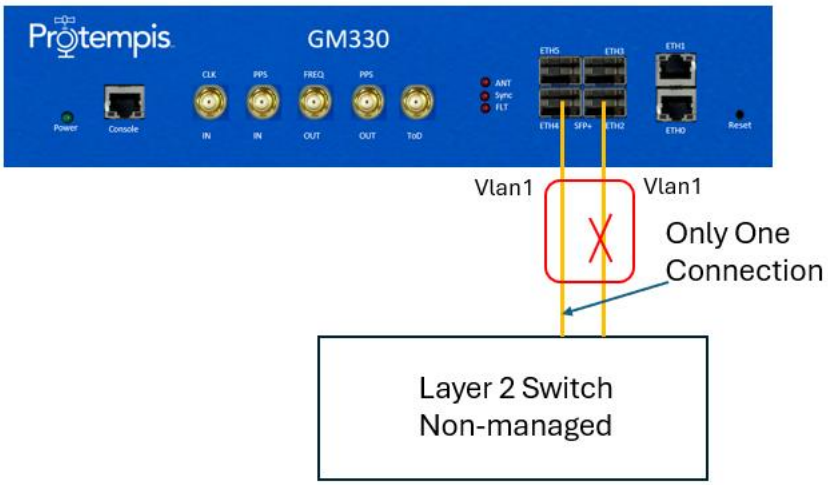
3.4.4 Connecting an external switch

If using an external switch, you can connect to the integrated 1G copper or 1/10G SFP+ ports with copper/fiber.



If you plan on connecting an external Layer 2 switch, make sure you are not creating a loop. Currently, the GM330 does not support spanning tree. This feature will be introduced in future firmware.

In the example below there are two Vlan 1 connections to the external switch. Only connect one to avoid possible loops.


Protempis
GM330
Power
Console
CLK
PPS
FREQ
PPS
IN
IN
OUT
OUT
ToD
ANT
Sync
FLT
ETH5
ETH3
ETH4
SFP+
ETH2
ETH1
ETH0
Reset
Vlan1
Vlan1
Only One
Connection
Layer 2 Switch
Non-managed

4. Startup Operation

When the Time server is turned on, it automatically begins to acquire and track GNSS satellite signals.

During the satellite acquisition process, the Time server is not in PTP operation mode but in GNSS acquiring mode to establish its accurate position so that it can generate accurate time/phase signals.

In its default configuration, the Time server takes around six minutes to lock with GNSS satellites and start operating PTP/NTP if the network configuration is done appropriately and the connected GNSS antenna has a clear view of the sky.

If the connected GNSS antenna is installed in a position with a limited sky view, the PTP operation mode takes longer to enable (up to 30 minutes), depending on the number of valid GNSS satellites that it is tracking.

In cold start, Protempis recommends that the PTP service is started 33 minutes later in OD (Over Determined) mode from the bootup, as the Time server should lock with GNSS satellites and calculate accurate position itself during the self-survey mode.

4.1 User levels

The Time server provides a hierarchy of CLI users that permits an increasing level of access to system parameters.

- User: This is the basic login level.
  This only allows for viewing of status, nothing can be changed other than their password.
- Admin: This is the middle level. This user can configure everything about the unit, except user accounts.
- Supervisor: This is the highest level. The login ID for this level is “protempissuper”. This allows the configuration of everything, including user accounts. By default, this is the Protempis user access level.

NOTE - See the CLI command use the set user command to update the user configuration. or the User section of the web interface.

4.1.1 Initial default login password

NOTE - There is a change in the default password to comply with the *California State Bill* SB-327-Information privacy: connected devices bill, which requires that the preprogrammed password is unique to each device manufactured. The SB-327 bill is effective from 1 January 2020. Only the user protempissuper is available by default, with the default password as outlined in this section.

Username: protempissuper
Password: Tbolt_<serial number>

For example, if the serial number is 1234567890, the password will be "Tbolt_1234567890".

As a 'Best security practice', Protempis recommends changing the default user credentials of the 'protempissuper' account. If required, the user accounts of 'protempis' and 'protempisadmin can be added with unique passwords to allow user and admin level access as were previously available by default.

4.2 Startup Configuration

4.2.1 Default configuration values for the Time server startup

The default setting of ...	Description	Notes

GNSS constellation	GPS and GLONASS	
Mask	Elevation Mask: 10.0 deg Signal level Mask: 0.0 dB/Hz PDOP Mask: 3.0	
Survey mode (position fix mode)	Automatic	
Self-surveying	2,000 times	Around 33 minutes
GNSS Antenna Power feeding	Enable	5 V DC
GNSS cable delay Compensation	0 (Zero)	
Network Interface IP address	Eth0(Vlan1): 192.168.1.250/24 Eth1(Vlan1): 192.168.1.250/24 Eth2(Vlan1): 192.168.1.250/24 Eth3(Vlan1): 192.168.1.250/24 Eth4(Vlan1): 192.168.1.250/24 Eth5(Vlan1): 192.168.1.250/24	Eth 0-5 are enabled and configured with a default configuration.
PTP configuration	Eth0(disabled): ITU-T G.8275.1 Eth1(disabled): ITU-T G.8275.1 Eth2(disabled): ITU-T G.8275.1 Eth3(disabled): ITU-T G.8275.1 Eth4(disabled): ITU-T G.8275.1 Eth5(disabled): ITU-T G.8275.1	The user must enable each PTP interface manually after GNSS locking and all related alarms are cleared.
NTP configuration	Eth0: NTPv4 Eth1: NTPv4 Eth2: NTPv4 Eth3: NTPv4 Eth4: NTPv4 Eth5: NTPv4	Automatically enabled after GNSS locking and all related alarms are cleared.

4.2.2 General conditions for normal startup of the Time Server

The following parameter values and actions are required in the default configuration for a correct PTP/NTP operation startup.

Conditions	Description	Notes

GNSS antenna status	Should be OK.	Open or Short are not valid statuses on start-up.
Required minimum GNSS number for self-surveying after a cold start	At least five satellites with > 35 dB each for C/No value.	
Required minimum GNSS number for self-surveying after warm start	At least four satellites with > 35 dB each for C/No value.	
GNSS receiver mode after cold restart	Start with Self-survey mode for 33 minutes. After Self-survey mode, get into OD (Over Determined mode).	If the time server is moved over 100 meters away from the first self-surveyed position, it automatically restarts for self-survey.
GNSS receiver mode after warm restart	Start with OD (Over-determined) mode after the first GNSS tracking.	If the time server is moved over 100 meters away from the first self-surveyed position, it automatically restarts for self-survey.
First GNSS signal receiving time after power-up	Normally less than two minutes after showing the Login prompt in CLI.	
Time of week information	Current GPS time	
UTC Offset	18	In case of a cold start, this information shows around 12 minutes after the first GNSS tracking.
Leap second status	0	
GNSS receiver status	Normal	
Required minimum GNSS satellite tracking number after OD mode	At least two satellites with > 35 dB each for C/No value.	

First PTP packet generation time (PTP/NTP operation mode Enable)	Normally around six minutes after showing the login prompt in CLI.	With a clear sky view for the installed GNSS antenna.

4.2.3 Alarm status for PTP startup of the Time server

Alarms are set during the boot-up sequence because the Time server does not receive any GNSS signals in the initialization stage.

These alarms are cleared sequentially. When all alarms are cleared in GNSS locking mode, the PTP and NTP operations for both Eth0 and Eth1 are enabled. Then, the Time server starts generating PTP/NTP packets.

However, those alarms may occur during user operation, based on alarm alert conditions.

Alarms list in the initial status	Description	Notes
GNSS-Comm-Loss	Should be cleared immediately right after the Time server boots up normally	Set at boot-up or can be set during user operation
GNSS-Time-Bad	Should be cleared immediately when the Time server is receiving any GNSS signal normally	Set at boot-up or can be set during user operation
UTC-Corr-Unk	Should be cleared when the Time server is receiving any GNSS signal normally	Set at boot-up or can be set during user operation
GNSS-Track-No	Should be cleared when the Time server is receiving any GNSS signal normally	Set at boot-up or can be set during user operation
GNSS-PPS-LOSS	Should be cleared when the GNSS antenna is connected normally and when the Time server is receiving any GNSS signal normally	Set at boot-up or can be set during user operation
Time-Set-Bad	Should be cleared when the Time server is in GNSS acquiring mode	Set at boot-up or can be set during user operation
Freq-Hold-Exceed	Should be cleared when the Time server is in GNSS acquiring mode	Set at boot-up or can be set during user operation

Freq-Hold	Should be cleared when the Time server is in GNSS acquiring mode	Set at boot-up or can be set during user operation
Freq-loop-unlock	Should be cleared when the Time server is in GNSS acquiring mode	Set at boot up or can be set during user operation
Freq-Out-Bad	Should be cleared when the Time server is in GNSS acquiring mode	Set at boot up or can be set during user operation
PPS-Sync-Bad	Should be cleared when the Time server is in GNSS locking mode	Set at boot-up or can be set during user operation
Time-sync-Bad	Should be cleared when the Time server is in GNSS locking mode	Set at boot-up or can be set during user operation

Alarms list in the initial status	Description	Notes
PTP-System-Bad	Should be cleared when the Time server is in GNSS locking mode	Set at boot-up or can be set during user operation
Eth-Port0-Down	Depends on the user's operating situation	Can be set during user operation
Eth-Port1-Down	Depends on user's operating situation	Can be set during user operation
Eth-Port2-Down	Depends on the user operating situation	Can be set during user operation

4.3 Initial Installation Procedure

The table below describes the sequence of the initial installation using the default configuration for a cold start.

Protempis recommends that you do not add RF splitter(s) between the GNSS antenna and the Time server (to distribute the GNSS RF signal to more than one Time server) since it can be a weak point at the GNSS reference and location redundancy perspective.

Seq #	Initial installation	Checking and CLI commands	Notes and Checkpoint
1	Install a GNSS antenna at the rooftop with a clear sky view.		
2	Install a surge protector between the GNSS antenna and the Time server.		
3	Install an appropriate coaxial cable.		
4	Install all required network configurations.		
5	Start the Time server.		
6	Login prompt.	Log in	Takes around two minutes after powering up
7	Check the system firmware version.	GM300> show firmware version	Check version firmware-version = 00.01.04 build-date = 2024-04-12T00:26:37+00:00
8	Check the hardware firmware version.	GM300> show prodconf	Check version product-id hardware-rev
9	Check the GNSS firmware version.	GM300> show firmware version	Check GNSS Info: name = RES 720 version = 1.02.00

10	Check the product information.	GM300> show prodconf	Check… - Serial number - HW production date - Product option information - Product P/N - Hardware version - other information
11	Check the cable delay configuration.	For adding cable delay compensation: GM300> enable GM300# configure terminal GM300(config)# gnss GM300(gnss)# cable-delay 30 GM300(gnss)# commit	Cable-delay [value] in nanoseconds

Seq #	Initial installation	Checking and CLI commands	Notes and Checkpoint
		For checking applied value: GM300(gnss)#show gnss config	
12	First GPS time showing.	GM300> show gnss operating-state	GNSS Time Info: time-base = gps utc-offset = 18 utc-valid = true leap-pending = 0 gps-time-at-pps = 1713470894 sys-time = 1713470876
13	Check the GNSS 'Acquiring' status.	> view freq	Check 'Mode: Acquiring'
14	Check the antenna status.	GM300> show gnss operating-state	GNSS Status: gnss-status = ok time-valid = true pps-valid = true ant-status = open
15	Check the GNSS signal status.	GM300> show gnss sat-status	Check… prn track-status CNo Type Freq Azimuth Elevation

16	Enable the network interface.	GM300> enable GM300> configure terminal GM300(config)#interface ethernet 4 GM300(config-if-eth4)# switchport mode access GM300(config-if-eth4)# switchport access vlan 20 GM300(config-if-eth4)# commit GM300(config-if-eth4)# exit GM300(config) copy running-config startup-config	Assign the port to a Vlan with an associated VIF GM300> enable GM300# config t GM300# vlan 20 GM300(config)# interface vlan 20 GM300(config-vlan-VLAN20)# vif-enable true GM300(config-vlan-VLAN20)# ip address 192.168.20.5 /24 GM300(config-vlan-VLAN20)# gateway 192.168.20.1 GM300(config-vlan-VLAN20)# commit Successfully applied configuration changes
17	Check the network configuration.	GM300> show interfaces all	Check interface configuration Check Status: Connected

Seq #	Initial installation	Checking and CLI commands	Notes and Checkpoint
			NOTE – If using the ITU-T G.8275.1 profile, the IP address should not be an issue since it is an L2 multicast profile.
18	Check the survey mode.	> view pos	Check 'Automatic(2D/3D)' for Self-survey mode
19	Check the OD mode.	GM300> show prtc operating-state	PRTC Status: prtc-status = ok oper-mode = prtc
20	Check GNSS 'LOCK' status	GM300> show prtc operating-state	PRTC PLL Status: state = locked
21	Check alarm status	GM300> show alarm active	Check for clearing all alarms
22	Set the PTP interface enable.	GM300> enable GM300# configure terminal GM300(config)# ptp GM300(ptp)# ptp-interface ethernet 0	As a default, both Eth0 and Eth1 will be enabled with the G.8275.1 profile

		GM300(ptp-if-eth0)# instance-enable true GM300(ptp-if-eth0)# commit GM300(ptp-if-eth0)# exit GM300(ptp)# copy running-config startup-config GM300(config)# exit	
23	Check the PTP operation status.	GM300>show ptp	Check first for both Eth0 and Eth1 with … Enabled: Yes - Mode: Master - Clock ID : 001747FFFE7xxxxx-1 Profile: G8275.1 Operational Mode: Normal ETC
24	Check the PTP locking status on the PTP slave device.		Check the Master Clock ID in the Slave device. It must be the same as the Time server ClockID.
25	Finished.		

5. Command Line Interface Reference

This chapter describes the Command Line Interface (CLI) conventions, prompts, features, and command syntax used.

5.1 CLI Overview

The Command Line Interface (CLI), also called the ASCII command set, can be used to control the Time server from a terminal connected to the console serial port, or the ethernet port via Telnet/SSH access.

5.2 Command line format

The command line format is as follows:

```
GM300>

To enter Privileged mode to make changes you need

to:

GM300> enable

GM300#
```

The type of actions in non-privileged mode > :

!	Insert a comment line
enable	Turn on privileged commands
exit	Exit from the CLI
help	Display an overview of the CLI syntax
ping	Send messages to network hosts
show	Show system information
whoami	Display username and access level of current user

The type of actions in privileged mode # :

!	Insert a command line
abort	Abort uncommitted changes
commit	Commit configuration changes
configure	Enter configuration mode
copy	Copy from one file to another
disable	Turn off privileged commands
exit	Exit from privileged mode

factory-reset	Perform factory reset
help	Display an overview of the CLI syntax
history	Specify the size of the command history buffer
ping	Send messages to network hosts
reboot	Halt and perform a software restart
show	Show system information
Whoami	Display username and access level of current user

Help on an individual command is available by typing “command ?”.

For example, "show ?".

TIP - The Time server has an extensive online, user-level context-aware, help system.

NOTE - After any configuration change, issue a “commit” and “copy config startup-config “ command to store the configuration.

5.3 Command show

```
GM300>
GM300> show
GM300> show gnss config
```

alarm	active	Active alarms (set and not ignored)
	all	All alarms
	config	Current alarm config (with any uncommitted changes)
	running-config	Alarm running configuration
	Startup-config	Alarm startup configuration
eventlog	Identity	(general/system/prtc/gnss/network/hardware/auth/ptp/ntp/ synce/update/all)
firmware	version	Display firmware version information
gnss	config	Current GNSS config (with any uncommitted changes)
	operating-state	GNSS operational state
	running-config	GNSS running configuration
	Startup-config	GNSS startup configuration
history	Lists previous commands	
interface Added in FW > 5.00	Ethernet Interface information	
	config	Current interface config (with any uncommitted changes) (eth0/eth1/eth2/eth3/eth4/eth5/all)
	operating-state	Display the state of the specified interface (eth0/eth1/eth2/eth3/eth4/eth5/all)
	running-config	interface running-config (eth0/eth1/eth2/eth3/eth4/eth5/all)
	startup-config	interface startup-config (eth0/eth1/eth2/eth3/eth4/eth5/all)
Iface Removed in FW > 5.00	config	Current iface config (with any uncommitted changes) (eth0/eth1/eth2/eth3/eth4/eth5/all)
	running-config	iface running-config (eth0/eth1/eth2/eth3/eth4/eth5/all)
	startup-config	iface startup-config (eth0/eth1/eth2/eth3/eth4/eth5/all)
Interfaces Removed in FW > 5.00	(eth0/eth1/eth2/eth3 /eth4/eth5/all)	Display the state of the specified interface

ip	IPV4 information		
	route	Show IPV4 route info	
ntp	authkey	NTP authentication keys	
		config	Current NTP authentication keys (with any uncommitted changes)
		running-config	NTP running authentication keys
		startup-config	NTP startup authentication keys
	config	Current NTP config (with any uncommitted changes)	
	key-profiles	NTP authentication key profiles	
	operating-state	NTP operational state	
	running-config	NTP running configuration	
	startup-config	NTP startup configuration	
prodconf	Display product configuration		
prtc	config	Current PRTC config (with any uncommitted changes)	
	operating-state	PRTC operating-state	
	running-config	PRTC running configuration	
	startup-config	PRTC startup configuration	
ptp	config	Current PTP config (with any uncommitted changes)	
	operating-state	PTP operational state	
	profile-defaults	PTP profile default values	
	running-config	PTP running configuration	
	startup-config	PTP startup configuration	
radius	RADIUS information		
	config	Current RADIUS config (with any uncommitted changes)	
	dictionary	Display RADIUS dictionary. Copy contents to RADIUS server.	
	running-config	RADIUS running configuration	
	startup-config	RADIUS startup configuration	
snmp	SNMP information		
	config	Current SNMP config (with any uncommitted changes)	
	running-config	SNMP running configuration	
	startup-config	SNMP startup configuration	
synce	SYNCE information		
	config	Current SYNCE config (with any uncommitted changes)	

	operating-state	SYNCE operating-state
	running-config	SYNCE running configuration
	Startup-config	SYNCE startup configuration
sysauth	SYStemAUTHentication information	
	config	Current SYSAUTH config (with any uncommitted changes)
	password-rule-presets	SYSAUTH password-rule-presets
	running-config	SYSAUTH running configuration
	startup-config	SYSAUTH startup configuration
	web-crt	SYSAUTH Web CRT contents
		String CRT basename (3..64)
	web-crt-list	SYSAUTH Web CRT basenames
	web-csr	SYSAUTH Web CSR contents
		String CSR basename (3..64)
	web-csr-list	SYSAUTH Web CSR basenames
system	SYSTEM information	
	config	Current SYSTEM config (with any uncommitted changes)
	running-config	SYSTEM running configuration
	startup-config	SYSTEM startup configuration
update	config	Remote update config (with any uncommitted changes)
	operating-state	Remote update operating-state
	running-config	Remote update running-config
	startup-config	Remote update startup-config
user	Local user account information	
	config	Current USER config (with any uncommitted changes)
	running-config	USER running configuration
	startup-config	USER startup configuration
vlan	config	Current vlan config (with any uncommitted changes) integer VLAN number (1..4094)
	brief	Show operational summary of VLANs
	ids	All vlan ids
	operating-state	vlan operating-state integer VLAN number (1..4094)
	running-config	vlan running-config integer VLAN number (1..4094)
	startup-config	vlan startup-config integer VLAN number (1..4094)
ztp	Zero Touch Provisioning (ZTP) information	
	config	ZTP config (with any uncommitted changes)
	csr	ZTP CSR
	running-config	ZTP running-config
	startup-config	ZTP startup-config

5.4 CLI command enable

```
GM300>
GM300> enable
GM300#
```

5.4.1.abort

Use the "*abort"* command to abort uncommitted changes

5.4.2 clear

Use the "*clear"* command to clear values

5.4.3 commit

Use the "*commit"* command to apply any uncommitted commands to the running-config

5.4.4 configure

terminal		Configure from the terminal	
	!	Insert a comment line	
	abort	Abort uncommitted changes	
	commit	Abort uncommitted changes	
	copy	Copy from one file to another	
	exit	Exit from configure mode	
	gnss	!	Insert a comment line
		abort	Abort uncommitted changes
		cable-delay	Specify cable/antenna delay
		cno-mask	Specify C/No mask
		commit	Commit configuration changes
		constellation	Specify constellation bits
		copy	Copy from one file to another
		disable_gnss	Disable GNSS
		elevation-mask	Specify elevation mask
		enable_gnss	Enable GNSS

		exit	Exit from gnss configuration mode
		frequency	Specify frequency bits
		help	Display an overview of the CLI syntax
		pps-offset	Specify PPS offset
		show	Show system information
	help	Display an overview of the CLI syntax	
	interface	ethernet	Ethernet IEEE 802.3
		vlan	VLAN IEEE 802.1Q
	no	Negate a command or set its defaults	
	ntp	!	Insert a comment line
		abort	Abort uncommitted changes
		auth-enable	Specify NTP auth-enabled choice
		commit	Commit configuration changes
		copy	Copy from one file to another
		enable	Specify NTP global enable choice
		exit	Exit from ntp configuration mode
		help	Display an overview of the CLI syntax
		port	Specify NTP port value
		show	Show system information
	prtc	!	Insert a comment line
		abort	Abort uncommitted changes
		commit	Commit configuration changes
		copy	Copy from one file to another
		exit	Exit from prtc configuration mode
		ext-freq-frequency	Specify external frequency selection
		ext-freq-ql	Specify external frequency quality level
		ext-phase-offset	Specify offset for external phase in nanoseconds
		ext-phase-ql	Specify external phase quality level
		freq-out-enable	Used to enable/disable the frequency output connector
		freq-out-select	Used to select the frequency output type
		get time	Get the time
		help	Display an overview of the CLI syntax

		input-lo	Specify input lockout	
		input-pr	Specify input priority	
		loop-state	Set the PLL loop state for user modes of operation	
		ntp-ip-address	Set the NTP server IP address	
		ntp-time	Set the NTP server timeout in minutes	
		oper-mode	Specify Time/Freq operating mode	
		pulse-out-enable	Used to enable/disable the pulse output connector	
		pulse-out-offset	Controlled pulse offset in nanoseconds	
		pulse-out-select	Used to select the pulse output type	
		pulse-out-width	Control pulse width in nanoseconds	
		ql-timeout	Specify the quality level timeout in seconds	
		set-time	Set the time manually (yyyy-mm-ddThh:mm:ss)	
		sf-timeout	Specify signal fault timeout in seconds	
		show	Show system information	
		synth-output	Parameters for the frequency synthesizer output	
		tod-out-enable	Used to enable/disable the TOD output connector	
		tod-out-select	Used to select TOD output type	
		whoami	Display username and access level of current user	
	ptp	Configure PTP parameters		
		!	Insert a comment line	
		abort	Abort uncommitted changes	
		commit	Commit configuration changes	
		copy	Copy from one file to another	
		exit	Exit from ptp configuration mode	
		help	Display an overview of the CLI syntax	
		ptp -Interface	Select a PTP interface to configure	
			ethernet	Ethernet IEEE 802.3
			Interface number	Ethernet interface number (0..5)
			announce-receipt-timeout	Specify the PTP announce-receipt-timeout value
			clock-class	Specify PTP clock-class value
			commit	Commit configuration changes

			copy	Copy from one file to another
			delay-mechanism	Specify PTP delay-mechanism
			domain-number	Specify PTP domain-number value
			dscp	Specify the PTP DSCP value
			duration-field	Specify PTP duration-field value
			exit	Exit from PTP interface configuration mode
			grantor	Specify PTP grantor
			help	Display an overview of the CLI syntax
			instance-enable	Specify PTP instance to enable choice
			ipmode	Specify PTP ipmode
			l2mac	Specify PTP l2mac
			local-priority	Specify PTP local-priority value
			log-announce-interval	Specify PTP log-announce-interval value
			m6scope	Specify PTP m6scope
			min-delay-req-interval	Specify PTP min-delay-req-interval value
			min-pdelay-req-interval	Specify PTP min-pdelay-req-interval value
			network-protocol	Specify PTP network-protocol
			priority1	Specify PTP priority1 value
			priority2	Specify PTP priority2 value
			profile	Specify PTP profile
			reset-ptp-profile	Restore to specified PTP profile
			show	Show system information
			sync-interval	Specify PTP log-sync-interval value
			ttl	Specify the PTP TTL value
			two-step	Specify PTP two-step choice
	radius	Configure RADIUS parameters		
		!	Insert a comment line	
		abort	Abort uncommitted changes	
		commit	Commit configuration changes	
		copy	Copy from one file to another	

		delete-server	Specify a RADIUS server configuration to delete	
		exit	Exit from radius configuration mode	
		help	Display an overview of the CLI syntax	
		server	Specify a RADIUS server name to configure	
		show	Show system information	
		timeout	Specify RADIUS timeout value	
		whoami	Display username and access level of current user	
	show	alarm	Alarm information	
		eventlog	active	Alarm information
		firmware	Identity	Display event logs
		gnss	version	Display firmware version information
		history	GNSS information	
		interface	Ethernet Interface information Added in FW > 5.00	
		iface	Command history Removed in FW > 5.00	
		interfaces	IFACE information Removed in FW > 5.00	
		ip	IPV4 information	
		ntp	NTP information	
		prodconf	Display the state of the specified interface	
		prtc	Display product configuration	
		ptp	PRTC information	
		radius	RADIUS information	
		snmp	SNMP information	
		synce	SYNCE information	
		sysauth	SYStemAUTHentication information	
		system	SYSTEM information	
		vlan	VLAN information	
			brief	Show operational summary of VLANs
			config	Current vlan config (with any uncommitted changes)
			ids	All vlan ids
			operating-state	vlan operating-state
			running-config	vlan running-config
			startup-config	vlan startup-config

		update	config		Remote update config (with any uncommitted changes)
			operating-state		Remote update operating-state
			running-config		Remote update running-config
		user	Local user account information		
		vlan	VLAN information		
		ztp	Zero Touch Provisioning (ZTP) information		
	snmp	Configure SNMP parameters			
		!	Insert a comment line		
		abort	Abort uncommitted changes		
		commit	Commit configuration changes		
		copy	Copy from one file to another		
		enable	Specify SNMP global enable choice		
		exit	Exit from snmp configuration mode		
		help	Display an overview of the CLI syntax		
		show	Show system information		
			alarm	Alarm information	
			eventlog	Display event logs	
			firmware	Firmware version information	
			gnss	GNSS information	
			history	Command history	
			interface	Ethernet Interface information Added in FW > 5.00	
			iface	IFACE information Removed in FW > 5.00	
			interfaces	Display the state of the specified interface Removed in FW > 5.00	
			ntp	NTP information	
			prodconf	Display product configuration	
			prtc	PRTC information	
				config	Current PRTC config (with any uncommitted changes)
				operating-state	PRTC operating-state

				running-config	PRTC running configuration
				starup-config	PRTC startup configuration
			ptp	PTP information	
				config	Current PTP config (with any uncommitted changes)
				operating-state	PTP operational state
				profile-defaults	PTP profile default values
				running-config	PTP running configuration
				startup-config	PTP startup configuration
			radius	RADIUS information	
				config	Current RADIUS config (with any uncommitted changes)
				dictionary	Display RADIUS dictionary. Copy contents to RADIUS server.
				running-config	RADIUS running configuration
				Startup-config	RADIUS startup configuration
			running-config	Current running configuration	
			snmp	SNMP information	
				config	Current SNMP config (with any uncommitted changes)
				running-config	SNMP running configuration
				startup-config	SNMP startup configuration
			startup-config	Contents of startup configuration	
			synce	SYNCE information	
				config	Current SYNCE config (with any uncommitted changes)

				operating-state	SYNCE operating-state
				running-state	SYNCE running configuration
				Startup-config	SYNCE startup configuration
			sysauth	SYStemAUTHentication information	
				config	Current SYSAUTH config (with any uncommitted changes)
				operating-state	SYSAUTH running configuration
				startup-config	SYSAUTH startup configuration
			update	Remote update information	
				config	Remote update config (with any uncommitted changes)
				operating-state	Remote update operating-state
				running-config	Remote update running-config
				Startup-config	Remote update startup-config
			vlan	VLAN information	
				brief	Show operational summary of VLANs
				config	Current vlan config (with any uncommitted changes)
				ids	All vlan ids
				operating-state	vlan operating-state
				running-config	vlan running-config
				Startup-config	vlan startup-config
		test-traps	Command for testing SNMP		
		trap-mgr	Specify a trap manager number to configure		

			Trap manager number	(1..4)	
		v2c-config	Specify SNMP v2c configuration		
		v3-user	Specify a V3 user number to configure		
			SNMPv3 user number	(1..4)	
	synce	Configure SYNCE parameters			
		!	Insert a comment line		
		abort	Abort uncommitted changes		
		commit	Commit configuration changes		
		copy	Copy from one file to another		
		enabled	Specify SYNCE enable choice		
		exit	Exit from synce configuration mode		
		help	Display an overview of the CLI syntax		
		outputs	Specify synce output bits		
			Select among:	[eth0] [eth1] [eth2] [eth3] [eth4] [eth5] | none	
		primary-input	Specify synce primary input		
			input select	(eth0/eth1/eth2/eth3/eth4/eth5/none)	
		show	Show system information		
			alarm	Alarm information	
				Active Alarms	(set and not ignored)
			eventlog	Display event logs	
				Identity	(general/system/prtc/gnss/network/hardware/auth/ptp/ntp/update/all)
			firmware	Display Firmware version information	
			gnss	GNSS information	
				config	Current GNSS config (with any uncommitted changes)
				operating-state	GNSS operational state
				running-config	GNSS running configuration

				sat-status	GNSS satellite status
				startup-config	GNSS startup configuration
			history	Command history	
			Interface Added in FW > 5.00	Ethernet Interface information	
				config	Current interface config (with any uncommitted changes) (eth0/eth1/eth2/eth3/eth4/eth5/all)
				operating-state	Display the state of the specified interface (eth0/eth1/eth2/eth3/eth4/eth5/all)
				running-config	interface running-config (eth0/eth1/eth2/eth3/eth4/eth5/all)
				startup-config	interface startup-config (eth0/eth1/eth2/eth3/eth4/eth5/all)
			Iface Removed in FW > 5.00	IFACE information	
				config	Current iface config (with any uncommitted changes)
				running-config	iface running-config
				Startup-config	iface startup-config
			Interfaces Removed in FW > 5.00	Display the state of the specified interface	
			ntp	NTP information	
			prodconf	Display product configuration	
			prtc	PRTC information	
			ptp	PTP information	
			radius	RADIUS information	
			running-config	Current running configuration	
			snmp	SNMP information	

			startup-config	Contents of startup configuration
			synce	SYNCE information
			sysauth	SYStemAUTHentication information
			update	Remote update information
			vlan	VLAN information
	sysauth	Configure system authentication parameters - Only Avaliable to super access-level users		
		!	Insert a comment line	
		abort	Abort uncommitted changes	
		commit	Commit configuration changes	
		copy	Copy from one file to another	
		exit	Exit from sysauth configuration mode	
		help	Display an overview of the CLI syntax	
		http	Set HTTP enable value	
			choice	HTTP enable value (true/false)
		Password-rules	Specify rules for user passwords	
			!	Insert a comment line
			abort	Abort uncommitted changes
			commit	Commit configuration changes
			copy	Copy from one file to another
			diff-password-needed	Specify whether password difference required
				choice: Password must be different (true/false)
			digit-needed	Specify whether digit required
				choice: At least one digit required (true/false)
			exit	Exit from sysauth passwd-rules configuration mode
			help	Display an overview of the CLI syntax
			lower-case-needed	Specify whether lower case letter required
				choice: At least one lower case letter required (true/false)
			min-length	Specify the minimum password length
				integer: Minimum password length (6..30)
			rule-preset	Specify password rule preset to utilize

				choice	Password rule preset selection (p0/p1/p2/p3/p4)
			show	Show system information	
			special-needed	Specify whether special character required	
				choice	At least one special character required (true/false)
			upper-case-needed	Specify whether upper case letter required	
				choice	At least one upper case letter required (true/false)
			whoami	Display username and access level of current user	
		portal	Specify a portal type to configure		
			System authentication portal type	(ssh/web/serial)	
		show	Show system information		
			alarm	Alarm information	
			eventlog	Display event logs	
			firmware	Firmware version information	
			gnss	GNSS information	
			history	Command history	
			Interface Added in FW > 5.00	Ethernet Interface information	
				config	Current interface config (with any uncommitted changes) (eth0/eth1/eth2/eth3/eth4/eth5/all)
				operating-state	Display the state of the specified interface (eth0/eth1/eth2/eth3/eth4/eth5/all)
				running-config	interface running-config (eth0/eth1/eth2/eth3/eth4/eth5/all)
				startup-config	interface startup-config (eth0/eth1/eth2/eth3/eth4/eth5/all)
			Iface Removed in FW > 5.00	IFACE information	
			Interfaces	Display the state of the specified interface	

			Removed in FW > 5.00		
			ip	IPV4 information	
			ntp	NTP information	
			prodconf	Display product configuration	
			prtc	PRTC information	
				config	Current PRTC config (with any uncommitted changes)
				operating-state	PRTC operating-state
				running-config	PRTC running configuration
				starup-config	PRTC startup configuration
			ptp	PTP information	
				config	Current PTP config (with any uncommitted changes)
				operating-state	PTP operational state
				profile-defaults	PTP profile default values
				running-config	PTP running configuration
				startup-config	PTP startup configuration
			radius	RADIUS information	
				config	Current RADIUS config (with any uncommitted changes)
				dictionary	Display RADIUS dictionary. Copy contents to RADIUS server.
				running-config	RADIUS running configuration
				Startup-config	RADIUS startup configuration
			snmp	SNMP information	
				config	Current SNMP config (with any uncommitted changes)
				running-config	SNMP running configuration
				startup-config	SNMP startup configuration
			synce	SYNCE information	
				config	Current SYNCE config (with any uncommitted changes)
				operating-state	SYNCE operating-state

				running-state	SYNCE running configuration
				Startup-config	SYNCE startup configuration
			sysauth	SYStemAUTHentication information	
				config	Current SYSAUTH config (with any uncommitted changes)
				operating-state	SYSAUTH running configuration
				startup-config	SYSAUTH startup configuration
			system	SYSTEM Information	
			update	Remote update information	
				config	Remote update config (with any uncommitted changes)
				operating-state	Remote update operating-state
				running-config	Remote update running-config
				Startup-config	Remote update startup-config
			user	Local user account information	
			vlan	VLAN information	
				brief	Show operational summary of VLANs
				config	Current vlan config (with any uncommitted changes)
				ids	All vlan ids
				operating-state	vlan operating-state
				running-config	vlan running-config
				Startup-config	vlan startup-config
			radius	RADIUS information	
			running-config	Current running configuration	
			VLAN number (1..4094)		
			ztp	Zero Touch Provisioning (ZTP) information	

		web-csr-crt	Specify configuration for CSRs and CRTs			
			!	Insert a comment line		
			abort	Abort uncommitted changes		
			Commit	Commit configuration changes		
			Copy	Copy from one file to another		
			create-web-csr	Create or modify a CSR by specifying name and parameters		
				Field is mandatory and contains invalid value. Enter name of CSR (length 3..64) (Mandatory): Create new key pair [y,n] (Return to skip): Enter 2-letter country code (Mandatory): Enter state or province name (Return to skip): Enter locality (e.g. city) name (Return to skip): Enter organization (e.g. company) name (Return to skip): Enter unit (e.g. company section) name (Return to skip): Enter common name (e.g. server name) (Return to skip): Enter email address (length 3..254) (Return to skip): Enter challenge pasword (Return to skip): Enter alternate company name (Return to skip):		
			delete-web-crt	Specify a CRT basename to delete		
				String	System authentication web CRT name (length 3..64)	
			delete-web-csr	Specify a CSR basename to delete		
				String	System authentication web CSR name (length 3..64)	
			exit	Exit from sysauth webcsrcrt configuration mode		
			help	Display an overview of the CLI syntax		
			show	Show system information		
				alarm	Alarm information	
				eventlog	Display event log	

				firmware	Firmware version information
				gnss	GNSS information
				history	Command history
				interface	Ethernet Interface information
				ip	IPV4 information
				ntp	NTP information
				prodconf	Display product configuration
				prtc	PRTC information
				ptp	PTP information
				radius	RADIUS information
				snmp	SNMP information
				synce	SYNCE information
				sysauth	SYStemAUTHentication information
				system	SYSTEM information
				update	Remote update information
				user	Local user account information
				vlan	VLAN information
				ztp	Zero Touch Provisioning (ZTP) information
			Web-cert-name	Specify web certificate to use for current certificate	
				String	Name to use as current web certificate (length 3..64)
			whoami	Display username and access level of current user	
	system	Configure system parameters			
		!	Insert a comment line		
		abort	Abort uncommitted changes		
		commit	Commit configuration changes		
		copy	Copy from one file to another		
			running-config	Copy from running system configuration	
		exit	Exit from system configuration mode		
		help	Display an overview of the CLI syntax		

		hostname	Change the hostname for next login	
			String	Host name
		remote-syslog	Specify a remote syslog server number to configure	
			integer	Remote syslog server number (1..4)
		show	Show system information	
			alarm	Alarm information
			eventlog	Display event logs
			firmware	Firmware version information
			gnss	GNSS information
			history	Command history
			interface	Ethernet Interface information
			ntp	NTP information
			prodconf	Display product configuration
			prtc	PRTC information
			ptp	PTP information
			radius	RADIUS information
			snmp	SNMP information
			synce	SYNCE information
			sysauth	SYStemAUTHentication information
			system	SYSTEM information
			update	Remote update information
			user	Local user account information
			vlan	VLAN information
		whoami	Display username and access level of current user	
	update	Configure Remote Update parameters		
		!	Insert a comment line	
		abort	Abort uncommitted changes	
		active-image	Activate remote update image	
		address	Specify IP address of remote server	
			String	IP address of remote server
		auto-cert	Specify auto certificate choice	
			choice	Auto certificate choice (true/false)

		cert-data	Specify certificate data for remote update	
		commit	Commit configuration changes	
		copy	Copy from one file to another	
			running-config	Copy from running system configuration
		defer-update	Specify defer update choice	
			choice	Defer update choice (true/false)
		download-image	Initiate remote update image download	
		exit	Exit from update configuration mode	
		help	Display an overview of the CLI syntax	
		image-name	Specify name of update image (.pkg) or config (.json)	
			String	Image name
		image-path	Specify path to update image	
			String	Image path name
		password	Specify password for remote update	
		port	Specify port number	
			integer	Remote port number (0..65535)
		protocol	Specify Update remote protocol	
			choice	Remote update protocol (none/scp/http/https/ftp/tftp/ftps/sftp)
		revert-image	Revert to previous updnate image	
		show	Show system information	
			alarm	Alarm information
			eventlog	Display event logs
			firmware	Firmware version information
			gnss	GNSS information
			history	Command history
			interface	Ethernet Interface information
			ntp	NTP information
			prodconf	Display product configuration
			prtc	PRTC information
			ptp	PTP information

			radius	RADIUS information
			snmp	SNMP information
			synce	SYNCE information
			sysauth	SYStemAUTHentication information
			system	SYSTEM information
			update	Remote update information
			user	Local user account information
			vlan	VLAN information
		username	Specify username for remote update	
		whoami	Display username and access level of current user	
	user	Configure Local User Account parameters		
		!	Insert a comment line	
		abort	Abort uncommitted changes	
		commit	Commit configuration changes	
		copy	Copy from one file to another	
			running-config	Copy from running system configuration
		delete-user	Specify other local user account to delete Only available to 'super' admin-level users 'super' access-level users are not allowed to delete themselves or all local super access-level users.	
			String	Other local user name to delete
		email	Specify your email address	
			String	email address
		exit	Exit from user configuration mode	
		help	Display an overview of the CLI syntax	
		password	Specify your new password value -User access-level users cannot save any password change or email address change persistently. This must be done by an admin access-level user or higher in order to make these changes persistent	
		set-user	Specify other local user name to configure	

			Only available to ‘super’ level users		
			String	Other local user name	
		show	Show system information		
			alarm	Alarm information	
			eventlog	Display event logs	
			firmware	Firmware version information	
			gnss	GNSS information	
			history	Command history	
			interface	Ethernet Interface information	
			ntp	NTP information	
			prodconf	Display product configuration	
			prtc	PRTC information	
			ptp	PTP information	
			radius	RADIUS information	
			snmp	SNMP information	
			synce	SYNCE information	
			sysauth	SYStemAUTHentication information	
			system	SYSTEM information	
			update	Remote update information	
			user	Local user account information	
			vlan	VLAN information	
		whoami	Display username and access level of current user		
	vlan	Select/create VLAN id	integer	VLAN number (1..4094)	
	whoami	Display username and access level of current user			
	ztp	Configure Zero Touch Provisioning (ZTP) parameters			
		!	Insert a comment line		
		commit	Abort uncommitted changes		
		copy	Commit configuration changes		
		copy	Copy from one file to another		
		create-ztp-csr	Create ZTP CSR if it does not exist		
		enable	Specify ztp enable choice		
		exit	Exit from ztp configuration mode		

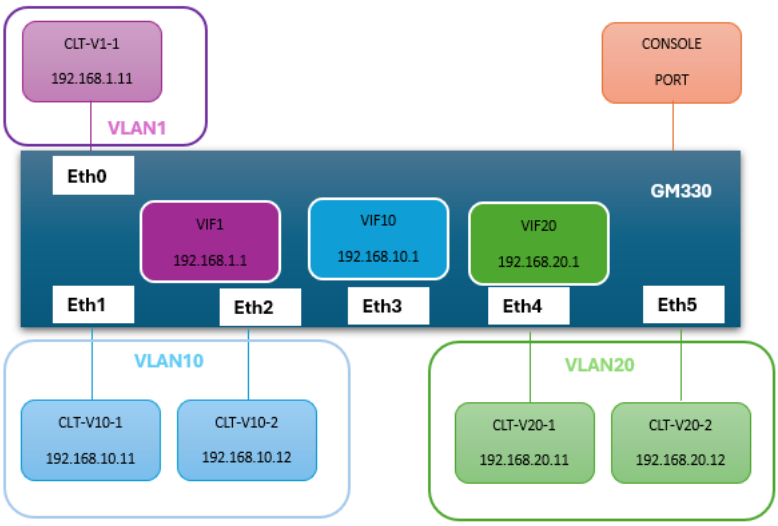
		help	Display an overview of the CLI syntax
		show	Show system information
		Status-reset	Request reset for ZTP operation
		whoami	Display username and access level of current user

Example Configuring a VLAN , VIF and assigning it to interface 4 :

The new configuration method is to create a Vlan with a static IP. In this example, we will create a Vlan 5 and a VIF 5. The configuration for Vlan5 will have the static IP configuration, then you assign Vlan 5 to interface 4.

```
gm3xx-1234> enable
gm3xx-1234# config t
gm3xx-1234# vlan 5
gm3xx-1234(config)# interface vlan 5
gm3xx-1234(config-vlan-VLAN5)# vif-enable true
gm3xx-1234(config-vlan-VLAN5)# ip enable
gm3xx-1234(config-vlan-VLAN5)# ip address 192.168.20.5 /24
gm3xx-1234(config-vlan-VLAN5)# gateway 192.168.20.1
gm3xx-1234(config-vlan-VLAN5)# commit
Successfully applied configuration changes
gm3xx-1234(config-vlan-VLAN5)# exit
gm3xx-1234(config)# interface ethernet 4
gm3xx-1234(config-if-eth4)# switchport mode access
gm3xx-1234(config-if-eth4)# switchport access vlan 5
gm3xx-1234(config-if-eth4)# commit
gm3xx-1234(config-if-eth4)# exit
gm3xx-1234(config) copy running-config startup-config
```

Configuring Internal L2 Switch:



Example:

```
GM330> enable
GM330# configure terminal
GM330(config)# vlan 10
GM330(config)# vlan 20
GM330(config)# interface ethernet 0
GM330(config-if-eth0)# switchport mode access
GM330(config-if-eth0)# switchport access vlan 1
GM330(config-if-eth0)# commit
GM330(config-if-eth0)# exit
GM330(config)# interface ethernet 1
GM330(config-if-eth1)# switchport mode access
GM330(config-if-eth1)# switchport access vlan 10
GM330(config-if-eth1)# commit
GM330(config-if-eth1)# exit
GM330(config)# interface ethernet 2
GM330(config-if-eth2)# switchport mode access
GM330(config-if-eth2)# switchport access vlan 10
GM330(config-if-eth2)# commit
GM330(config-if-eth2)# exit
GM330(config)# interface ethernet 3
GM330(config-if-eth3)# switchport mode trunk
GM330(config-if-eth3)# switchport trunk native vlan 10
GM330(config-if-eth3)# switchport trunk allowed vlan 10,20
GM330(config-if-eth3)# commit
GM330(config-if-eth3)# exit
```

```
! eth4: access mode, access VLAN (PVID) = VLAN20
GM330(config)# interface ethernet 4
GM330(config-if-eth4)# switchport mode access
GM330(config-if-eth4)# switchport access vlan 20
GM330(config-if-eth4)# commit
GM330(config-if-eth4)# exit
! eth5: access mode, access VLAN (PVID) = VLAN20
GM330(config)# interface ethernet 5
GM330(config-if-eth5)# switchport mode access
GM330(config-if-eth5)# switchport access vlan 20
GM330(config-if-eth5)# commit
GM330(config-if-eth5)# exit
! Enable VIF1. Assign static IPV4 address 192.168.1.1 with relevant netmask and gateway
GM330(config)# interface vlan 1
GM330(config-if-vlan1)# vif-enable true
GM330(config-if-vlan1)# ip enable
GM330(config-if-vlan1)# ip address 192.168.1.1/24
GM330(config-if-vlan1)# gateway 192.168.1.100
GM330(config-if-vlan1)# commit
GM330(config-if-vlan1)# exit
! Enable VIF10. Assign static IPV4 address 192.168.10.1 with relevant netmask and gateway
GM330(config)# interface vlan 10
GM330(config-if-vlan10)# vif-enable true
GM330(config-if-vlan10)# ip enable
GM330(config-if-vlan10)# ip address 192.168.10.1/24
GM330(config-if-vlan10)# gateway 192.168.10.100
GM330(config-if-vlan10)# commit
GM330(config-if-vlan10)# exit
! Enable VIF20. Assign static IPV4 address 192.168.20.1 with relevant netmask and gateway
GM330(config)# interface vlan 20
GM330(config-if-vlan20)# vif-enable true
GM330(config-if-vlan20)# ip enable
GM330(config-if-vlan20)# ip address 192.168.20.1/24
GM330(config-if-vlan20)# gateway 192.168.20.100
GM330(config-if-vlan20)# commit
GM330(config-if-vlan20)# exit
GM330(config)# copy running-config startup-config
GM330(config)# exit
```

Example “show gnss operating-state”

```
GM330> enable
GM330# show gnss operating-state
GNSS State:

GNSS Status:
gnss-status = ok
time-valid = true
pps-valid = true
ant-status = open


GNSS Time Info:
time-base = gps
utc-offset = 18
utc-valid = true
leap-pending = 0
gps-time-at-pps = 1727739042
sys-time = 1727739024

Satellite Counts:
channels = 54
tracked = 54
used = 46

Measurements:
time-unc = 0
temperature = 51.8

Geo-Location:
coord-accuracy = 3.85
height-accuracy = 11.21
pos-type = surveyed
survey-progress = 100
latitude = 41.6916
longitude = -88.1543
height = 167.261
v-north = 0.0061
v-east = 0
v-up = 0
heading = 1.5708
speed = 0.0061
pdop = 0.9
tdop = 0.4

GM330#
```

5.4.5 copy

running-config	Copy from the running system
startup-config	Copy from startup system

Use the "*copy*" command to make the configuration persistent

Example:

```
GM300(config)# copy running-config startup-config
GM300(config)# exit
```

5.4.6 disable

Use the "*disable*" *to turn off privileged* commands

5.4.7 exit

Use the "*exit*" *from the privileged* mode

```
GM300(config)# copy running-config startup-config
GM300(config)# exit
GM300#exit
GM300>
```

5.4.8 factory-reset

Use the "*factory-reset*" command to restore factory defaults

5.4.9 help

Use the "*help" command to display an overview of the CLI syntax*

Example:

"help"

```
GM300> enable
GM300#
GM300# help
CONTEXT SENSITIVE HELP
[?] - Display context sensitive help. This is either a list of possible
      command completions with summaries, or the full syntax of the
      current command. A subsequent repeat of this key, when a command
      has been resolved, will display a detailed reference.

AUTO-COMPLETION
The following keys both perform auto-completion for the current command line.
If the command prefix is not unique then the bell will ring and subsequent
repeat of the key will display possible completions.

[enter] - Auto-completes, syntax-checks then executes a command. If there is
          a syntax error then an error message will be displayed.

[space] - Auto-completes, or if the command is already resolved inserts a space.

MOVEMENT KEYS
[CTRL-A] - Move to the start of the line
[CTRL-E] - Move to the end of the line.
[up]     - Move to the previous command line held in history.
[down]   - Move to the next command line held in history.
[left]   - Move the insertion point left one character.
[right]  - Move the insertion point right one character.

DELETION KEYS
[CTRL-C]    - Delete and abort the current line
[CTRL-D]    - Delete the character to the right on the insertion point.
[CTRL-K]    - Delete all the characters to the right of the insertion point.
[CTRL-U]    - Delete the whole line.
[backspace] - Delete the character to the left of the insertion point.
```

5.4.10 history

Use the "*history*" *command to display history buffer*

history	Command history

Example:

```
GM300>
GM300> show history
set auto off
show prtc operating-state
show gnssoperating state
config t
enable
configure terminal
show gnss
quit
exit
show prtc
show gnss operating-state
show ptrc o
show ptrc operating-state
show gnss
show prtc operating-state
show gnss operating-state
show alarm
show alarm active
show ptp operating-state
show ptp operating-state all
show history
GM300>
```

5.4.11 ping

ip	Send ICMP IPv4 messages to network hosts (default)	
ipv6	Send ICMP IPv6 messages to network hosts	
arp	Send ARP requests to a neighbor host	
String	source	Source IP-address (ip) or interface (ip and arp)
	repeat	Request to send count, default is 5

Example:

```
GM300>
GM300> ping ip 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
64 bytes from 192.168.1.5: icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=64 time=0.580 ms
64 bytes from 192.168.1.5: icmp_seq=3 ttl=64 time=0.531 ms
64 bytes from 192.168.1.5: icmp_seq=4 ttl=64 time=0.522 ms
64 bytes from 192.168.1.5: icmp_seq=5 ttl=64 time=0.666 ms

--- 192.168.1.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4061ms
rtt min/avg/max/mdev = 0.522/0.682/1.113/0.221 ms
GM300>
```

5.4.12 reboot

Use the "*reboot*" command to Halt and perform a software system restart

5.4.13 show

alarm	active	Active alarms (set and not ignored)
	all	All alarms
	config	Current alarm config (with any uncommitted changes)
	running-config	Alarm running configuration
	startup-config	Alarm startup configuration
eventlog	<general/system/prtc/gnss/network /hardware/auth/ptp/ntp/update/all>	Display event logs
firmware	version	Display firmware version information
gnss	config	Current GNSS config (with any uncommitted changes)
	operating-state	GNSS operational state
	running-config	GNSS running configuration
	Startup-config	GNSS startup configuration
history	Lists previous commands	
Interface Added in FW > 5.00	Ethernet Interface information	
	config	Current interface config (with any uncommitted changes)
	operating-state	Display the state of the specified interface

	running-config	interface running-config	
	startup-config	interface startup-config	
Iface Removed in FW > 5.00	IFACE information		
Interfaces Removed in FW > 5.00	Display the state of the specified interface		
ntp	authkey		NTP authentication keys
		config	Current NTP authentication keys (with any uncommitted changes)
		running-config	NTP running authentication keys
		startup-config	NTP startup authentication keys
	config	Current NTP config (with any uncommitted changes)	
	key-profiles	NTP authentication key profiles	
	operating-state	NTP operational state	
	running-config	NTP running configuration	
	startup-config	NTP startup configuration	
prodconf	Display product configuration		
prtc	PRTC information		
	config	Current PRTC config (with any uncommitted changes)	
	operating-state	PRTC operating-state	
	running-config	PRTC running configuration	
	startup-config	PRTC startup configuration	
ptp	config	Current PTP config (with any uncommitted changes)	
	operating-state	PTP operational state	
	running-config	PTP running configuration	
	Startup-config	PTP startup configuration	
radius	RADIUS information		

	config	Current RADIUS config (with any uncommitted changes)
	dictionary	Display RADIUS dictionary. Copy contents to RADIUS server.
	running-config	RADIUS running configuration
	startup-config	RADIUS startup configuration
running-config	Current running configuration	
snmp	SNMP information	
	config	Current SNMP config (with any uncommitted changes)
	running-config	SNMP running configuration
	startup-config	SNMP startup configuration
startup-config	Contents of the startup configuration	
synce	SYNCE information	
	config	Current SYNCE config (with any uncommitted changes)
	operating-state	SYNCE operating-state
	running-config	SYNCE running configuration
	Startup-config	SYNCE startup configuration
sysauth	SYStemAUTHentication information	
	config	Current SYSAUTH config (with any uncommitted changes)
	running-config	SYSAUTH running configuration
	Startup-config	SYSAUTH startup configuration
update	Remote update information	
	config	Remote update config (with any uncommitted changes)
	operating-state	Remote update operating-state
	running-state	Remote update running-config
	startup-config	Remote update startup-config
vlan	VLAN information	
	brief	Show operational summary of VLANs

	config	Current vlan config (with any uncommitted changes)	
		Vlan number	(1..4094)
	ids	All vlan ids	
	operating-state	vlan operating-state	
	running-config	vlan running-config	
	startup-config	vlan startup-config	

Example:

```
GM3xx> show gnss operating-state

GNSS State:

GNSS Status:
gnss-status = update
time-valid = false
pps-valid = false
ant-status = open

GNSS Time Info:
time-base = utc-glo
utc-offset = 19
leap-pending = 1
gps-time-at-pps = 1700157652
sys-time = 1700157652

Satellite Counts:
channels = 1
tracked = 0
used = 0

Measurements:
time-unc = 558
temperature = 50

GM3xx>
```

5.4.14 whoami

Display username and access level of current user

5.6 List of "How to" help topics

List of frequently used tasks and helps on the related CLI options.

The list of frequently used tasks:

5.6.3 How do I disable ethernet port 0?

```
GM3xx> enable
GM3xx# configure terminal
GM3xx<config> interface ethernet 0
GM3xx<config-if-eth0> shutdown
GM3xx<config-if-eth0> commit

To re-enable:
GM3xx<config-if-eth0> no shutdown
GM3xx<config-if-eth0> commit
```

5.6.4 How do I set an IP address of 192.168.0.9, and set a netmask and a gateway address on ethernet 0 port?

Since the integration of the internal switch, this feature is not supported. Now a Vlan Needs to be created first with the associate VIF configured for Static or DHCP and then assigned to the port.

5.6.7 How do I set the console serial port baud rate to 19200 bps?

It has not been implemented yet, will be supported in a future firmware release.

5.6.8 How do I get the current eth0 status?

```
GM3xx>

GM3xx> show interface operating-state eth0

interface state:

eth0 state:

admin-status = up
oper-status = up
port-socket-type = RJ45

Auto-negotiation status:
speed = 1
duplex = full
speed-string = Auto 1Gfdx

counters:
in-octets = 2936
in-unicast-pkts = 29
in-broadcast-pkts = 3
in-multicast-pkts = 0
in-discards = 0
in-errors = 0
in-unknown-protos = 0
out-octets = 515109
out-unicast-pkts = 32
out-broadcast-pkts = 5338
out-multicast-pkts = 1018
out-discards = 0
out-errors = 0

GM3xx>
```

5.6.12 How do I restore factory default settings?

```
GM300> enable

GM300# factory-reset
```

5.6.13 How do I reboot the system?

```
GM300> enable
GM300# reboot
Perform system restart (y/N)? y
```

6. Web Interface

This chapter describes the configuration and status pages of the web interface.

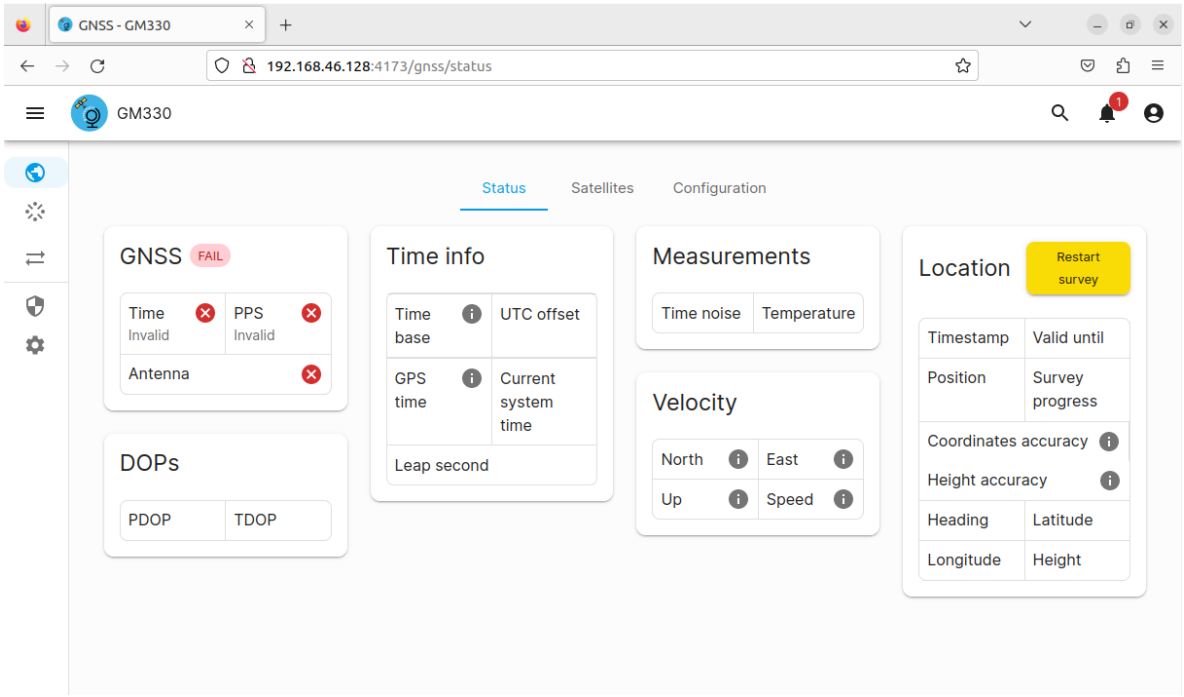
6.1 Home page

To launch a web browser and open a connection to the Time server, enter the IP Address that was assigned by the DHCP server.

Web access is permitted on any ethernet interface. The interface defaults to DHCP.
A static IP can be configured through the front console serial port.

> NOTE - Internet Explorer 11, Firefox, and Chrome browsers are supported on Windows® and Linux operating systems. Protempis recommends using the Chrome browser for better rendering of the web pages.

Entering the IP address will open the main or home page.



Ethernet Port:		Identifies the Ethernet port – Ethernet 0 - 5	
Query:		Get the current configuration for the selected Ethernet port	
Save:		Save the configuration	
Save to multiple:		Select	Ethernet 0 to Ethernet 5 to apply configuration
			Reset Profile defaults
GNSS Status:			OK, Fail, Disabled
	Time:		valid, invalid
	PPS:		valid, invalid
	Antenna:		shorted, not connected, fault, high current
Time info:			
	Time base:		UTC, UTC(Glonass), GPS, Glonass, BeiDou, NavIC

	UTC offset:	e.g.) 18 s
	GPS time	e.g.) 11/20/2023, 1:47:43 PM
	Current system time:	e.g.) 11/20/2023, 1:48:22PM
	Leap second:	Insertion, Deletion, Nothing pending
Measurements Status:		
	Time noise:	No info, e.g.) 1970 ns
	Temperature:	e.g.) 10°C
Location:		
	Timestamp:	e.g.)11/20/2023, 1:52:30PM
	Valid until:	e.g.) 11/20/2023, 1:53:09PM
	Position:	Active, Surveyed
	Survey progress:	0-100%
	Coordinates accuracy:	e.g.) 128.78 Accuracy of Lat/Long Pair
	Height accuracy:	e.g.) 106.29 Accuracy of Height Value
	Heading:	e.g.) 192.073°
	Latitude:	e.g.) -78.776 °
	Longitude:	e.g.) 38.67 °
	Height:	e.g.) 1045 m
	Restart survey	Recalculate the Location
Velocity:		
	North:	e.g.) 188.15 m/s
	East:	e.g.) 199.5 m/s
	Up:	e.g.) 166.7 m/s
	Speed:	e.g.) 126.6 m/s
DOPs:		
	PDOP:	e.g.) 98.5
	TDOP:	e.g.) 70.2

Refresh Rate

The main page is refreshed at a rate of one second.

6.2 Login page

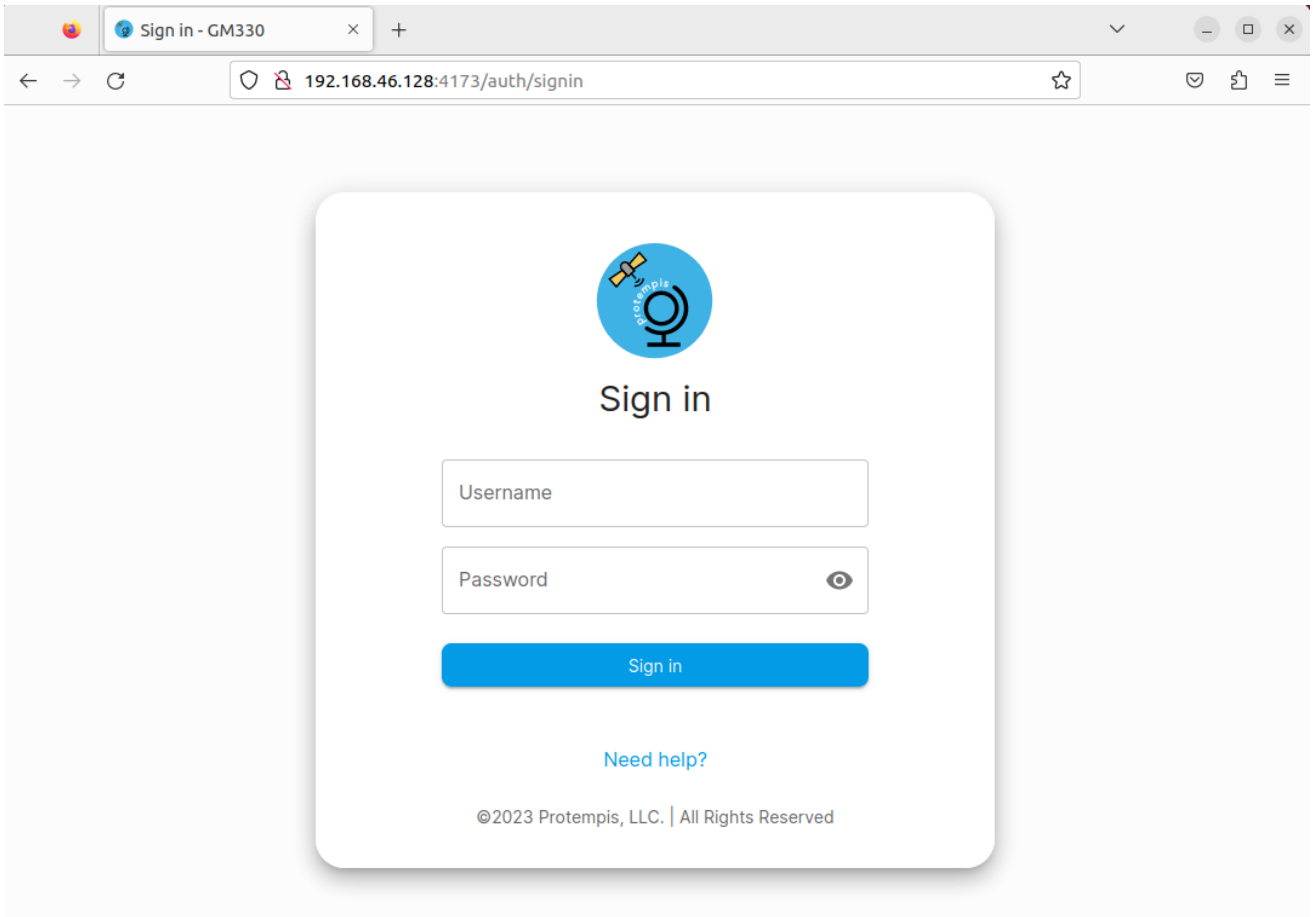
Log in to view the status of the system. The login page requires a valid username and password.

> NOTE - There is a change in the default password to comply with the California State Bill SB-327-Information privacy: connected devices bill, which requires that the preprogrammed password is unique to each device manufactured. The SB-327 bill is effective from 1 January 2020.
>
> Only the user protempissuper is available by default, with the default password as outlined in this section.

Starting with v1.01.00, the unique password is based on the unit's serial number. Here is the format:

Username: protempissuper
Password: Tbolt_<serial number> -If using DEMO/1.0.0 “super”

For example, if the serial number is 1234567890, the password will be Tbolt_1234567890.

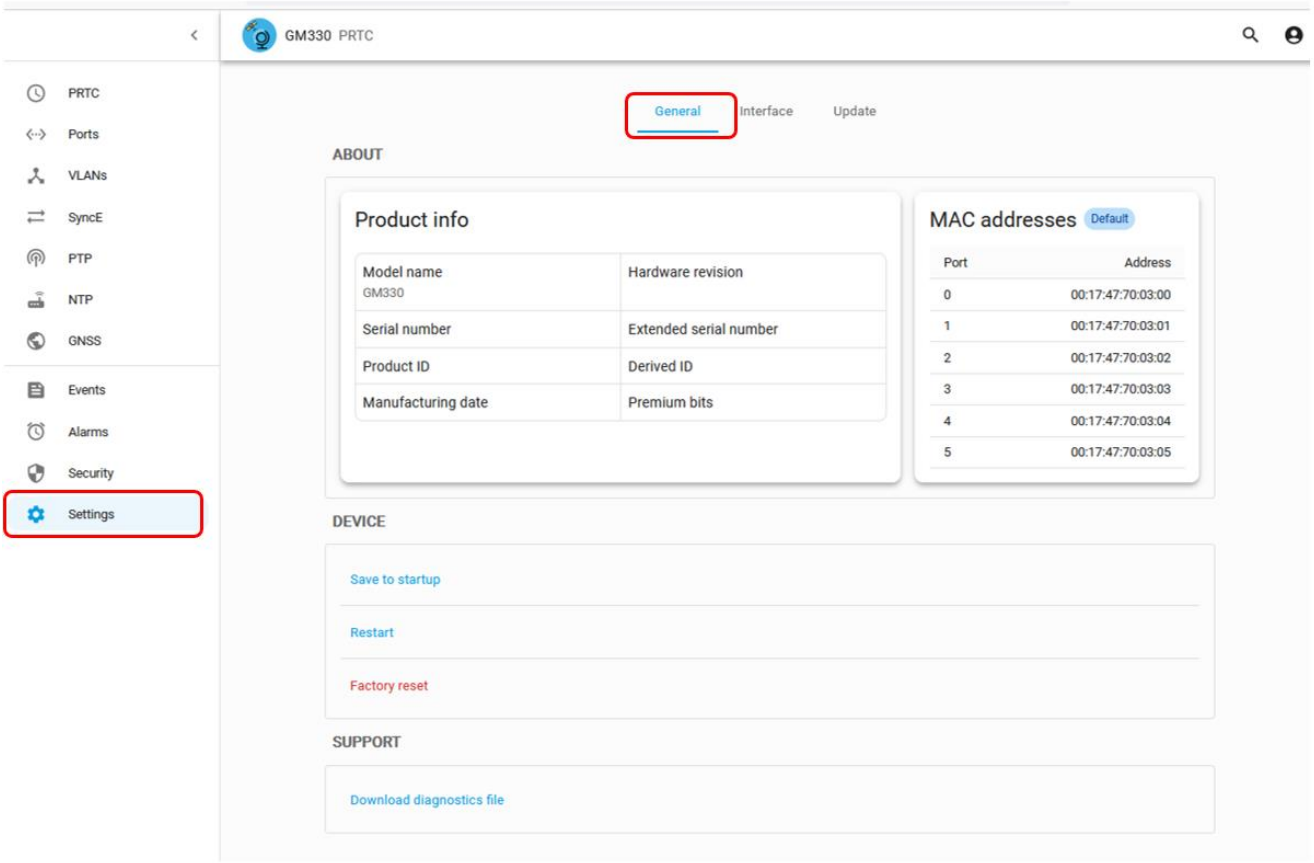


As a 'Best security practice’ Protempis recommends changing the default user credentials of the ‘protempissuper’ account.

6.3 Settings

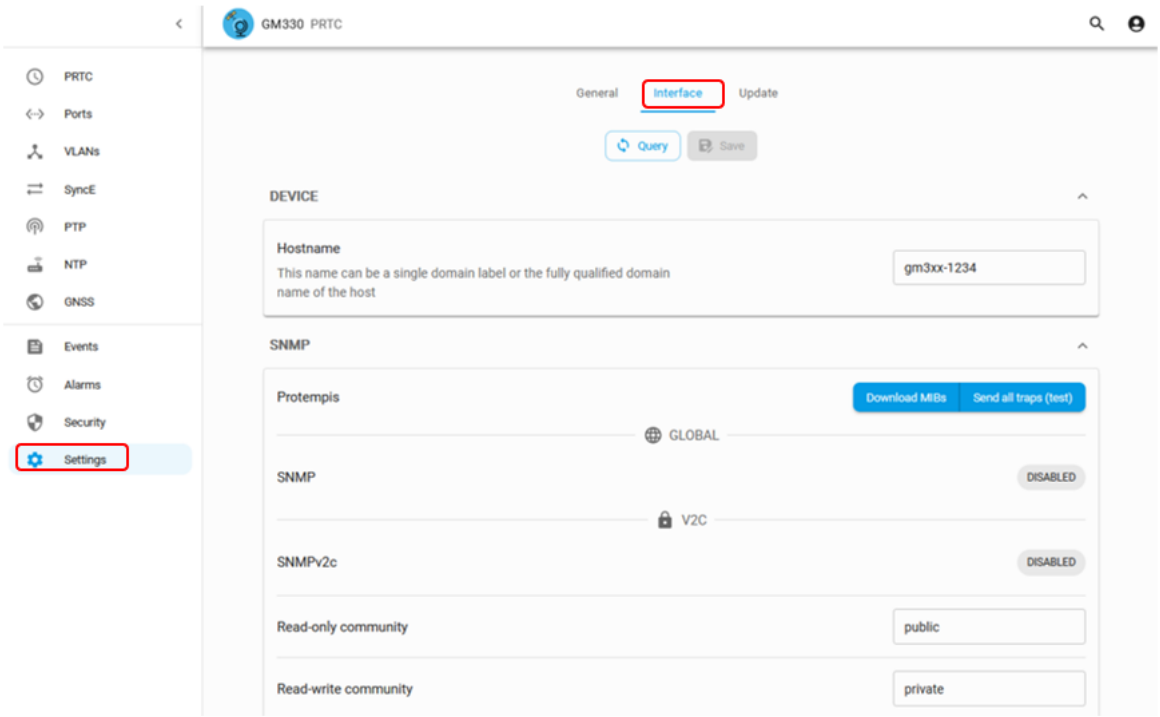
By using the navigation menu on the left side of the screen, you can view several configuration pages, which are described in the following pages.

6.3.1 General

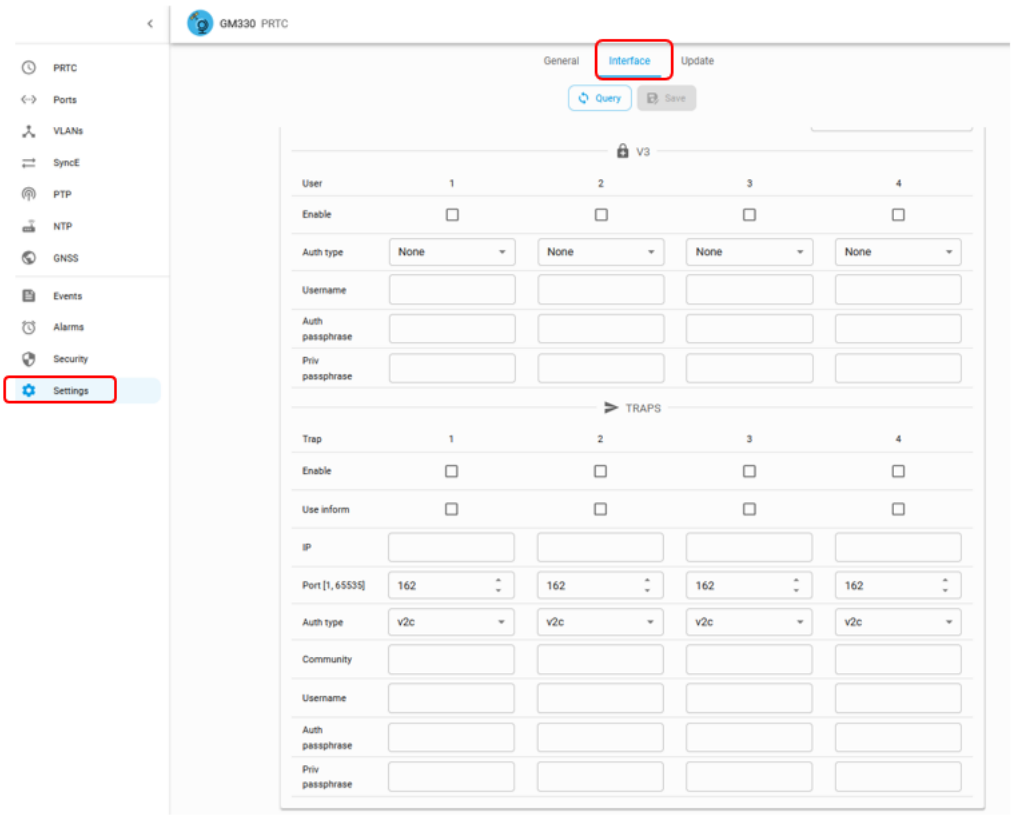


Configuration	Hostname	Name of the Unit
Device	Save to Startup	Save current configuration to the startup configuration
	Restart	Reboot the unit using the startup configuration
	Factory Reset	Restore unit to factory default settings
Support	Download Diagnostic file	Protempis may request this file to help in debugging an issue

6.3.2 Interface



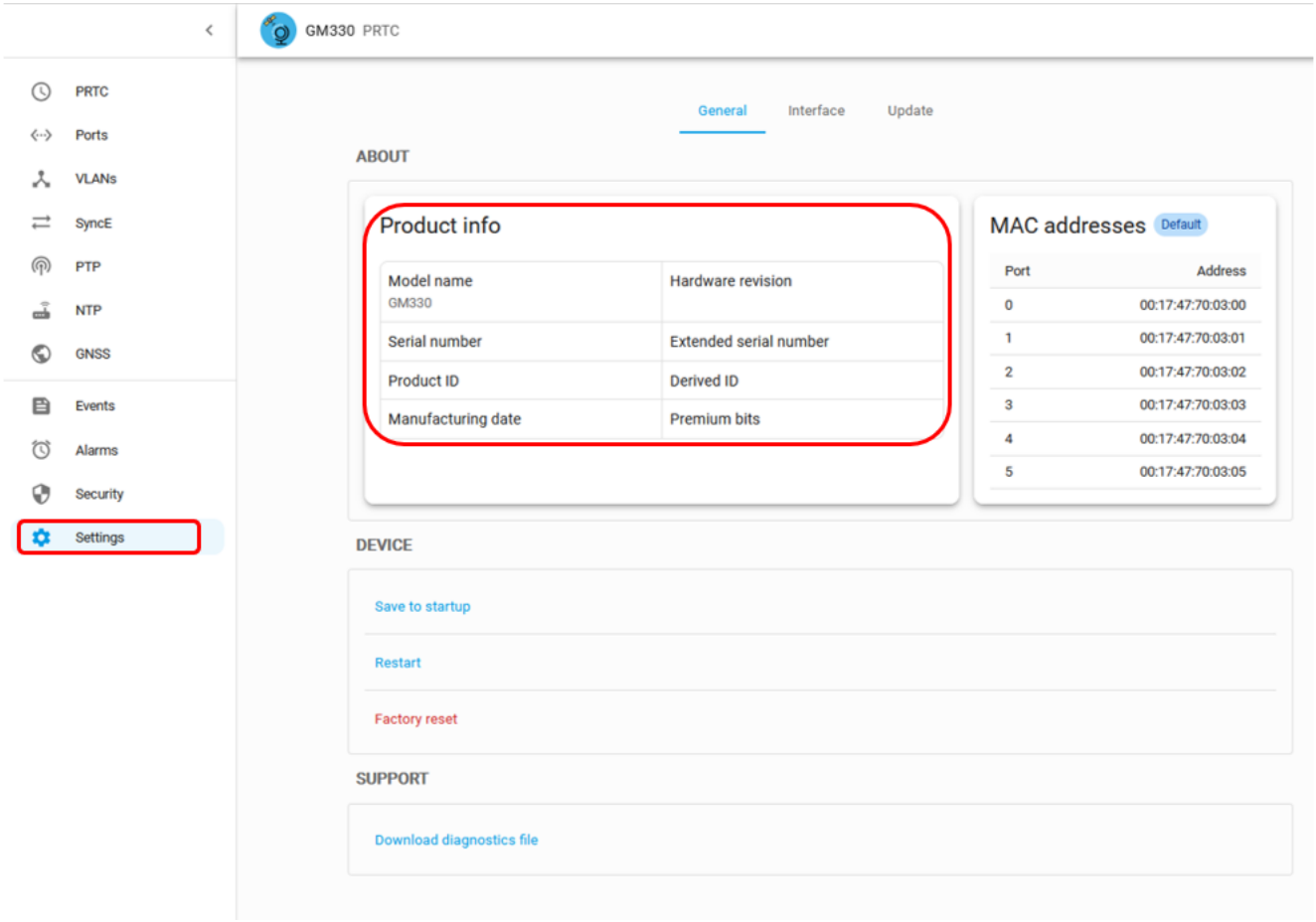
Device	Hostname	Name Of the Device
SNMP	Protempis	Download SNMP MiBs
	SNMP	Global Configuration Enable/Disabled
	SNMPv2c	Use Agent v2c Enable/Disabled
	Read Only community	community string for read only public/private
	Read-write community	Community string for read write public/private



V3	User	Configure 1 to 4 users by selecting “box”
	Auth Type	None, Auth, Auth+Priv
	Username	
	Auth passphrase	
	Priv passphrase	
Traps	Trap	
	Enable	Enable up to 4 Traps by selecting “Box”
	Use Inform	To Set use inform instead of “generating trap”
	IP	IP address of the SNMP manager that receives the TRAP.
	Port	Port number of the SNMP manager [1..65535]
	Auth type	v2c, v3 none, v3 auth, v3 auth+priv
	Community	
	Username	
	Auth passphrase	

	Priv passphrase	

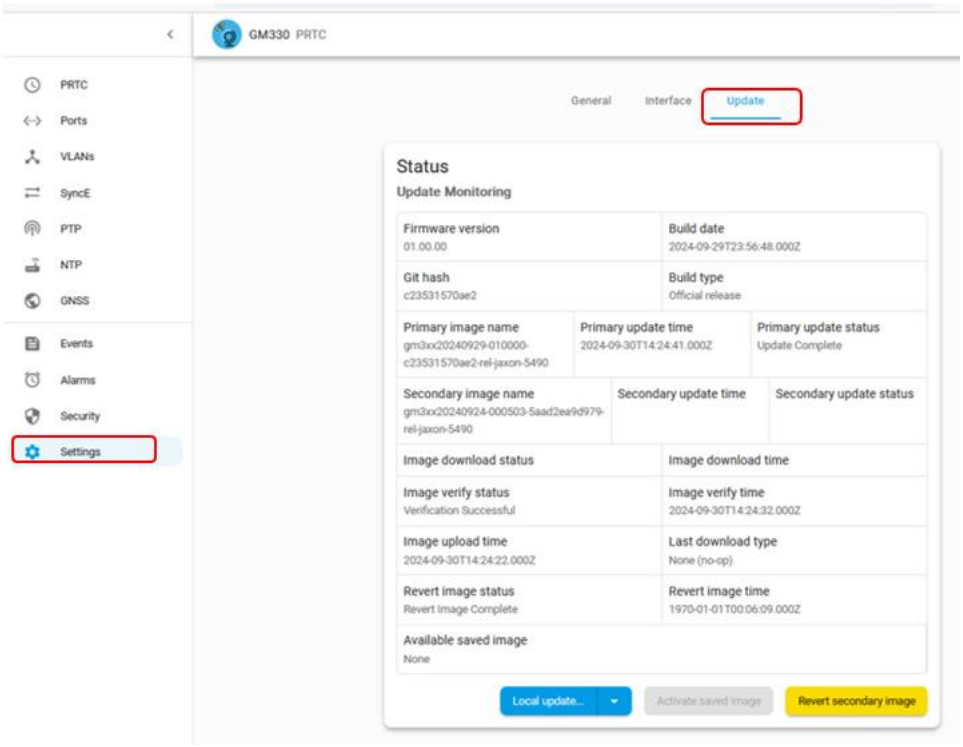
6.3.3 Product Info



Model Name	Unit Model Name
Serial Number	Serial Number assigned at the factory
Product ID	Product Model Number
Manufacturing Date	When the unit was built
Hardware revision	Hardware Version
Extended serial number	
Derived ID	
Premium Bits	
Ports MAC address	Default Mac Address for each port

6.3.4 Update

This page allows for updating, changing, or reverting the firmware from a local Or remote .pkg file.

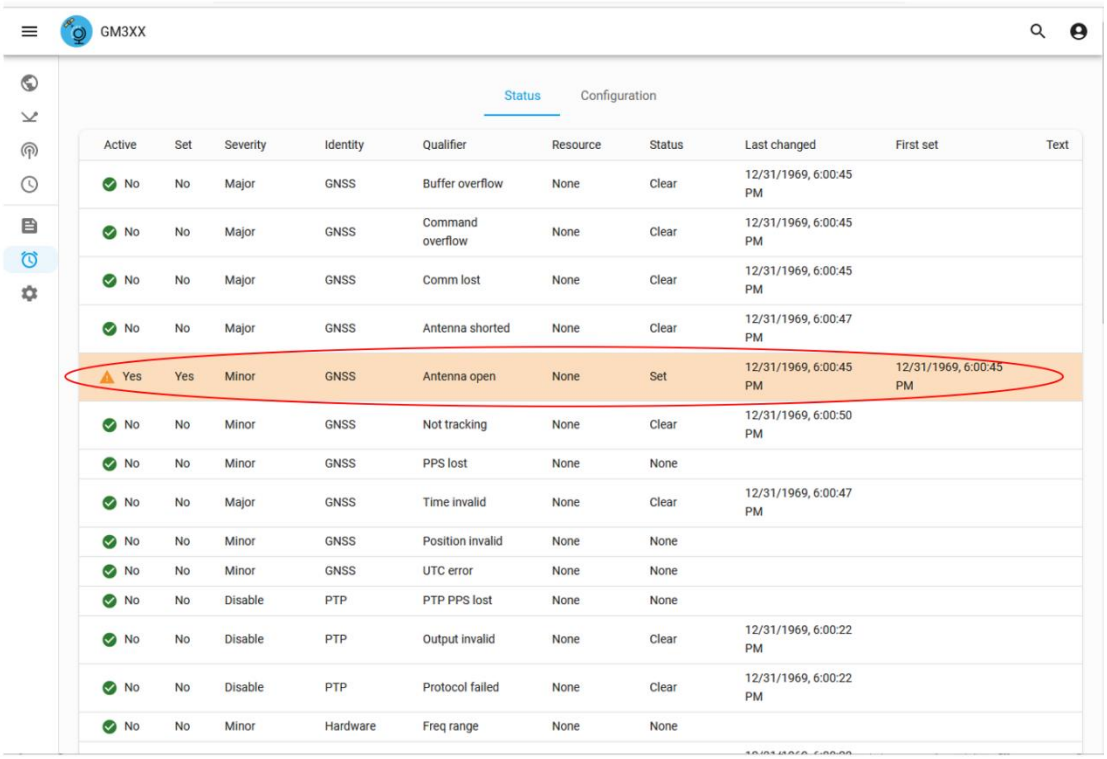


	Version, Build Date, Build Type, Primary Image Name
Local/Remote Update	Where is the new firmware locally or remotely
Activate Saved Image	Update the firmware and activate the new firmware
Revert Secondary Image	Revert to a previous version of firmware and reboot

6.4 Alarms

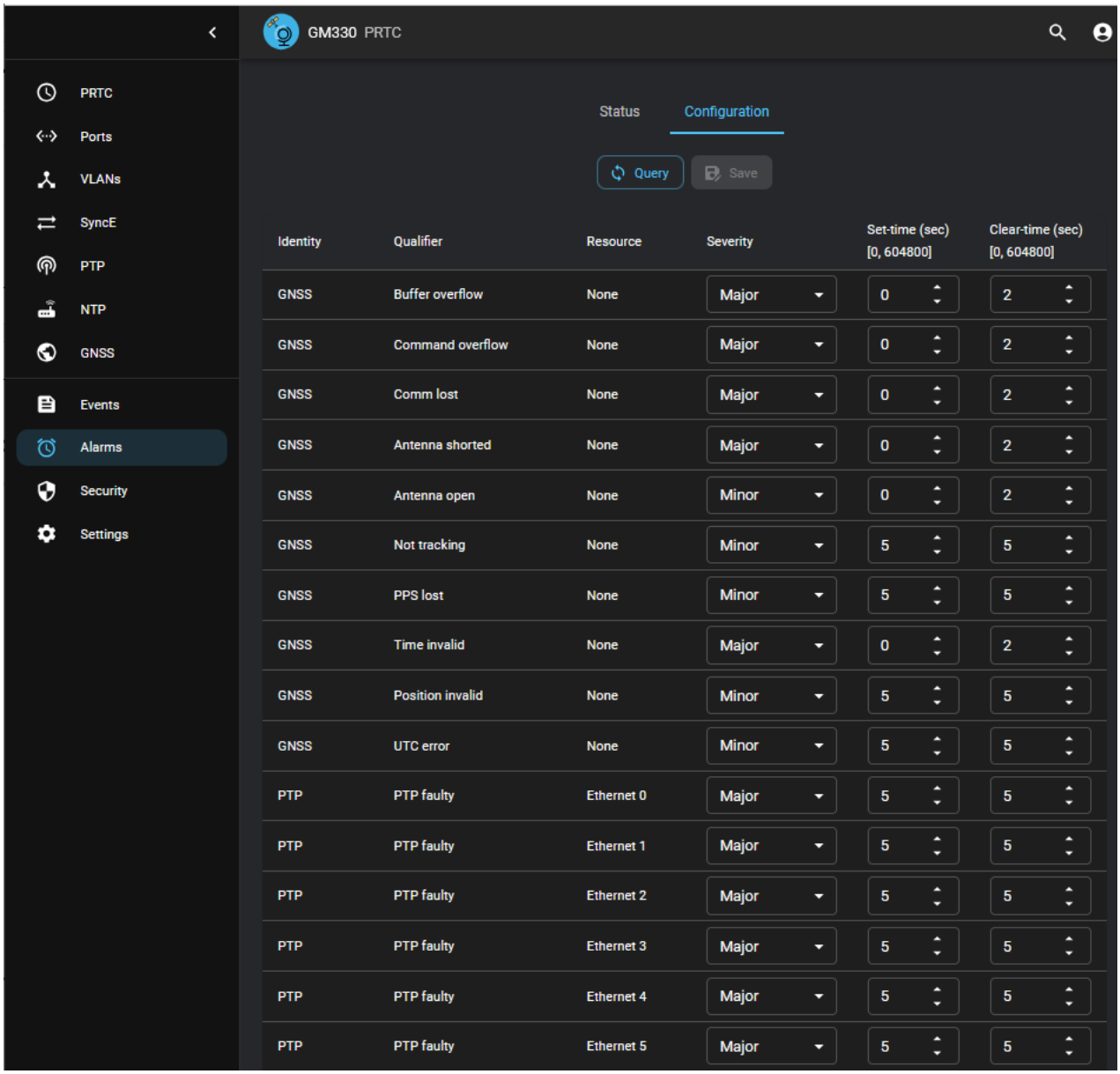
6.4.1 Alarm Status

Below is an example of an alarm that has been triggered. The status page indicates an “Open Antenna” alarm.



1	Click on “Alarms”
2	Click on “Status”

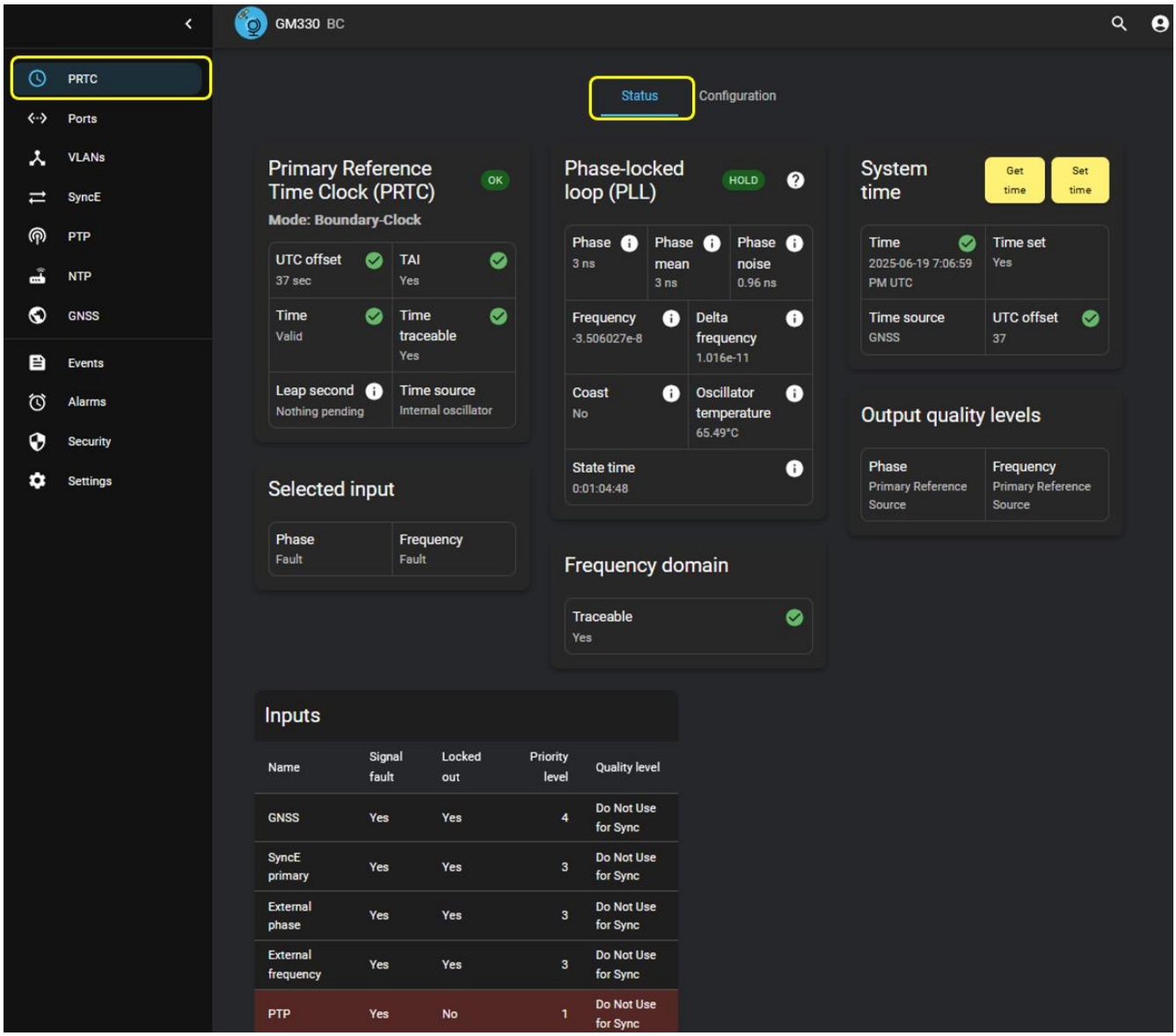
6.4.2 Alarm Configuration



Identity	Qualifier	Resource	Severity	Set-time (sec) [0, 604800]	Clear-time (sec) [0, 604800]
GNSS	Buffer overflow	None	Major	0	2
GNSS	Command overflow	None	Major	0	2
GNSS	Comm lost	None	Major	0	2
GNSS	Antenna shorted	None	Major	0	2
GNSS	Antenna open	None	Minor	0	2
GNSS	Not tracking	None	Minor	5	5
GNSS	PPS lost	None	Minor	5	5
GNSS	Time invalid	None	Major	0	2
GNSS	Position invalid	None	Minor	5	5
GNSS	UTC error	None	Minor	5	5
PTP	PTP faulty	Ethernet 0	Major	5	5
PTP	PTP faulty	Ethernet 1	Major	5	5
PTP	PTP faulty	Ethernet 2	Major	5	5
PTP	PTP faulty	Ethernet 3	Major	5	5
PTP	PTP faulty	Ethernet 4	Major	5	5
PTP	PTP faulty	Ethernet 5	Major	5	5

6.5 Primary Reference Time Clock PRTC

The GM330 is a PRTC device, it sources Frequency, Phase, and Time (Traceable to UTC).

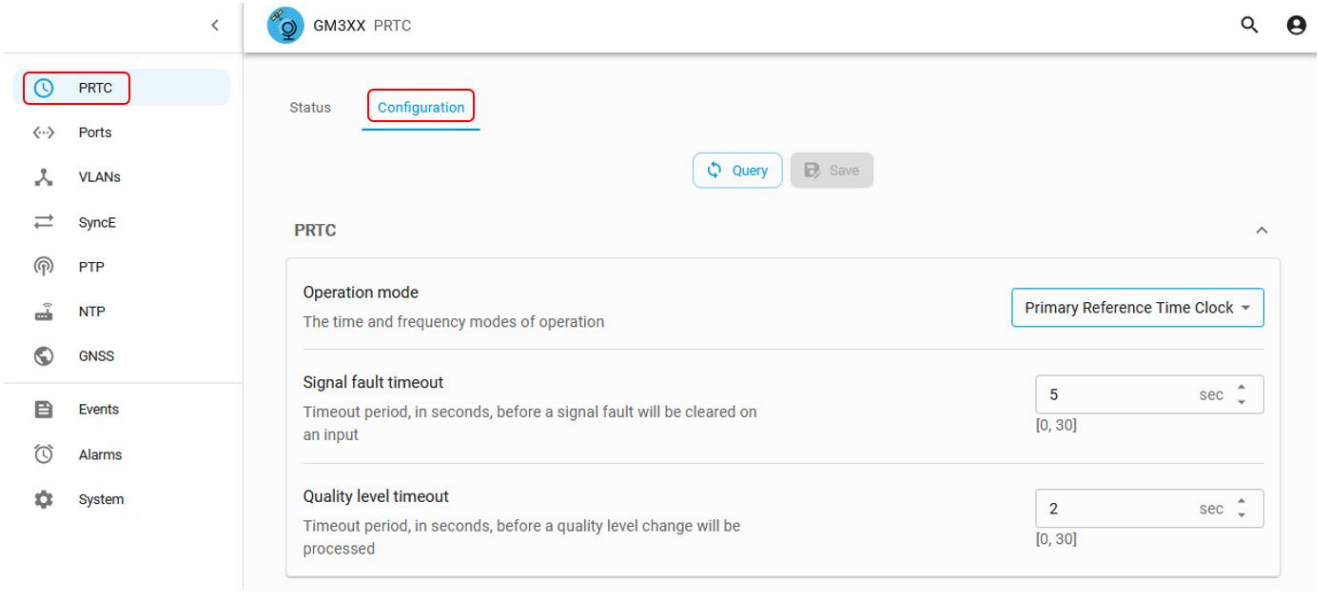


6.5.1 Status

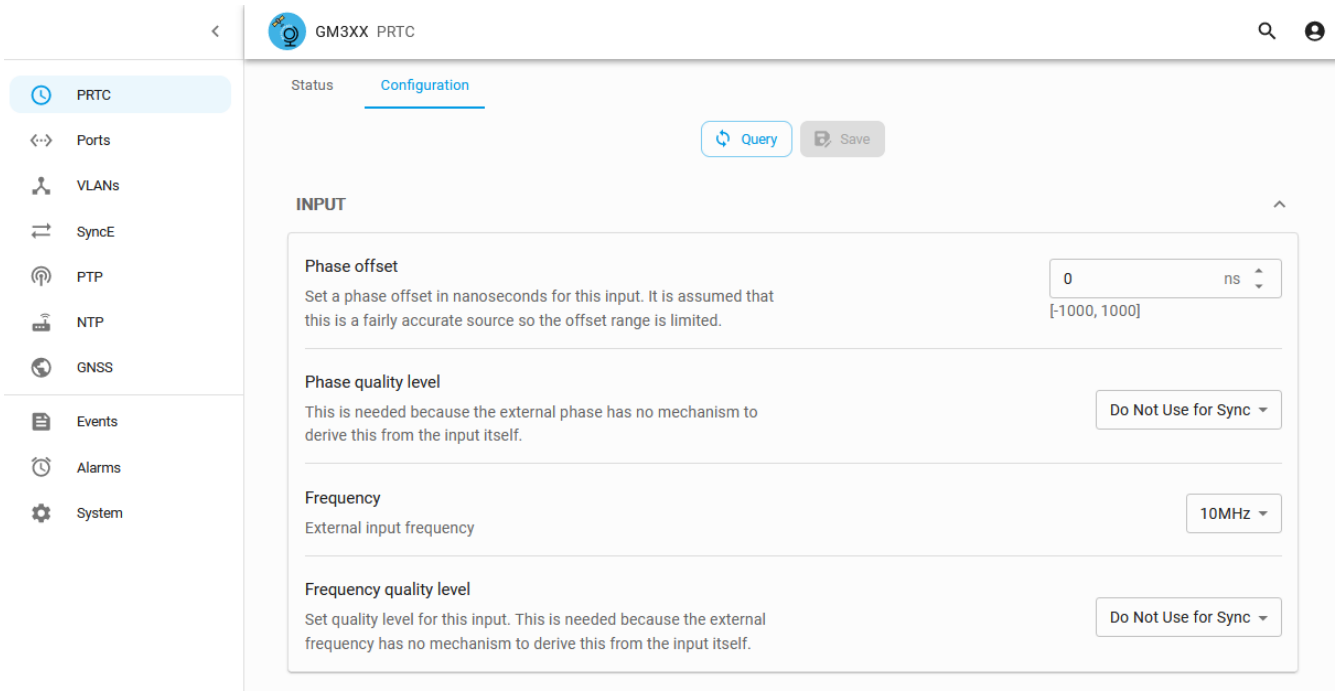
PRTC	UTC	Current UTC Status (Valid, Not Valid)
	UTC Offset	In Seconds
	TAI	Can TAI be derived (Yes, No)
	Time	Is time Valid
	Time Traceable	Is time traceable to a known reference
	Leap Second	Nothing Pending
	Time Source	GNSS
Selected Input	Phase	GNSS
	Frequency	

PLL	States	**Fail**: This could be due to hardware issues that prevent the system from running **Init**: Has not been started yet **Jam**: Forcing a synchronization of its output phase to the input phase by jamming **Acquiring**: Is in acquisition mode **Recovering**: This is similar to acquisition, but indicates that the loop was previously in a locked condition **Locked**: This is an indication that it is operating normally **Freerun**: Has never controlled the frequency of its internal oscillator. This means that there was no usable input available from the start of the system. **Halt**: This means that there is no usable input available. There was an input previously, and the unit had transitioned to 'locked' at some point but there was not enough valid historical information to allow the unit to go into holdover. In this mode there are no corrections. **Hold**: This means that there is no usable input available. There was an input previously, and the unit had transitioned to 'locked' at some point and there was enough valid historical information to allow the unit to be able to project the oscillator stability such that it can maintain good phase operations for a period of time. The parameters that will be compensated for include frequency changes over temperature as well as the change of the oscillator frequency over time, which is called aging. **User halt**: In this mode, there may be a usable input, but the user has put the control loop into an open loop condition. In a halt mode, the control loop will not attempt to provide any corrections to the oscillator frequency. If there is an input available, the phase values can be used to measure the performance of the system in a halt mode. **User hold**: In this mode, there may be a usable input, but the user has put the control loop into an open loop condition. In a hold mode, the control loop will attempt to provide any corrections to the oscillator due to temperature changes and aging over time. If there is an input available, the phase values can be used to measure the performance of the system in a hold mode.
	Phase	Measured Input to System Output (nS)
	Phase Mean	Average Phase Measurement over time
	Phase Noise	Noise of the Phase Input
	Frequency	Frequency offset of the Oscillator
	Delta Frequency	Change of Frequency offset since the last update
	Coast	Indication of current measurement used in the control loop
	State Time	Time Control Loop in a given state
Output Quality Levels	Phase	PRS
	Frequency	
Frequency Domain	Traceable	Indication if Frequency traceable to current Stratum Source
System Time	Get Time	Display current Time
	Set Time	Set Time

6.5.2 Configuration

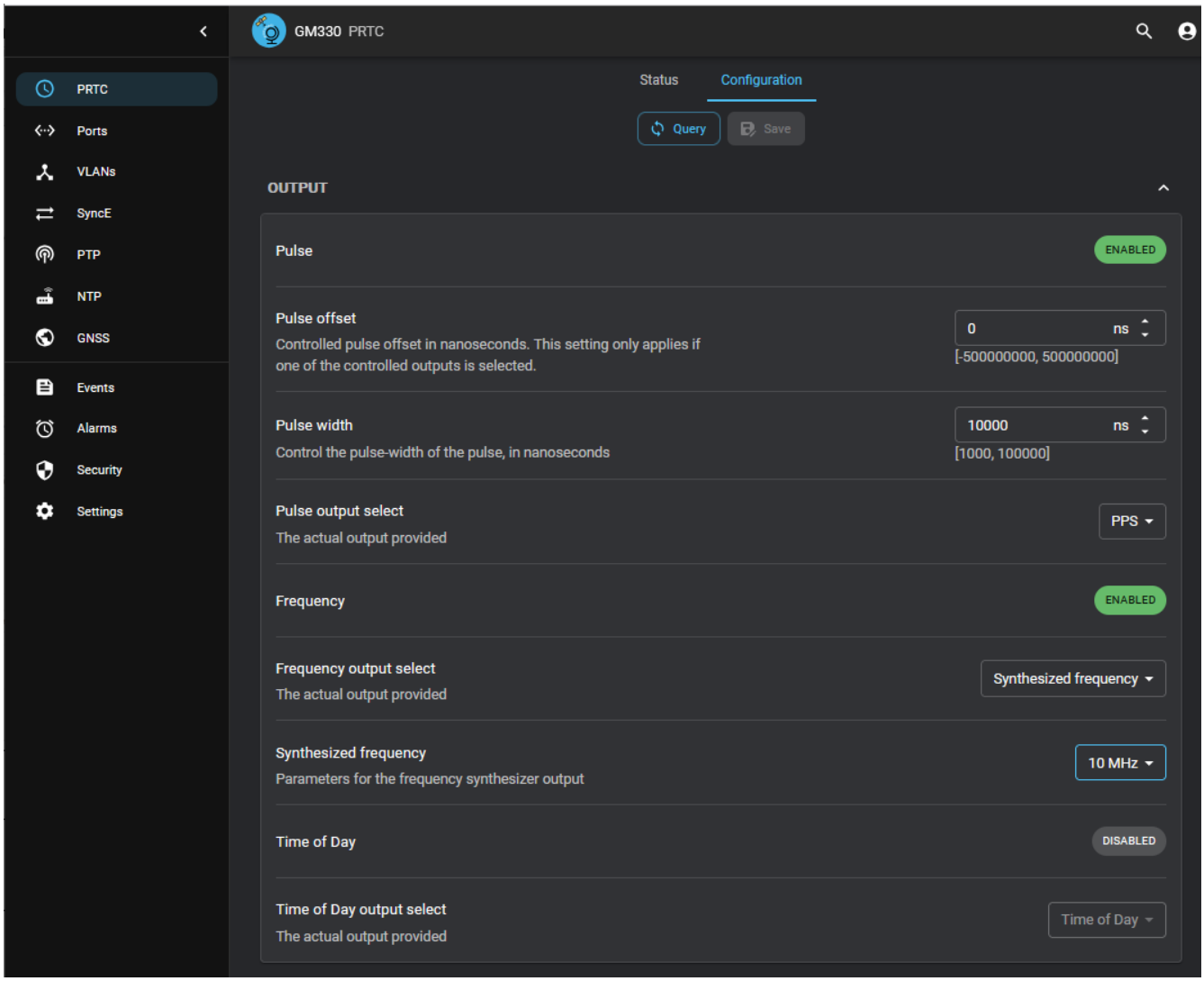


PRTC	Operation Mode	The time and frequency modes of operation	Primary Reference Clock Assisted Partial Timing Support Boundary Clock
	Signal Fault Timeout	Timeout period, in seconds, before a signal fault will be cleared on an input	[0, 30] Sec
	Quality level timeout	Timeout period, in seconds, before a quality level change will be processed	[0, 30] Sec



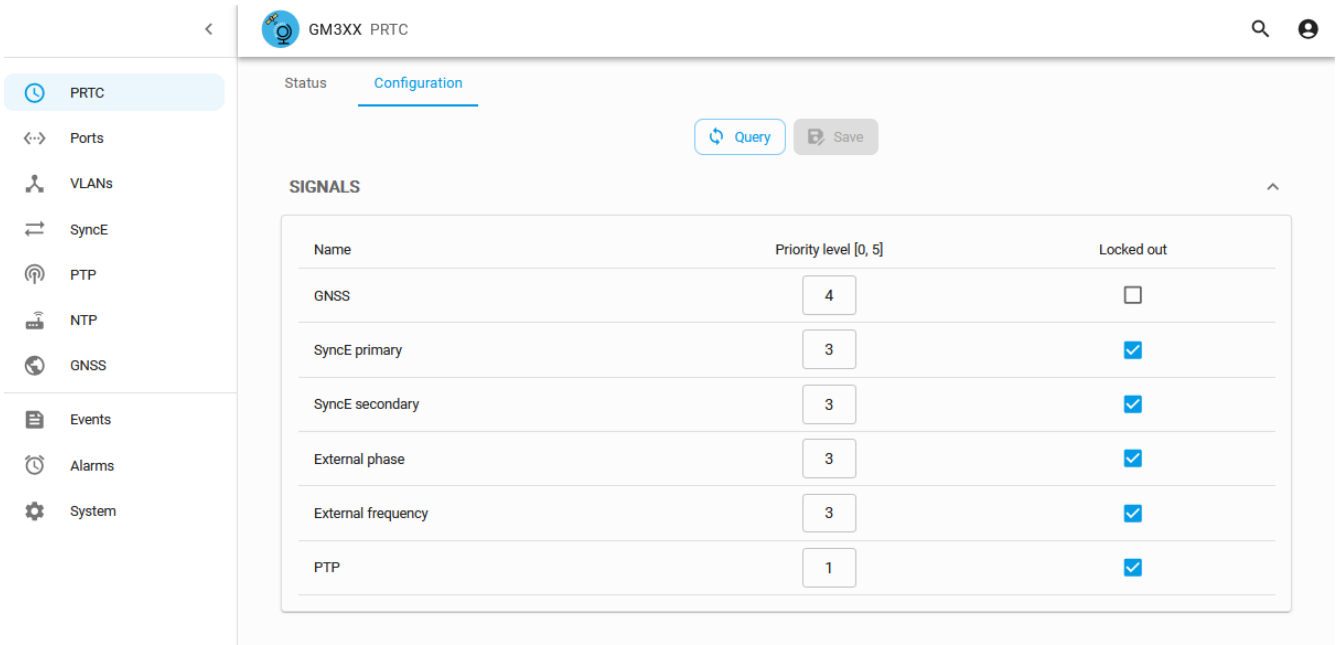
INPUT	Phase offset	Set a phase offset in nanoseconds for this input. It is assumed that this is a fairly accurate source so the offset range is limited.	[-1000, 1000] nS
	Phase quality level	This is needed because the external phase has no mechanism to derive this from the input itself.	Primary Reference Time Clock Enhanced Primary Reference Time Clock Primary Reference Source Stratum Unknown Stratum 2 Telecom Network Clock Stratum 3E Stratum 3 SMC Stratum 4 Provisioned Do Not Use for Sync Invalid Hardware failure All others
	Frequency	External input frequency	10Mhz

	Frequency quality level	Set the quality level for this input. This is needed because the external frequency has no mechanism to derive this from the input itself.	Primary Reference Time Clock Enhanced Primary Reference Time Clock Primary Reference Source Stratum Unknown Stratum 2 Telecom Network Clock Stratum 3E Stratum 3 SMC Stratum 4 Provisioned Do Not Use for Sync Invalid Hardware failure All others



OUTPUT	Pulse		Enable/Disable
	Pulse offset	Controlled pulse offset in nanoseconds. This setting only applies if one of the controlled outputs is selected.	[-500000000, 500000000] nS
	Pulse width	Control the pulse-width of the pulse, in nanoseconds	[1000, 100000] nS
	Pulse output select	The actual output provided	PPS PP2S External phase PTP

	Frequency		System PPS GNSS
			Enable/Disable
	Frequency output select	The actual output provided	Synthesized frequency External frequency Recovered clock (eth0/eth1)
	Synthesized frequency	Parameters for the frequency synthesizer output	10Mhz, 2048 kHz, 25 Mhz
	Time of Day		Enable/Disable
	Time of Day output select	The actual output provided	Time of Day System PPS



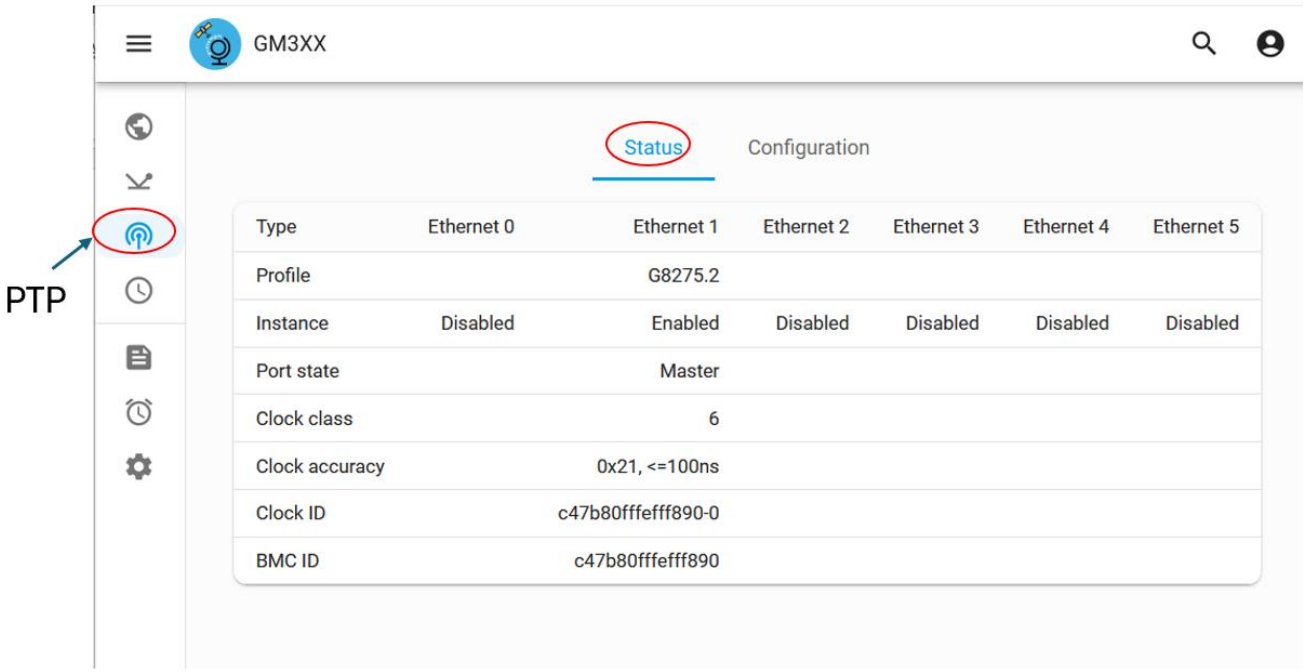
6.6 PTP

This menu allows the display of the current PTP interface status or the PTP configuration of the interface.

6.6.1 Status

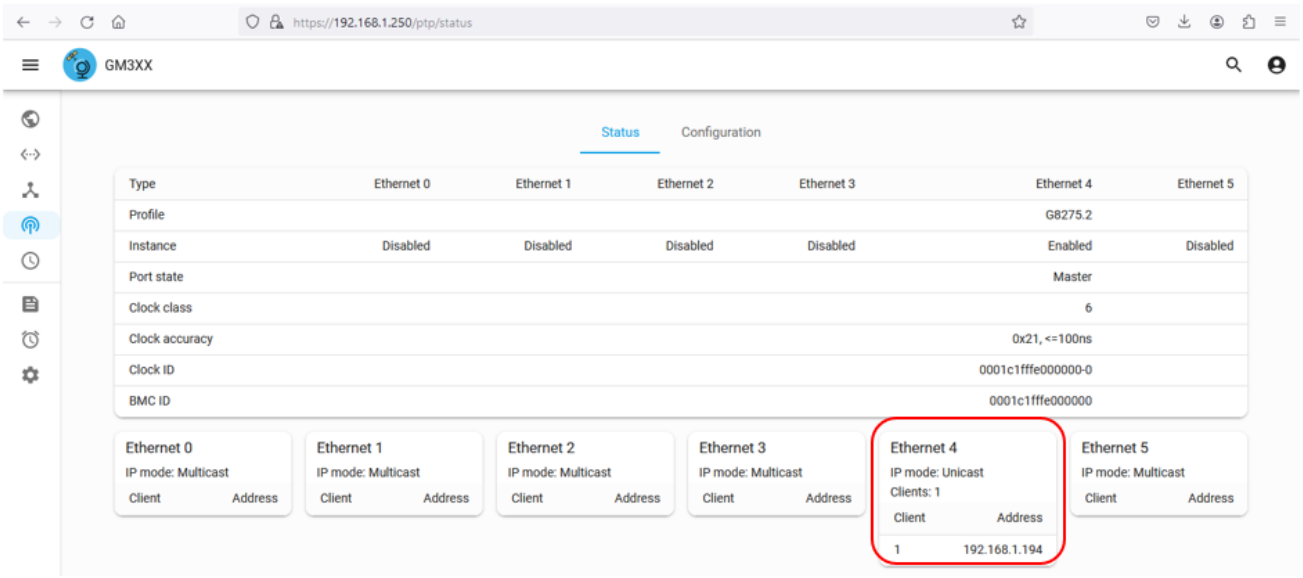
Select PTP on the left-hand menu then click on Status.

All ethernet interfaces are displayed. In this case, only one interface ethernet 1 is enabled.



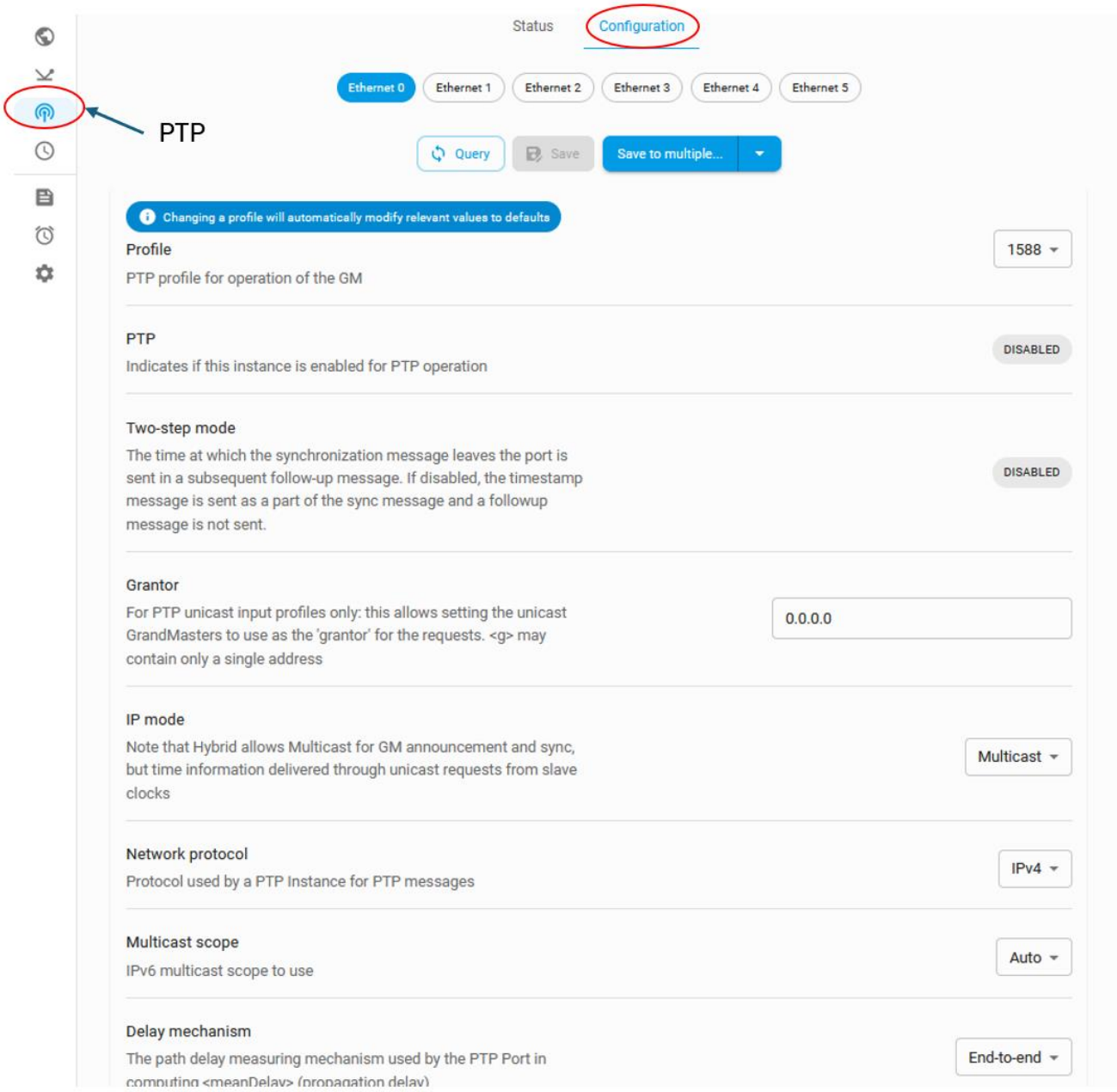
6.6.2 Client list

PTP clients that connect will be displayed on the status page. In this example, client 192.168.1.194 Is connected to Ethernet 4. Currently, only the unicast layer 3 client's IP address will be displayed.



6.6.3 Configuration

To access this page, select PTP Configuration

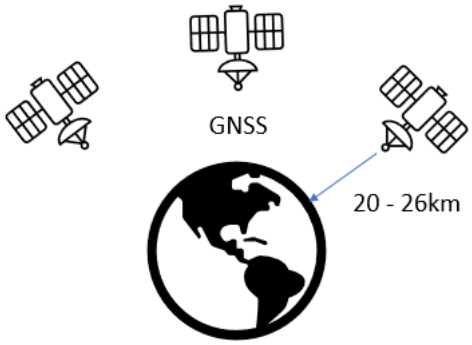


Ethernet Port:	Identifies the Ethernet port – Ethernet 0 - 5	
Query:	Get the current configuration for the selected Ethernet port	
Save:	Save the configuration	
Save to multiple:	Select	Ethernet 0 to Ethernet 5 to apply configuration
		Reset Profile defaults

PTP Profile:	1588, G8265-I, G8265-II, telecom, G8275.2, G8275.1, Power, SMPTE, Enterprise or 802.1AS.
IP Mode:	Multicast, Unicast, or Hybrid
Sync Mode:	1-step or 2-Step
Network Protocol:	Transport mechanism –IPv4, IPv6, or 802.3 (Ethernet).
Log announce Interval:	The mean time interval between successive announce messages
Delay Request Interval:	The mean time interval between delay requests
PDelay Request Interval:	The mean time interval between delay requests of peers.
Announce Receipt Timeout:	Mean timeout interval between successive announce messages.
Duration Field:	
Delay Mechanism:	E2E or P2P
Domain Number:	The PTP domain number
Grantor Address:	For PTP unicast input profiles only, IP address(es) of the unicast Grandmasters to use as the 'grantor' for the requests.
Local Priority 1:	Priority 1 value between 0 and 255
Priority 2:	Priority 2 value between 0 and 255.
Sync Interval:	The mean time interval between successive sync messages
Multicast TTL:	Set the multicast TTL value for the transmission (from 1 to 255)
Layer 2 Multicast MAC:	Multicast MAC address selection is either Routable (01-1B-19-0000-00) or Non-Routable(01-80-C2-00-00-0E).
DiffServ Code Point:	Diff-Serv Code Point (from -128 to 127)
Multicast Scope:	

6.7 GNSS

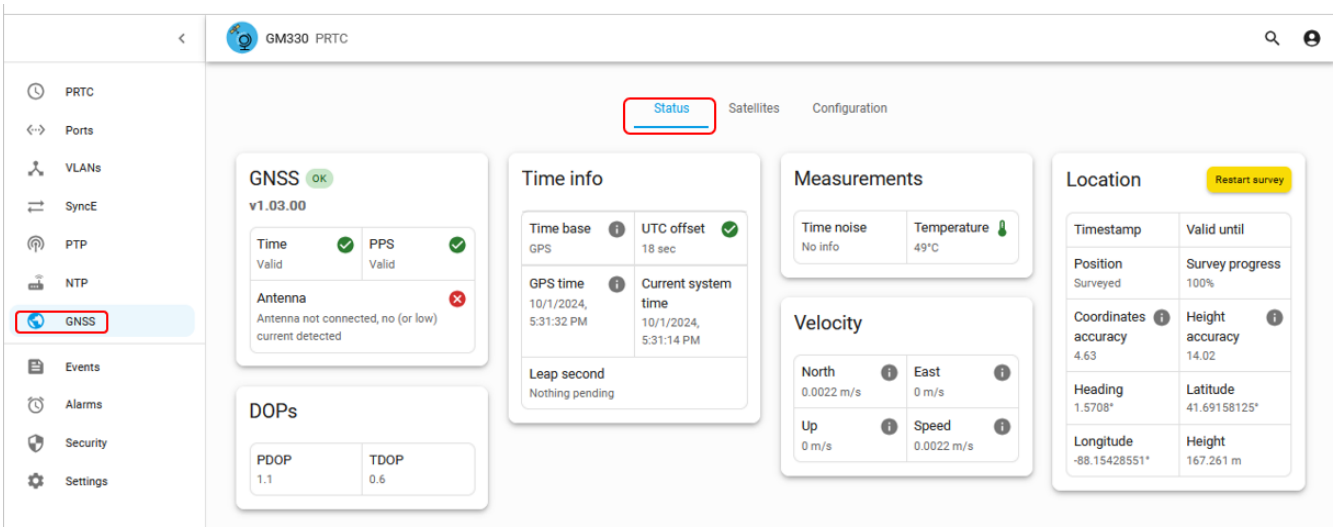
GNSS satellites are located 20-26km from the earth's surface. By the time the signals reach the surface, they are weak. The GNSS web page gives a list of visible satellites and if they are being tracked.



6.7.1 GNSS/Status

This page displays GNSS receiver status information.

To access this tab, select GNSS / Status.



GNSS Status:		OK, Fail, Disabled
	Time:	valid, invalid
	PPS:	valid, invalid

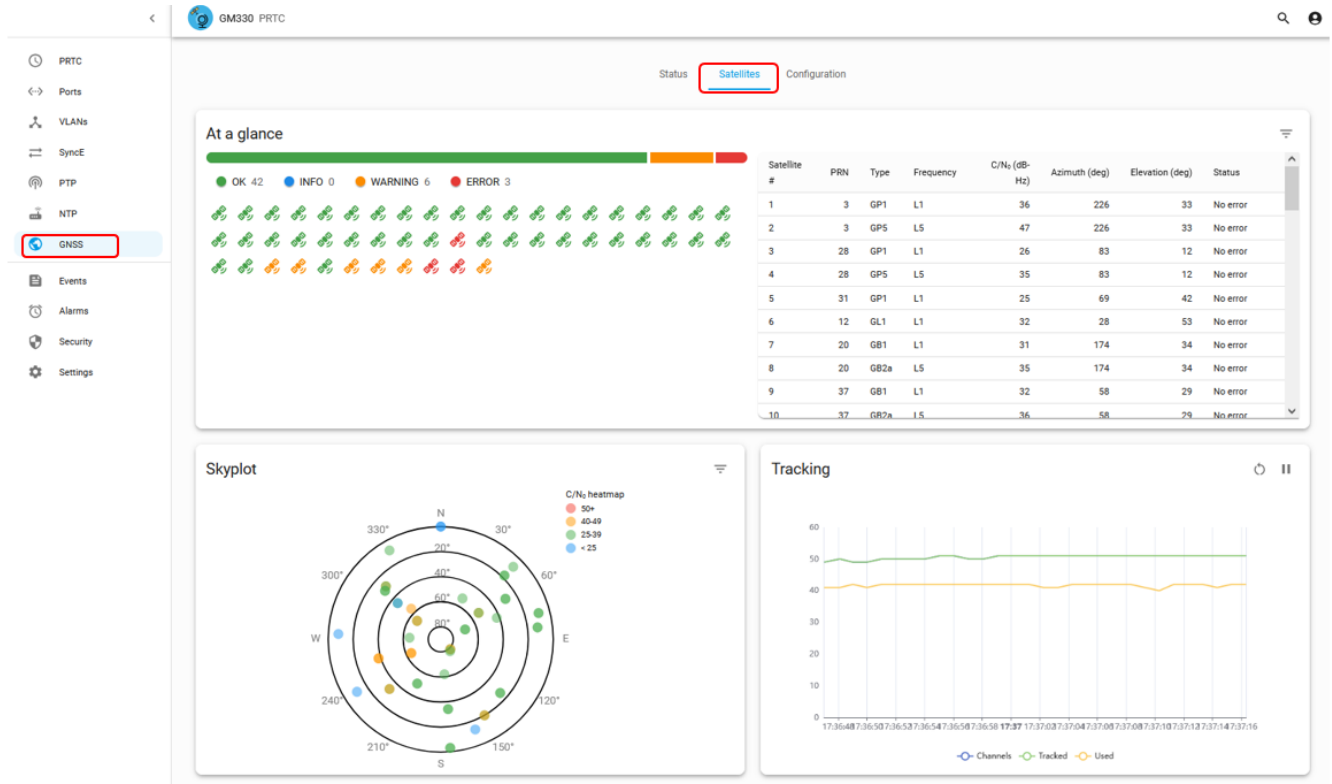
	Antenna:	shorted, not connected, fault, high current
Time info:		
	Time base:	UTC, UTC(Glonass), GPS, Glonass, BeiDou, NavIC
	UTC offset:	e.g.) 18 s
	GPS time	e.g.) 11/20/2023, 1:47:43 PM
	Current system time:	e.g.) 11/20/2023, 1:48:22PM
	Leap second:	Insertion, Deletion, nothing pending
Measurements Status:		
	Time noise:	No info, e.g.) 1970 ns
	Temperature:	e.g.) 10°C
Location:		
	Timestamp:	e.g.)11/20/2023, 1:52:30PM
	Valid until:	e.g.) 11/20/2023, 1:53:09PM
	Position:	Active, Surveyed
	Survey progress:	0-100%
	Coordinates accuracy:	e.g.) 128.78 Accuracy of Lat/Long Pair
	Height accuracy:	e.g.) 106.29 Accuracy of Height Value
	Heading:	e.g.) 192.073°
	Latitude:	e.g.) -78.776 °
	Longitude:	e.g.) 38.67 °
	Height:	e.g.) 1045 m
	Restart survey	Recalculate the Location
Velocity:		
	North:	e.g.) 188.15 m/s
	East:	e.g.) 199.5 m/s
	Up:	e.g.) 166.7 m/s
	Speed:	e.g.) 126.6 m/s
DOPs:		
	PDOP:	e.g.) 98.5
	TDOP:	e.g.) 70.2

Refresh Rate

The main page is refreshed at a rate of one second.

6.7.2 GNSS/ Satellites

To access this page, select GNSS then Satellites

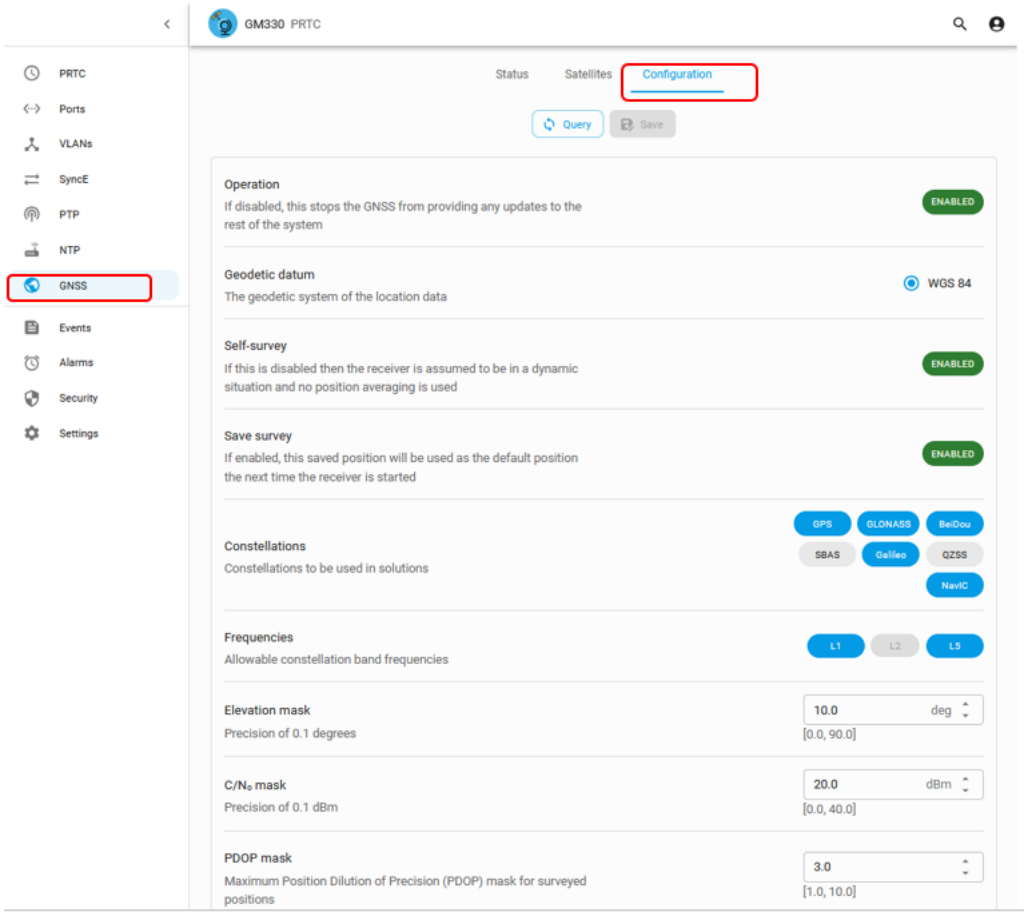


At a glance		Color-coded for OK, INFO, WARNING, ERROR
	Satellite	Satellite number
	PRN	Pseudo-random noise code that identifies the satellite
	Type	GPS, GLONASS, BeiDou, Galileo, NAVIC, QZSS, SBAS
	Frequency	L1, L2, L5
	SNR (dBm)	Signal to Noise Ratio (Signal Strength)
	Azimuth (deg)	What direction to face North 0 °, East 90°, South 180°, West 270°
	Elevation (deg)	How high up in the sky
	Status	No Error, No Measurement, No Ephemeris, No time, Bit sync, Low elevation, Low C/No, Not Usable, Rate Reject

Skyplot	Satellites that are in view of the antenna
	Color-coded based on the Signal Strength (C/No) and the Azimuth in degrees
Tracking	Satellites that the receiver is getting a signal from
	Color-coded for the number of Channels, Tracked, Used

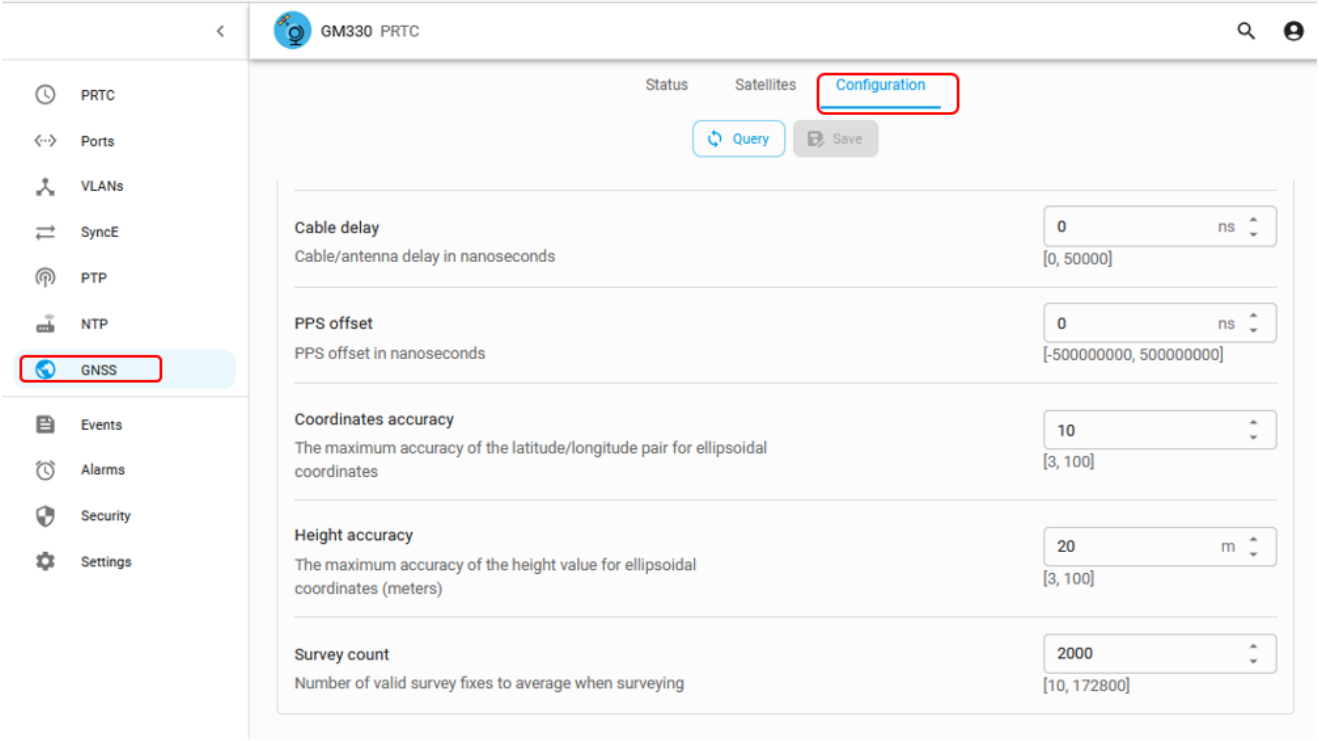
6.7.3 GNSS Configuration

To access this page, select GNSS / Configuration. Two important parameters that you need to pay attention to are the Elevation and the C/No Masks. A 10° Elevation mask will remove any weak satellites that are close to the horizon. A C/No mask of 20 dbm will eliminate any satellites with a lower value from the timing calculation.



Operation:	Enabled, Disabled
Geodetic datum:	WGS 84
Self-survey:	Enabled, Disabled, NOT CONFIGURED
Save survey:	Enabled, Disabled, NOT CONFIGURED
Frequencies:	L1, L2, L5
Constellations:	GPS, GLONASS, BeiDou, SBAS, Galileo, NavIC
Elevation mask:	0° to 90 °
C/No mask:	0.0 dBm to 40.0 dBm

PDOP Mask:	1.0 to 10.0



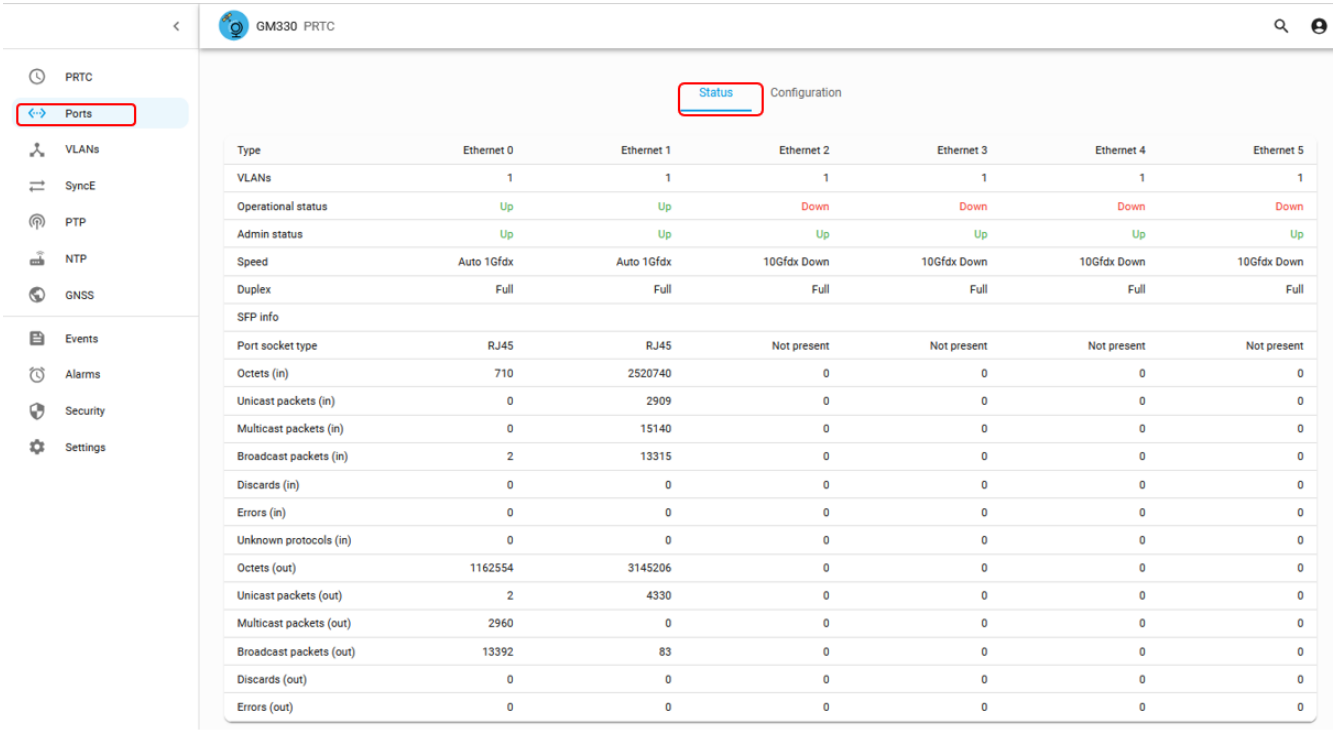
Cable Delay:	0 ns to 50K ns
PPS offset:	-500 ns to 500M ns
Coordinates accuracy:	3.0 to 100
Survey count:	10 to 172800
Height accuracy:	3.0 m to 100 m

6.8 Ports

6.8.1 Status and Statistics Ethernet Ports (0 to 5)

To access this page, select Network/ Status

If debugging an issue, view the Discards (in/out) and Errors (in/out) statistics to help narrow down the issue. If you see an increase in the error count, this could be an indication of a bad ethernet cable.



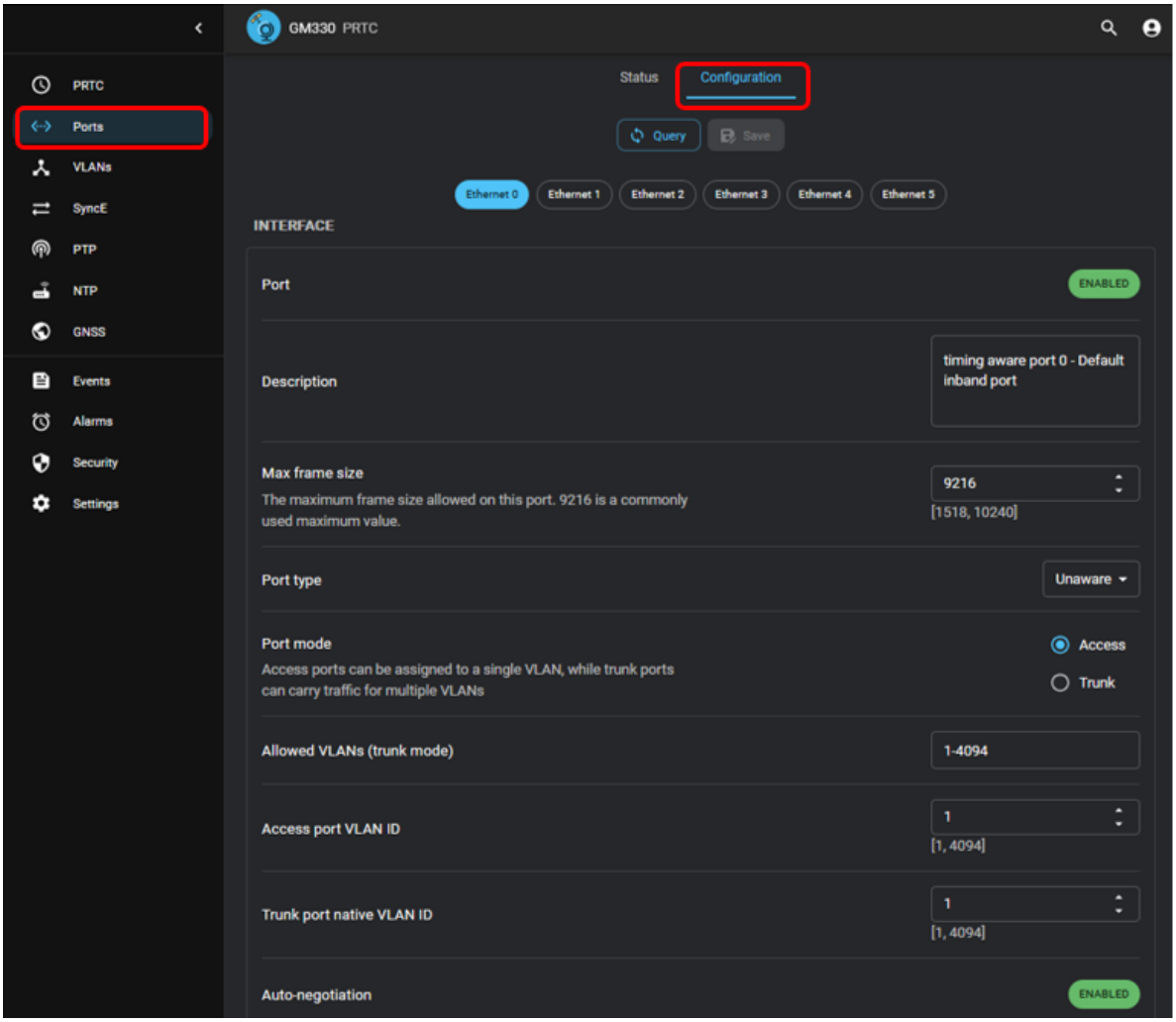
Type	Ethernet 0	Ethernet 1	Ethernet 2	Ethernet 3	Ethernet 4	Ethernet 5
VLANs	1	1	1	1	1	1
Operational status	Up	Up	Down	Down	Down	Down
Admin status	Up	Up	Up	Up	Up	Up
Speed	Auto 1Gfdx	Auto 1Gfdx	10Gfdx Down	10Gfdx Down	10Gfdx Down	10Gfdx Down
Duplex	Full	Full	Full	Full	Full	Full
SFP info						
Port socket type	RJ45	RJ45	Not present	Not present	Not present	Not present
Octets (in)	710	2520740	0	0	0	0
Unicast packets (in)	0	2909	0	0	0	0
Multicast packets (in)	0	15140	0	0	0	0
Broadcast packets (in)	2	13315	0	0	0	0
Discards (in)	0	0	0	0	0	0
Errors (in)	0	0	0	0	0	0
Unknown protocols (in)	0	0	0	0	0	0
Octets (out)	1162554	3145206	0	0	0	0
Unicast packets (out)	2	4330	0	0	0	0
Multicast packets (out)	2960	0	0	0	0	0
Broadcast packets (out)	13392	83	0	0	0	0
Discards (out)	0	0	0	0	0	0
Errors (out)	0	0	0	0	0	0

Ethernet Port:	Identifies the Ethernet port – Ethernet 0 to 5	
Query:	Get the current configuration for the selected Ethernet port	
Save:	Save the configuration	
Save to multiple:	Select	Ethernet 0 to Ethernet 5 to apply configuration
		Reset Profile defaults
Operational Status:	Up, Down, Testing, Unknown, Dormant, Not Present, Lower Layer down	
Admin Status:	Up, Down, Testing	
Auto-negotiation	In Progress, Complete, Failed, Unknown, No negotiation	
Speed:	0 bps, 100 Mbps, 1G bps, 10G bps, 100 Gbps	
Physical address	e.g.) 00:1a:2b:3c:4d:5e	
IPV4 mode	Static, DHCP,	
Ipv4 address	e.g.) 192.168.1.10	
IPv4 Gateway:	e.g.) 192.168.1.1	

IPv4 prefix length:	0 to 32
IPv6 Mode:	Static, Link-local, SLACC, DHCPv6
IPv6 Address:	Fe6c::
IPv6 gateway:	::
IPv6 prefix length:	0 to 128
Discontinuity:	Date and Time e.g.) 11/2/2023, 2:34:46 PM
Octets(in)	8-bit Quantity, Bytes
Unicast packets (in)	Point to Point Packets
Multicast packets (in)	Point to multi Point Packets
Broadcast packets (in)	Point to all Points Packets
Discards (in)	Bytes Dropped because of Congestion
Errors (in)	Bytes Indicating errors in the Interface Hardware
Unknown protocols (in)	Not TCP or UDP
Octets (out)	8-bit Quantity, Bytes
Unicast packets (out)	Point to Point Packets
Multicast packets (out)	Point to multi Point Packets
Broadcast packets (out)	Point to all Points Packets
Discards (out)	Bytes Dropped because of Congestion
Errors (out)	Bytes Indicating errors in the Interface Hardware

6.8.2 Configuration

To access this page, select Ports / Configuration

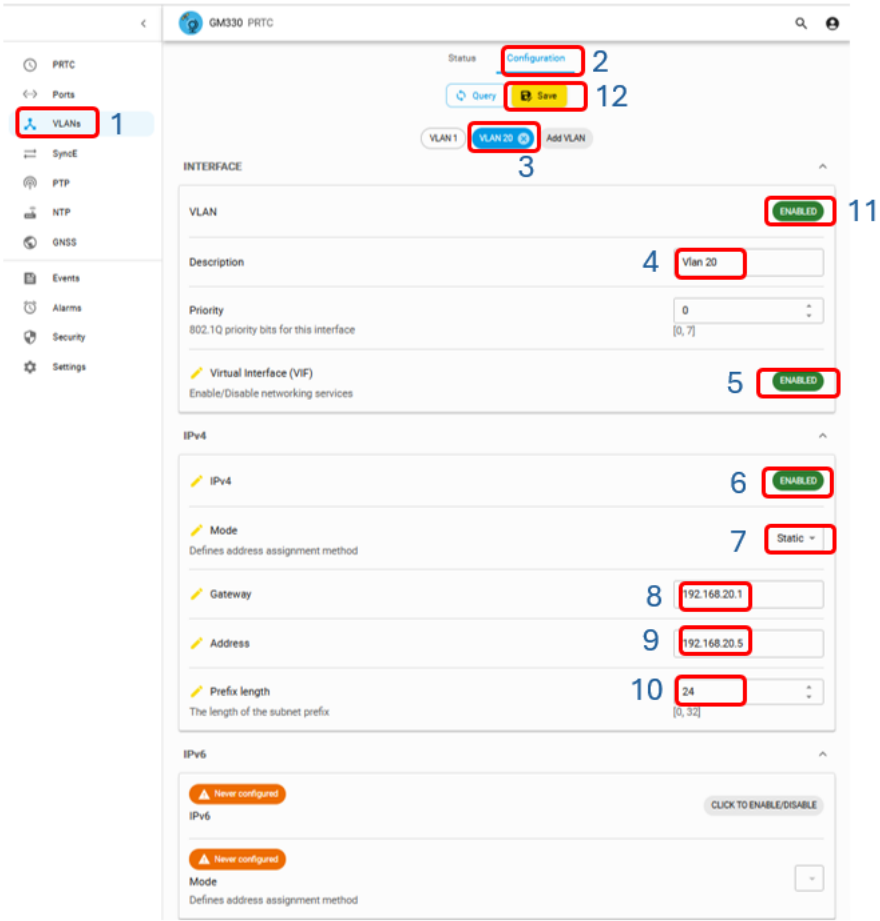


Ethernet Port:	Identifies the Ethernet port – Ethernet 0 to 5
Query:	Get the current configuration for the selected Ethernet port
Save:	Save the configuration
Interface:	Enabled, Disabled, Not Configured
Max Frame Size:	The maximum frame size allowed on this port. 9216 is a commonly used maximum value.
Port Type:	Unaware, C-Vlan, S-VLAN, S-Custom-VLAN
Port Mode	Access (one VLAN), Trunk (Multiple VLANS)
Allowed VANS (Trunk Mode)	1-4094

Access port VLAN ID	[1.4096] “choose only one”
Trunk port native VLAN ID	[1,4094]
Auto-negotiation:	NOT Configured, enabled, disabled

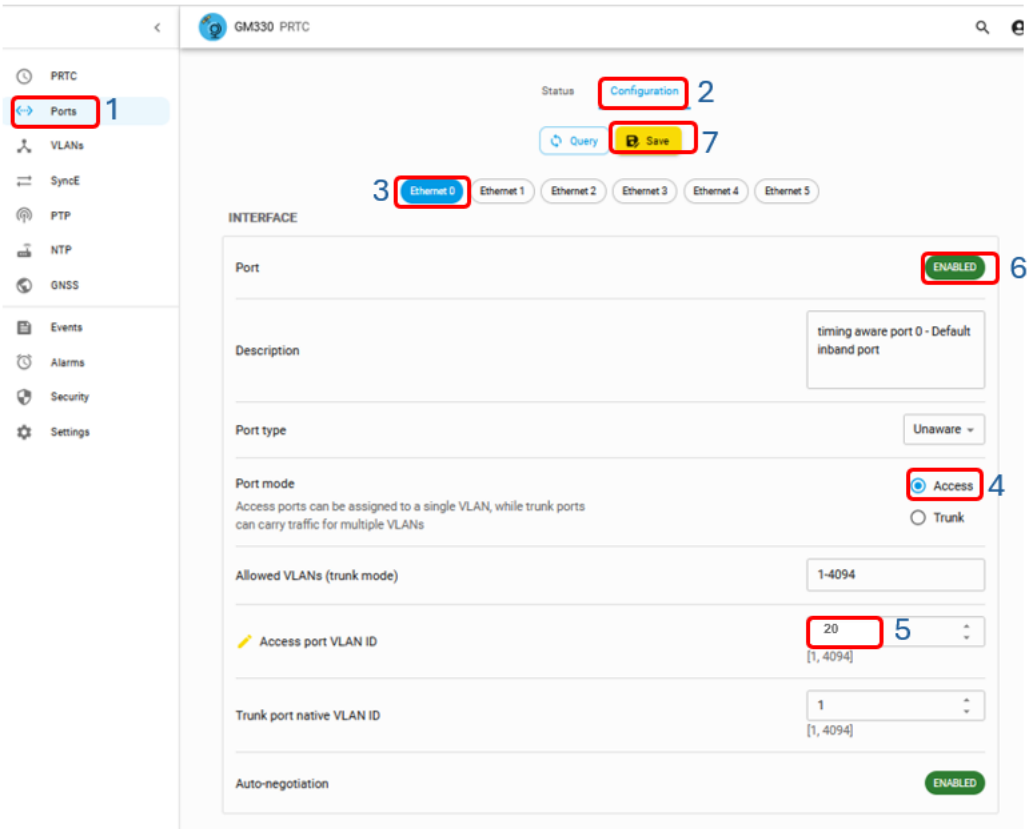
6.8.4 Adding Vlan 20, VIF20 with Static IP and assigning Vlan 20 to Ethernet 0

Adding Vlan 20, VIF20 with Static IPVLAN



1	Select “Vlans” on left
2	Select “Configuration”
3	Add vlan 20
4	Name it Vlan 20
5	Enable “VIF”
6	Enable “IPv4”
7	Select “Static”
8	Enter Gateway IP address
9	Enter IP address
10	Enter subnet mask /24 = 255.255.255.0
11	Enable the Vlan
12	Click on “Save”

Assigning vlan 20 to Ethernet 0

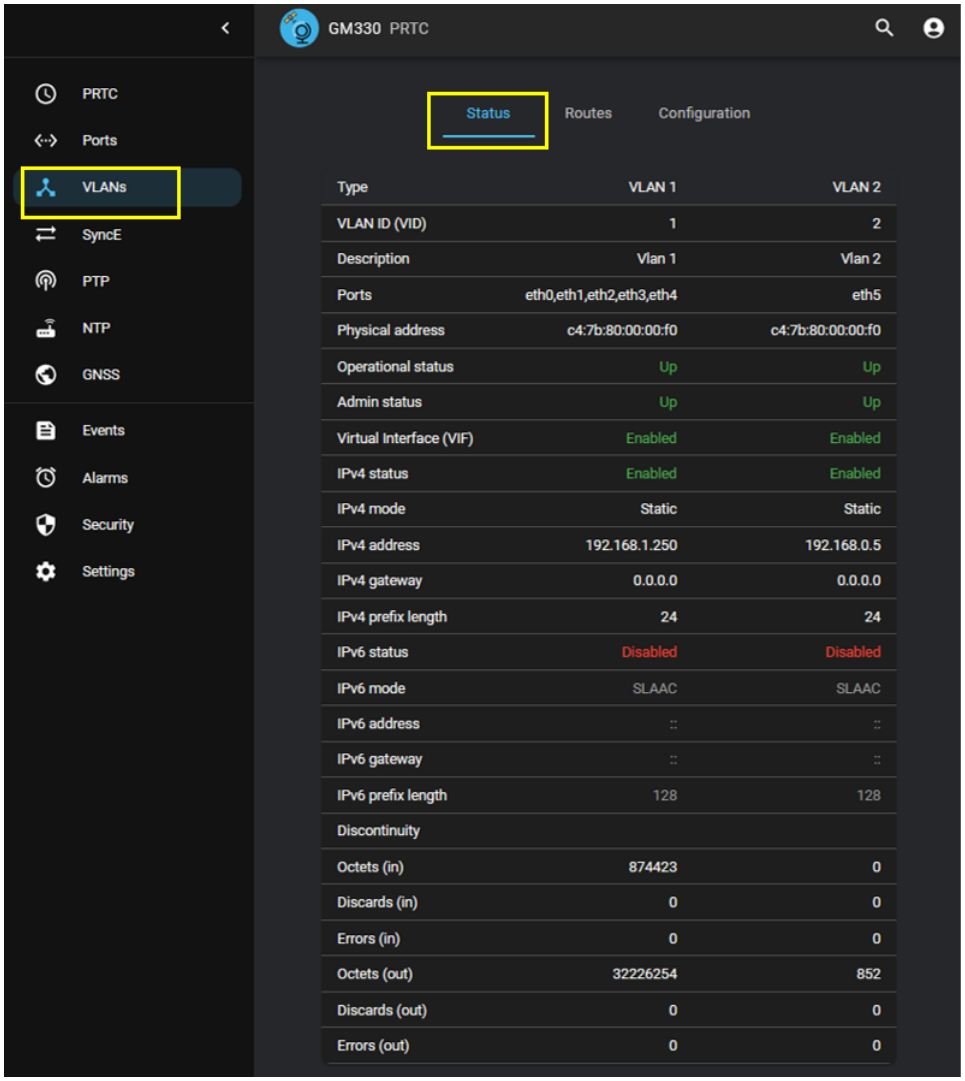


1	Select Ports Icon
2	Click on “Configuration”
3	Select “Ethernet 0”
4	Select “Access”
5	Type in “20” for the Vlan
6	Enable “Interface”
7	Click “Save”

6.9 VLANs

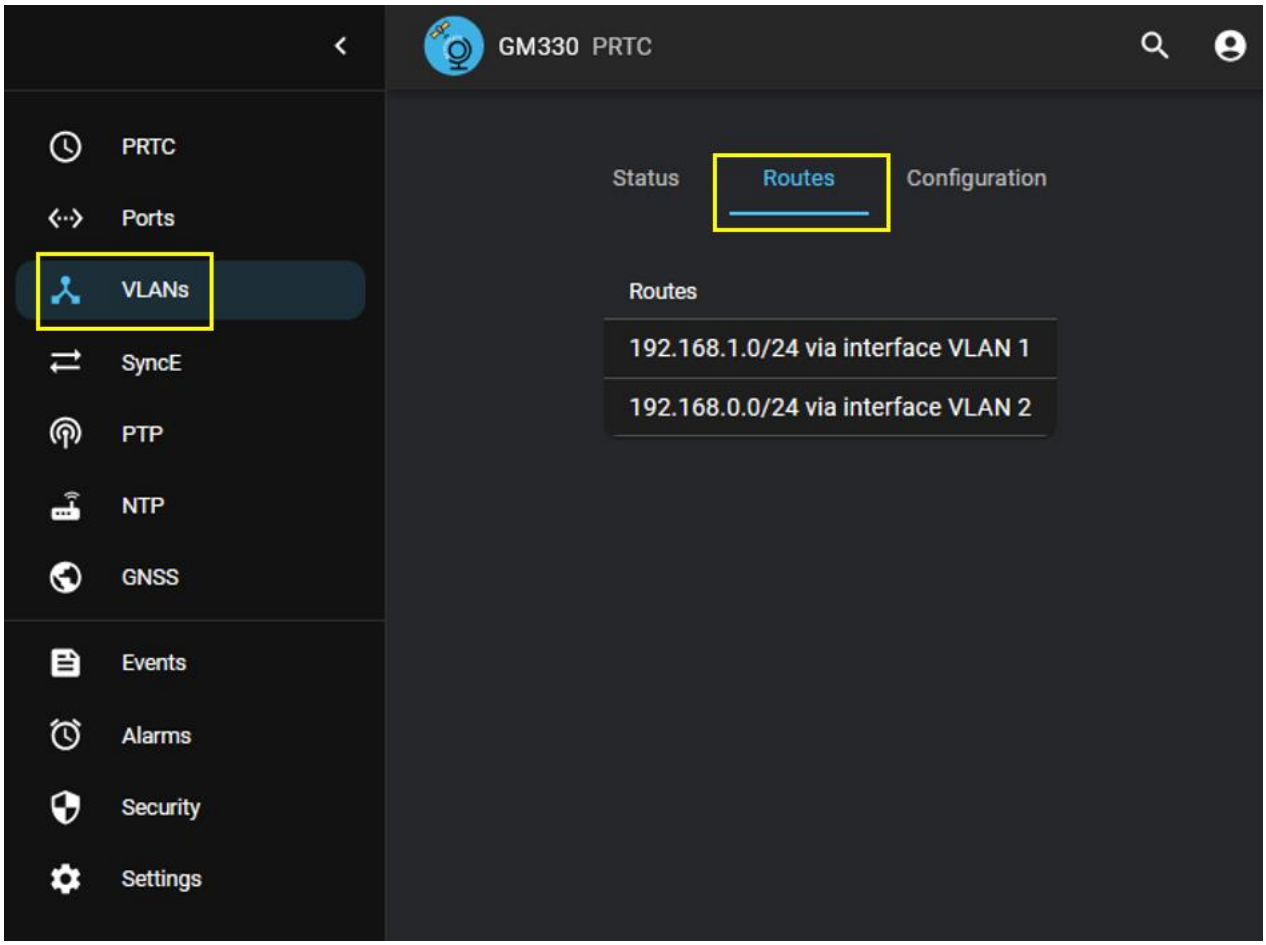
To assign multiple Vlans to an interface, the port mode needs to be configured as “Trunk”.

6.9.1 Status



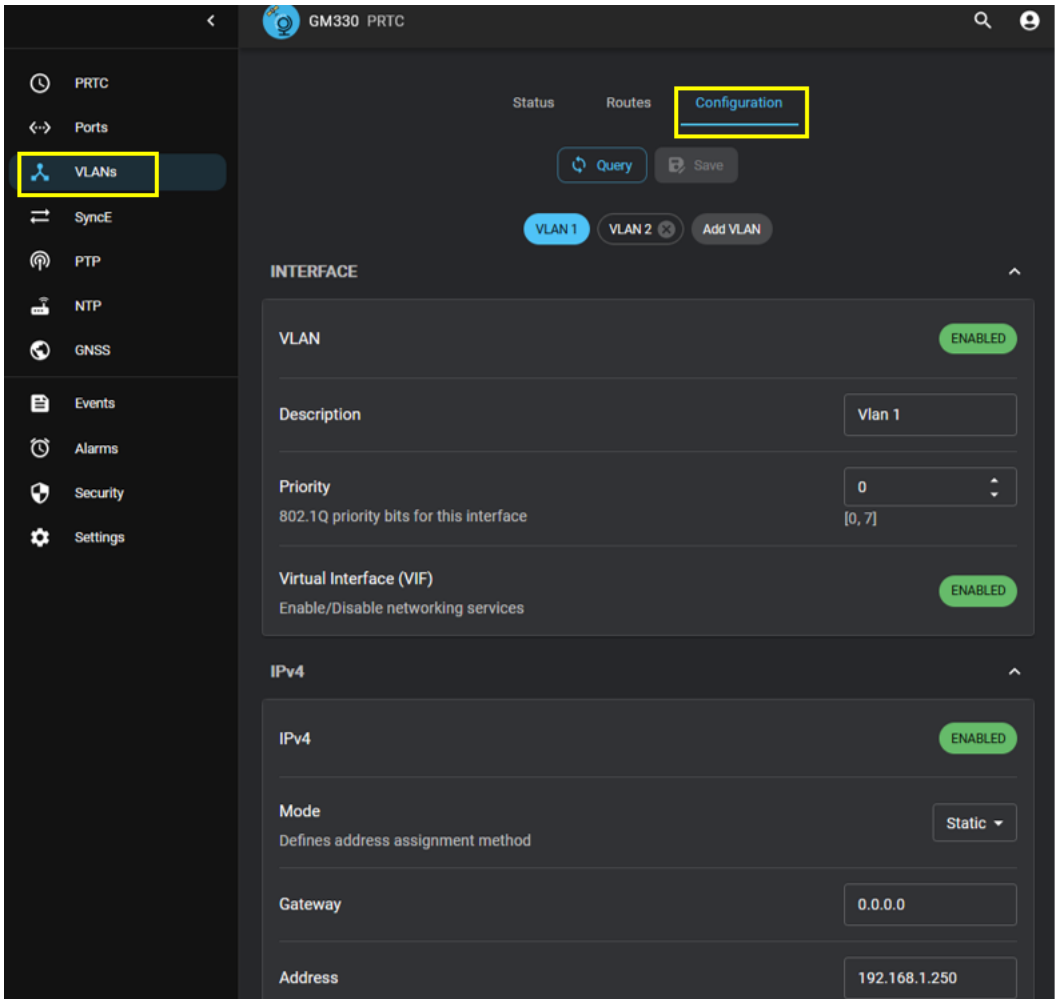
6.9.2 Routes

This page summarizes the configured IP subnets and associated VLANs.

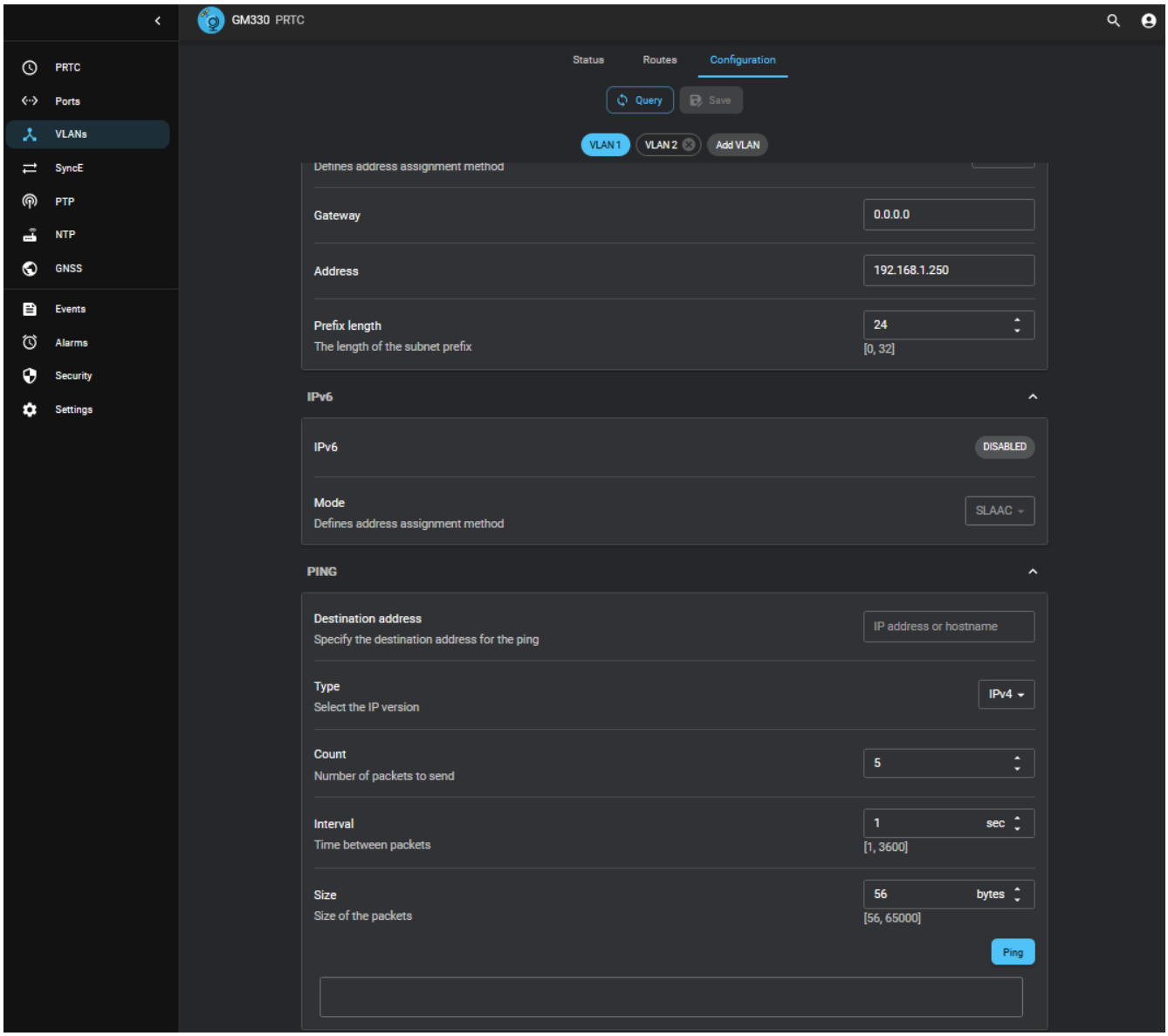


6.9.3 Configuration

To access this page, select Network / IPV4. If you configured the port for DHCP and you have completed the testing and provisioning, it is a good practice to set a static IP. When the DHCP server gives out an IP address, there is usually a lease time associated with the IP address.



Interface	Vlan ID	Vlan Tag Number
	Vlan	Enabled/Disabled
	Description	Name the vlan
	Priority	COS (Class of Service) [0,7]
	VIF	Enable/Disable Virtual Interface (VIF)
	Add Vlan	Add, Delete a Vlan
	Query	Get current Vlans
	Save	Save current Configuration



Vlan Tag:	Identifies the Vlan
Query:	Get the current configuration for the selected Ethernet port
Save:	Save the configuration
IPV4:	Enable/Disable
Mode:	Static, DHCP
Gateway:	IP Address of the Router/Gateway
Address:	IP Address Associated with the IPv4 address
Prefix Length:	[0,32] ie mask value /24 = 255.255.255.0
IPv6	Enabled, Disabled
IPv6 Mode:	DHCPv6, Static, SLAAC or Link-Local

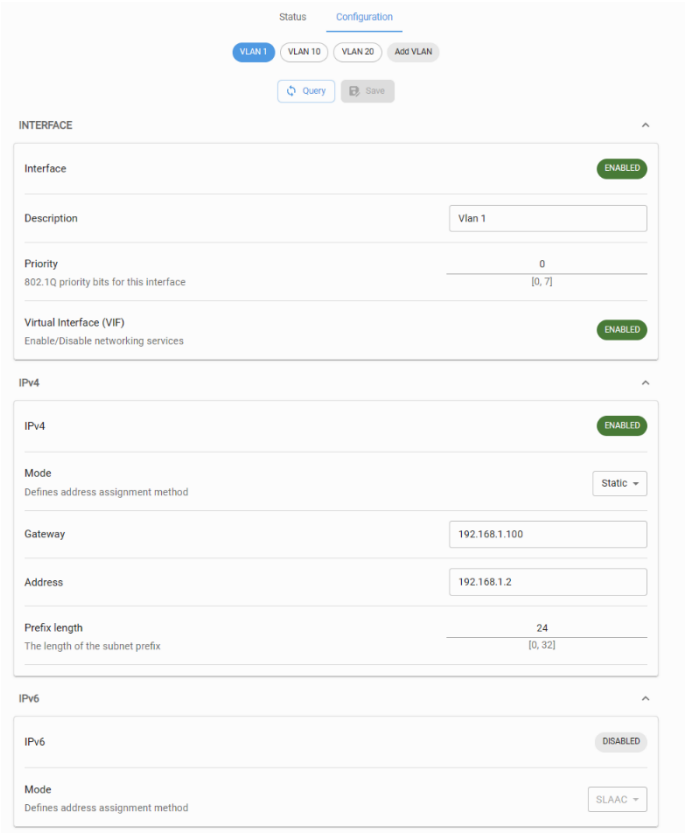
PING	Ping an IP address

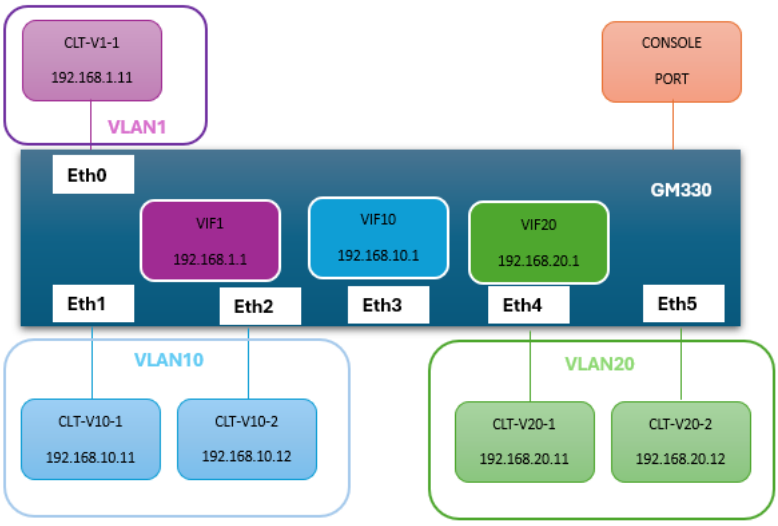
6.10 Configuring L2 Integrated Switch

The new configuration model is to create a Vlan with a VIF(Static or DHCP) and assign the vlan to the port. Assigning an IP address to a port is not supported.

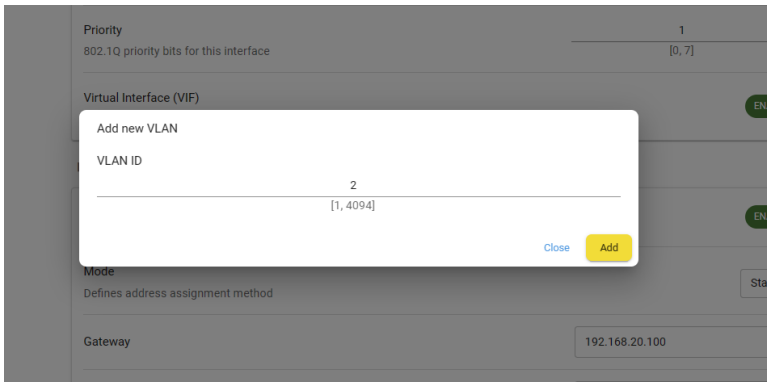
Example:

Configure VLAN 1 Virtual interface

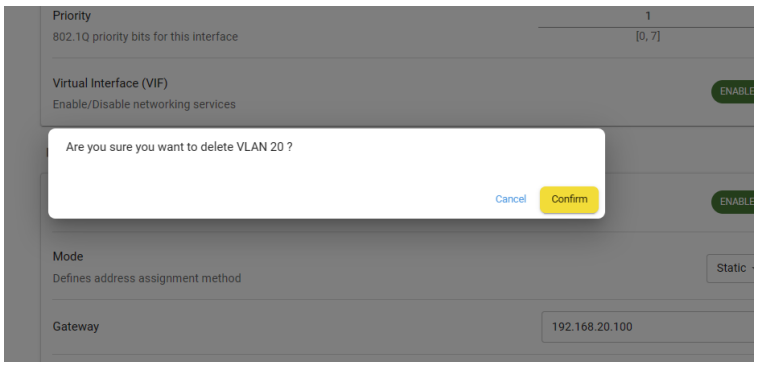




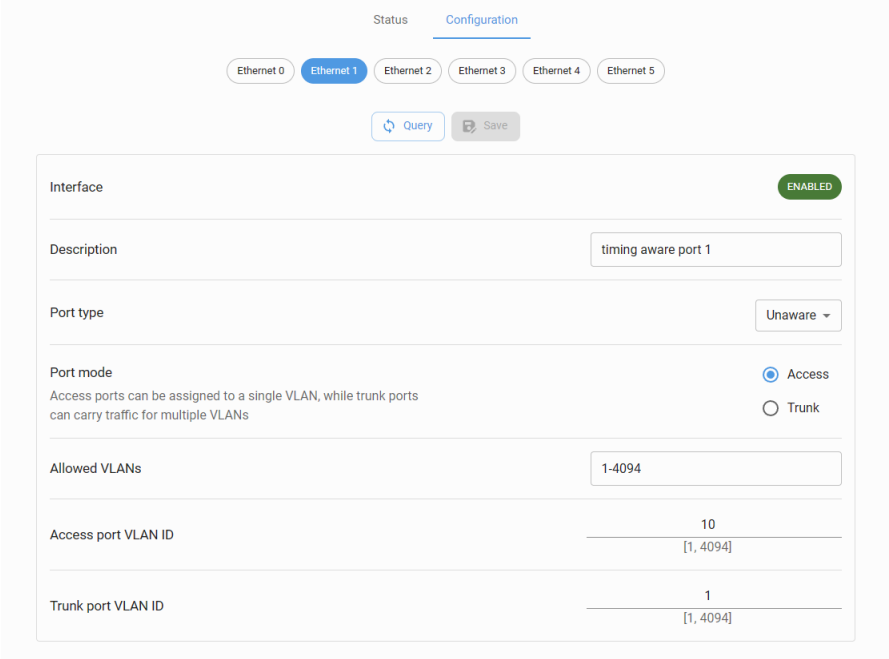
Use the “Add VLAN button to add VLANs 10, 20

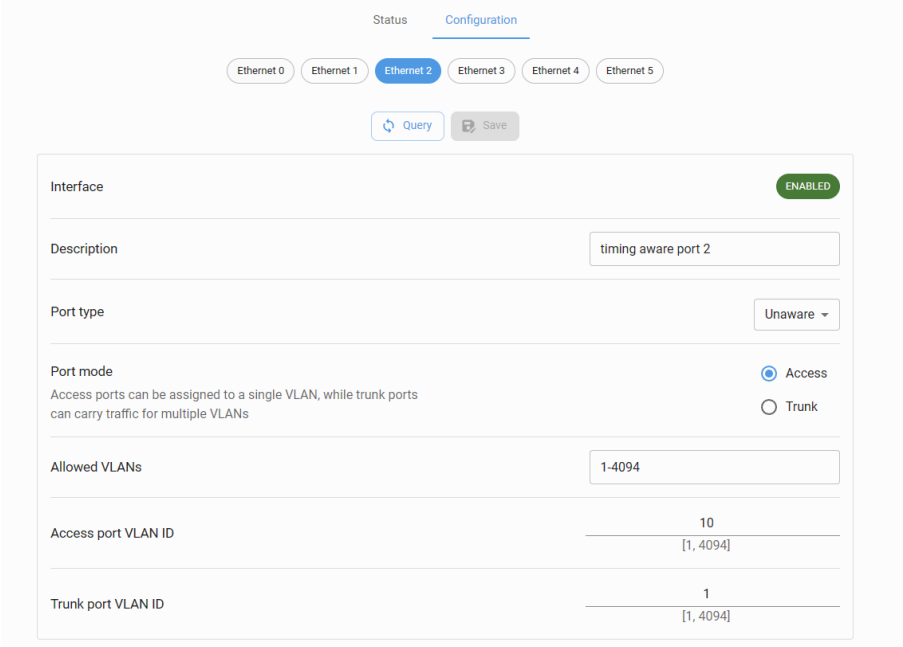


Delete a VLAN (if you made a mistake)

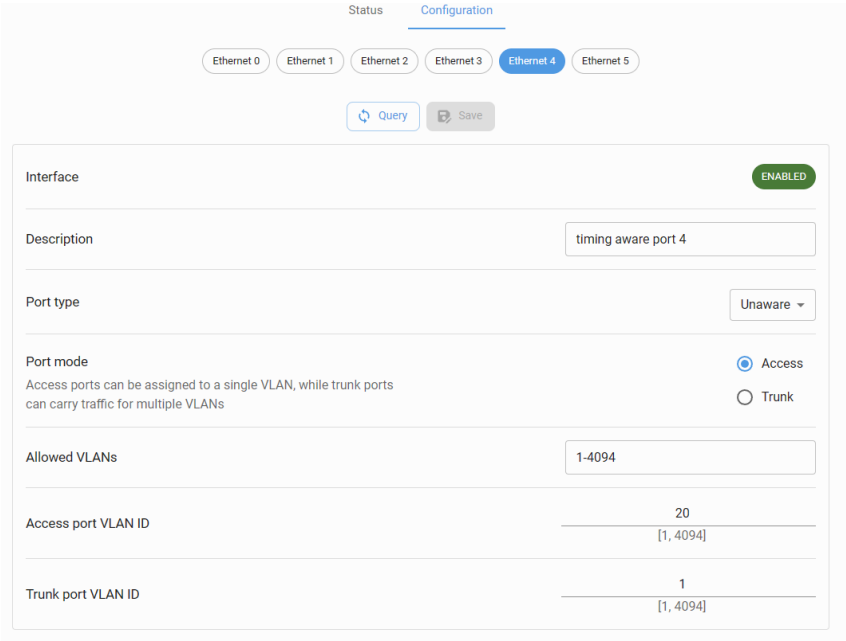


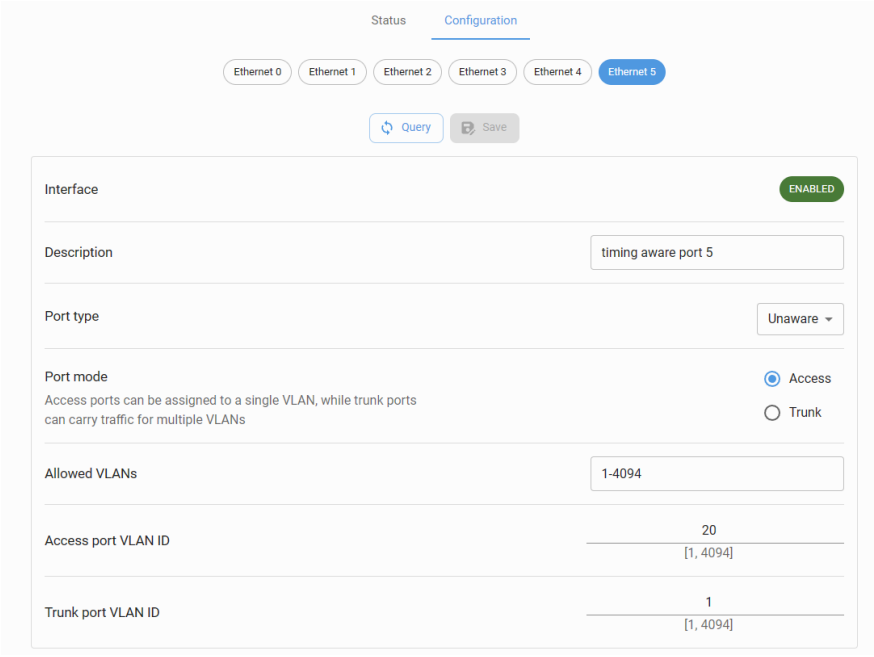
Configure eth1, eth2 for VLAN 10





Configure eth4,eth5 for VLAN20

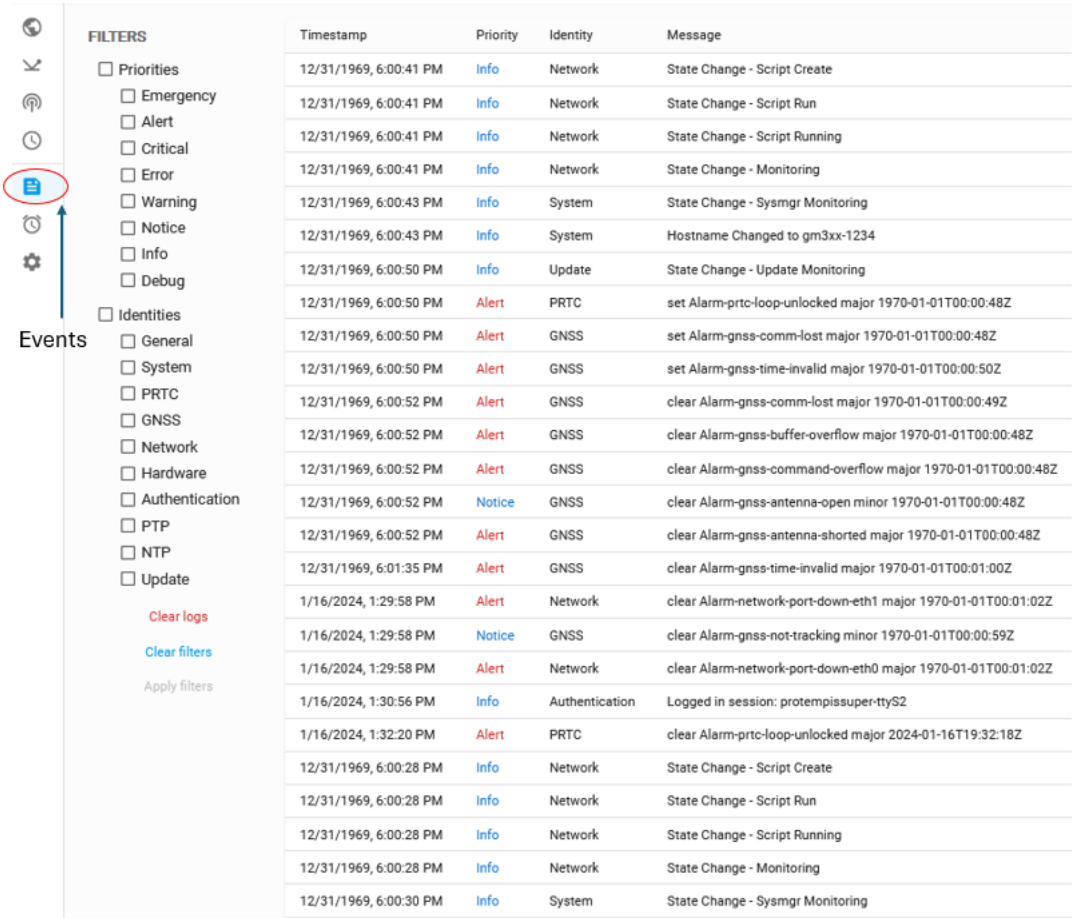




6.11 Events

To access the Events page, select Events

Filters	Display Events of Interest
Clear logs	Erase all Captured Events
Clear Filters	Remove previous Filters
Apply Filters	Click to apply selected event filters



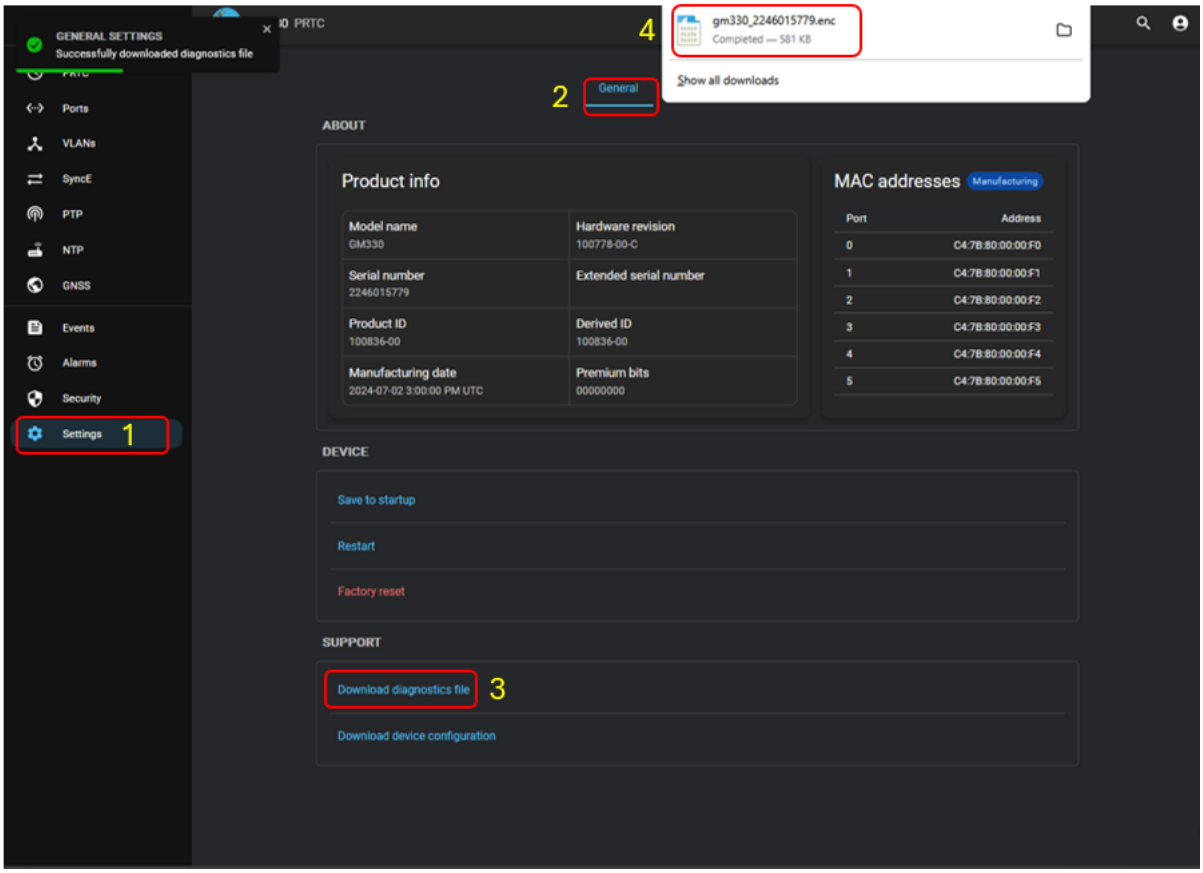
6.11.1 Filter Events

If you would like to focus on certain events, you need to choose at least one of the priorities and one of the identities and apply the filter.

For the example below: Priorities -Alerts and Identities – GNSS where chosen click on “Apply filter”

6.12 Support Diagnostic File

If you run into an issue and you want Protempis Support to look into your issue Create and Download the Diagnostic file. Send the *.enc file to support@protempis.com.

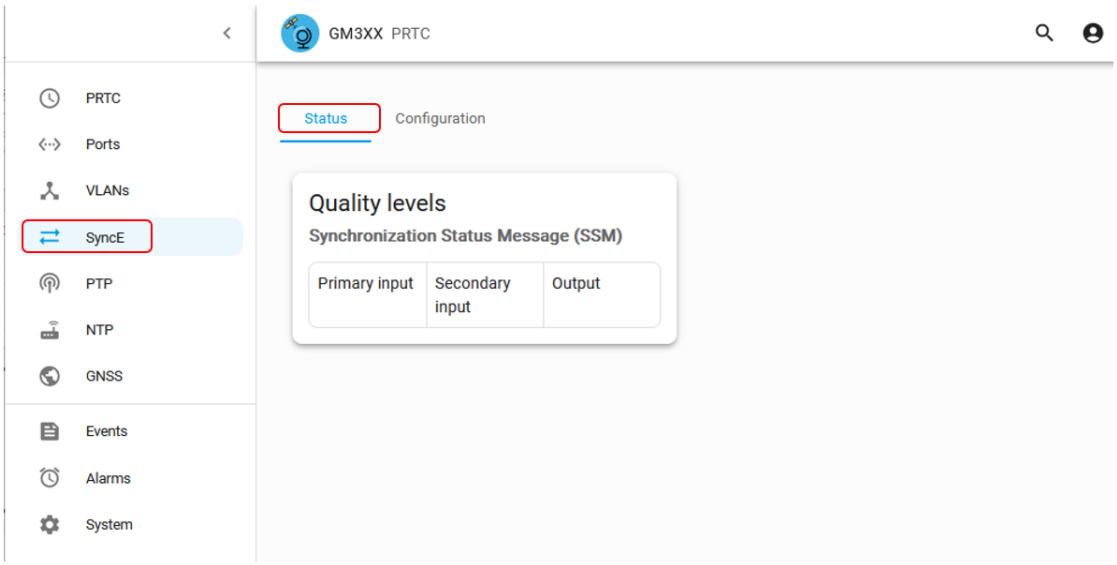


1	Click on “Settings”
2	Click on “General”
3	Click on “Download diagnostic file”
4	Name of the file that was downloaded

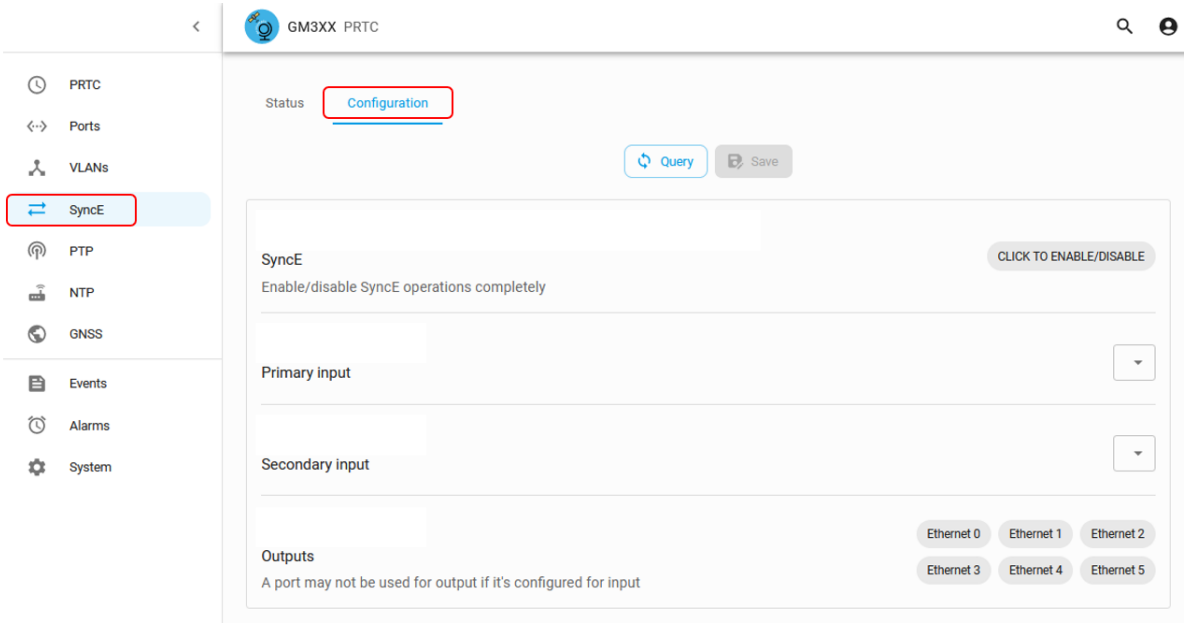
6.13 SyncE

The Synchronous Ethernet (SyncE) signal is transmitted over the Ethernet physical layer.
This signal allows devices that support SyncE to be able to synchronize to a common frequency reference.

Select “SyncE” then click on the “Status” Tab



Select “SyncE” then click on the “Configuration” Tab



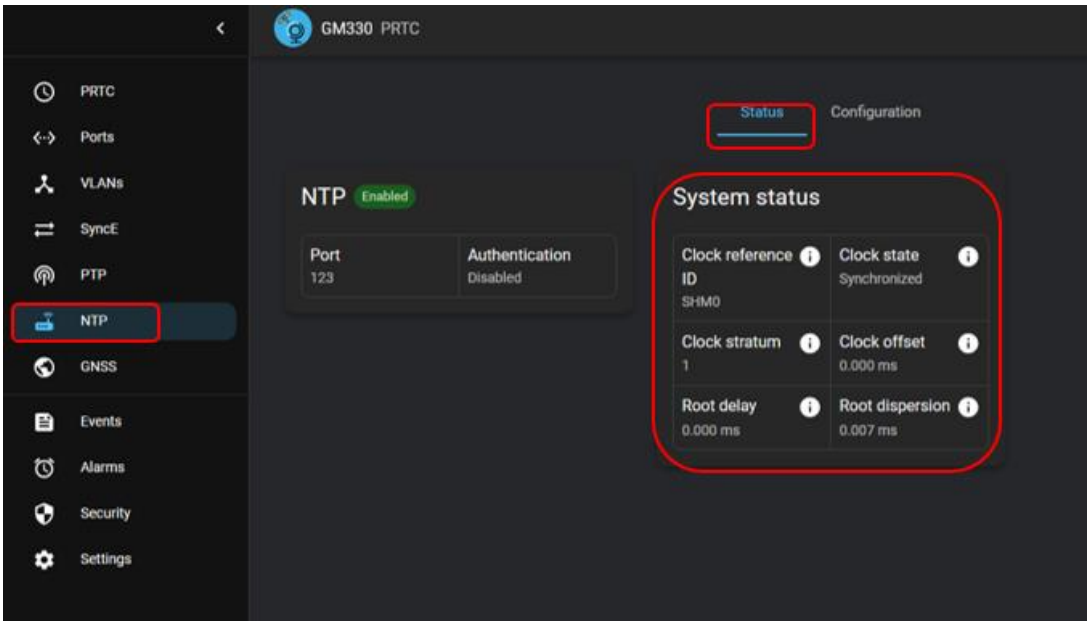
SyncE	Enable/Disable Note: When Synce is enabled on a port, the network connection will be briefly interrupted.
Primary input	Choose a SyncE input port (Ethernet 0 to Ethernet 5)
Secondary input	Choose a SyncE Secondary (backup) port (Ethernet 0 to Ethernet 5)
Outputs	Choose Ethernet ports that will output a SyncE signal. More than one can be selected but, they need to be configured as an output

6.14 NTP

The NTP server allows network devices usually servers to synchronize to a clock source.
The Server can be enabled/disabled and has a client-server relationship with the client

6.14.1 Status

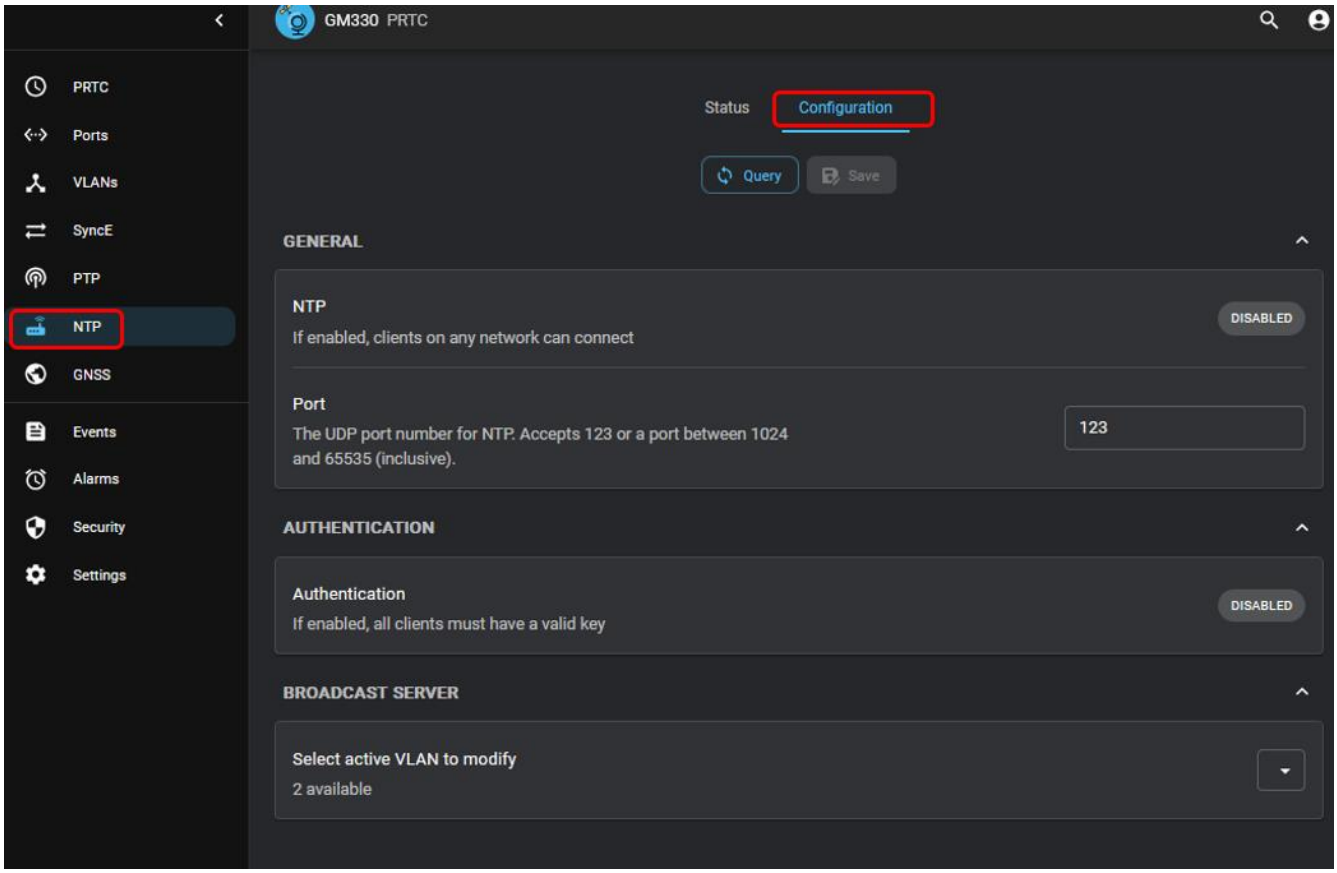
Select the “NTP” icon on the left side and then select the “Status” Tab



NTP	Enable/Disabled	
	Port	UDP Port used for Communication
	Authentication	Enabled / Disabled
System Status		
	Clock reference ID	A code identifying the particular server or reference clock. The interpretation depends upon the stratum
	Clock State	**Synchronized** - The local clock has been synchronized with an NTP server or the reference clock **Unsynchronized** - The local clock has not been synchronized with any NTP server
	Clock Staratum	The level of each server in the hierarchy is defined by a stratum. Primary servers are assigned with stratum one; secondary servers at each lower level are assigned with one stratum greater than the preceding level.
	Clock Offset	The signed time offset to the current selected reference time source. The negative value indicates that the local clock is behind the current selected reference time source.
	Root delay	Total delay along the path to the root clock (mS)
	Root dispersion	The dispersion to the local clock and the root clock (mS)

6.14.2 Configuration

Select the “NTP” icon on the left side and then select the “Configuration” Tab

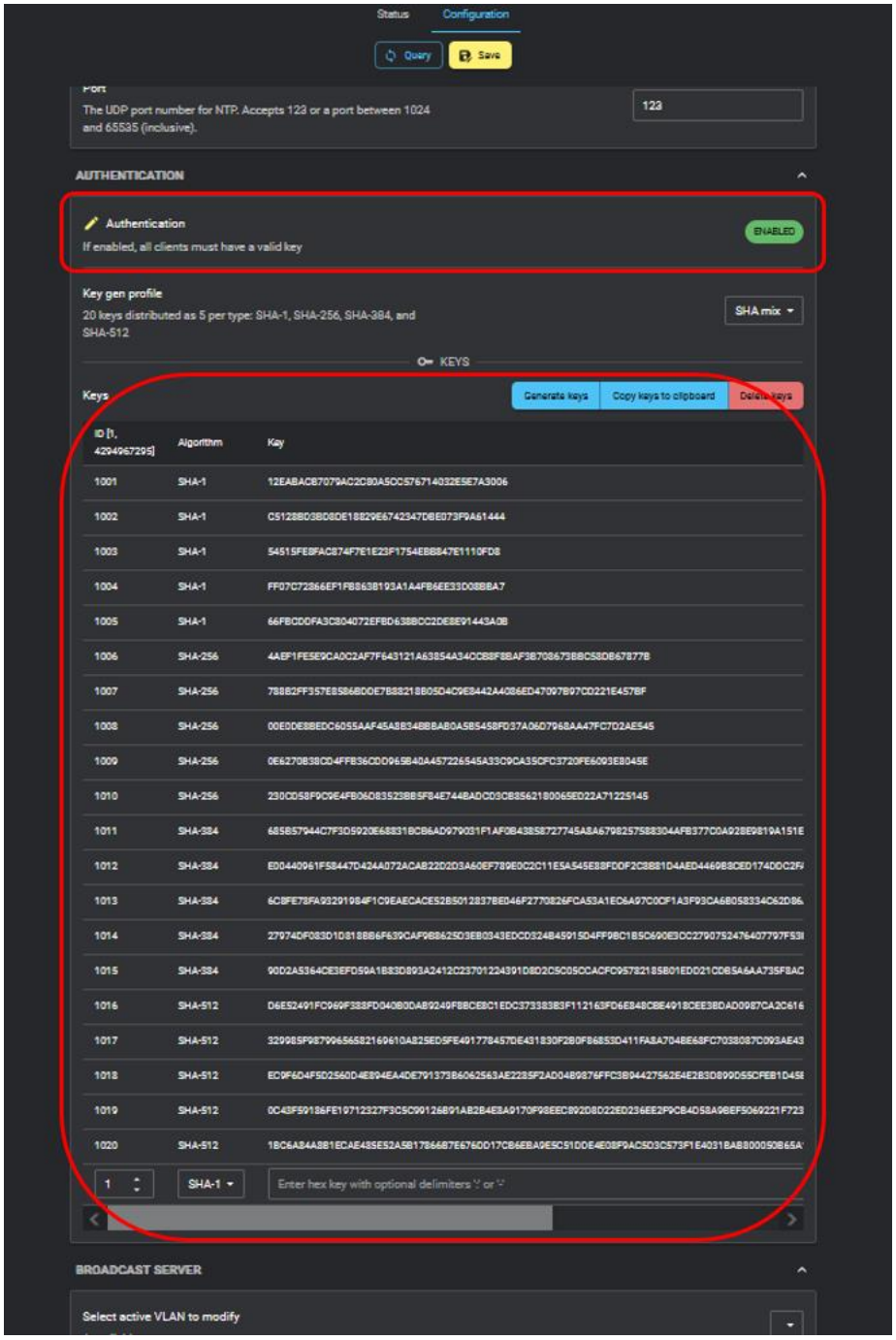


General	NTP	If enabled clients can connect enabled/disabled
	Port	Specify NTP udp port value default (123)
Authentication	Specify NTP auth-enabled choice enabled/disabled Used for Peering and Client/Server Authentication	
Broadcast Server	Specify the Vlan which the server can use to broadcast	

6.14.2.1 Configuration Authentication

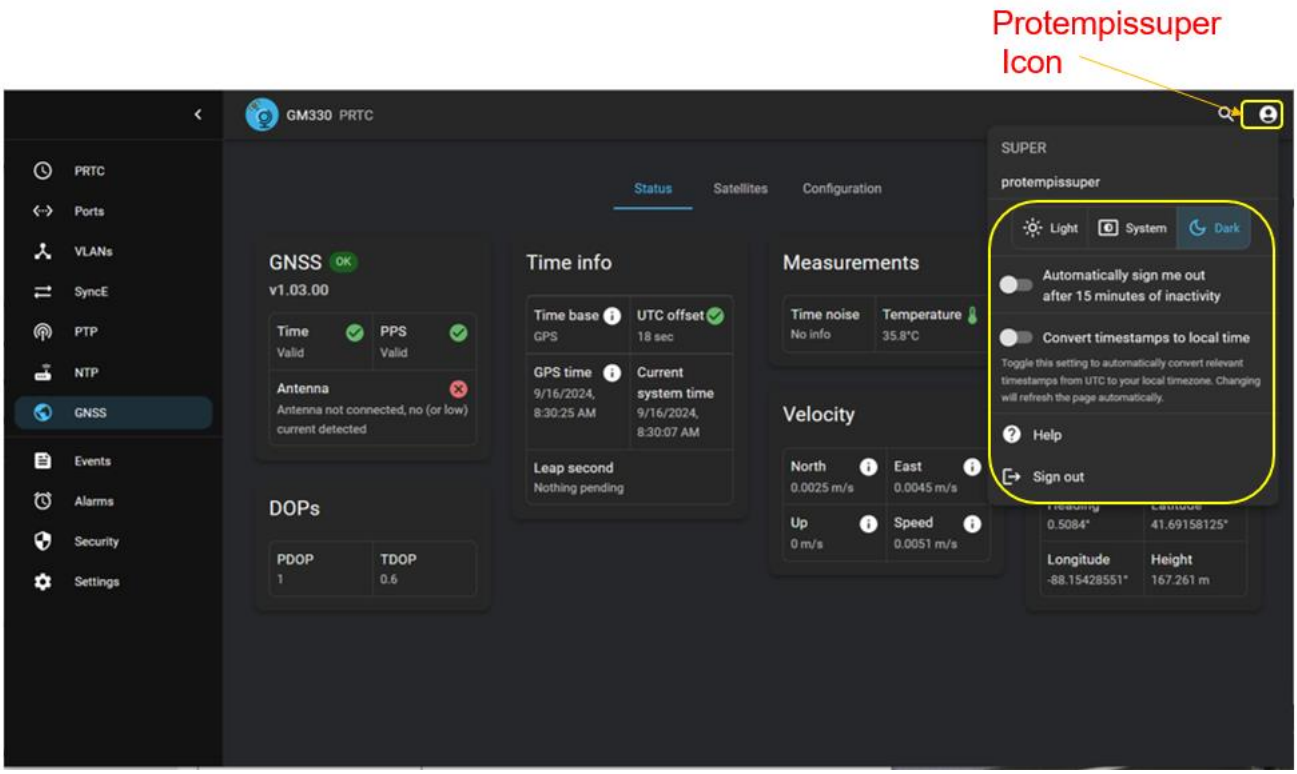
The GM330 “reserves” keyid values 1001 to 1020. The values are autogenerated at bootup if they have not been saved persistently to the start-up config.

The user should be aware that UI commands exist to regenerate keyids, and that the authentication parameters for these keyids will replace the keyid parameters for keyids from 1001 to 1020. Therefore the user is responsible for not overwriting these keyid parameters if they want to retain them.



6.15 Web Page Settings

To configure web page settings select “Protempissuper Icon”. A menu will appear with option Seting for the web page. In the example below the “Dark” setting was selected.

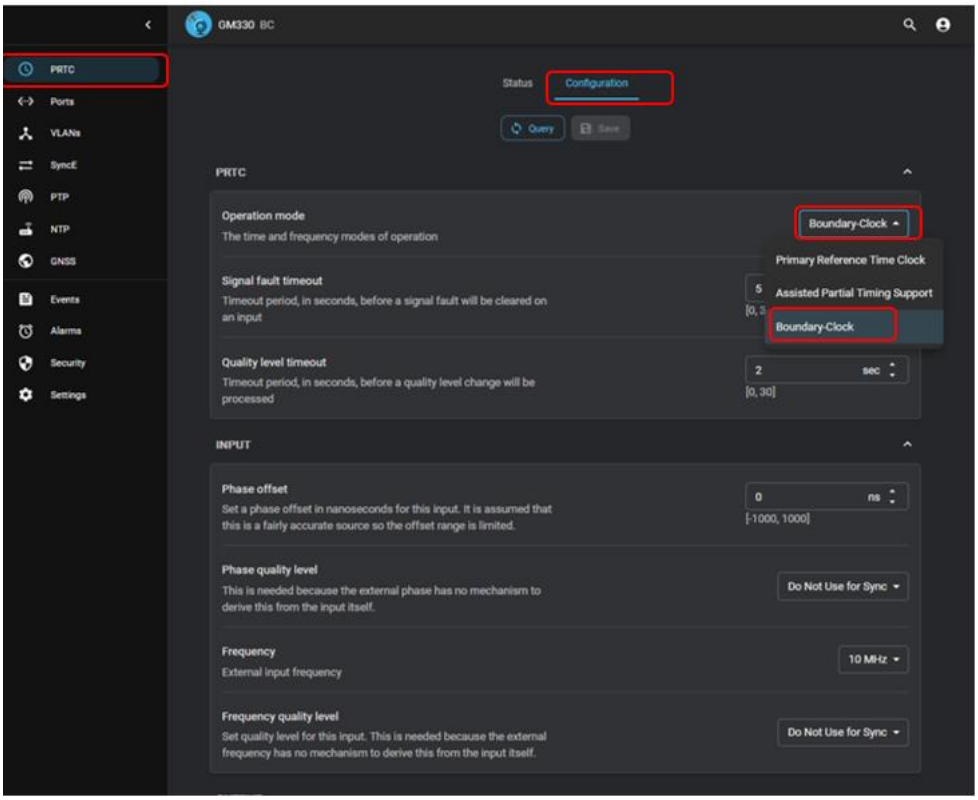


Light/Dark	Web page background
Inactivity Timeout	If turned on, you will automatically get signed out after 15 minutes of in Activity
Convert	Toggle this setting to automatically convert relevant timestamps from UTC to your local timezone. Changing will refresh the page automatically.
Help	If selected this will take you to a copy of the datasheet
Log Out	If selected this will log you out of the session

6.16 Boundary Clock

To configure the GM330 for Boundary clock mode select

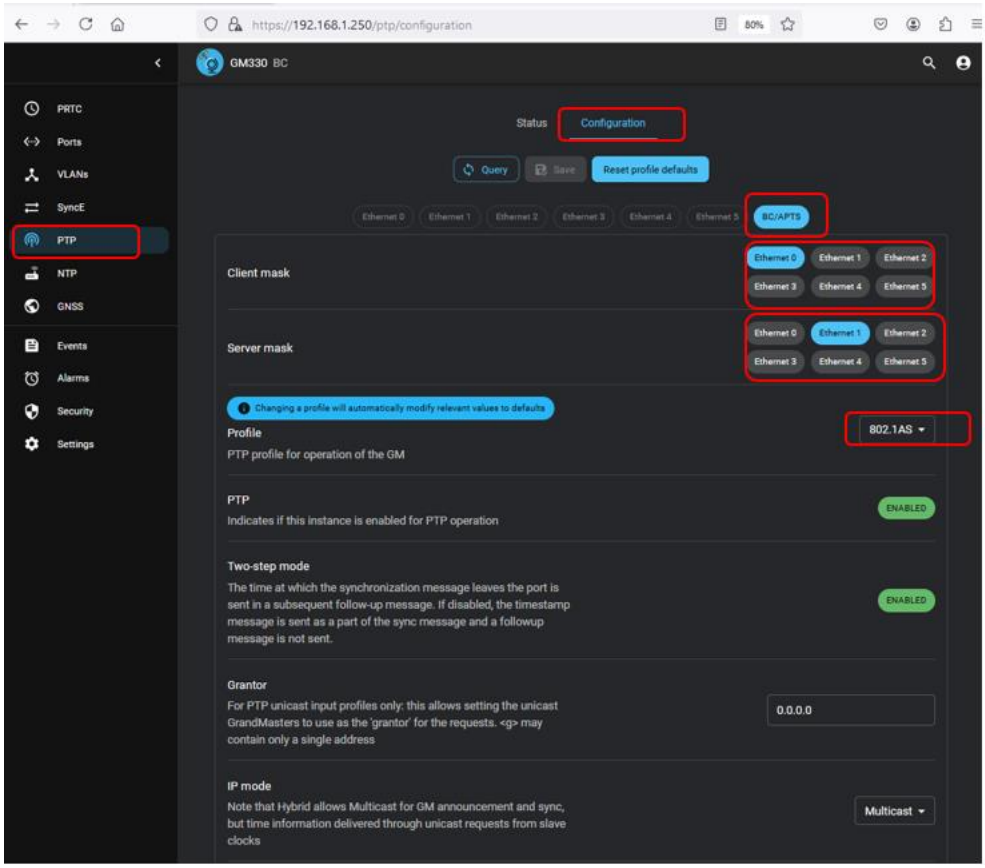
PRTC -> Configuration. In the Operation mode section select the drop down menu
Then select “Boundary-Clock”. PTP need to be disabled when changing operating modes.



6.16.1 Boundary Clock Mode Configuration

In Boundary clock mode, go to PTP->Configuration-> BC/APTS
There will be a section client mask and server mask. These sections
will allow you to select/configure which ports Ethernet 0 to 5 will participate
as a client and server.

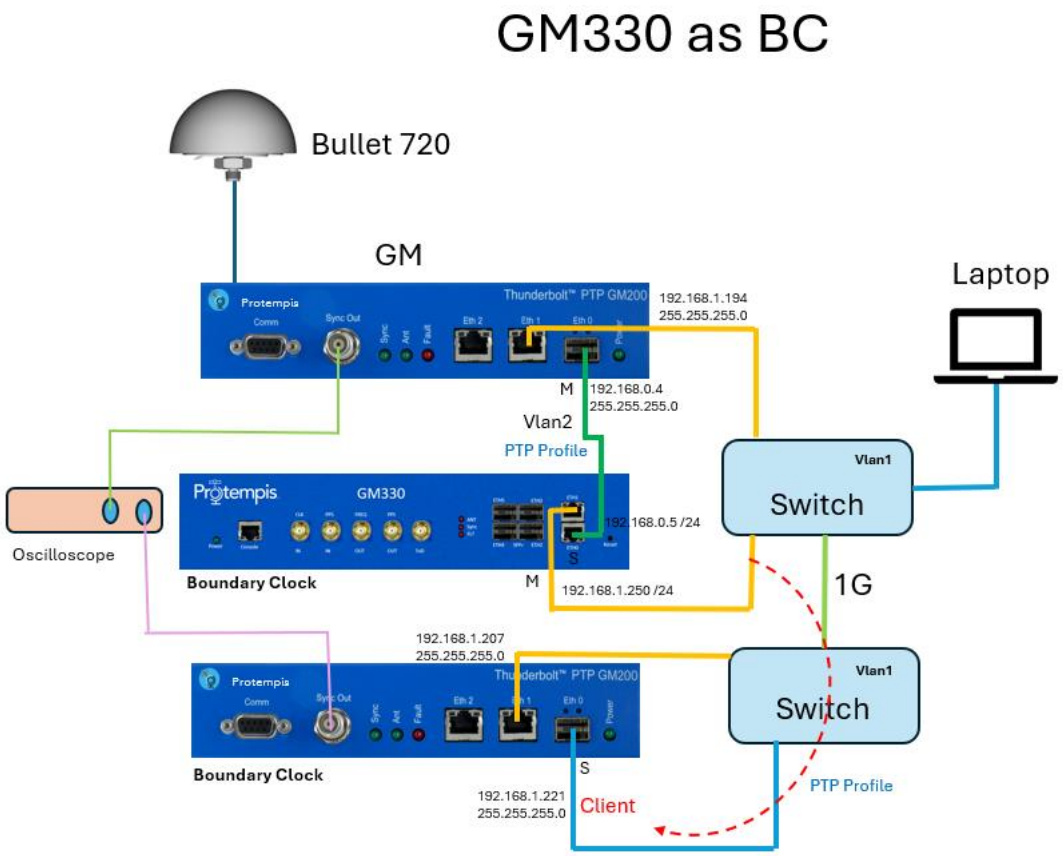
Client Mask	Ethernet 0 to 5 Port selected functions as a PTP Slave. This port will lock to a PTP master
Server Mask	Ethernet 0 to 5 Port selected functions as a PTP master. This port will send ptp timing to a PTP client/slave.



6.16.2 Example of a GM330 as a Boundary Clock

In the example below, two Vlans on different subnets were configured on the GM330.

Vlan1 is connected via network switches and Van2 is a direct connection.



6.17 Assisted Partial Timing Support

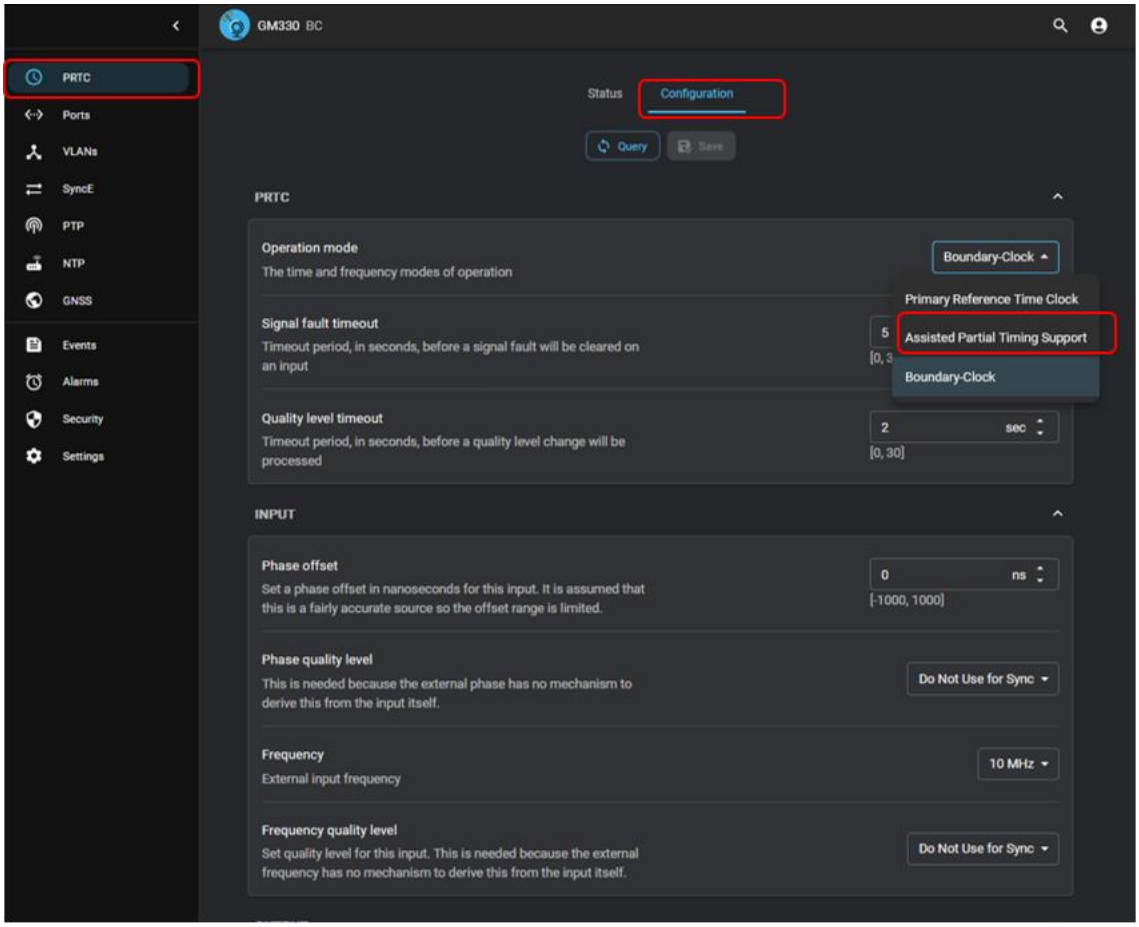
PTP Input is designed as a secondary(backup) reference of GNSS reference of the Time server.

If GNSS is lost or interrupted, in APTS mode the Server will automatically switch over to the backup source.

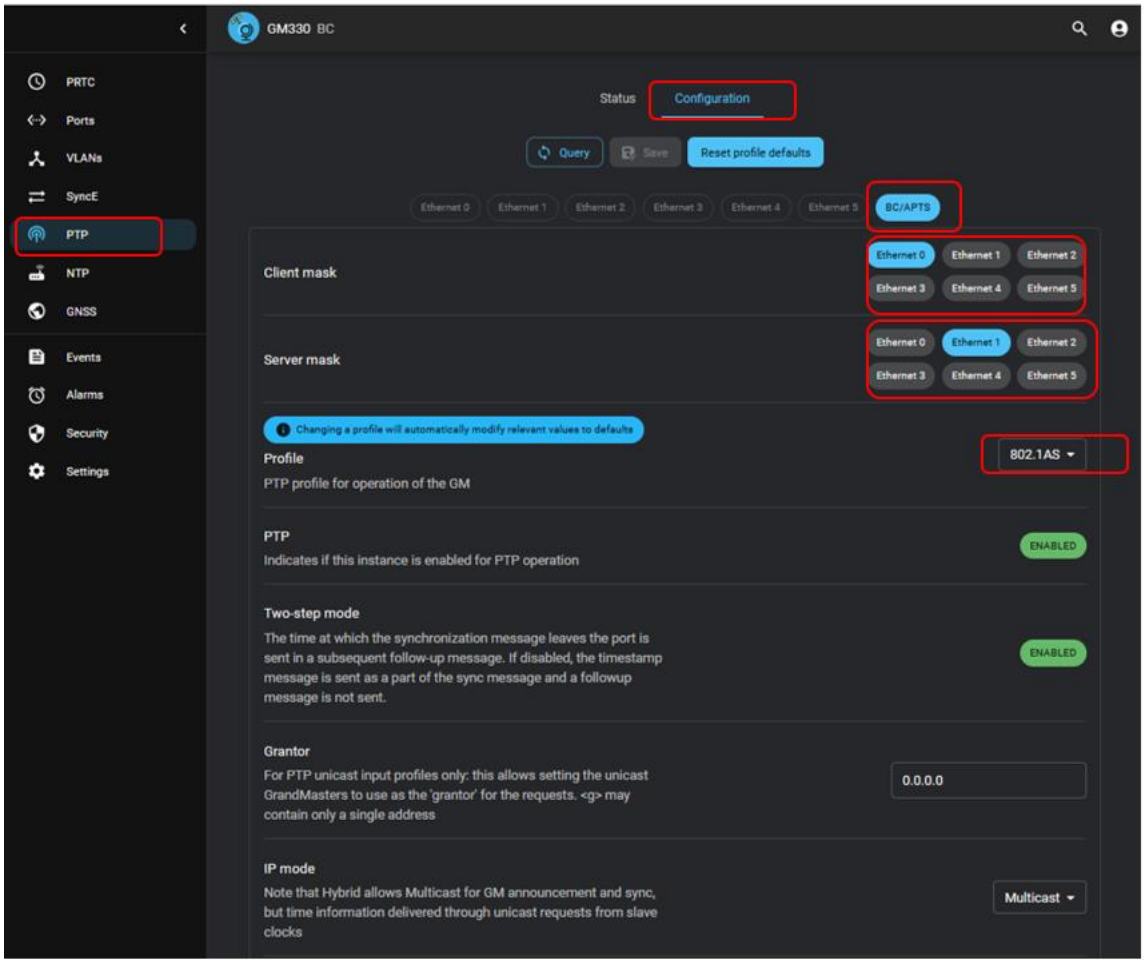
It can be configured in Ethernet port 0 to 5. It will be an additional input for the Time server. The Ethernet port will be configured as a PTP slave for the Time server.

Since the Ethernet port will be configured as PTP slave, it will require a grandmaster reference or ‘grantor’.

6.17.1 APTS Mode Configuration

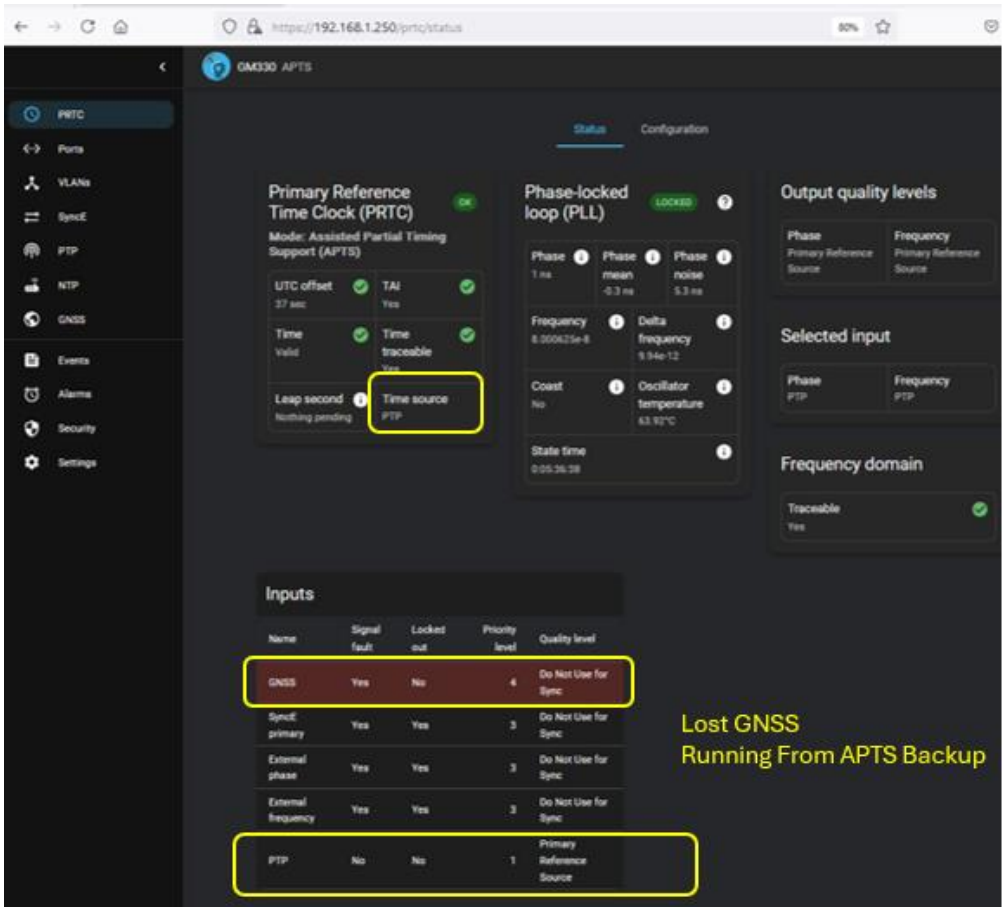


6.17.2 APTS Backup Input Configuration



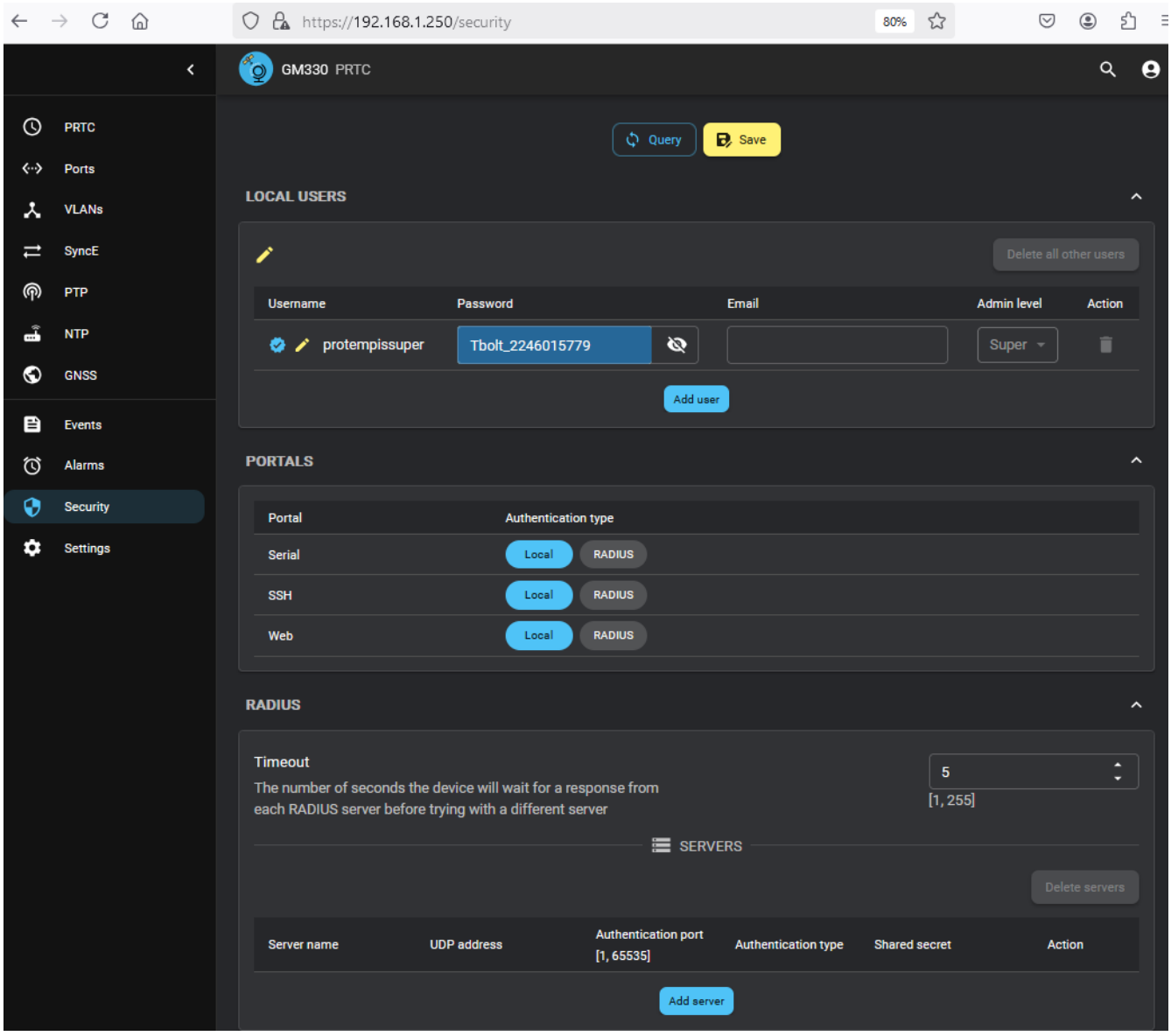
6.17.3 APTS Backup Automatic Switch Example

In this example, the Primary GNSS source was lost and the Secondary PTP input source was automatically chosen.



6.18 Security

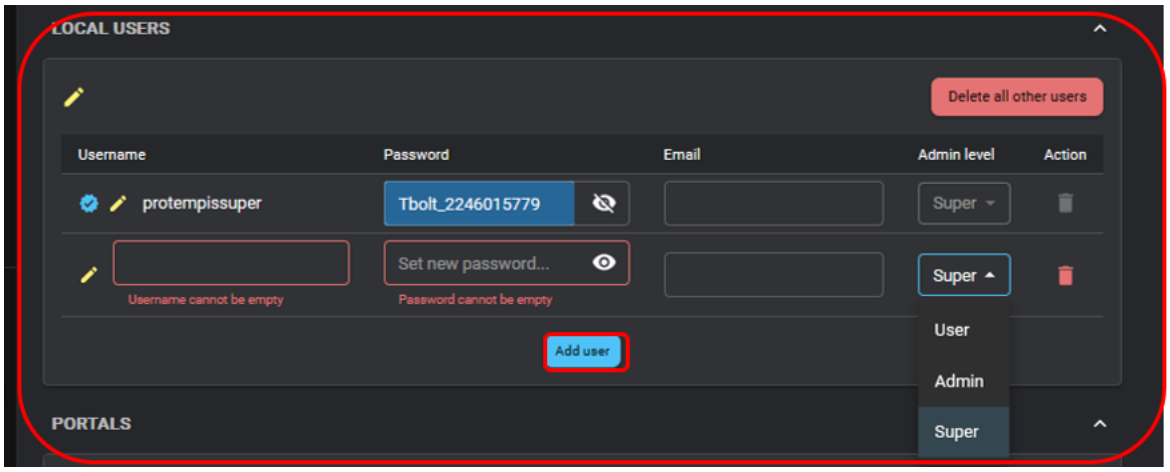
To get to this page select “Security” button on left menu



6.18.1 Local Users

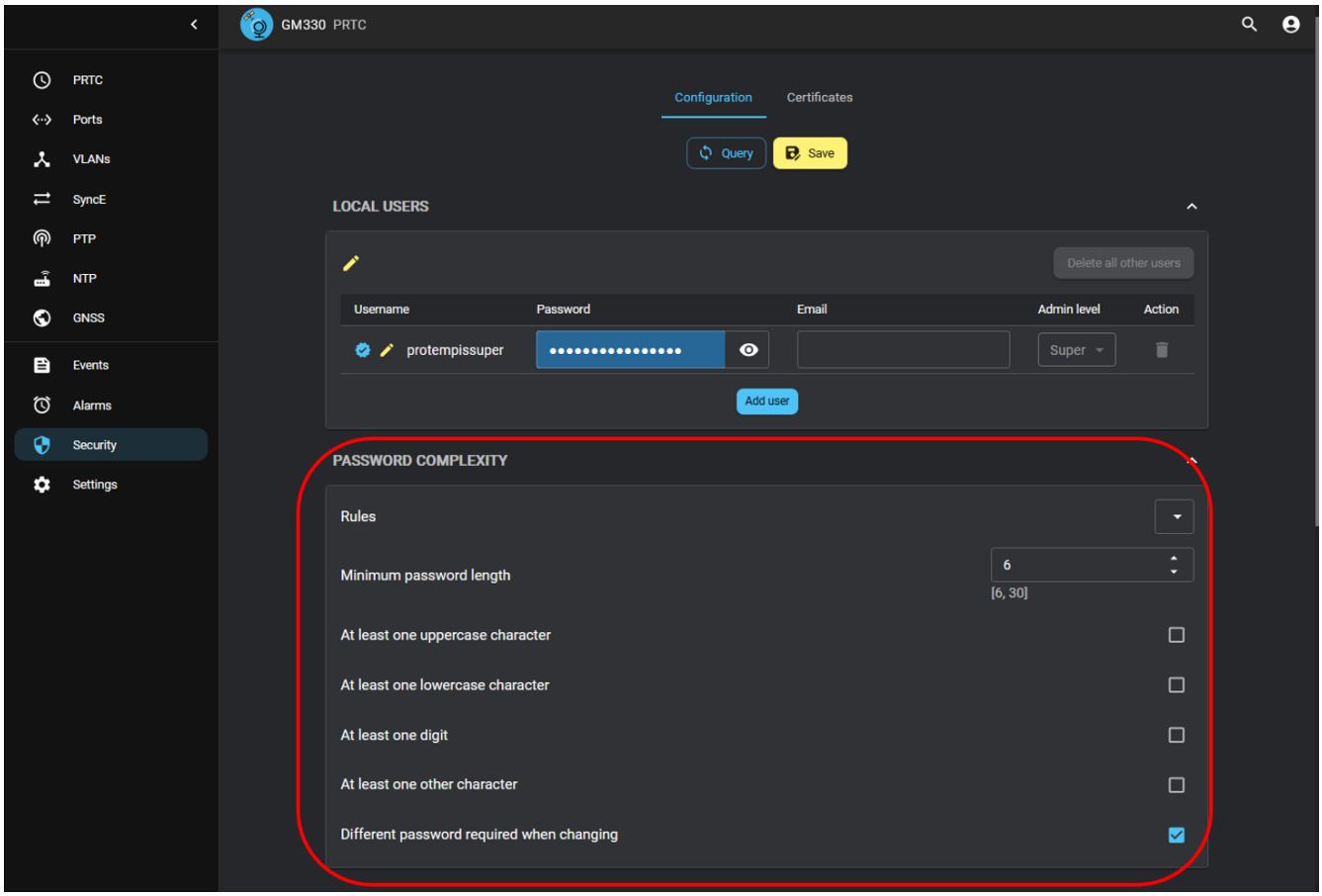
This section allows adding and deleting Usernames and passwords. The user can be configured as A “User”, “Admin” or “Super”.

Select the “Add user” button to get to the add fields shown below.



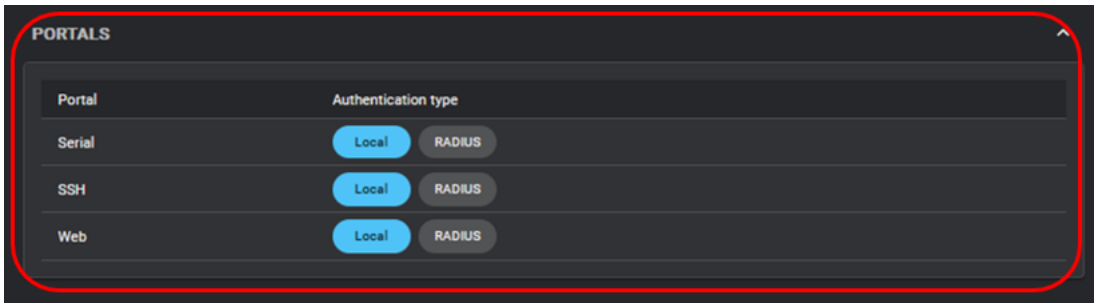
6.18.2 Password Complexity

Add complexity by selecting different password rules



6.18.3 Portals

To enable Radius Authentication for “Serial”, “SSH” or “Web” select the “Radius” button.

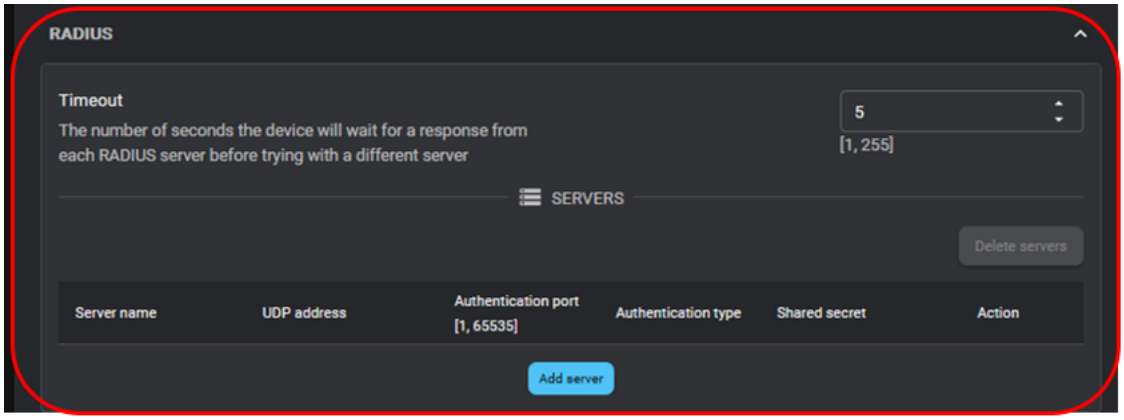


Portals	Serial	Local - RADIUS Authentication for Serial Port Disabled RADIUS - RADIUS Authentication for Serial Port Enabled
	SSH	Local - RADIUS Authentication for SSH Port Disabled RADIUS - RADIUS Authentication for SSH Port Enabled
	Web	Local - RADIUS Authentication for Web_UI Port Disabled RADIUS - RADIUS Authentication for Web_UI Port Enabled

6.18.4 Radius Server

The GM330 supports RADIUS authentication

Select Security -> Authentication

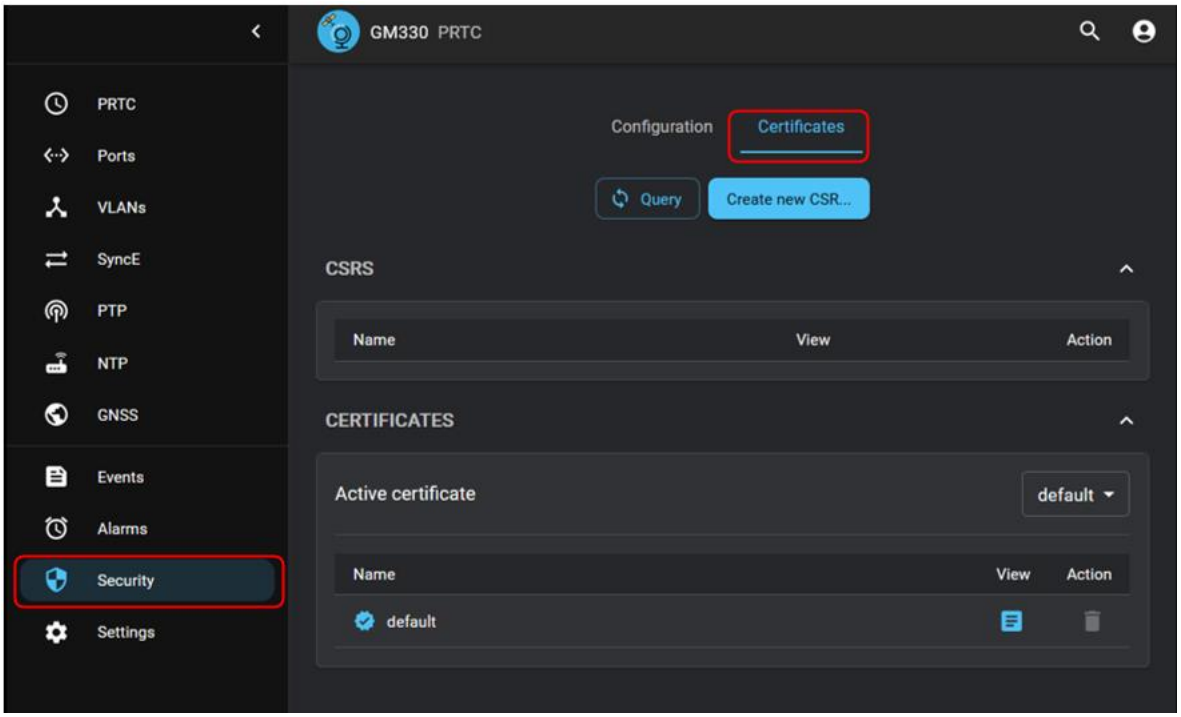


Server	Server name	Server Name
	UDP	Server IP address

	address	
	Authenication Port	Displays or allows to set the IP port for the RADIUS server
	Authenication Type	Password Authentication Protocol (PAP) CHAP (Challenge-Handshake Authentication Protocol)
	Shared Secret	Set the shared secret value for the RADIUS server

6.18.5 Certificates

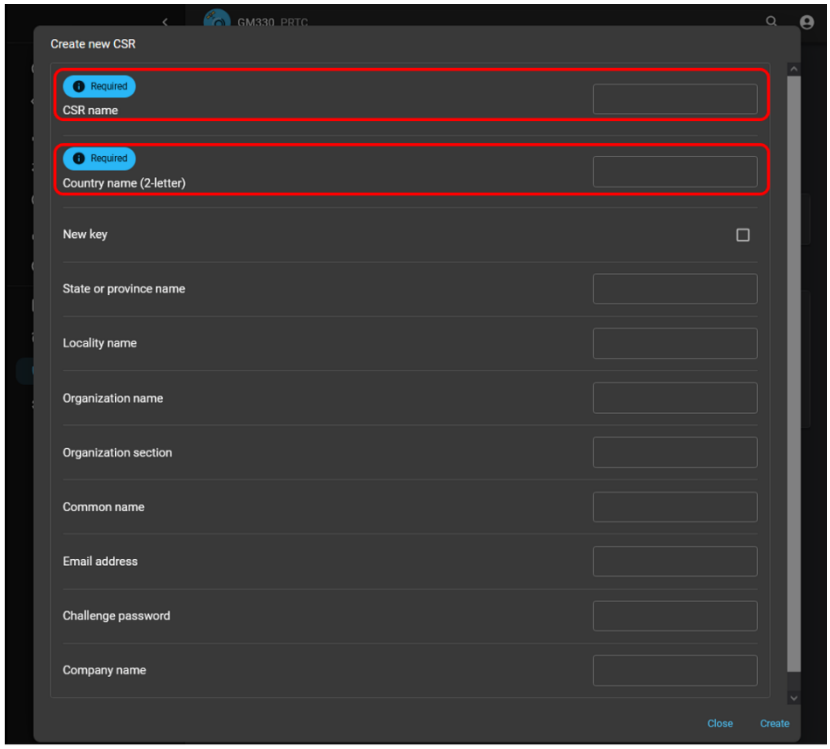
For more information, refer to “GM330_Certificate_Guide.pdf”.



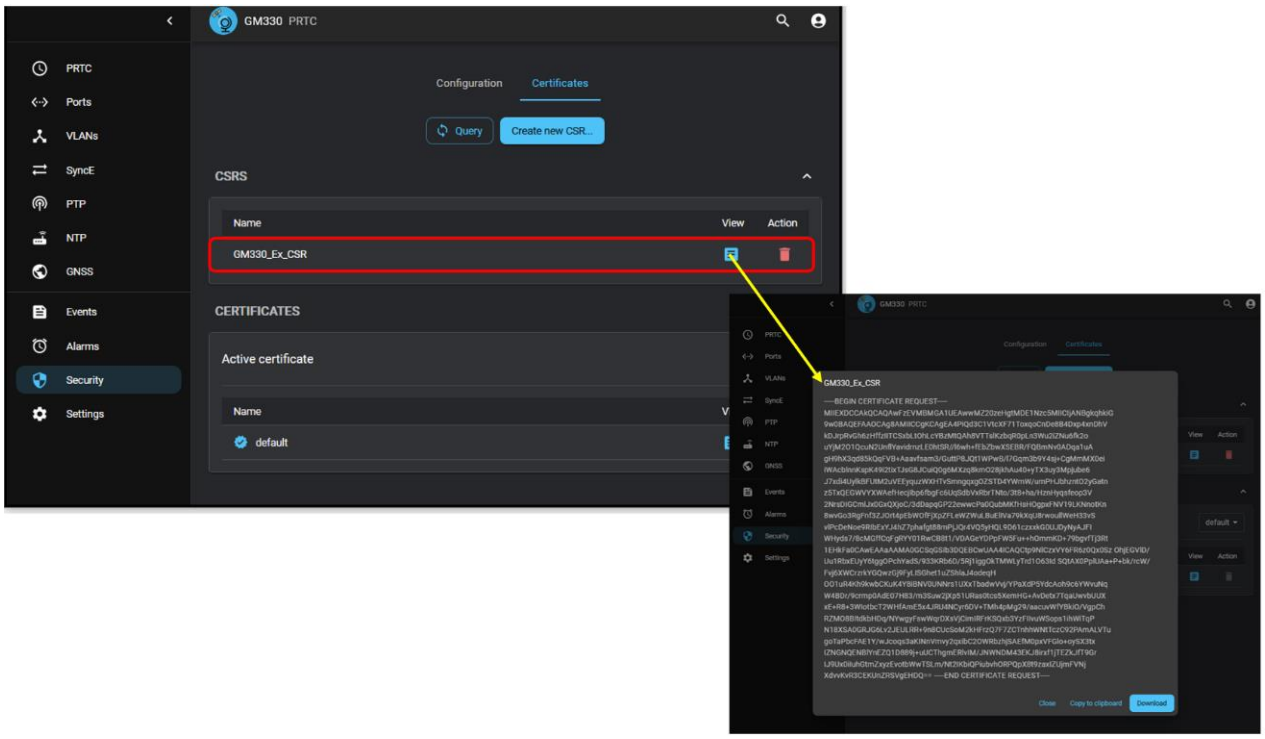
Create a new CSR	Create a new CSR (Certificate Signing Request)
Active certificate	Choose the active certificate from the dropdown menu
View	Click to view the Certificate
Action	Delete Certificate

6.18.6 Creating a new CSR (Certificate Signing Request)

The “CSR Name” and “Country name” fields are required.



As an example, I created a CSR and named the file “GM330_Ex_CSR”. It will show up as shown below. You can then view, copy to the clipboard or download and get it signed by a CA “Certifying Authority”.



Note:

Make sure that you keep the same name for the *.csr and *.crt

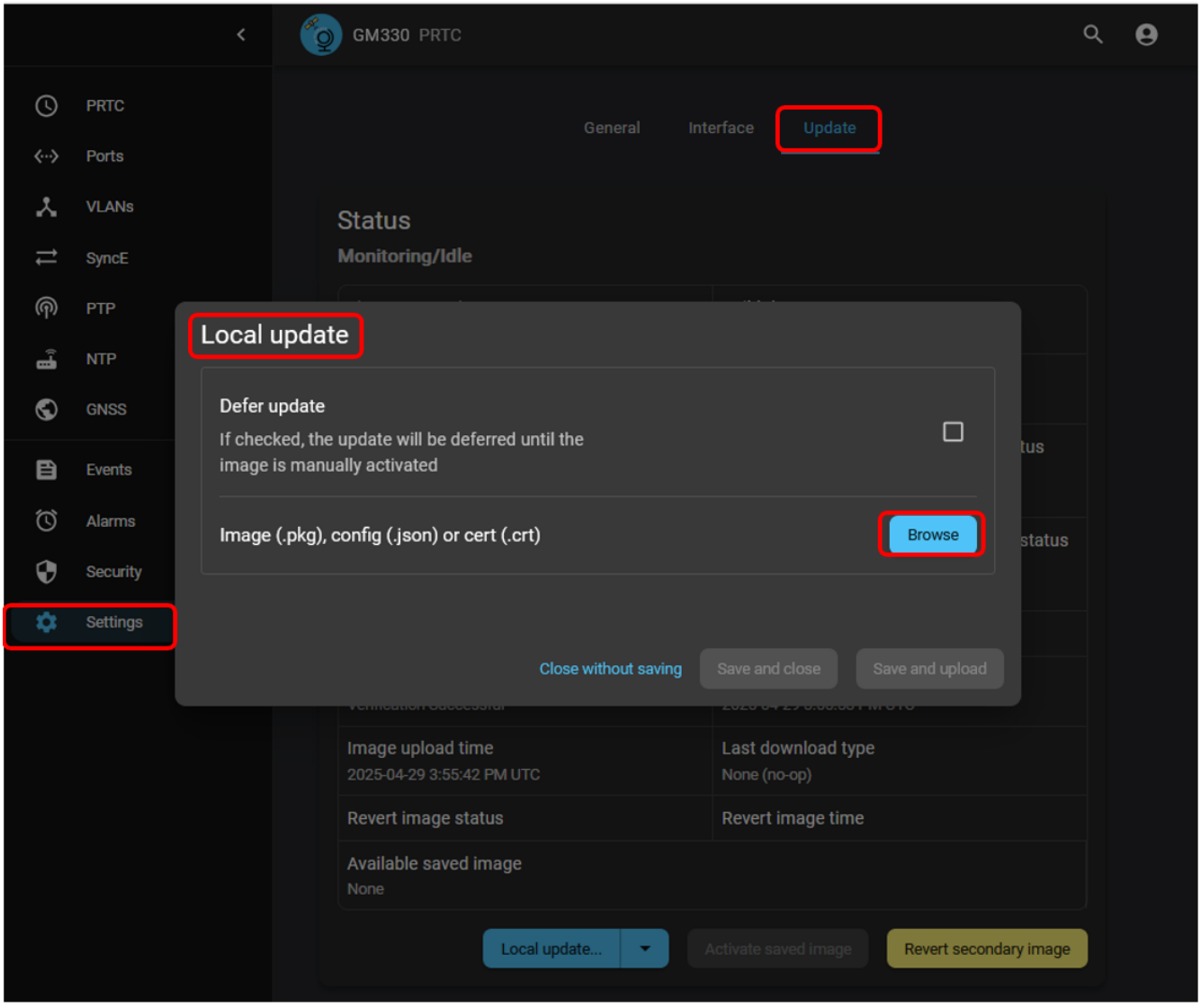
Example:

Request "cert1.csr" after signing, name it with the same name, use the .crt extension "cert1.crt", and then import the file

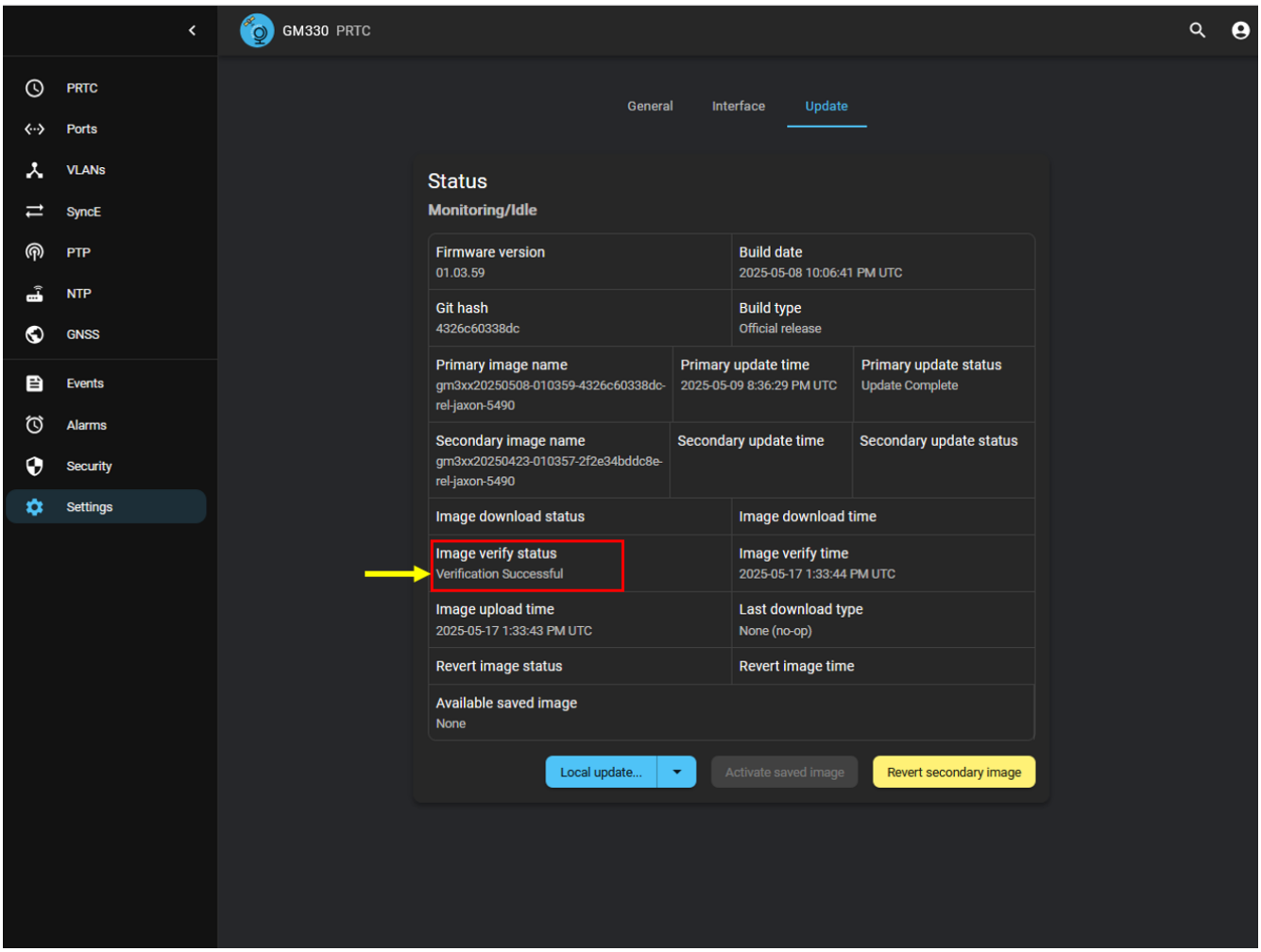
6.18.7 Uploading Custom Web Certificate (Local Update)

To upload a custom Certificate, go to Settings->Update->Local Update. The file

Must have a *.crt extension. Click the “Browse” button and navigate to the file.



Once *.crt is selected click on “Save and Upload”. Confirm the file was uploaded successfully by Looking at the “image verify status” field as shown below.



Note:

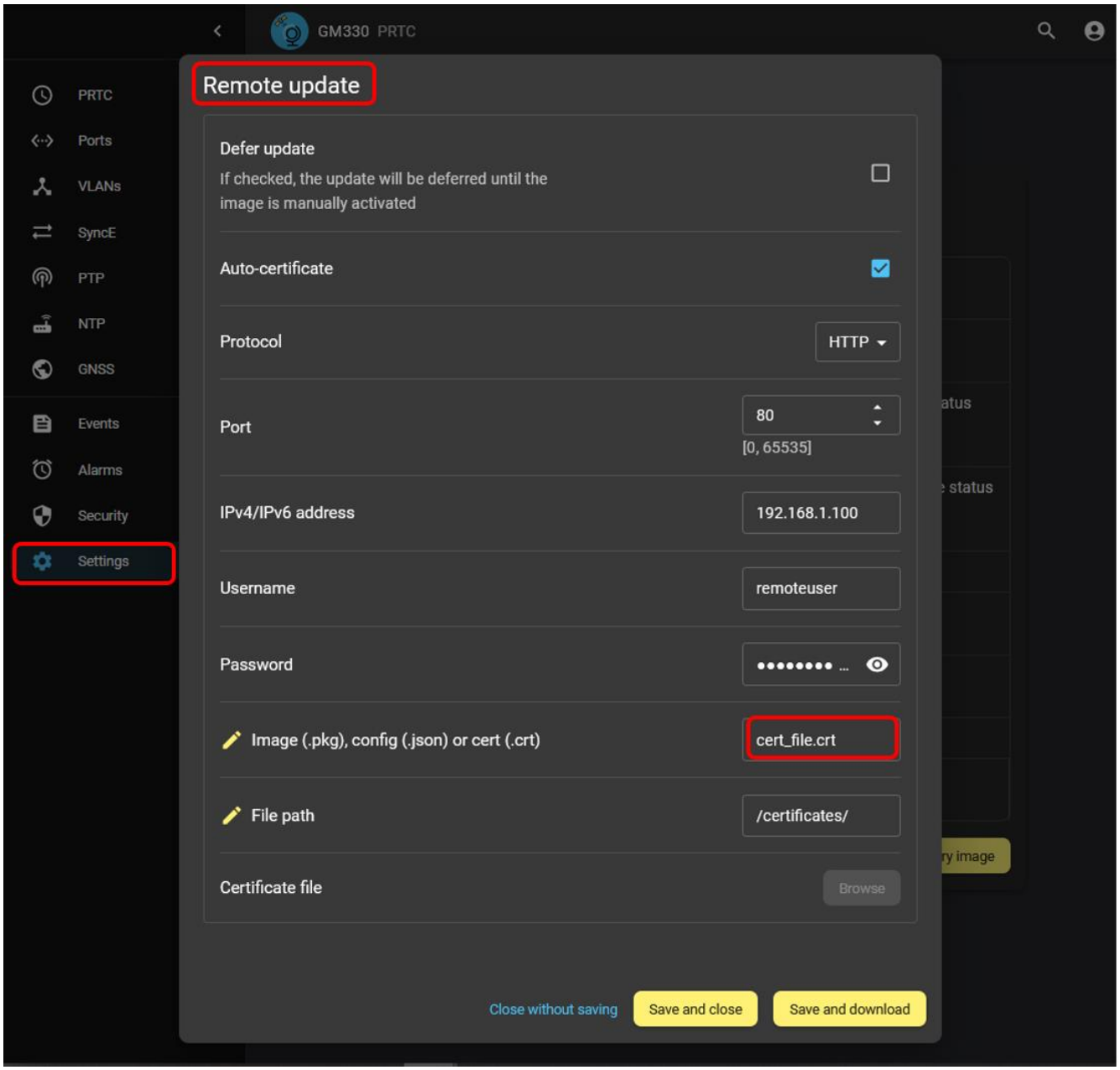
The GM330 only supports a .crt file in PEM format (x509).

Example:

```
-----BEGIN CERTIFICATE-----
MIIEgTCCA2mgAwIBAgIUfok5iOQH1XsfgYeW7M4DTG861jswDQYJKoZIhvcNAQEL
BQAwXzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMREwDwYDVQQHDAhTYW4gSm9z
ZTESMBAGA1UECgwJUHJvdGVtcG1zMQwwCgYDVQQLDANTUUExDjAMBgNVBAMMBU1h
cmlvMB4XDTI1MDUxNTE3MjQwMVoXDTI2MDUxNTE3MjQwMVowMTELMAkGA1UEBhMC
aWwxCzAJBgNVBAgMAmlsMRUwEwYDVQQDDAxnbTN4eC0wMTU3NzkwggIiMA0GCSqG
SIb3DQEBAQUAA4ICDwAwggIKAoICAQC+hJNwH92GjNpK0aO96JrcU2ecDdFgwVHS
h4eNsxPo2aoW3FmpZUy1Ecc4JUiTo/vFi9RCmzHxG7dGxNDYUpJ3LnKud8gx65fJ
XMJ0dwASoej0kuqe4U7V1vadSAHPWJEZCsAkJ1ViXRVYyQ4IC5+meX7EefniVzUS
huFjZ1UFoom4Iv3ty9kKgAfUxZeYH5fGsgw6zXKpPq7f5k8ztXkeh5Eh7EMh7egP
R+jL71hdmIwSbmZIAq/URxKSkzR2mBawDBzt9sLt6e/1OpJCYhN+FmPRhBRTyVvu
/S4uQPKmPPVA0c/SbJ1vWiVP48bhkgTKOn3A/nXwTJY+r+6NtXKE6C21/uVk8EMT
RkBVwoP9Nim0KnacevWmwIZFHHHxKzR+0aZBgiOe61nB5NifBmPdqDokv7mjfvya
CW9sgWQfuN6rXerHWIX9XJDTXudHb5t0wwwWaFr9JO8q1HjefJ3eBshCn28H1hIy
/ePbwKgMgksEoDF12MeNp2T/AAt2R56wcK0EYrf/Pnpf84EykMbuvu7GQEgyRK/D
KziaY4JOpjfM8OfIwyEbv1LBSCSq0HQuOoTAp72zKWLQwQ7p6EWZkBecLWSdXtcJ
wZibJVWNDJBvMwCj5mIpzj1Fp0zd7ptgnXqTYT8bgKm/zCCM11e+czPOdfUGqWKG
RkVOt7RKaQIDAQABo2MwYTAfBgNVHREEGDAWgg5teWRvbWFpbi5sb2NhbIcEwKgB
+jAdBgNVHQ4EFgQU463rxeDZct1OzHfP0a6O5JDiLecwHwYDVR0jBBgwFoAUHVGo
PgeXV86cGL/GXw7vaHdsfn4wDQYJKoZIhvcNAQELBQADggEBAFeHHGecscvo6cu8
TTTrKGdVee9k7WVLC5PZ1Ak4Ext0j5uRN8oOgbzC75CnGZoeownFjGSFAOQ+MgzF
+tbW8RBcQXHfDE19vR1QSEMM90Kkx2rIt7t8H42xtqCxHNyW07rqRizeK9ew5S9h
fLOuDYszikbPJjFrB0gMx2X6Ad3Mh9iA0aNzW+hswyZrhBEn3nxX6UUuAK45EuAr
PG593Rsx8qLR1+pSLUM9+5fahFwdKQZAmHGYW+1H5aG7u3gLkDCwtOPZ4vnAht+e
+Ei0o+oY1+dZXx7TxG45yZtq9OJDrMeo+aUFGsfPn30iBbn1Ui4uB9oJizgcPHSz
TESe7d0=
-----END CERTIFICATE-----
```

6.18.8 Uploading Custom Web Certificate (Remote Update)

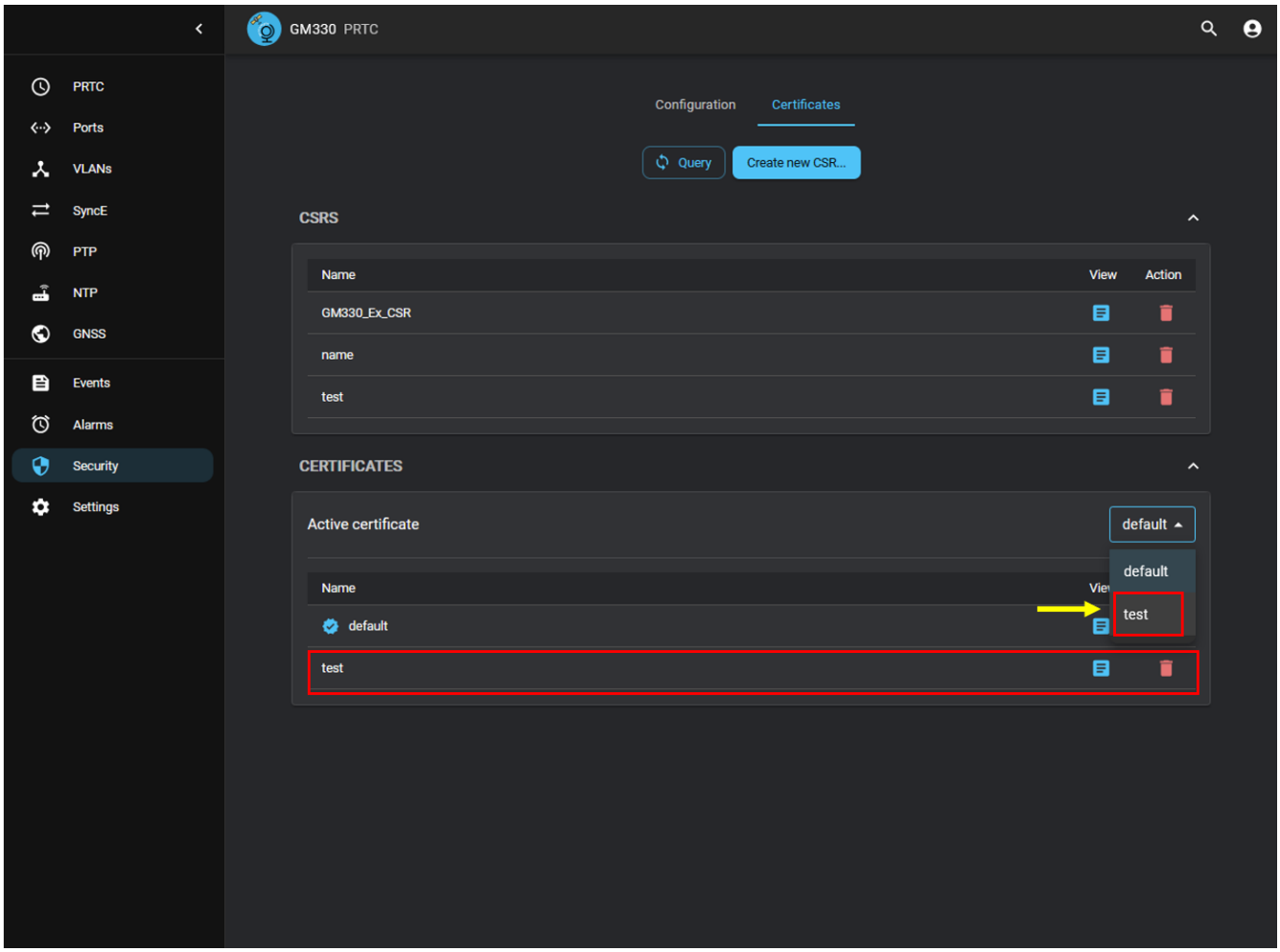
To upload a custom Certificate, go to Settings->Update->Remote Update. The file Must have a *.crt extension. Fill out the remote login Server Information.



6.18.9 Activate Custom Web Certificate

Once the *.crt is successfully uploaded, the certificate needs to be activated.

In the example below, a “test.crt” file is uploaded. Then navigate to Security->Certificates “Active Certificate” section. Select the certificate from the drop-down menu as shown below.

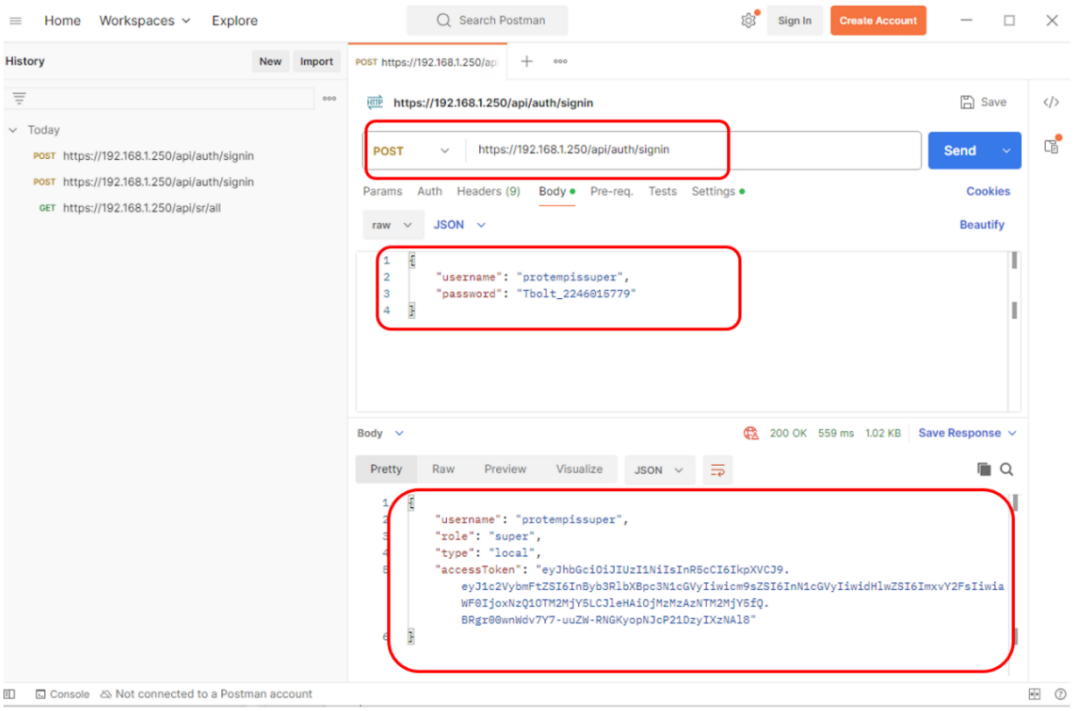


6.19 Rest API

The API supports retrieving, setting, validating, and deleting configuration data.

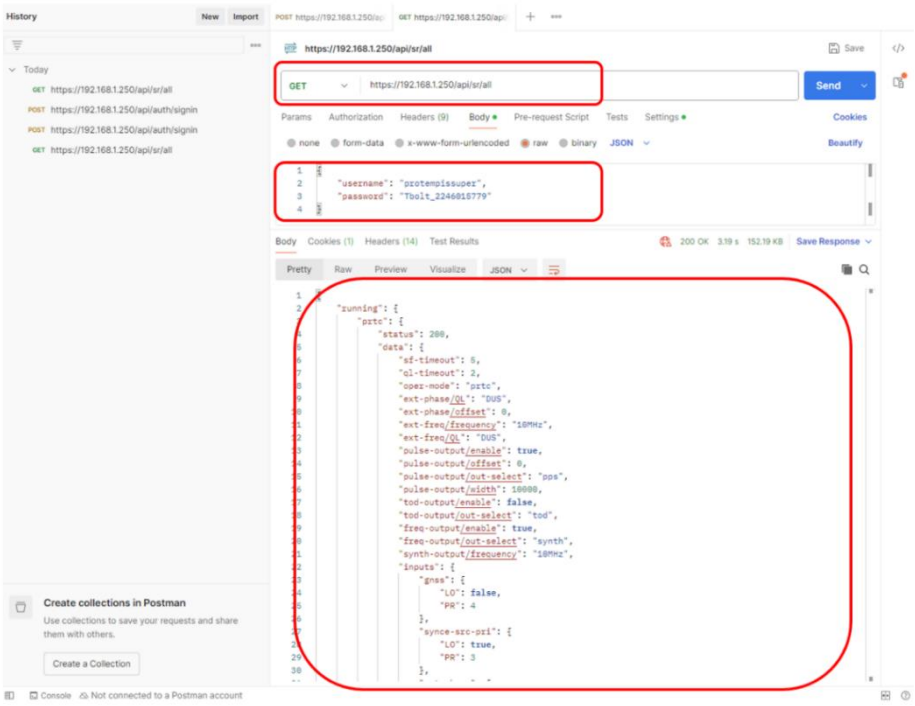
For firmware versions 1.04.00+. For more information, refer to the "*GM330_API_Guide.pdf*" document.

6.19.1 POST Login Example Using Postman



6.19.2 GET Parameters example Using Postman

Request All Parameters



6.20 Zero Touch Provisioning (ZTP)

For deploying several GM330. The GM330 is implementing ZTP. ZTP automatically

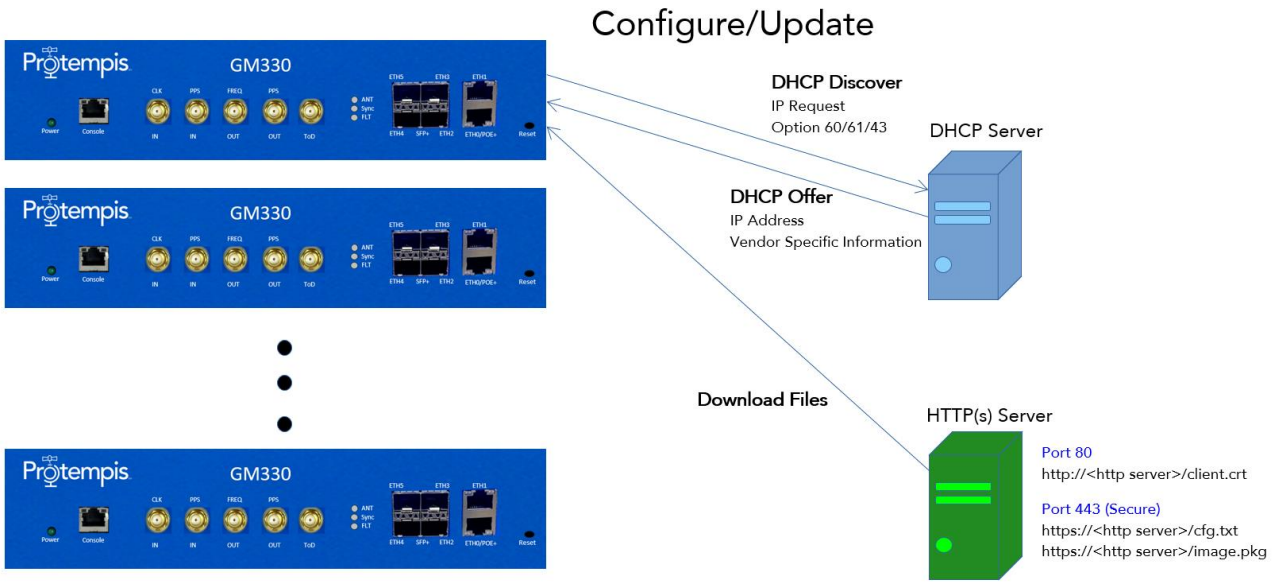
obtains configuration information that allows configuration and firmware image files to be located and downloaded from servers.

The device uses information you have configured on a Dynamic Host Configuration Protocol (DHCP) server Option 60/61/43 (Vendor Specific Information). If you do not configure the DHCP server to provide this information, the device boots with the preinstalled software and default factory configuration.

For HTTPS, a client certificate will need to be applied.

For more information refer to "*GM330_ZTP_Guide.pdf*" document.

Overview



7. Updating firmware

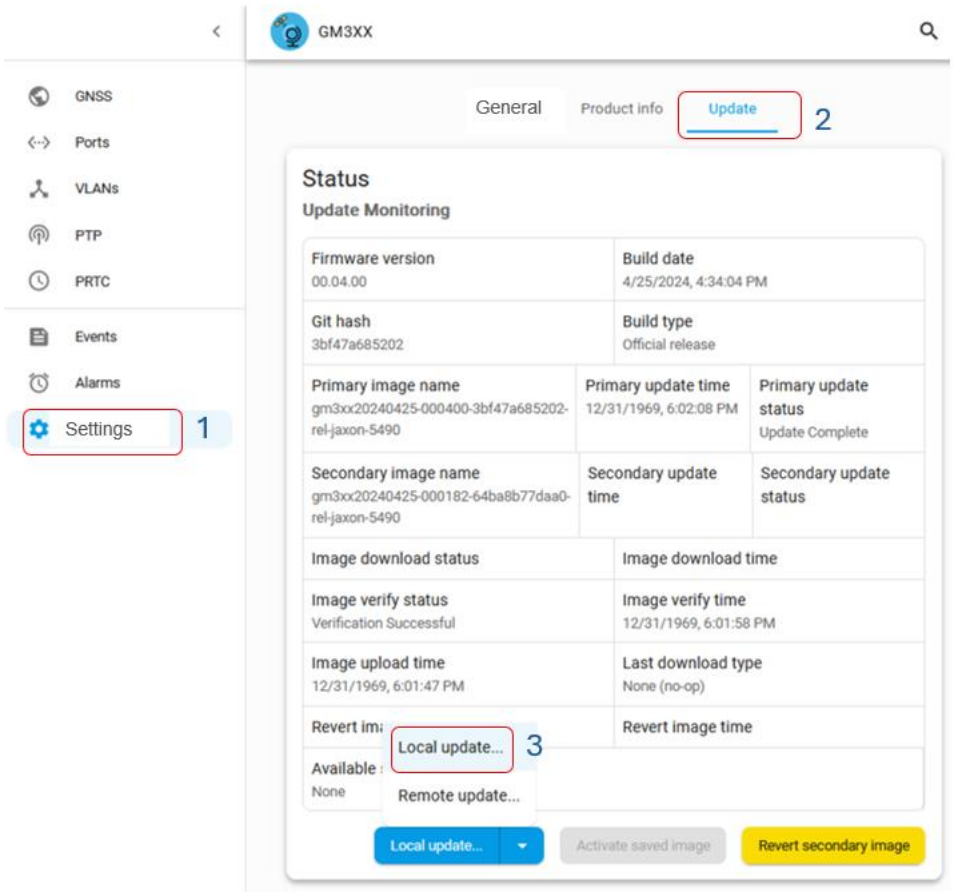
You can use the Web interface.

7.1 Update

	Click on "Settings"

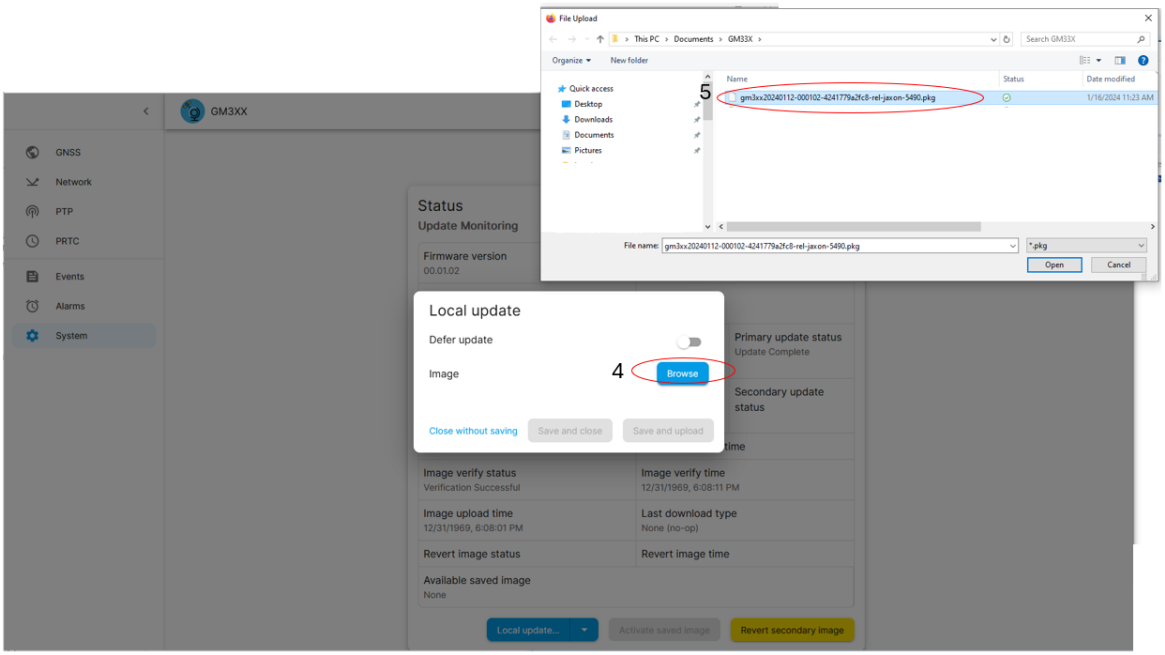
7.2 New Firmware File

Navigate to System then Update in the WebUI. The steps are outlined below.



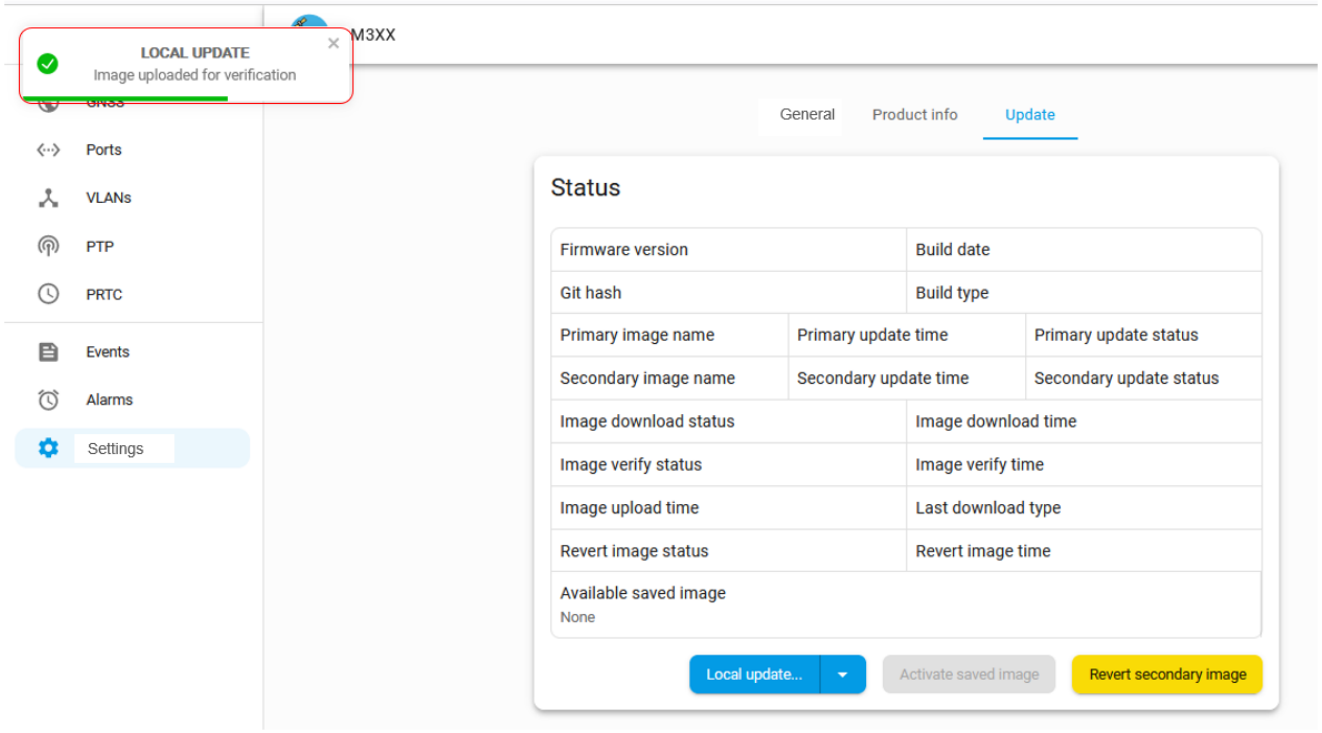
1	Click on “Settings”
2	Click on “Update”
3	Select “Local update”

Make sure “Defer update” is unchecked. This will allow the new firmware to activate automatically.

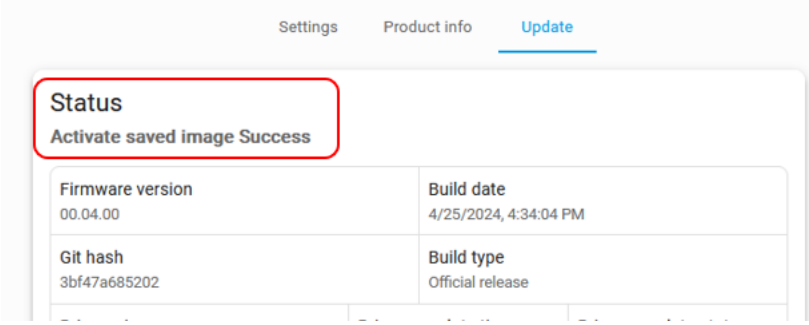


4	Click on “Browse”
5	Navigate to where the New Firmware file is located .pkg “Click Open”
6	Click on “Save and Update”

The Local Update will appear



The status field will change to “Activate saved Image Success”



The Status field will change from “Activate” to “Rebooting”. Now wait Until the unit boots.

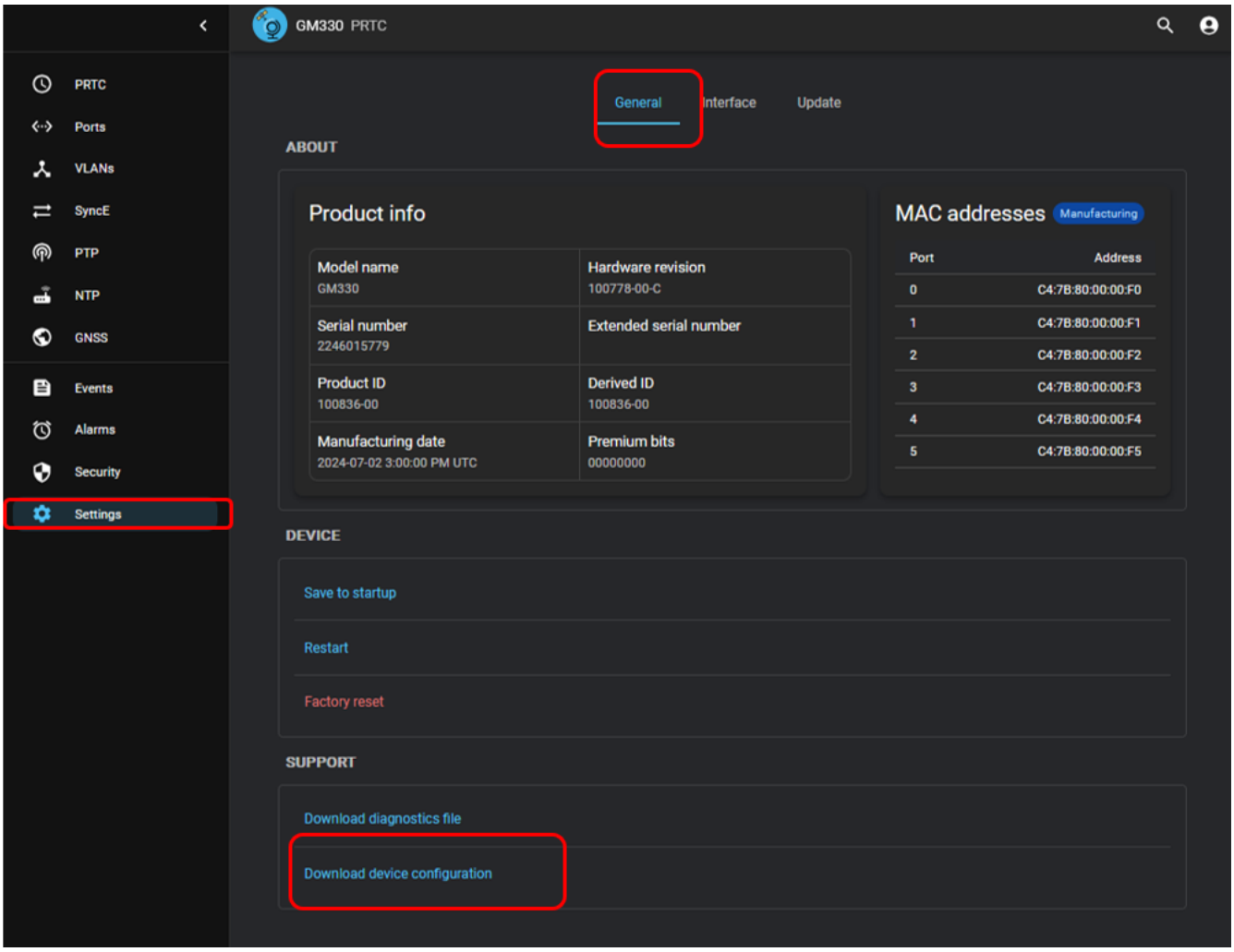
8. Configuration

The configuration can be saved to a file and restored. The file is saved in a JSON format.

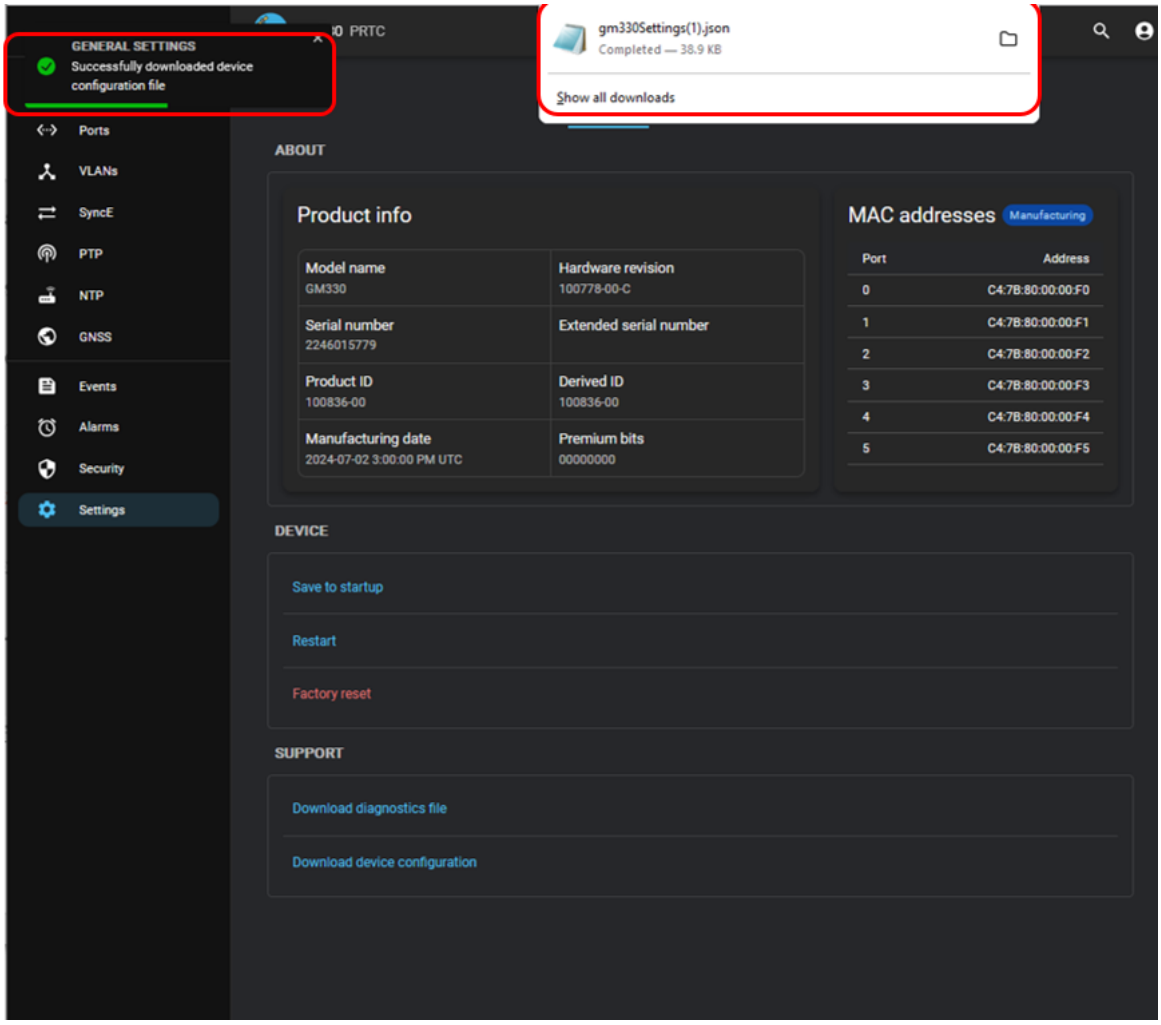
8.1 Saving the Configuration

Go to Settings->General

Click on “Download device configuration”



The configuration file will be downloaded with a “.json” file extension.

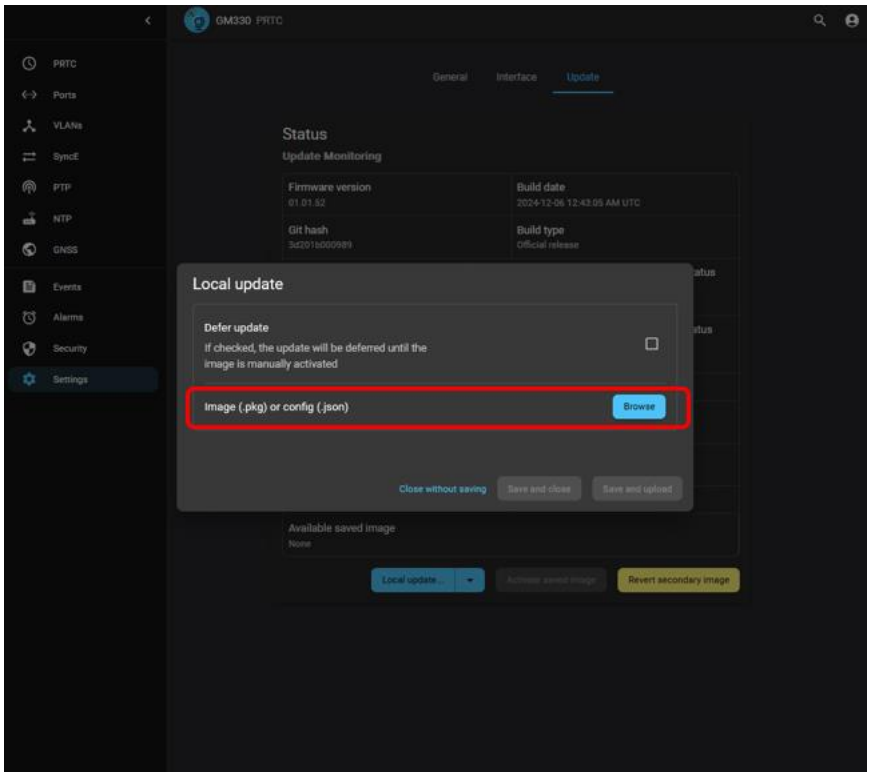


8.2 Restoring a saved Configuration

Go to Settings->Update

Click on “Local Update” -> Browse

Navigate to where the configuration .json file is located.



Select the file and click on “save and upload"