TM3000A

v1.1.2

PTP and NTP Time Server
GNSS Time Sourced

Installation and Operation Manual

TimeMachines, Inc.
300 S68th St Place, Suite 100
Lincoln, NE 68510
402-486-0511

Engineered and Manufactured in Lincoln, NE, USA
Rev 1.1.2 March 2026

TIME MACHINES

Table of Contents

TIME MACHINES

1 Introduction

The TimeMachines TM3000A is a simple to use GNSS sourced time server that will supply accurate time for all computers and devices needing accurate time on the network. By placing a time server on the local network, a PTP and NTP time source is provided without requiring systems to go to the Internet to get time. The system uses an active GNSS antenna to maintain the current time as broadcast by United States, Chinese, EU, and Russian GNSS satellites. With this device installed on the local network, there is no longer the worry that if the Internet connection goes down, time synchronization is lost across the network. In addition, the TM3000 includes a high precision internal clock based on an OCXO (Oven controller oscillator) that allows the unit to serve accurate time beyond loss of the GNSS antenna signal.

The TM3000A includes a pair of SMB outputs to allow for 1PPS and a synchronized 10MHz reference signal to be output from the device.

The unit is small and can be placed anywhere within the network layout. The built in high sensitivity GNSS receiver is able to lock multiple satellites from within many buildings or from a window location, removing the requirement that outdoor antennas be installed.

Setup and use of this time server is straightforward. Simply connect both the included power supply and the GNSS antenna to the base unit and then connect the base unit to the local network. Go to a computer on the network and browse to the device at its default address to enter the software setup within the control box. Set parameters to match your network and the system will start to send out time packets to any device on the system that asks for an update from it.

When paired with TimeMachines digital Power Over Ethernet (PoE) or WiFi clocks, synchronized time is assured no matter the state of your network, or the state of the internet time server the clocks are pointed to. Accuracy is also improved because the network delay of the internet is highly variable, while the local LAN connection is likely sub-millisecond delay.

TimeMachine GNSS based time servers are suited to any application where coordination of events at multiple locations is required. Without coordinated network time, searching for problems across multiple system logs becomes much more difficult. Education, industrial facilities, military installations, public safety command rooms, government, broadcasting, and hospitals are all candidates for synchronized time systems.

TM3000A Upgrades from TM2X00 models:

- Dual gigabit network ports supporting two different network segments without routing between them. SNMP, Web, PTP, and NTP can be selectively routed or denied on each port.
- Encryption support for web (https://), NTP, and SNMP traffic
- LCD display showing live status information about the device
- High precision, low jitter, PTP, typically within a few hundred nano-seconds of reference
- 48V power input compatible
- Multi constellation GNSS supporting GPS, Beidou, Galileo, and Glonass in various combinations. Increases the number of viable locations for antenna placement.

2 Installation

2.1 Location

To receive GNSS signals the Time Server's antenna must be located in a location where it can “see” the sky. The GNSS module itself is highly sensitive and able to “see” the GNSS satellite signals from within many RF transparent structures. Multi-Story or metal structures will likely block the GNSS signals such that the antenna must be located elsewhere. In these cases, the GNSS antenna may be located in a window. Best function, with quickest lock time, is achieved with a roof mounted outdoor antenna with an unobstructed 360 degree view of the sky. The Time Server box can be located anywhere on the network. All that is required is power and a wired network connection.

2.2 Connections

2.2.1 Antenna

The GNSS antenna is connected through the circular female SMA GPS connector on the rear of the Time Server. By default, the GNSS antenna connection provides 5.0V to power the LNA in the GNSS antenna. This is correct for the supplied GNSS patch antenna with the magnetic base. This voltage can be changed with a jumper on the inside of the Time Server. The Time Server has to be opened up and a jumper moved.

Jumper J8 A: 3.3V B: 5.0V (default)

The only time this jumper would be changed would be to allow use of a different antenna that requires +3.3V max for the LNA in the antenna. The TM3000 also has an antenna current monitor that can be used to detect if the GNSS antenna has been disconnected.

2.2.2 Power – 5.5mm

A +12V international power supply is supplied with the unit. Connect to your local power outlet and the barrel connector to the rear of the Time Server. The time server will begin trying to find the GNSS satellites. On power-up, synchronization to the GNSS satellites will take several minutes and depends heavily on the signal strength and number of GNSS satellites in view of the antenna. No battery backup of position is provided to allow for a warm start so the Time Server is always starting from scratch in determining its location to achieve GNSS lock.

2.2.3 Power – 2 Pin Plug

A two pin plugin power connector is also provided with a removable screw terminal block. This can be used to connect other power sources to the TM3000 without having to use the 5.5mm / 2.5mm barrel connector. This input is in parallel with the 5.5mm barrel connector and supports up to 48V DC.

2.2.4 Network

Connect the 10/100/1000 RJ45 port(s) on the back of the Time Server to a network connection. Verify that the network settings are correct for your system. See the configuration section of this manual for more information on doing this. The front LCD display can be used to see what the current IP address

setting are.

2.2.5 Serial

The serial port is connected by a USB-C type connector and will enumerate as a COM port on most modern operating systems. It is an output only port used for some basic status information. No configuration of operating system access is possible through this port. It is setup as 115200,n81.

2.2.6 PPS

The PPS output is a 3.3V logic output driven by the DPLL hardware and derived from the 1PPS output of the GNSS receiver through a DPLL. It is a 50% duty cycle output where the positive rising edge denotes the second boundary. The GNSS receiver 1PPS output is specified at +/20 nano-seconds. Best results are achieved with an outdoor antenna with a full 360 degree view of the sky. Degraded signal quality will degrade the precision of this output. Note that configuring different constellations of satellites between servers will result in offset from each other, as such best synchronization between multiple units is achieved by having them all set to view the same group of satellites.

2.2.7 10MHz

The 10MHz output is a 3.3V logic signal driven by the DPLL hardware and derived from the frequency corrected internal OCXO. It is synchronized to the 1PPS such that it will have a positive rising edge that corresponds to the rising edge of the 1PPS signal.

2.2.8 Front Panel Indications

The front panel of the Time Server is upgraded from the previous products. Four LEDs show the current GNSS lock status of the unit. The “POW” LED indicates that the unit is connected to power. By default to serve time, GNSS lock is required.

Additional information is displayed on the 2 line LCD display. The Select button can be pressed to move through the different displays including internal UTC time, GPS status and top 4 Sat SNR value average. Other screens display networking information.

2.2.9 Parameter Reset

Most parameters of the device can be reset by pressing and holding the Select button for 5 seconds. Follow the display prompts to confirm the desired reset function.

2.2.10 GNSS Lock Sequence and Holdover

The GNSS lock process proceeds through several steps and can be followed by watching the front Yellow LEDs, 2D, 3D, and PPS. Initially, when no lock is present, the Yellow LEDs will be OFF. When a 2D lock is achieved, the 2D LED will turn on. This is the first stage of GNSS lock process. Next the 3D LED would typically turn ON, indicating a better lock. 3D lock is recommended for PTP

time serving, and pretty much required for accurate 10MHz/1PPS outputs. The PPS indication will begin blinking one time per second when the PPS signal is received from the GNSS module.

It is also possible for the 2D/3D LEDs to turn off, after a GNSS timing lock has occurred and the PPS LED continues to blink. This signifies that the TM3000 has an accurate internal time and is serving time in holdover mode, which will also be indicated on the display. The TM3000 is still trying to re-establish the GNSS lock because it was lost for some reason.

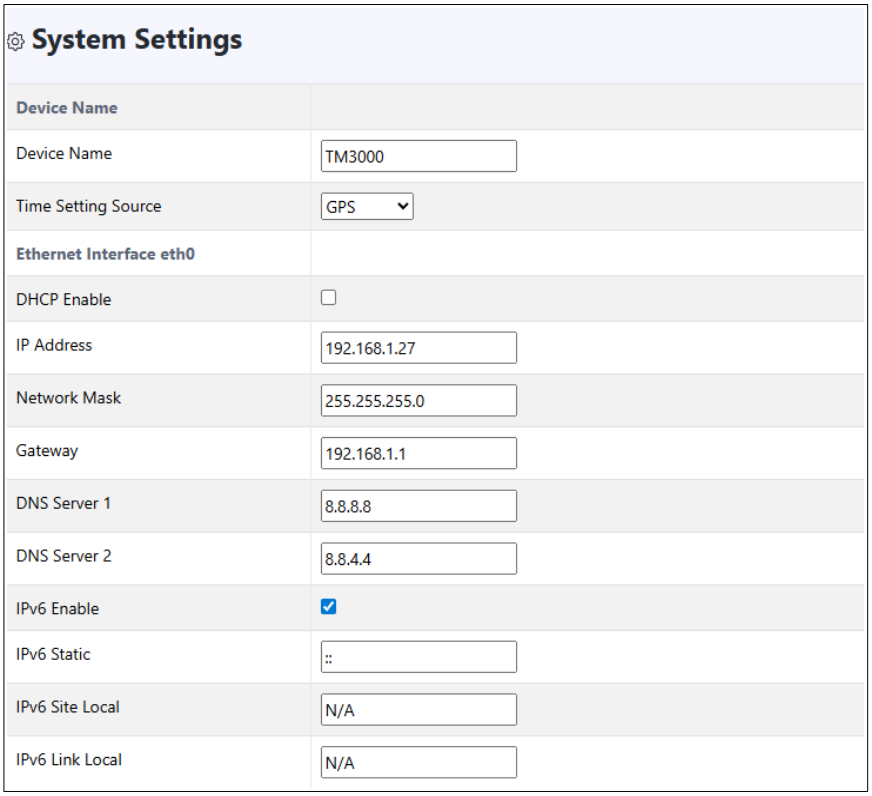
3 Configuration

3.1 Web Page – Default username/password is "admin/tmachine"

3.2 Default IP address is 192.168.1.27 / 10.1.1.28

All Time Server parameters are accessed on the configuration web page. The page can be accessed by pointing any web browser at the IP address of the Time Server. The initial IP address is 192.168.1.27 / 10.1.1.28 from the factory.

3.3 System Settings Page – eth0 section



3.3.1 DeviceName

This is a generic entry that has no effect on the TM3000 operation other than to allow the user to enter a name for the device to help recognize it when parameter updates are required.

3.3.2 Time Setting Source

This pulldown has three options that allow the source time for the device to be GNSS, Peer NTP, or Manually set. The GNSS is always scanning such that if the device is set to run from Peer NTP or Manually set, the GNSS antenna is typically left disconnected.

3.3.3 eth0-DHCP Enable

When checked, the eth0 interface will attempt to set its IP parameters from a DHCP server. The LCD display can be used to determine the resulting address assignment. Generally, a time server is assigned statically, or at least statically through the DHCP server such that its IP address is constant.

3.3.4 eth0-IP Address

The IP address of the unit is set by entering a standard IPv4 dotted quad in this field. 192.168.1.20 or

10.10.0.96 are examples of acceptable formats for this field. Clicking the Save Changes button will set the entered IP parameters.

3.3.5 eth0-Netmask

The Netmask entry determines what addresses are on the local network and what addresses are reached through the Gateway. Typical Netmasks are 255.255.0.0 or 255.255.255.0. Consult the network administrator for more information on how this entry should be set. Clicking the Save Changes button will set the entered IP parameters.

3.3.6 eth0-Gateway

The Gateway IP address is used when a destination address is determine to not be on the local network. Consult the network administrator for this setting. Clicking the Save Changes button will set the entered IP parameters.

3.3.7 eth0-DNS1 and DNS2

Enter the IP addresses for the DNS servers on your network.

3.3.8 eth0-Enable IPv6

Setting this option to Enable will turn on support for IPv6 in the device. This includes SNMP, NTP, Web, and PTP. Currently, the TimeMachines Locator protocol is not setup to support IPv6.

3.3.9 eth0-IPv6 Static

This entry is user editable and can be set to any valid IPv6 address. Routing and communication on the local network are assumed.

3.3.10 eth0-IPv6 Site Local

The Site Local address is the equivalent to a private address in IPv4. It is technically a deprecated feature, but is typically provided by a router on the local network and starts with FEC0. This is not user editable

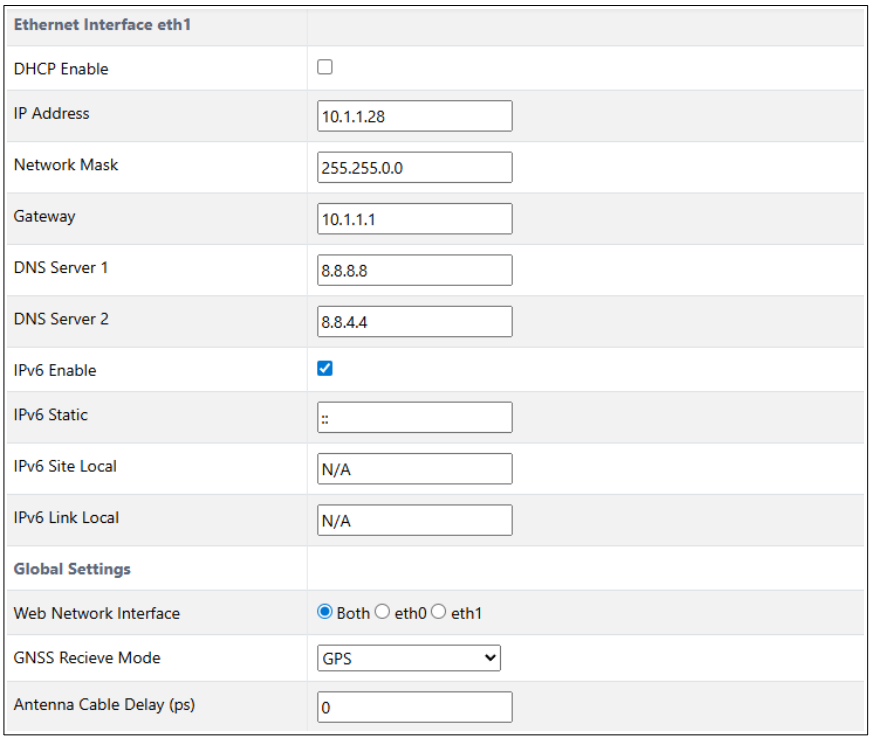
3.3.11 eth0-IPv6 Link Local

The Link Local address is derived from the MAC address of the device. This address is not forwarded by routes but does allow computers on the same network link to communicate via IPv6. This is not user editable

3.4 System Settings Page – eth1 section

3.4.1 eth1-DHCP Enable

When checked, the eth1 interface will attempt to set its IP parameters from a DHCP server. The LCD display can be used to determine the resulting address assignment. Generally, a time server is assigned statically, or at least statically through the DHCP server such that its IP address is constant.



3.4.2 eth1-IP Address

The IP address of the unit is set by entering a standard IPv4 dotted quad in this field. 192.168.1.20 or 10.10.0.96 are examples of acceptable formats for this field. Clicking the Save Changes button will set the entered IP parameters.

3.4.3 eth1-Netmask

The Netmask entry determines what addresses are on the local network and what addresses are reached through the Gateway. Typical Netmasks are 255.255.0.0 or 255.255.255.0. Consult the network administrator for more information on how this entry should be set. Clicking the Save Changes button will set the entered IP parameters.

3.4.4 eth1-Gateway

The Gateway IP address is used when a destination address is determine to not be on the local network. Consult the network administrator for this setting. Clicking the Save Changes button will set the entered IP parameters.

3.4.5 eth1-DNS1 and DNS2

Enter the IP addresses for the DNS servers on your network.

3.4.6 eth1-Enable IPv6

Setting this option to Enable will turn on support for IPv6 in the device. This includes SNMP, NTP, Web, and PTP. Currently, the TimeMachines Locator protocol is not setup to support IPv6.

3.4.7 eth1-IPv6 Static

This entry is user editable and can be set to any valid IPv6 address. Routing and communication on the local network are assumed.

3.4.8 eth1-IPv6 Site Local

The Site Local address is the equivalent to a private address in IPv4. It is technically a deprecated feature, but is typically provided by a router on the local network and starts with FEC0. This is not user editable

3.4.9 eth1-IPv6 Link Local

The Link Local address is derived from the MAC address of the device. This address is not forwarded by routes but does allow computers on the same network link to communicate via IPv6. This is not user editable

3.4.10 Web Interface

The webserver in the TM3000 can be set to listen to both the eth0 and eth1 network ports, or to a specific port. This is useful if the device is tied to a network where time is served, but configuration of the device should not be allowed.

3.4.11 GNSS Receive Mode

This pulldown allows selecting which GNSS systems the device will listen to. Not all combinations are possible. If a good antenna location, for example rooftop with a 360 degree view of the sky is installed, GPS is sufficient for excellent operation.

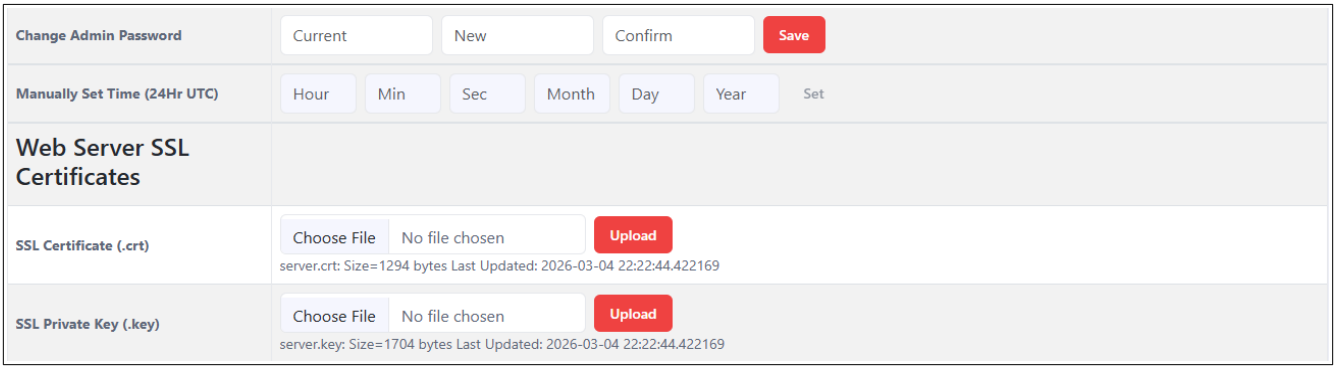
3.4.12 Antenna Cable Delay (ps)

This entry is to compensate for cable delay introduced by the antenna cable. The value is in pico seconds. The Delay, in pico-seconds, through a cable is D=(L*C*1000)/V. Where:

- L is the cable length in feet
- C is a constant based on the speed of light, adjusted for feet: 1.016
- V is the velocity of propagation for a a specific cable. The cable datasheet is the source for this. The LMR-195/RG-58 sold by TimeMachines has a value of 0.77.

When multiplied out, the delay for the TimeMachines sold cable is 1319 pico-seconds per foot. Determine the total length of cable between the TM3000 SMA jack and the antenna in feet, multiply it by 1319 and enter that value in this field. This is only important for phase alignment of the 1PPS and 10MHz outputs and has no effect on the NTP/PTP accuracy.

3.5 System Settings Page – Other



3.5.1 Change Admin Password

This section of the page is used to change the admin password. The old password is entered followed by two copies of the new password. Clicking the Save button on that row will update the password. Note that the username 'admin' cannot be changed. The maximum length of the password is 16 characters.

3.5.2 Set TM3000 time manually

This set of fields allows the TM3000 to have its time set manually from the web page. Entering the UTC time of day, 24 hour mode, and clicking the Set Time button below the fields will set the time of the TM3000 accordingly and enable the NTP server software to responds to requests from clients. Holdover settings have no effect when the time has been set manually. If at any point the GNSS gains a lock, then the manual mode will be overridden. To use this option, the device must be set to Manual Time Mode in the System Settings.

3.5.3 Web server SSL Certificates

The TM3000 supports https functionality. A set of default certificates are installed on the device but because they are generic, the user will generally be alerted that the connection isn't private. This is a common occurrence for https devices used primarily on private networks. This occurs because the certificate will not match the assigned device name/IP address and there is no way to confirm the certificate. Allowing the connection in the browser session will make the encrypted web connection. The user has the option of providing their own certificate and key files to enable a smoother interface interaction. Select the correct SSL Certificate and Key file from the local machine and upload them. A reboot is required to start using them. The process to create the certificate files, and to get rid of the browser warning messages, is more or less the same for Linux and Windows, but is shown here for Linux. See openssl documentation for more details about how this is done. This example is similar to the one used for secure NTP. The major difference is the addition of the subjectAltName (SAN) information that allows a browser to lookup and trust the certificate eliminating the security risk notifications. This uses ntptest1.timemachinescorp.com, the user should use whatever their organization needs.

Step 1 – Create the certificate files using openssl

Command line: `openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout server.key -out server.crt -addext "subjectAltName=DNS:ntptest1.timemachinescorp.com"`

```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Nebraska
Locality Name (eg, city) []:Lincoln
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TimeMachines
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:ntptest1.timemachinescorp.com
Email Address []:.
```

This command will create a server.crt and server.key output to the local directory.

Step 2 – Add to local repository of trusted certificates

In Linux, moving it to trusted certs directory involves using the ca-certificates package. Exact directories may be different with different Linux flavors. Start by moving it to /usr/local/share/ca-certificates.

```
sudo cp server.crt /usr/local/share/ca-certificates/
```

Then update the local certificates store.

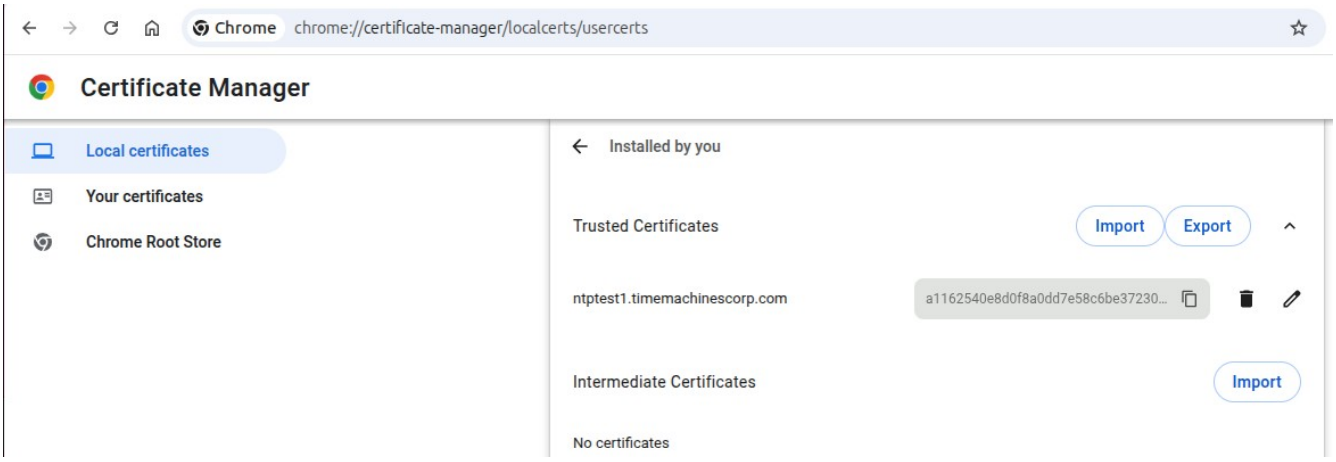
```
sudo update-ca-certificates
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
Updating Mono key store
Mono Certificate Store Sync - version 6.8.0.105
Populate Mono certificate store from a concatenated list of certificates.
Copyright 2002, 2003 Motus Technologies. Copyright 2004-2008 Novell. BSD licensed.

Importing into legacy system store:
I already trust 147, your new list has 148
Certificate added: C=US, S=Nebraska, L=Lincoln, O=TimeMachines, CN=ntptest1.timemachinescorp.com
1 new root certificates were added to your trust store.
Import process completed.

Importing into BTLS system store:
I already trust 148, your new list has 148
Certificate added: C=US, S=Nebraska, L=Lincoln, O=TimeMachines, CN=ntptest1.timemachinescorp.com
1 new root certificates were added to your trust store.
```

```
Import process completed.
```

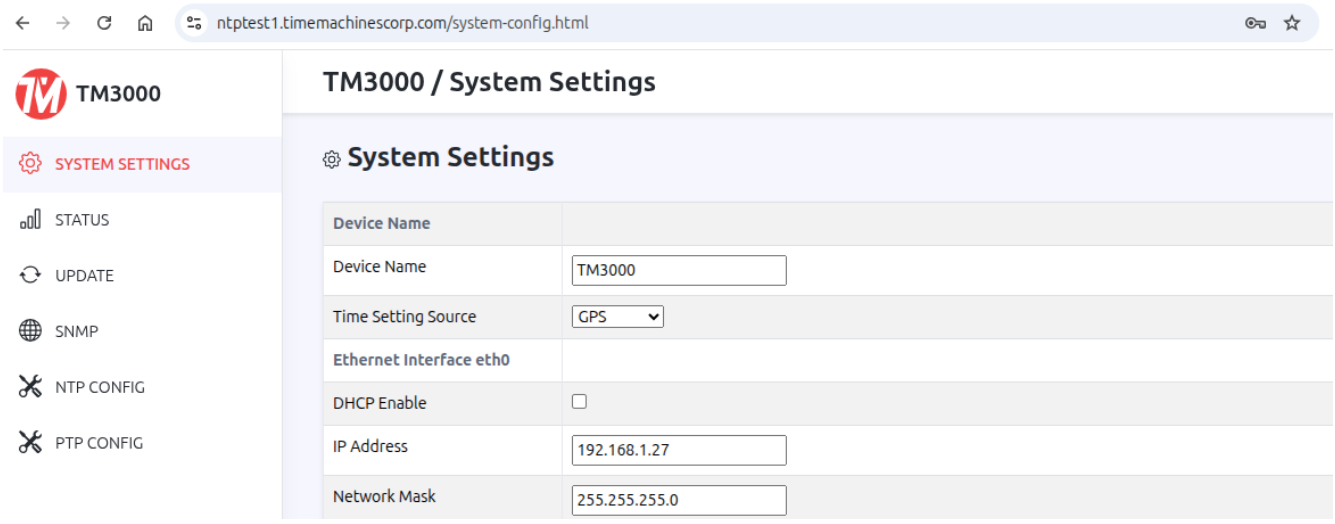
The certificate is now part of the list of trusted certificates on the local machine.

Step 3 – Getting rid of browser security warnings

While the web traffic is encrypted, the browser warning message can be tedious. To get rid of the browser certificate warnings when the device is accessed, the same certificate needs to be imported in to the browser itself. On Chrome that is done by connecting to chrome://settings/certificates and importing the server.crt file created in the first step. Other browsers will have similar processes, see their documentation for specifics. Import into the Trusted Certificates section, should look like below when done.



Once that is done, and the browser is restarted, connecting to the time server should look like (no red https://) below. Note that in this example, a DNS entry for ntptest1.timemachinescorp.com was created to point to the IP address of the TM3000.



3.6 Status Page

The status page is an information only page. It shows the various pieces of information about the current working state of the device.

Status	
Time Source	GPS
Location	40.81060,-96.62745 Altitude: 395.332m
Date/Time	Thu Mar 5 21:22:33 UTC 2026
Satellites Used	10
GPS Fix	3D
NTP Lookups	132885
eth0 MAC Address	1E:3F:5F:8F:00:03
eth1 MAC Address	1E:3F:5F:8F:00:04
Uptime	0 days 22 hours 59 minutes 38 seconds
Holdover Time	0
OCXO Correction	-2.3356 Hz Save Reset
DPLL Status	Inputs: OCXO 1PPS Outputs: PPS 10MHz Sysclk: LOCK STABLE CALIB
DPLL Temp	45 C
Antenna Current	0 mA
Serial Number	A300002260005
Firmware Version	v0.1.1-MX93

3.6.1 Time Source

This field displays the current source of time. It can be GNSS, Peer Time Server, or Manually set.

3.6.2 Location

Location shows the latitude and longitude of the device itself based on the GNSS receiver. Paste this set of coordinates into Google Maps to see your location.

3.6.3 Date/Time

The Date/Time entry shows the current UTC date and time of the device. This is not updated realtime. Refreshing the page will update this time. Note that it is the clients responsibility to adjust for

timezone and daylight savings adjustments. Time servers always operate in UTC for NTP and TAI for PTP.

3.6.4 Satellites Used

This shows the current number of satellites that are in view and locked by the GNSS receiver.

3.6.5 GNSS Fix

This displays the level of the current GNSS lock.

No GNSS Fix – Check cable connections. If connected correctly, likely the antenna needs a better view of the sky. Obstructions, building materials, window tinting can all cause possible signal issues.

2D - GNSS satellites found.

3D – Required for serving time.

3.6.6 NTP Lookups

This field updates on a page reload and shows how many NTP time requests have been requested from client devices.

3.6.7 eth0/eth1 MAC addresses

This is an information only field and displays the MAC addresses for each of the Ethernet ports of the Time Server.

3.6.8 Uptime

Time elapsed since last boot up.

3.6.9 Holdover Time

When the GNSS lock is lost and time is being served by the internal OCXO, this will show the amount of time in minutes that the holdover state has been active.

3.6.10 OCXO Correction

This field shows the frequency correction being applied to correct the OCXO back on to its root frequency. This value can be saved or reset from this web page. The purpose of saving this value, after the device has run for a period of a couple hours with 3D lock, is to give a more accurate starting point for the correction algorithm to begin on power up. If for some reason the value seems wrong or not working, a Reset is allowed that will, after a reboot, start the algorithm from default and restart the correction process.

If using the TM3000 for manual PTP time generation (at the time of this writing NTP time is not served based on the OCXO) having the device on the GNSS for a period of time to determine the correction, then saving it, will dramatically improve drift of the TM3000 when operated without GNSS reception. The Reset button resets the OCXO to its starting point to restart the convergence process. Once locked again, the setting can be Saved.

3.6.11 DPLL Status

This line on the Status web page give a quick view of the Inputs, Outputs, and Clock quality of the

Digital PLL (DPLL) in the TM3000. The items will be colored either Red or Green. Red meaning the input or output is not locked and stable, Green meaning the input or output is locked to the clock.

- Sysclk status information is information about the internal operation of the DPLL. These typically go green almost immediately upon startup of the device and short of some hardware failure, will be green any time they are checked by the Status page reload.
- Inputs to the chip are the OCXO, which will be stable to the DPLL essentially from the startup of the device. The 1PPS however, will stay Red until some time after the GNSS locks to the satellites in view. At least a 2D lock is required before the 1PPS input will go to Green.
- Outputs, which are dependent on both the OCXO and 1PPS inputs will stay red until both inputs are stable. Once these outputs turn green on the Status page, their respective output signals will be present on the SMB connectors. The DPLL does require a little bit of time after 2D lock to converge and start outputting signals.

3.6.12 DPLL Temp

This is the temperature of the Digital PLL chip on the TM3000 circuit board. It has an operation range of -40C to +85C.

3.6.13 Antenna Current

This displays the approximate current being delivered to the antenna. If an antenna is connected, this should not be 0 mA. Note that a DC blocked antenna will read 0mA for this field.

3.6.14 Serial Number

The serial number of the TM3000

3.6.15 Firmware Version

Displays current software version running on device.

3.6.16 Satellites

GPS Satellites

Satellite ID	11	12	6	21	25	5	48	17	29	19	9	4
Satellite SNR	48	48	47	47	46	45	44	39	39	38	35	27

NTP Peers

Peer IP	Mode	State	Stratum	Reach	Poll	Last Update (sec)	Offset	Error
NMEA	Local	Unused	0	377	4	13	+412.3ms	±100.0ms
PPS	Local	Source	1	377	4	13	-389ns	±351ns

PTP Clients

Client IP	MAC Address	Lease (Sec)	Announce Interval	Sync Interval	Interface
192.168.1.12	00:1b:21:66:d1:6d	1000	-2	-2	eth0
10.1.1.21	00:1b:21:66:d1:6f	1000	0	0	eth1

These tables shows the current list of locked satellite numbers and their signal strengths (SNR). When receiving multiple constellations, a table will be here for each. Refreshing the web page updates the table to their current values.

3.6.17 NTP Peers

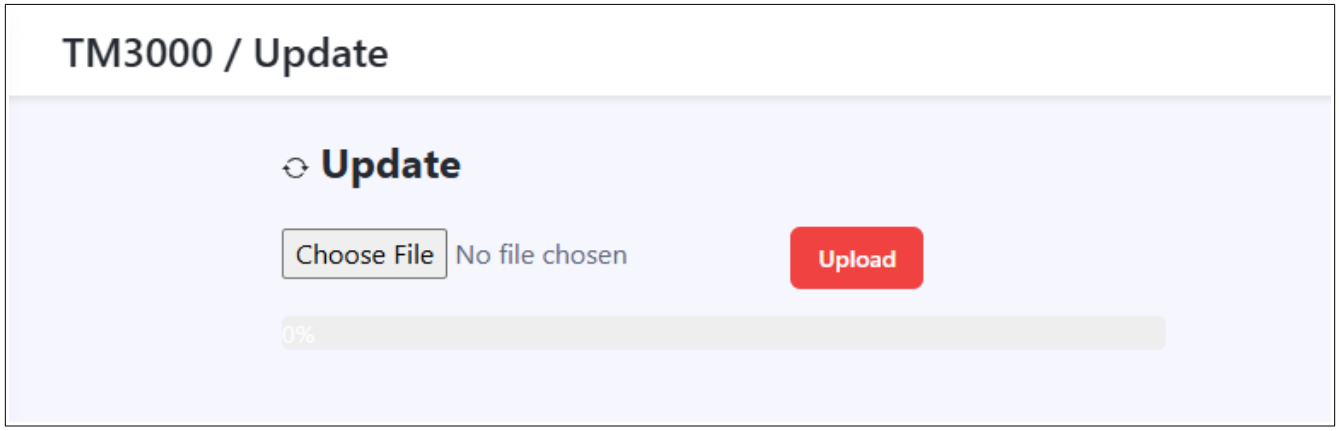
If time is being updated from a Peer time server, then this table shows the current list of Peer servers that are being checked to maintain the time in the TM3000. Several Fields are displayed for each time server.

- Peer IP – The Peer IP address is the first field displayed. Depending on the active time set mode, the GNSS module may also be listed as NMEA and PPS. Otherwise, the IP address of the external NTP server will be listed. Note that if 127.127.1.1 is listed, that is to enable the NTP server software to serve time from the internal real time clock.
- Mode – This tells the type of source being tracked
- State – This reports whether the source is being used, monitored, or potentially ignored
- Stratum - This field shows the stratum level being reported by the peer time server
- Reach – This is a base 8 bit field that shows the result of the last 8 lookup attempts of the peer time server. A value of 377 signifies that the last 8 attempts have been answered by the time server. A successful lookup causes a 1 to be shifted in to the LSB of the right digit and all other bits to be shifted 1 bit to the left. A non 377 value signifies that either the server has just started or that some lookup requests are not getting answered.
- Poll – This value is the exponent of 2^X and is the approximate time between time requests. For example, a value of 5, means that it is roughly 32 seconds between request for peer time.
- Last Update – This the time in seconds since the last time the source was queried for time
- Offset – This is the offset of the peer time servers' time when compared to the internal clock of the TM3000.
- Error – This shows the range of the values being received compared to the internal time.

3.6.18 PTP Clients

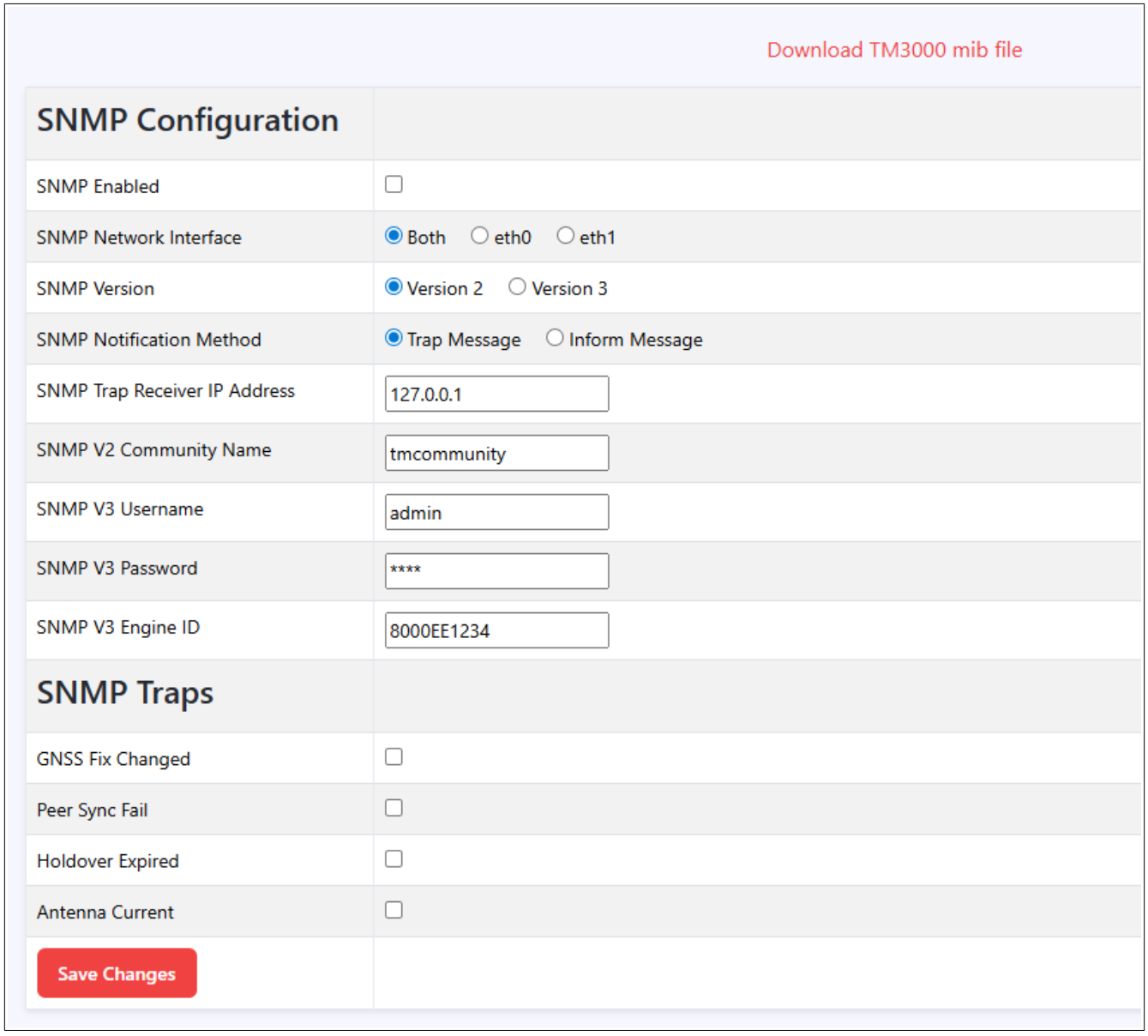
This area is used to show the current PTP clients that have successfully logged into the device for unicast PTP. This will display entries only if the TM3000 is in Unicast PTP mode. In multicast mode, the TM3000 does NOT keep track of all clients getting time from it. The client's IP address, MAC address, lease time, and update rates (1/2^value) for Announce and Sync packets is displayed. The zero values for Announce and Sync Intervals show a 1 packet per second rate. It also lists which interface the PTP stream is using.

3.7 Update Page



The update page is used to update firmware of the unit. The firmware updates will be archived and available for download from the timemachinescorp.com website. Save the file to the local computers drives. The file type that is used for the update is a .zst file which is compress. Browse to it using the Choose File button on the Update Page. Once the file is found the update can begin. This process takes about 5 minutes and power should not be removed during the process or the device may require a different method to recover. The LCD display will also show some status messages. Once completed, the unit will reset and resume operation. Login to the device with a web browser to confirm the version update. It is likely some settings will be lost during update to avoid incompatibilities with the updates. The IP addresses are expected to be kept, but ALL other settings should be checked after update and potentially resaved.

3.8 SNMP Setup



3.8.1 MIB File-Download TMI-TM3000-SHI.txt

At the top of the page, is the option to download the MIB file for the TM3000. This is useful in many monitoring systems. It will download to the browsers default download directory.

There are currently 4 supported trap notifications: GNSS Fix Changed, Peer Sync Fail, Holdover expired, and Antenna Current.

3.8.2 Enable

This will enable the SNMP application to startup after bootup, or once enabled in real time.

3.8.3 SNMP Network Interface

The TM3000 can be set to listen on both, or one specific interface for SNMP requests. The interface used for trap messages will be determined by the IP address settings on the TM3000 and the correct routing.

3.8.4 SNMP Trap Version

This sets the version to SNMPv2 or SNMPv3. It affects format of the trap/inform messages in the next option. If set to V2, then the trap/inform message will only identify itself with the community name with no other security features. The V3 mode supports a username/password combination and encryption using OpenSSL. The encryption is set for SHA and AES.

3.8.5 Notification Method

This sets the notification method to either Trap or Inform. A Trap message is an un-acknowledged status packet, while the Inform message is acknowledged by the receiver. The Inform message creates a higher reliability that the receiver received the packet and can act on it. The Trap method is also widely used. Version 2 of these messages is a simpler format and setup, without the username/password authentication. Version 3 will require the username and password to be setup on the SNMP web page, as well as using the Engine ID setting to synchronize the encryption when using Trap messages. Version 3 messages are encrypted with SHA and AES.

Trap/Inform messages are status checked every 30 seconds.

3.8.6 Trap Receiver IP Address

Enter the IP Address of the device being used to receive the trap/inform packets

3.8.7 SNMP V2 Community Name

The SNMP community name is used as a simple authentication for Version 2 SNMP packets.

3.8.8 SNMP V3 R/W User Name

Enter the desired SNMPv3 username.

3.8.9 SNMP V3 R/W Password

Enter the SNMPv3 password associated with the username.

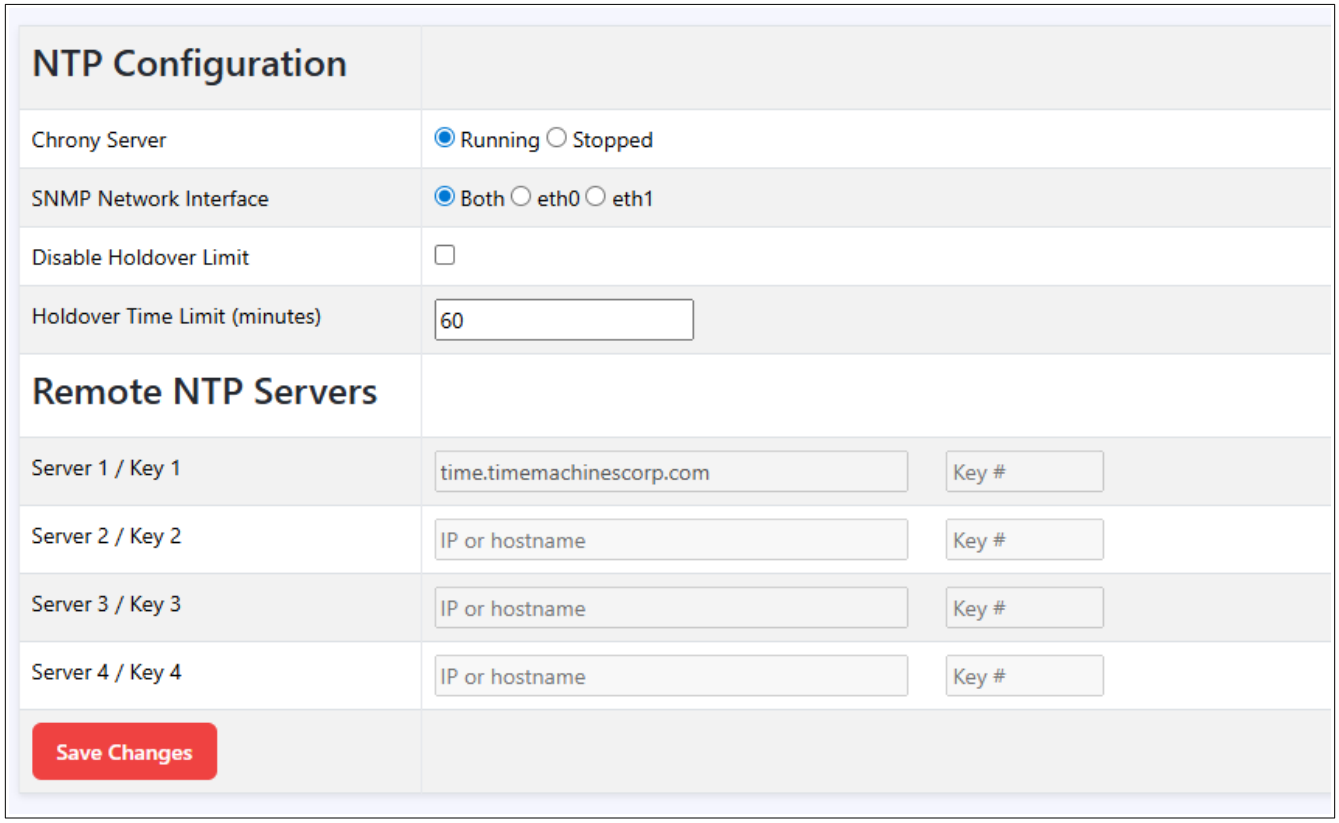
3.8.10 SNMP V3 Engine ID

When using SNMPv3 Trap messages, the engine ID needs to match between the trap receiver and the TM3000 as the sender. This entry specifically allows setting of the SNMP engineID. This is handled in this way because the bulk of the file system for the TM3000 is not R/W and parameters that are updated by the SNMP daemon are stored in RAM and lost on a power cycle/reboot. A reboot may be required when setting up Trap/Inform messages.

3.8.11 SNMP Traps

The four checkboxes allow selective enable of the four different trap notification messages. If running on GNSS as a time source, selecting the Peer Sync Fail option is not needed. If the antenna connection is DC blocked, monitoring the Antenna Current will not be useful.

3.9 NTP Settings Page



The NTP Settings page is used to control the function of the NTP client and server options of the TM3000.

3.9.1 Start / Stop NTP Server

The NTP daemon (Chrony) can be started and stopped from this page. By default, NTP support is enabled. Click the desired option and then click the Save Changes button. Once a time source is available, GNSS, Peer, or Manually Set, the TM3000 will enable the NTP server service and NTP requests will be serviced.

3.9.2 Disable Holdover Limit

When checked, this option allows the holdover limit of the device to extend forever. The TM3000 requires a GNSS lock, peer server, or manual time set, to initially set its time, but by checking this option, it can then be run without a GNSS lock. The time WILL drift off of standard at a rate that is dependent on the accuracy of a crystal in the device, but this option is included for cases where exact accuracy isn't required, just synchronization of devices withing a closed system. ***This setting also governs the holdover behavior of the PTP modes.***

3.9.3 NTP Holdover Time (Minutes)

This setting is used to set how long holdover is allowed GNSS lock is lost. The device will shutdown the NTP time service when the set holdover time is expired and GNSS lock is not achieved.

3.9.4 Remote NTP Servers Enable

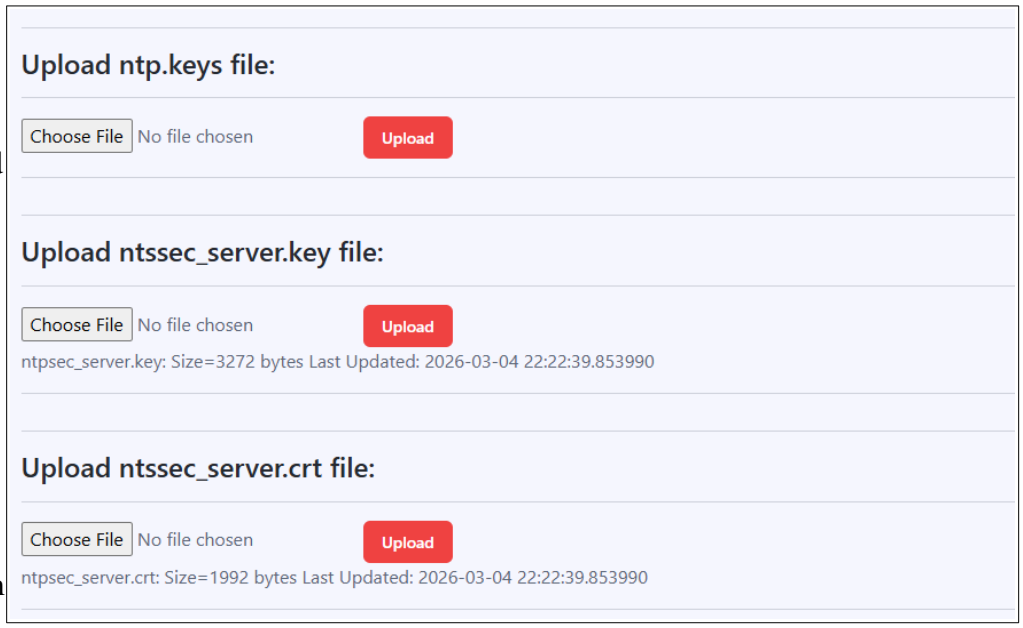
Enable this mode in the System Setting→Time Setting Source→Peer NTP. Once that is done, setting a list of remote NTP servers will allow the TM3000 to get its time from another NTP server using the NTP protocol. When operating in this mode, the TM3000 can begin serving time shortly after it has booted up because it doesn't have to wait for the GNSS to lock. It will also allow the TM3000 to operate without a GNSS at all if desired. If at some point after boot up, GNSS lock is obtained, then the GNSS becomes the time source, but Peer NTP lookups will continue and there can be conflicts. It is best to only operate in the intended mode.

3.9.5 Remote NTP Servers List

The NTP Servers list allows setting of up to three different time sources. The TM3000 runs a version of Chrony that will select the "best" source for setting its time, but will also keep tabs on all of the time sources. If authentication is being used, a key value, 1-65535 can be entered into the key field on the same line as the server.

3.9.6 Upload ntp.keys file

The NTP server of the TM3000 supports the authentication option. MD5, SHA1, SHA2 (256, 384, and 512), and AES-CMAC (128, 256) hashes are supported. This maintains the compatibility required of most NTP clients requiring authentication and allows the stronger modern hashes to be used.



A standard ntp.keys file can be uploaded through this page. Simply choose the file to upload from your local computer and allow the upload to complete. This is a one way transaction, there is no way to pull the ntp.keys file from the TM3000 back to the local browser.

The Chrony documentation can be found here: https://chrony-project.org/doc/latest/chrony.conf.html, see the keyfile section of the page. The allowed formats for the key file are as follows (this is the default key file in the device):

```
#
#ntp.keys file
#
#Multiple types of keys supported, MD5 (default, or M) and SHA1, SHA256, SHA384, SHA512, AES128, AES256
# also AEAD keys supported, but not documented here
#Keyformat A or ASCII (default) the key is an ascii text string
#   H or HEX: Key is hexidecimal string
#Line Format:  Key # <space> Key Type <space> Key
```

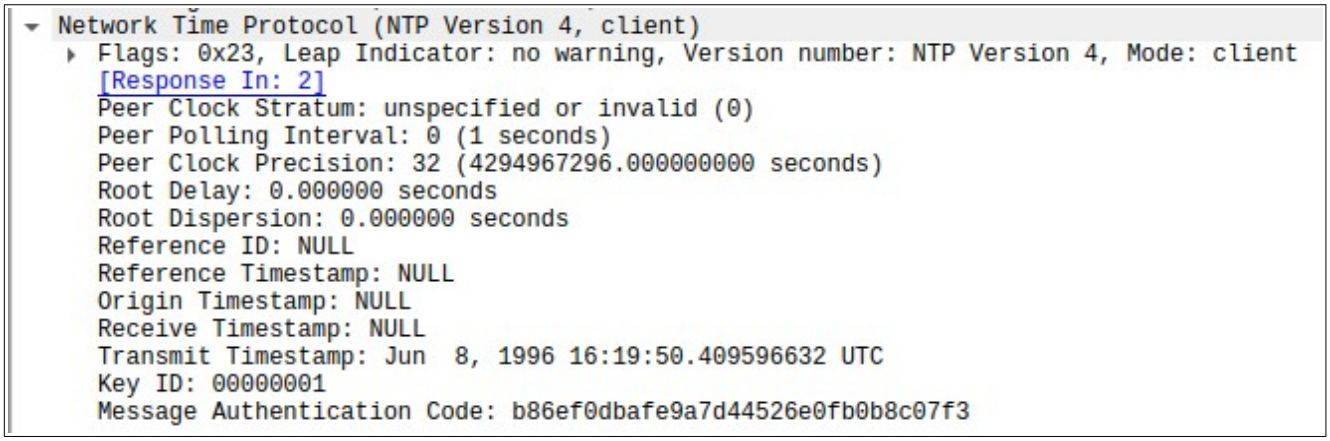
```
#Key# is a positive integer number greater than 0
#Key:  For MD5 is a character string 1-32 character ASCII String, or for SHA a 40 character hex string
#See chrony documentation for more details
#Examples:
1 tmachine
2 SHA256 MySecretKey
3 SHA1 HEX:D5C9F80F7B1220D9710049AE41FB5BB5B18D148E
10 SHA256 my_secure_passphrase
11 SHA256 HEX:2666B8099BFF2D5BA20876121788ED24D2BE59111B8FFB562F0F56AE6EC7246E
12 AES128 HEX:2DA837C4B6573748CA692B8C828E4891
13 AES256 HEX:2666B8099BFF2D5BA20876121788ED24D2BE59111B8FFB562F0F56AE6EC7246E
```

The ntp.keys file is created in a text editor on a computer. The resulting ntp.keys file is then uploaded to the TM3000 by finding the file and clicking the upload button on the web page. A matching copy of the ntp.keys file will need to be present on the client device, or remote server if the Peer Time Server mode is being used. All of the above modes are supported by Chrony on both ends. The NTPD implementation didn't support the AES keys as of the last update of this manual.

When setting up an NTPD implementation, the ntp.conf file on the server will need to include directives to load the key file and authorize them. The basic lines in the ntp.conf file are:

```
keys /etc/ntpsec/ntp.keys
trustedkey 1
requestkey 1
controlkey 1
server 192.168.1.27 iburst key 1
```

A packet capture from Wireshark is shown below. The last two lines show the addition to the packet to support authentication. The Key ID and the Authentication Code are appended to a standard NTP formatted packet.



There are many tutorials on the Internet that discuss setting up authentication on the NTPD implementation. Other clients supporting authentication will have other instructions to follow.

3.9.7 Network Time Security (NTS) certificates

The TM3000 also supports the NTS protocol, which provides a modern cryptographic security protocol for NTP. It is based on the widely used standard TLS protocol for key exchange. The setup of this fully secured NTP protocol requires certificates be uploaded to the device that match the name it will be referenced from. The example that follows utilizes a DNS entry that corresponds to

ntptest1.timemachinescorp.com which points to 192.168.1.27, which is the eth0 port of a TM3000. The server must utilize a Fully Qualified Domain Name (FQDN), an IP address alone won't work.

The first step is to create a set of certificates that has the name ntptest1.timemachinescorp.com embedded in it such that it matches the device network name. Openssl can be used for this purpose. Please note, this information is intended as guideline to get the customer started. TimeMachines is unable to walk customers through this process. It can be involved and take some iteration to get working. There is a significant amount of information available on the Internet about how to do this.

Step 1 – generate the server key and certificate files:

Command Line: `openssl req -x509 -nodes -days 3650 -newkey rsa:4096 -keyout ntpsec_server.key -out ntpsec_server.crt`

```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Nebraska
Locality Name (eg, city) []:Lincoln
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TimeMachines
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:ntptest1.timemachinescorp.com
Email Address []:.
```

It is the .key and .crt files which must be uploaded to the TM3000 through the webpage. Finding the files, selecting them, and finally uploading them is all done with the respective buttons.

Step 4 – Client certificates

The client end of this connection will also use the public certificate previously generated. The .crt file must be added to the list of trusted certificates on the client device. In Windows this is done with mmc, in Linux use the ca-certificates package. In general, the certificate file will be copied to /usr/local/share/ca-certificates and then the update-ca-certificates command will be used to update the consolidated certificate file located at /etc/ssl/certs. This may be different on some distributions but is well documented on the Internet.

Step 5 – ntpd or other client setup

The major entries in the ntp.conf file, which may live in different locations for the ntpsec version of ntpd are:

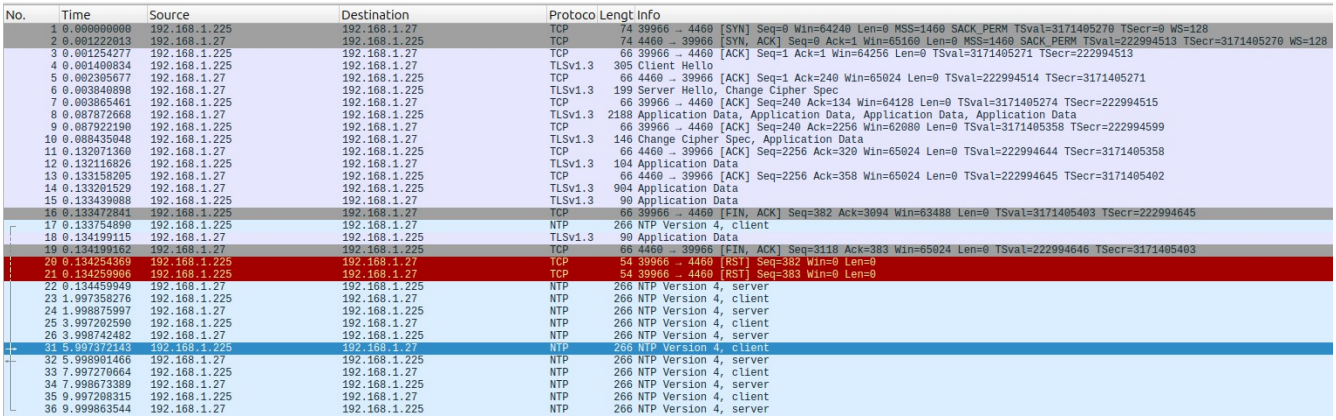
nts enable

nts cert /etc/ntpsec/ntpsec_server.crt

nts key /etc/ntpsec/ntpsec_server.key

server ntptest1.timemachinescorp.com iburst nts

The ‘nts’ is the setting that tells the ntpd/ntpsec client to connect using encryption utilizing the installed certificates. The below Wireshark capture shows the typical startup of the ntpd/ntpsec daemon in Linux where the initial TLS based key exchange is completed and then the encrypted NTP packets are passed shortly after.



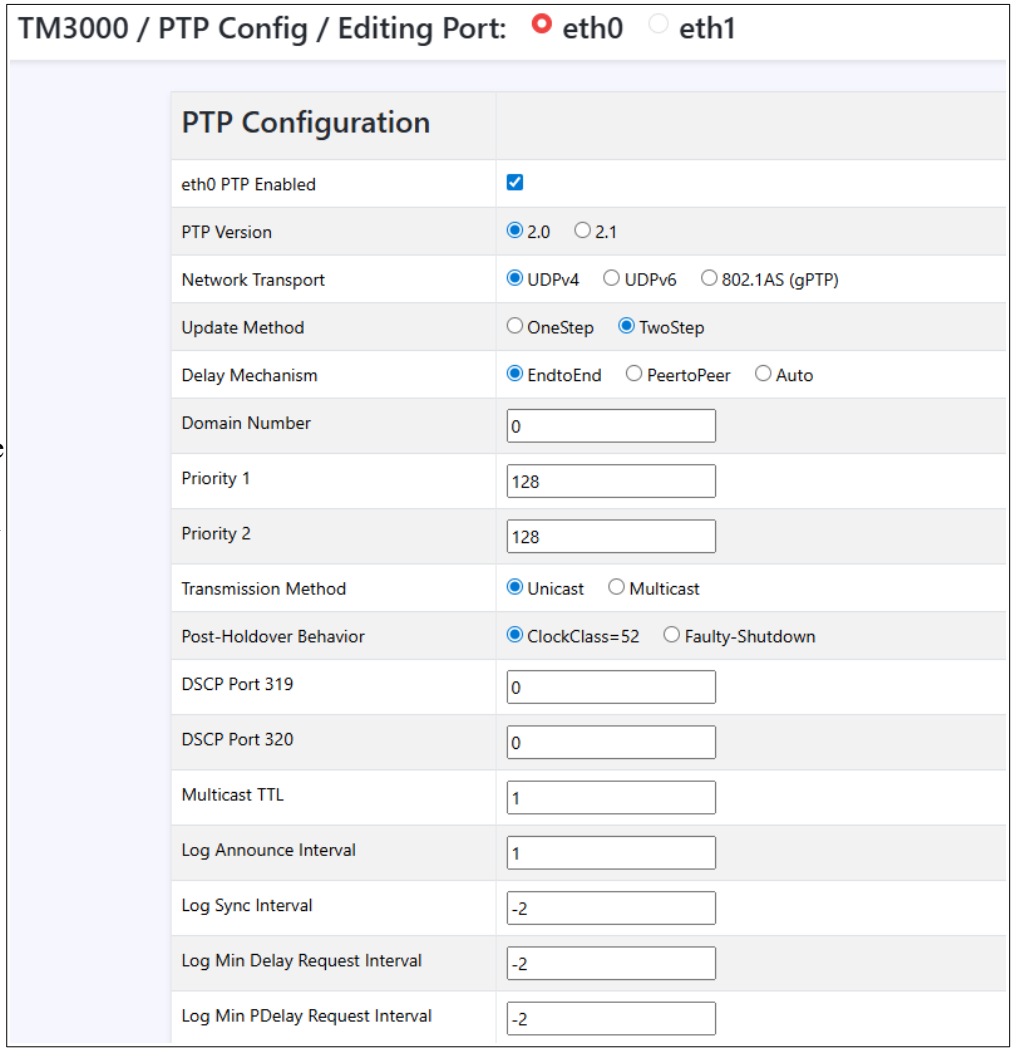
No.	Time	Source	Destination	Protoco	Lengt	Info
1	0.000000000	192.168.1.225	192.168.1.27	TCP	74	39966 → 4460 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3171405270 TSecr=0 WS=128
2	0.001222013	192.168.1.27	192.168.1.225	TCP	74	4460 → 39966 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=222994513 TSecr=3171405270 WS=128
3	0.001254277	192.168.1.225	192.168.1.27	TCP	66	39966 → 4460 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3171405271 TSecr=222994513
4	0.001400834	192.168.1.225	192.168.1.27	TLSv1.3	305	Client Hello
5	0.002305677	192.168.1.27	192.168.1.225	TCP	66	4460 → 39966 [ACK] Seq=1 Ack=240 Win=65024 Len=0 TSval=222994514 TSecr=3171405271
6	0.003840898	192.168.1.27	192.168.1.225	TLSv1.3	199	Server Hello, Change Cipher Spec
7	0.003865461	192.168.1.225	192.168.1.27	TCP	66	39966 → 4460 [ACK] Seq=240 Ack=134 Win=64128 Len=0 TSval=3171405274 TSecr=222994515
8	0.087872668	192.168.1.27	192.168.1.225	TLSv1.3	2188	Application Data, Application Data, Application Data, Application Data
9	0.087922190	192.168.1.225	192.168.1.27	TCP	66	39966 → 4460 [ACK] Seq=240 Ack=2256 Win=62080 Len=0 TSval=3171405358 TSecr=222994599
10	0.088435048	192.168.1.225	192.168.1.27	TLSv1.3	146	Change Cipher Spec, Application Data
11	0.132071360	192.168.1.27	192.168.1.225	TCP	66	4460 → 39966 [ACK] Seq=2256 Ack=320 Win=65024 Len=0 TSval=222994644 TSecr=3171405358
12	0.132116826	192.168.1.225	192.168.1.27	TLSv1.3	104	Application Data
13	0.133158205	192.168.1.27	192.168.1.225	TCP	66	4460 → 39966 [ACK] Seq=2256 Ack=358 Win=65024 Len=0 TSval=222994645 TSecr=3171405402
14	0.133201529	192.168.1.27	192.168.1.225	TLSv1.3	904	Application Data
15	0.133439088	192.168.1.225	192.168.1.27	TLSv1.3	90	Application Data
16	0.133472841	192.168.1.225	192.168.1.27	TCP	66	39966 → 4460 [FIN, ACK] Seq=382 Ack=3094 Win=63488 Len=0 TSval=3171405403 TSecr=222994645
17	0.133754890	192.168.1.225	192.168.1.27	NTP	266	NTP Version 4, client
18	0.134199115	192.168.1.27	192.168.1.225	TLSv1.3	90	Application Data
19	0.134199162	192.168.1.27	192.168.1.225	TCP	66	4460 → 39966 [FIN, ACK] Seq=3118 Ack=383 Win=65024 Len=0 TSval=222994646 TSecr=3171405403
20	0.134254369	192.168.1.225	192.168.1.27	TCP	54	39966 → 4460 [RST] Seq=382 Win=0 Len=0
21	0.134259906	192.168.1.225	192.168.1.27	TCP	54	39966 → 4460 [RST] Seq=383 Win=0 Len=0
22	0.134459949	192.168.1.27	192.168.1.225	NTP	266	NTP Version 4, server
23	1.997358276	192.168.1.225	192.168.1.27	NTP	266	NTP Version 4, client
24	1.998875997	192.168.1.27	192.168.1.225	NTP	266	NTP Version 4, server
25	3.997202590	192.168.1.225	192.168.1.27	NTP	266	NTP Version 4, client
26	3.998742482	192.168.1.27	192.168.1.225	NTP	266	NTP Version 4, server
31	5.997837143	192.168.1.225	192.168.1.27	NTP	266	NTP Version 4, client
32	5.998901466	192.168.1.27	192.168.1.225	NTP	266	NTP Version 4, server
33	7.997270664	192.168.1.225	192.168.1.27	NTP	266	NTP Version 4, client
34	7.998673389	192.168.1.27	192.168.1.225	NTP	266	NTP Version 4, server
35	9.997208315	192.168.1.225	192.168.1.27	NTP	266	NTP Version 4, client
36	9.999863544	192.168.1.27	192.168.1.225	NTP	266	NTP Version 4, server

The ntpd/ntpsec log entries, typically found in /var/log/syslog for Linux, will look something like:

```
2026-03-12T15:55:54.193456-05:00 Archer ntpd[1149199]: NTSc: Using system default root certificates.

2026-03-12T15:55:55.211983-05:00 Archer ntpd[1149199]: DNS: dns_probe: ntptest1.timemachinescorp.com,
cast_flags:1, flags:21901

2026-03-12T15:55:55.213090-05:00 Archer ntpd[1149199]: NTSc: DNS lookup of
ntptest1.timemachinescorp.com took 0.001 sec

2026-03-12T15:55:55.220947-05:00 Archer ntpd[1149199]: NTSc: connecting to
ntptest1.timemachinescorp.com:4460 => 192.168.1.27:4460

2026-03-12T15:55:55.220965-05:00 Archer ntpd[1149199]: NTSc: set cert host:
ntptest1.timemachinescorp.com

2026-03-12T15:55:55.301702-05:00 Archer ntpd[1149199]: NTSc: Using TLSv1.3, TLS_AES_256_GCM_SHA384
(256)

2026-03-12T15:55:55.301759-05:00 Archer ntpd[1149199]: NTSc: certificate subject name:
/C=US/ST=Nebraska/L=Lincoln/O=TimeMachines/CN=ntptest1.timemachinescorp.com

2026-03-12T15:55:55.301785-05:00 Archer ntpd[1149199]: NTSc: certificate issuer name:
/C=US/ST=Nebraska/L=Lincoln/O=TimeMachines/CN=ntptest1.timemachinescorp.com

2026-03-12T15:55:55.301795-05:00 Archer ntpd[1149199]: NTSc: matching with subject:CN
ntptest1.timemachinescorp.com

2026-03-12T15:55:55.301809-05:00 Archer ntpd[1149199]: NTSc: certificate is valid.

2026-03-12T15:55:55.301825-05:00 Archer ntpd[1149199]: NTSc: Good ALPN from
ntptest1.timemachinescorp.com

2026-03-12T15:55:55.346609-05:00 Archer ntpd[1149199]: NTSc: read 816 bytes

2026-03-12T15:55:55.346683-05:00 Archer ntpd[1149199]: NTSc: Got 8 cookies, length 96, aead=15.

2026-03-12T15:55:55.346698-05:00 Archer ntpd[1149199]: NTSc: NTS-KE req to
ntptest1.timemachinescorp.com took 0.135 sec, OK
```

This log is probably the best location to confirm function and see what settings might not yet be correct in your implementation. Reference it frequently during initial configuration to confirm things are working as expected.

3.10 PTP Settings Page



3.10.1 Network Port Selection

Two completely separate PTP sessions can exist on the TM3000 at the same time. One on each Ethernet interface. The top of the web page selects which settings are displayed and active. The webpage will switch immediately between them with no need to click Save to make the switch. Unsaved changes are lost on the switch between ports. Parameters are essentially identical between the two interfaces.

3.10.2 PTP Holdover

PTP holdover duration is governed by the settings on the NTP Settings page.

3.10.3 PTP Enabled

This enables the PTP server on the identified port.

3.10.4 PTP Version

This allows the TM3000 to support legacy devices that don't support PTP version 2.1. This will set the PTP version reported in the packets.

3.10.5 Packet Output

Packet output types supported, include IPv4, Layer 2, and IPv6 Ethernet packets. Only one of these modes can be active at a time on the port.

3.10.6 PTP Update Method One/Two Step

This setting controls the Sync/Delay packet generation mode of the TM3000. Default normal operation

is to use 1 Step. In this mode, a single Sync packet is generated at the requested/setup rate and HW time stamping is applied to the packet just before it goes onto the Ethernet wire. In the two step mode, two Sync packets are generated also with hardware time stamping, with the second packet containing the launch time of the first packet to allow the receiver to determine the accuracy.

3.10.7 Delay Mechanism

Selection of End to End or Peer to Peer delay determination is supported. End to End is typically used when network routers are not PTP aware. Peer to Peer is the standard for 802.1AS. Also available is Auto. Typical selection is E2E or P2P. The auto mode will start in End to End but switch to Peer to Peer if a peer delay request is received.

3.10.8 Domain Number

Use this entry to set the Domain number to be included in the PTP packets. The domain number is a method to allow multiple PTP servers on the same network, but to separate their traffic between client devices.

3.10.9 Priority 1 & Priority 2

Allows setting the Priority 1 value in the packets. Lower numbers are higher priority in the Best Master Clock Algorithm (BMCA). Priority 1 is used before Priority 2.

3.10.10 PTP Transmission Method

The PTP transmission method can be set to either Multicast or Unicast. When Multicast mode is set, the device will start generating Announce and Sync packets shortly after saving the parameters or GNSS lock is achieved. In the Unicast mode, it is required that the client connect to the time server and request PTP packets. Unicast mode supports 3-5 clients typically depending on the packet request rates. Multicast, supports more clients.

3.10.11 PTP Post-Holdover Behavior

There are two options here: Update Clock Class to 52 which in the PTP protocol means: “A clock of clock Class 52 shall not be a slave to another clock in the domain.” If set to Faulty, the protocol will shutdown after the holdover time and not resume operation until timing is restored. **Holdover time limits for the TM3000 are set in the NTP settings page.**

3.10.12 DSCP Port 319 and 320 Settings

This allows the DSCP/Diffserve/TOS value to be set. This is the value for first bye of the IP header. Valid values are 0-63 decimal. Announce packets are sent to port 320, Sync and Delay messages are sent to port 319. Consult your network documentation for the setting of these values

3.10.13 Multicast Configuration – TTL

This sets the Multicast UDP Time to Live value. It will default to 1 which would support only a single router hop. Increasing this value allows a PTP packet to propagate further on a network.

3.10.14 Multicast Configuration – Log Announce Interval

Set the Announce Message interval. The rate of sync packets is 2^(-value). The default setting of 1, sets the interval at 2^(-1) = 0.5 packets per second, or every 2 seconds. A value of 0, generates a packet

1 time per second, etc.

3.10.15 Multicast Configuration – Log Sync Interval

Sets the requested Sync Message interval. The rate of sync packets is 2^(-value). The default of -7, therefore makes the default rate 2^-(-7) = 128 packets per second.

3.10.16 Multicast Configuration – Log Min Delay Request Interval

The minimum permitted mean time interval between Delay_Req messages. A shorter interval makes the TM3000 react faster to the changes in the path delay. It's specified as a power of two in seconds. Generally, this setting doesn't need adjustment on the TM3000.

3.10.17 Multicast Configuration – Log min Peer Delay Request Interval

The minimum permitted mean time interval between Pdelay_Req messages. It's specified as a power of two in seconds. Generally, this setting doesn't need adjustment on the TM3000.

3.10.18 802.1AS Configuration – PTP Destination MAC

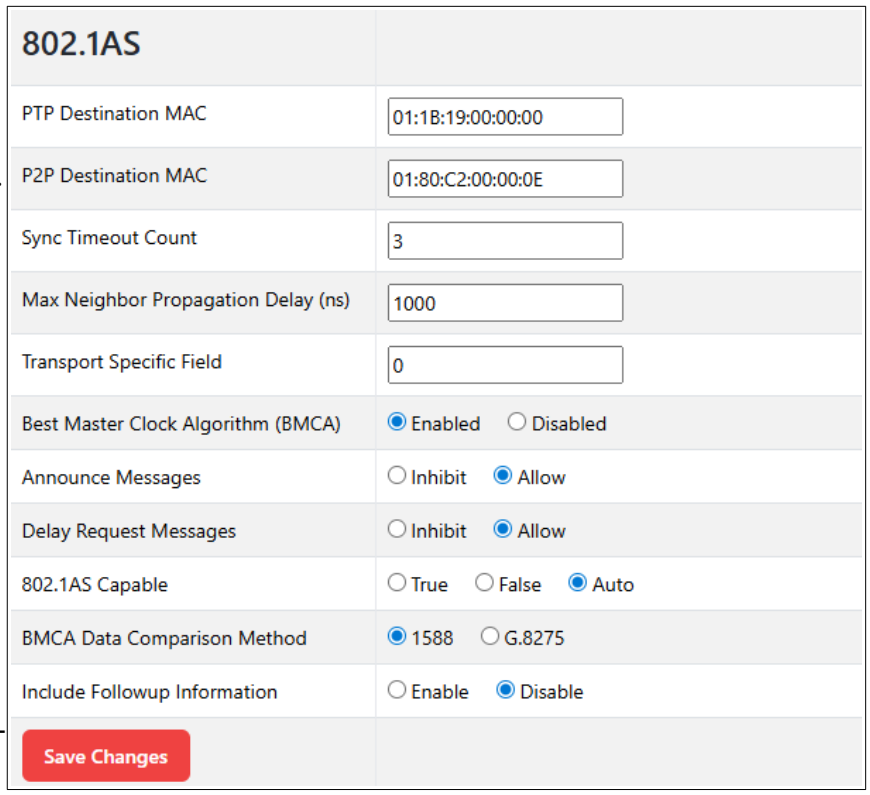
This is the MAC address that 802.1AS PTP messages will be sent. Default: 01:1B:19:00:00:00

3.10.19 802.1AS Configuration – P2P Destination MAC

This is the MAC address that 802.1AS Peer to Peer Delay messages are sent. Default: 01:80:C2:00:00:0E

3.10.20 802.1AS Configuration – Sync Timeout Count

This sets the number of sync/follow-up messages that can be missed before the Best Master Clock election code is started. Setting this option to 0, disables it.



3.10.21 802.1AS Configuration – Max Neighbor Propagation Delay (ns)

This is the upper limit for peer delay measurements, in nano-seconds, before the port is marked as not being 802.1AS capable.

3.10.22 802.1AS Configuration – Transport Specific Field

The transport specific field, it should range from 0 to 255. It generally has to match the client setting.

It should be 0 when running in a UDP mode.

3.10.23 Best Master Clock Algorithm (BMCA)

This enables/disable the BMCA algorithm. In automotive mode for example, BMCA is typically disabled as the master is known and startup should occur as quickly as possible.

3.10.24 Announce Messages Inhibit

This disables the timer for Announce messages and stops the generation of the Announce Messages. Announce Messages are typically inhibited in Automotive Profile, otherwise enabled.

3.10.25 Delay Request Messages Inhibit

This disables and stops the generation of the Delay Request Messages. Delay Request Messages are typically inhibited in Automotive Profile, otherwise enabled.

3.10.26 802.1AS Capable

There are three options: false, true, and auto. When set to true, the PTP server skips functional checks to unset 802.1AS mode. In auto, 802.1AS is set to false initially, but once checks are completed, it can be set to true. In false, 802.1AS will not be configured.

3.10.27 BMCA Data Comparison Method

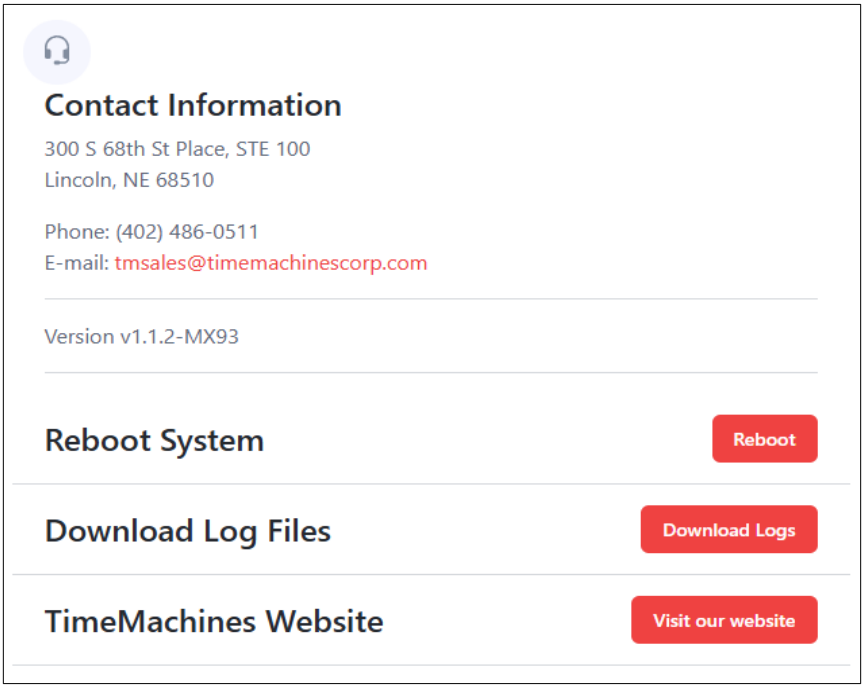
Typically the 1588 mode is used. The exception is when running G.8275.X modes when this should be set to G.8275.

3.10.28 Include Followup Information

When enabled, this appends additional 802.1AS data to the 2nd Sync packet required in Automotive Profile. If this setting is enabled along with a UDP transport, the UDP transport will not function. It is an 802.11 mode only setting.

3.11 About Page

The About Page shows contact information and software version.



3.11.1 Reboot System

Clicking the Reboot button will cause the TM3000 to do a software based reset. This is a full kernel reset of the unit and takes 15-20 seconds to complete.

3.11.2 Download Log Files

This will create a tar.gz file of the current log stored on the TM3000 as well as the configuration for the NTP and PTP pages. This can be useful in troubleshooting NTP cryptography issues, PTP setup issues, etc.

3.11.3 TimeMachines Website

Full documentation and other support materials can be found on the TimeMachines website. Click the button to go there.

4 Setting Up PTP without GNSS

All time source modes make it possible to provide PTP timing information without a GNSS lock. The major steps to do that are:

1) Provide a time to the device, by doing one of the following:
   - Manually set the time from the System Setup page, OR
   - Use NTP Peers to set the device time. This will be much more accurate and having 2 or 3 sources for NTP time is preferred
   - Ideally the device has been run with GNSS for several days/weeks to age the crystal, and the OCXO correction saved on the Status Web page. This will significantly improve drift performance of the device. While this doesn't help with accuracy of the device compared to atomic time, it does help maintain consistency over a period of time.
2) The TM3000 stamps packets in hardware in all time source modes.

From this point, PTP should operate normally with significantly degraded accuracy compared to GNSS, but for a local system without GNSS, it does allow PTP to operate without GNSS.

5 Using TimeMachines TM3000 with LinuxPTP

See the Applications section of the website for multiple configuration examples with LinuxPTP.

6 Troubleshooting

6.1 GNSS Lock

Getting GNSS lock on the Time Server is required for it to function. Most GNSS lock issues come down to issues with Antenna location, or cabling. If there are problems getting GNSS lock (i.e. the Lock LEDs don't turn on and the 1 PPS LED doesn't flash each second) trying moving the antenna outside and see if that resolves the issue. If it does, try a window and see if lock is maintained. If that works, move the antenna back to its original location and see if lock is lost. This will help determine where lock can be received and where it cannot. If no lock is achieved outdoors, then something is either wrong with the cabling or the Time Server itself. Contact TimeMachines for help.

6.2 Resetting to Factory Defaults

Front Panel Button: Push and hold the front panel button for 5 seconds. A second confirmation press and hold will be prompted on the display. This will cause the TM3000 to reset to mostly factory default settings.

6.3 Contacting TimeMachines for Support

The first thing that should typically be sent with any email request for support is a screen shot of the Status Page from the TM3000. Please provide as much information as possible when requesting support. If you are calling, please have the device in front of you along with a computer that is connected to it. Tech support will generally ask questions that are best answered with hands on the equipment.

7 Locator Data Query

The Locator service employed by TimeMachines clock products is also included in the TM3000. This makes it easier to manage and monitor a time system on a local network using the TM-Manger software. See the TM-Manager documentation for more information on this feature.

Locator Data Format

The Locator Data Service is a simple UDP/IP protocol that can be used by other network applications to extract status and location information from the TM1000A.

Requesting information from the TM3000 is done by sending a 3 byte message to the TM3000, using UDP/IP, to port 7372. The three bytes, in hexadecimal, are: 0xA1 0x04 0xB2 The TM3000 will also respond to a broadcast to the same port.

The response packet is 80 bytes and will be formatted as follows:

Bytes	Description
0	TM3000 response value = 0x06
1 to 4	eth0 IP address
5 to 10	eth0 MAC address
11 and 12	firmware version Major:Minor
13	Lock status 0=No Lock, 1=2D Lock, or 2=3D Lock
14 to 17	NTP Sync count, 32 bits, MSB to LSB
18 to 20	Current Time, H:M:S, UTC
21 to 45	Location of unit 25 bytes, Latitude, Longitude, null terminated
46 to 61	Name of Time Server, null terminated
62 to 65	eth1 IP address
66 to 71	eth1 MAC address
72-79	GPS Altitude, null terminated.

TM-Manager uses this protocol to find a monitor TM3000's on the network. A Wireshark capture of that software can be used to see an example of the data transfer. TM-Manager support of the TM3000 started in version 2.2.5.

8 Specifications

8.1 Time Server Features and Specifications

- Receive time information from GNSS satellites anywhere on the surface of the earth
- RFC1119/1305 NTP Protocol to serve time (Network Time Protocol)
- RFC1769/2030/4330 SNTP Protocol (Simple Network Time Protocol)
- IEEE 1588:2008 Version 2 PTP protocol
  - Telecom Profiles: G.8265.1, G.8275.1, and G.8275.2
  - 802.1AS
  - End to End and Peer to Peer Delay options
  - Postive and Negative Leap second support for NTP and PTP
- Server Time Level: Stratum 1
- NTP Server Time Precision: better than 1mS + network jitter.
- PTP Server Time Precision: better than 500nS + network jitter.
- All networked computing platforms support time synchronization either natively or with add on drivers including Windows, Macintosh, and Linux. Many other devices can access the device as well including VoIP phones and digital clocks.
- 10M/100M/1000M adaptive network interface
- Unit is capable of serving 1900+ NTP synchronizations per second. That provides support for 1.5M+ devices updating every 15 minutes on the network.
- Active Patch GNSS antenna included. Magnetic base.
- Compliant with FCC Part 15B, and CE marked for radiated emissions and is a lead free product.
- Power Requirements:
  - TM3000: 8W at startup and 6W continuous at 12V DC
- Environmental Requirements: Commercial temperature range, -20 to +70C, 95% humidity non-condensing. Altitude -304m to 18,000m.
- Networking: Static or DHCP IPv4 addressing. Standard browser interface for setup.
- Indications: Power, GNSS Signal Lock 2D/3D LEDS, and 1PPS indication LED, LCD Display
- Rear Connections:
  - Power 8-48VDC, Connector: 5.5mm outside diameter, 2.5mm inside, center positive
  - 2 pin screw terminal with included connector for 8-48VDC input
  - Cat5 Ethernet 10/100/1000 Ethernet
  - Serial (status information only, 115200,n81), mini-USB enumerates as Com port
  - GNSS antenna via SMA connection. Supports +3.3V and 5V active GNSS antennas with

internal jumper setting

- Mechanical Dimensions: 6.5 in. x 6.375 in. x 1.3in.

8.2 GNSS Module Specifications

- Based on MediaTek MT3333 Chipset
- 33 tracking/ 99 acquisition-channel GNSS receiver (GPS/GLONASS/GALILEO/BeiDou)
- Sensitivity: -165dBm
- High accuracy 1-PPS, ±20ns jitter
- Antenna Connection: 1575.42MHz (GPS L1 Band) / 1598.0625-1605.375MHz (GLONASS)
- TTFF (Time To First Fix)
  - Cold start @-125dBm typically 35 seconds
  - Re-acquisition (<10s obstruction) typically 1 second

8.3 Antenna Specifications

- Triple-Band Active patch antenna with magnetic base.
- Size: 55mm x 50mm x 17mm thick, 110 grams.
- Amplifier: LNA +30dB Noise: 2dB VSWR: 2.5 Voltage: 2.7-5.5V
- Cable: RG174, 5m length, SMA male.
- Environmental: -40 to +85C
- Waterproof to Ipx6

8.4 TM3000 OCXO Timing Information / Specifications

- 1 PPS / 10MHz output is 3.3V logic signal
- Standard SMB connections
- 1PPS signal is +/20 nS, 3.3V logic signal
- 10MHz Synchronized signal. Correlation between signals +/- 20nS. Highest correlation occurs with outdoor antenna with 360 degree view of sky.
- Best stability of the OCXO and 10Mhz reference in holdover is achieved:
  - 8 hours of operation required if TM3000B off for 24 hours
  - 24 hours of operation required if TM3000B off for 1 week
  - 48 hours of operation required if TM3000B off for 1 month
  - Stable temperature and mechanical conditions

(Specifications are subject to change without notice)