VelaSync™

High-Speed Enterprise Time Server

User's Manual

Spectracom Part No.: 1225-5000-0050

Revision: 1.0

Date: 14-Jan-2016

spectracom.com

© 2014-16 Spectracom Corp. All rights reserved.

The information in this document has been carefully reviewed and is believed to be accurate and up-to-date. Spectracom assumes no responsibility for any errors or omissions that may be contained in this document, and makes no commitment to keep current the information in this manual, or to notify any person or organization of updates. This User's Manual is subject to change without notice. For the most current version of this documentation, please see our web site at spectracom.com.

Spectracom reserves the right to make changes to the product described in this document at any time and without notice. Any software that may be provided with the product described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Spectracom Corp.

Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Spectracom Corp.

• 1565 Jefferson Road, Suite 460, Rochester, NY 14623 USA
• 3, Avenue du Canada, 91974 Les Ulis Cedex, France
• Room 208, No. 3 Zhong Guan Village South Road, Hai Dian District, Beijing 100081, China

Questions or comments regarding this User's Manual?

➔ E-mail: techpubs@spectracom.orolia.com

SPECTRACOM LIMITED WARRANTY

Five Year Limited Warranty

Spectracom, a business of the Orolia Group, warrants each new standard product to be free from defects in material, and workmanship for five years after shipment in most countries where these products are sold, EXCEPT AS NOTED BELOW (the “Warranty Period” and "Country Variances").

Warranty Exceptions

This warranty shall not apply if the product is used contrary to the instructions in its manual or is otherwise subjected to misuse, abnormal operations, accident, lightning or transient surge, or repairs or modifications not performed by Spectracom authorized personnel.

Items with a variance to the Five Year Warranty Period are as follows:

90 Days Warranty

TimeKeeper Software

One Year Limited Warranty

Timeview Analog Clock
Path Align-R Products
Bus-level Timing Boards
IRIG-B Distribution Amplifiers

Two Year Limited Warranty

Rubidium Oscillators
Epsilon Board EBO3
Epsilon Clock 1S, 2S/2T, 3S, 31M
Epsilon SSU
Power Adaptors
Digital and IP/POE Clocks
WiSync Wireless Clock Systems and IPSync IP Clocks
Rapco 1804, 2804, 186x, 187x, 188x, 189x, 2016, 900 series

Three Year Limited Warranty

Pendulum Test & Measurement Products GPS-12R, CNT-9x, 6688/6689, GPS-88/89, DA-35/36, GPS/GNSS Simulators

Country Variances

All Spectracom products sold in India have a one year warranty.

Warranty Exclusions

Batteries, fuses, or other material contained in a product normally consumed in operation.

Shipping and handling, labor & service fees

EXCEPT FOR THE LIMITED WARRANTY STATED ABOVE, SPECTRACOM DISCLAIMS ALL WARRANTIES OF ANY KIND WITH REGARD TO SPECTRACOM PRODUCTS OR OTHER MATERIALS PROVIDED BY SPECTRACOM, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Spectracom shall have no liability or responsibility to the original customer or any other party with respect to any liability, loss, or damage caused directly or indirectly by an Spectracom product, material, or software sold or provided by Spectracom, replacement parts or units, or services provided, including but not limited to any interruption of service, excess charges resulting from malfunctions of hardware or software, loss of business or anticipatory profits resulting from the use or operation of the Spectracom product or software, whatsoever or howsoever caused. In no event shall Spectracom be liable for any direct, indirect, special or consequential damages whether the claims are grounded in contract, tort (including negligence), or strict liability.

Extended Warranty Coverage

Extended warranties can be purchased for additional periods beyond the standard warranty. Contact Spectracom no later than the last year of the standard warranty for extended coverage.

Warranty Claims

Spectracom's obligation under this warranty is limited to the cost of in-factory repair or replacement, at Spectracom's option, of the defective product or the product's defective component. Spectracom's Warranty does not cover any costs for installation, reinstallation, removal or shipping and handling costs of any warranted product. If in Spectracom's sole judgment, the defect is not covered by the Spectracom Limited Warranty, unless notified to the contrary in advance by customer, Spectracom will make the repairs or replace components and charge its then current price, which the customer agrees to pay.

In all cases, the customer is responsible for all shipping and handling expenses in returning product to Spectracom for repair or evaluation. Spectracom will pay for standard return shipment via common carrier. Expediting or special delivery fees will be the responsibility of the customer.

Warranty Procedure

Spectracom highly recommends that prior to returning equipment for service work, our technical support department be contacted to provide troubleshooting assistance while the equipment is still installed. If equipment is returned without first contacting the support department and "no problems are found" during the repair work, an evaluation fee may be charged.

Spectracom shall not have any warranty obligations if the procedure for warranty claims is not followed. Customer must notify Spectracom of a claim, with complete information regarding the claimed defect. A Return Authorization (RMA) Number issued by Spectracom is required for all returns.

Returned products must be returned with a description of the claimed defect, the RMA number, and the name and contact information of the individual to be contacted if additional information is required by Spectracom. Products being returned on an RMA must be properly packaged with transportation charges prepaid.

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

APPENDIX

BLANK PAGE.

CHAPTER 1

INTRODUCTION & OVERVIEW

The following topics are included in this Chapter:

1.1 Product Overview

VelaSync™ High-Speed Time Server with TimeKeeper™ inside is an enterprise-class time serving appliance designed for high-frequency trading and other network applications that require low latencies.

VelaSync's customized configuration, comprising state-of-the-art network synchronization software, precision GPS timing technology, and reliable server hardware allows it to provide high-performance time management over multiple 1GbE (RJ-45) and 10 GbE (SFP+) network interfaces.

Hardware

The customized Supermicro® server platform is a 1U server comprised of a standard chassis and motherboard, as well as a GPS receiver plus oscillator (OCXO, or Rubidium), two hard disks (RAID), two power supplies, and several time, frequency and communication ports.

Software

The pre-installed TimeKeeper time synchronization and management software allows to distribute very accurate time throughout a network, supporting NTP and PTP protocols. In day-to-day operation, the software allows system administrators to centrally monitor time synchronization accuracy throughout the network in an efficient manner. For more information on TimeKeeper, see "What is TimeKeeper?" on page 30.

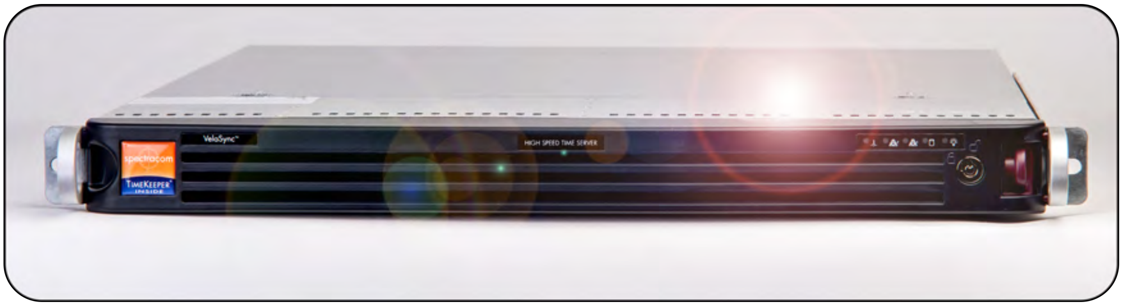


Figure 1-1: VelaSync High Speed Time Server

1.2 About this Manual

This User's Manual for the VelaSync High-Speed Enterprise Time Server provides you with:

- descriptions of features and functions, as well as
- installation and configuration guidance
- instructions for specific tasks related to using this product
- safety-related information

- technical specifications
- other reference information.

The main objectives of this User's Manual are:

a. to assist you with the installation and configuration of this product in a safe and efficient manner

b. to help you familiarize yourself with VelaSync's user interfaces, features and functionality.

This User's Manual is written for a professional audience, targeting experienced system integrators and PC technicians.

Other relevant documentation

This Spectracom User's Manual is complemented by the Spectracom VelaSync Quick Reference Guide (PN: 1225-5000-0051), a printed copy of which is shipped with the unit, and the user documentation for the Supermicro™ SuperO® SuperServer 5017R-WRF, which can be found under:

- http://www.supermicro.com.tw/manuals/superserver/1U/MNL-1328.pdf

Manual Organization

This User's Manual is organized as follows:

CHAPTER 1: Introduction and Overview

This chapter describes the main features of VelaSync, its hardware operating elements and status indicators. Furthermore, the introductory chapter also includes VelaSync's technical specifications, and regulatory information.

CHAPTER 2: Installation

This chapter describes the preparatory measures, as well as the actual steps necessary to install VelaSync in a server rack. Also included are SAFETY notes, and typical configuration steps required prior to, or after initial powering on the system.

CHAPTER 3: TimeKeeper

The TimeKeeper™ software running on VelaSync not only serves time during normal operation, but also represents the main user interface for configuring and monitoring VelaSync. CHAPTER 3 guides you through TimeKeeper's web user interface "Web UI", explaining its features and functions.

CHAPTER 4: Frequently Used Tasks

Frequently executed tasks are described in CHAPTER 4, broken down into the categories "TimeKeeper Tasks" on page 64, and "Hardware Tasks" on page 80.

APPENDIX

The document appendix includes "TimeKeeper: Additional Information" on page 86 , "Troubleshooting" on page 84 , as well as administrative information, e.g., how to contact Spectracom Support, and license notices.

1.3 Designated Use of this Product

This product has been designed and built in accordance with state-of-the-art standards and the recognized safety rules. Nevertheless, its use may constitute a risk to the operator or installation/maintenance personnel if used under conditions that must be deemed unsafe, or for purposes other than the product's designated use.

The VelaSync High-Speed Enterprise Time Server is intended for use in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.

Installation and maintenance of this device should be performed by experienced technicians only.

For additional information on how and where to use this product, see also "Selecting the Right Installation Location" on page 18 and "YOUR SAFETY" on page 11.

1.4 Technical Specifications

1.4.1 Hardware

1.4.1.1 Server

- Supermicro SuperServer 5017R-WRF rackmount server with 1U chassis and X9SRW-F motherboard:
  - Three 4cm counter-rotating PWM fans
  - One passive CPU heatsink
  - Two riser cards
  - Four hot-swap 3.5" drive bays (SATA)
- Intel 1.8 GHz Quad-Core Xeon Processor
- 8 GB RAM
- Two Western Digital Re 500 GB Enterprise-Class Hard Drives in RAID Mirroring configuration
- Two redundant, hot-swap power supplies, 100-240 V_{AC} auto-switch, 50-60 Hz, 500 W each, with IEC60320 C14 inlet coupler
- Connectivity:
  - I/O connectors: See "Rear Panel Overview" on page 10.

1.4.1.2 GPS Receiver

- Connector: SMA, +5V to power active antenna (SMA to Type N adapter cable included)
- Frequency: GPS L1 (1575.42 MHz)
- Satellite tracking: 1 to 50, T-RAIM satellite error management
- Synchronization time:
  - Cold start < 15 minutes (includes almanac download)
  - Warm start < 5 minutes (assumes current almanac downloaded)
- GPS Antenna system: See antenna installation guide (antenna sold separately)

1.4.1.3 Oscillator

Table 1-1: Oscillator accuracies

	OCXO	Rb
Accuracy to UTC (1 sigma locked to GPS)	50 ns	25 ns

	OCXO	Rb
Holdover Accuracy (loss of GPS signal after 2 weeks locked, constant temperature		
After 4 hours	1μs	0.2 μs
After 24 hours	25 μs	1 μs

Notes:

- Accuracy to UTC is measured by comparing the internal 1PPS with the GPS ontime point.
- When ordering a VelaSync unit, either an OCXO or Rubidium oscillator must be specified.
- The specifications are subject to a steady environment temperature.

1.4.2 I/O Connectors

1.4.2.1 Time and Frequency Output

» 1PPS: TTL (5V_{P-P}), SMA

1.4.2.2 Communication Ports

2x **10 GbE** SFP+ (optionally 4x, or 2x 10 Gb plus 2x 40 Gb[1])

3x **1GbE** RJ-45 with HW time stamping

1x IPMI (V.2.0)

1x RS-232 (Fast UART)

4x USB 2.0

1x VGA

1.4.3 Environmental Specifications

» Operation: 10°C to 35°C, RH: 8 to 90% (non-condensing @ 35°C)

» Storage: –40°C to +50°C , RH: 5 to 95% (non-condensing @ 35°C)

1.4.4 Size, Weight & Power

» Dimensions: (WxHxD) 437 x 43 x 650 mm (17.2 x 1.7 x 25.6 in.)

» Weight: 23.5 lbs. (10.7 kg)

» Max. power draw (@ 20°C, 2 power supplies running, 2 hard disks installed)

  » 100 W typical

  » 120 W startup

[1] Please inquire about availability.

- AC input: 100 to 240 V, 50 to 60 Hz, 6.2 to 2.6 A

For additional hardware specifications, see the User's Manual of the Original Equipment Manufacturer:

http://www.supermicro.com.tw/manuals/superserver/1U/MNL-1328.pdf

1.5 Front Panel Overview

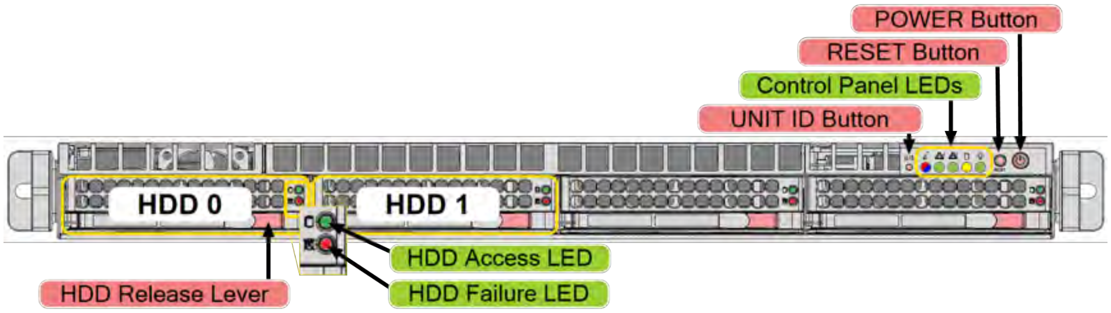
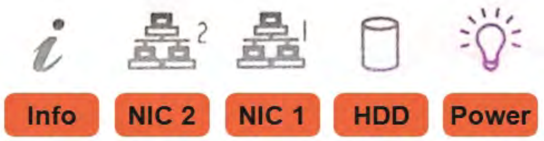


Figure 1-2: Front Panel (bezel removed)

1.5.1 Control Buttons

- **UNIT ID** ("UID"): Unit identifier button – to identify this unit, press this button (or activate via IPMI) to turn the blue "i" LED in front and back of unit on/off.
- **RESET button**: Reboot the system
- **Power button**: Apply/remove power from the power supply of the server. (Note: Standby power continues to be supplied to the system, i.e. the power supplies and the IPMI remain energized)
- **HDD Release Lever**: Pull to release one of the two hot-swap RAID hard disks.

1.5.2 Control Panel LEDs



- **Info (red):**
  - Red blinking fast (1x/sec): Fan fail
  - Red blinking slowly (1x/4 sec): Power fail
  - Red solid: CPU overheat
- **Info (blue):**
  - Blue solid: Local UID button depressed
  - Blue blinking: IPMI activated unit UID
- **NIC 2, 1**: Activity on GLAN 1,2 when flashing green

- **HDD**: IDE channel activity when flashing yellow
- **Power**: Power is applied to power supplies (bright green)

1.5.3 Hard Disk Drives

Each hard disk drive (HDD) carrier has two LEDs:

- **Green LED**: Indicates drive activity, when illuminated.
- **Red LED**:
    - When blinking, the drive is rebuilding.
    - When solid, indicates drive failure (you should also receive an automatic message from your system management software).

To release a hard disk drive carrier, in order to remove the hot-swappable hard disk drive, push the red button for the carrier to release the lever, then pull the carrier out, using the lever.

For additional instructions on how to replace a hard disk, see "Removing/Installing a Hard Disk Drive" on page 81.

1.6 Rear Panel Overview

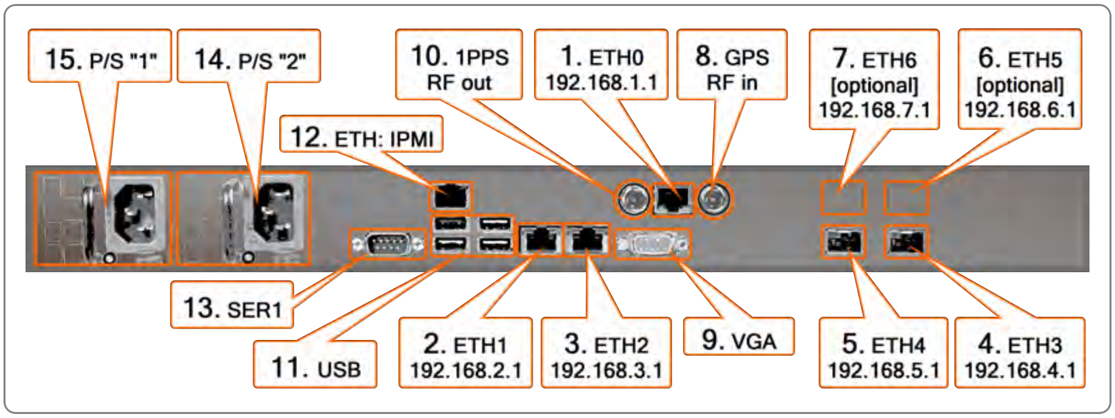


Figure 1-3: VelaSync rear panel

Legend:

1./2./3.: 1GbE ports (RJ-45)

4./5.: 10 GbE ports (SFP+)

6./7.: optional 10 GbE ports (SFP+), or 40 GbE[1]

8.: GPS antenna connector (SMB or SMA [2016])

9.: VGA

10.: PPS Out (SMB, or SMA [since 2016])

11.: USB (4x)

12.: IPMI

13.: Serial

14./15.: Power supplies

Note: TimeKeeper™ does not support having multiple network interfaces on the same subnet or multipath routing.

[1] Please inquire about availability.

1.7 YOUR SAFETY

This product has been designed and built in accordance with state-of-the-art standards and the recognized safety rules. Nevertheless, its use may constitute a risk to installation/maintenance personnel if used under conditions that must be deemed unsafe, or if the warnings and precautions explained below are ignored.

Additional Safety Notes pertaining to hardware installation can be found under "Rack Mounting: SAFETY" on page 19.

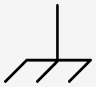
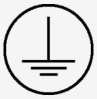
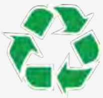
1.7.1 SAFETY: Symbols Used

Figure 1-4: Do not ignore the Safety Instructions!

The following symbols may be found in Spectracom technical documentation, or on Spectracom products:

Table 1-2: Spectracom safety symbols

Symbol	Signal word	Definition
	DANGER!	Potentially dangerous situation which may lead to personal injury or death! Follow the instructions closely.
⚠	CAUTION!	Potential equipment damage or destruction! Follow the instructions closely.
ℹ	NOTE	Tips and other useful or important information.
	ESD	Risk of Electrostatic Discharge! Avoid potential equipment damage by following ESD Best Practices.

Symbol	Signal word	Definition
	CHASSIS GROUND	This symbol is used for identifying the functional ground of an I/O signal. It is always connected to the instrument chassis.
	Analog Ground	Shows where the protective ground terminal is connected inside the instrument. Never remove or loosen this screw!
	Recycle	Recycle the mentioned components at their end of life. Follow local laws.

1.7.2 SAFETY Advisories

DANGER! Electrical hazard — DO NOT OPEN THE ENCLOSURE: No user-serviceable parts inside (the warranty will be voided, if opened). Should you ever decide to open the enclosure at your own risk, unplug and remove BOTH power supplies first (the POWER button will NOT de-energize the system!)

Caution: Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

DANGER! — GROUNDING: A reliable ground must be maintained at all times. To ensure this, the rack itself should be grounded. Particular attention should be given to power supply connections other than the direct connections to the branch circuit (i.e. the use of powerstrips, etc.).

Caution: CIRCUIT OVERLOADING — Consideration should be given to the connection of the equipment to the power supply circuitry and the effect that any possible overloading of circuits might have on overcurrent protection and power supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

DANGER! Hazardous voltage or energy is present on the back panel when the system is operating. Use caution when servicing.

Caution: Do not use power supplies other than the p/s model installed in your VelaSync™, and do not mix power supplies with different power ratings.

NOTE: Replacement power supplies can be purchased directly from Spectracom (Part no. PS09R-070J-SL01).

Please be sure to also consult local and national electrical codes, and the **User's Manual** of the **Original Equipment Manufacturer** which can be accessed online under:

http://www.supermicro.com.tw/manuals/superserver/1U/MNL-1328.pdf.

Ultimate disposal of this product should be handled according to all national laws and regulations.

SAFETY: General Advice

- Make sure you possess the professional skills, and have received the training necessary for the type of work you are about to perform.
- The equipment must only be used in technically perfect condition. Check components for damage prior to installation. Also check for loose or scorched cables on other nearby equipment.
- Do not modify the equipment.
- Use only spare parts authorized by Spectracom.

SAFETY: Hands-On Advice

- Before working with or on the equipment, familiarize yourself with the location of the ON/OFF switch on the unit, the closest disconnection switch in the room, and electrical outlet, so that you can quickly remove power from the unit in the event of an emergency.
- Do not work alone. The other person should also know how to disconnect power to the unit you are working on.
- Always remove power from the unit, before working on it. Before disconnecting power, gracefully shut down the unit.
- Should you ever have to work on powered on electrical equipment, use only one hand, in order to avoid making a complete circuit.
- To protect yourself from electrical shock, use rubber mats specifically designed as electrical insulators (not ESD mats).
- Keep these instructions at hand, near the place of use.
- Keep your workplace tidy.

- Do not wear loose clothing.
- Remove any metal objects, such as jewelry, from your body.
- Apply technical common sense: If you suspect that it is unsafe to use the product, do the following:
  - Disconnect the supply voltage from the unit.
  - Clearly mark the equipment to prevent its further operation.

ESD: Best Practices

No user serviceable parts inside – ELECTRICAL HAZARD, Warranty Void

This VelaSync unit does not require opening. In the event that an internal component failed (e.g., a fan), contact Spectracom service (see "Technical Support" on page 102).

DANGER! If the equipment MUST be opened: Do not open the panel before unplugging and removing BOTH power supplies (the POWER button will NOT de-energize the system!)

Caution: Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.

- Use a grounded wrist strap to prevent static discharge.
- Put components and PCBs back into their antistatic bags, while not in use.
- Touch a grounded metal object before removing a PCB from its antistatic bag.
- Make sure the unit's chassis, its power supply, and main components are electrically connected to one another, so as to allow reliable grounding.
- Do not let components or PCBs come into contact with your clothing.
- Handle PCBs on their edges only; avoid touching electronic components or contacts. If you have to handle a chip, avoid touching its pins.

1.8 Regulatory Compliance

This product has been found to be in conformance with the following regulatory publications.

Excerpt from OEM User's Manual:

http://www.supermicro.com.tw/manuals/superserver/1U/MNL-1328.pdf, page B-2:

- **Electromagnetic Emissions**: FCC Class A, EN 55022 Class A, EN 61000-3-2/-3-3, CISPR 22 Class A
- **Electromagnetic Immunity**: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)
- **Safety**: CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)
- **California Best Management Practices Regulations for Perchlorate Materials**: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. “Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate”
- **FCC Statement**: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer’s instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

DANGER! Handling of lead solder materials used in this product may expose you to lead, a chemical known to the State of California to cause birth defects and other reproductive harm.

BLANK PAGE.

CHAPTER 2

Installation and Setup

The following topics are included in this Chapter:

2.1 Unpacking and Inventory

Caution: Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling the unit.

Unpack the equipment and inspect it for damage. If any components have been damaged in transit, you should file a damage claim with the with the carrier who delivered the unit.

Should you experience any problems during installation and configuration of your Spectracom product, please contact your closest Spectracom Customer Service Center (see "Technical Support" on page 102.)

Note: Retain all original packaging for use in return shipments, if necessary.

What's in the box?

- VelaSync Unit
- Two (2) sets of rail assemblies
- Two (2) rail mounting brackets, extension elements, and mounting hardware
- Front bezel, and keys
- Two (2) power cables
- Spectracom Ancillary kit, containing one (1) PPS cable, one (1) antenna cable, and one (1) adapter, if needed
- Optional equipment e.g., GPS antenna and surge suppressor
- Documentation: VelaSync Quickstart Guide, Supermicro documentation, Mellanox documentation.

After inspecting the contents of the shipment, continue with Chapter "Selecting the Right Installation Location" below.

2.2 Selecting the Right Installation Location

VelaSync has been designed to be installed in an industry-grade, slide-mount 19" server rack or cabinet. Note that VelaSync is not suitable for use with a visual display work place device (§2 of the German Ordinance for Work with Visual Display Units).

Select a suitable location that meets the following requirements:

- A dedicated room with **restricted access**
- **Electrically grounded** and **mechanically stable rack**, with **physical clearance** for unrestricted air flow and servicing: approx. 650 mm [25"] in front of rack, 770 mm [30"] in the back of rack
- Clean, **dust-free**, and **stable**[1] **ambient temperature** not to exceed 35°C [95°F].
- Virtually free of **EMC noise**
- Access to a reliable **grounded power outlet**
- Sufficiently dimensioned **power supply circuitry**, to prevent overloading of circuits.
- The use of a regulating **UPS** (Uninterruptible Power Supply) is recommended.

Next Steps:

- Read "YOUR SAFETY" on page 11, and "Rack Mounting: SAFETY" below before familiarizing yourself with the procedure for the "Rack Installation" below.

2.3 Rack Mounting: SAFETY

- Read "YOUR SAFETY" on page 11.
- Before installing VelaSync in the fully extended rails, or before extending the unit from the rack, ensure that the rack is stable enough to support the weight of the fully extended unit. If you are using a standalone rack, it may be necessary to install stabilizers to the rack.
- Always extend only one unit at a time.
- Install heavier servers near the bottom of the rack.
- The unit weighs approximately 24 lbs (11 kg). Depending on your chosen installation location, it may be advisable to lift the unit with two persons.

2.4 Rack Installation

> **Note:** We recommend that you read this Chapter in its entirety before you begin with the installation.

[1] An environment where a constant temperature can be maintained during operation, to allow for the best possible timing accuracy.

> **Note:** Also consult the installation instructions that came with the rack or cabinet you plan on using.

All VelaSync units are shipped with two rack rail assemblies, each of which consists of two sections:

- the **inner rail**, which is pre-installed to the server chassis
- the **outer rail assembly**, which faces the rack

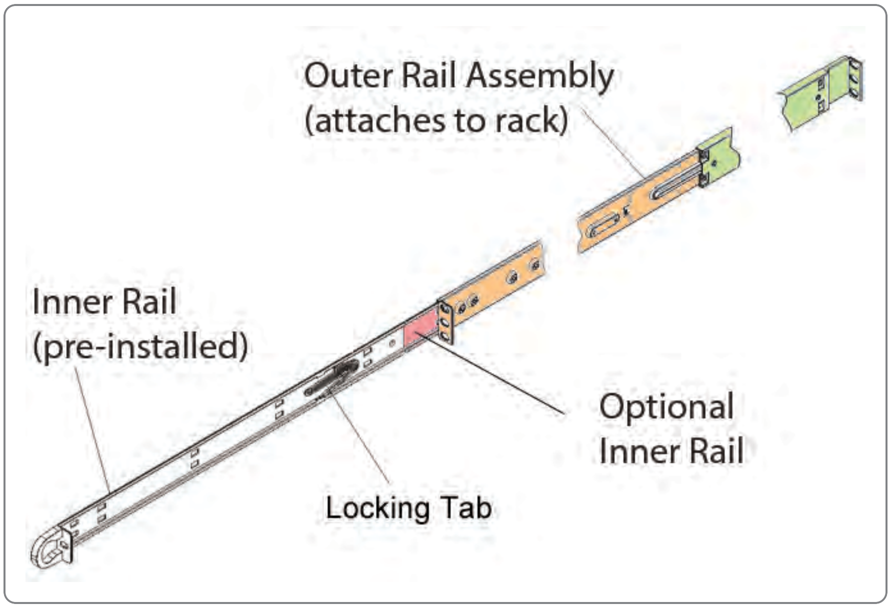


Figure 2-1: Rack rail assembly

Optional inner rail extension elements (shown in red) are provided to accommodate installation scenarios requiring maximum unit extension from the rack, e.g. for service & maintenance. Consult your rack manufacturer's user manual for additional information.

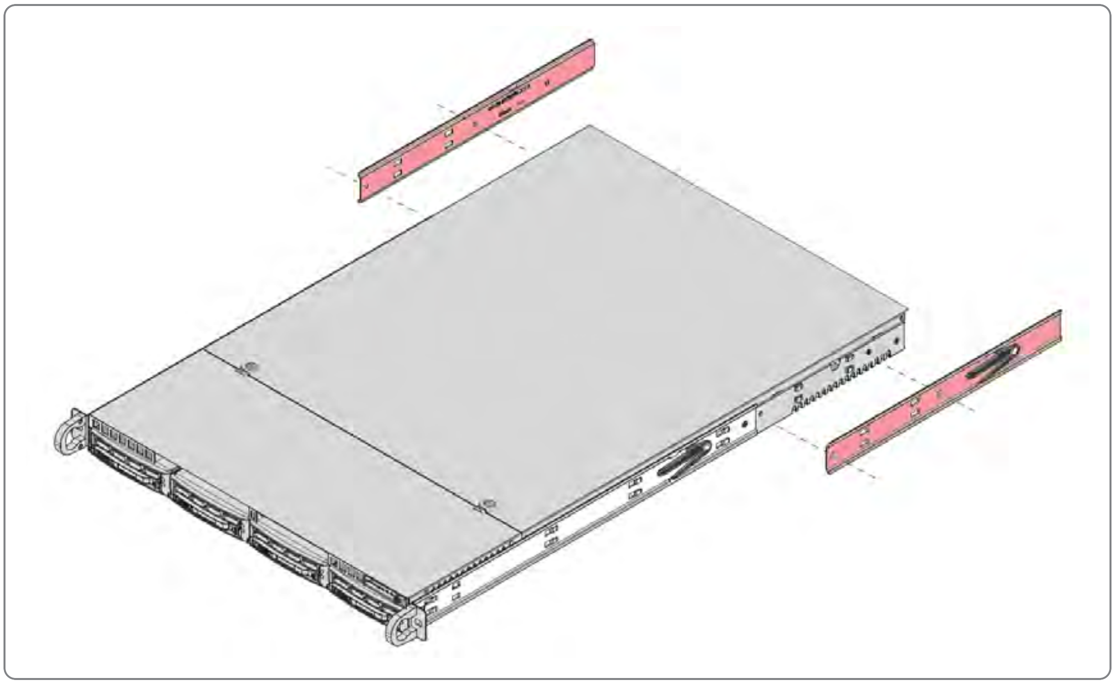


Figure 2-2: Optional inner rails

Installing the outer rail to the rack:

1. Measure the distance from the front rail to the rear rail of the rack. Attach a **short bracket** to the front side of each of the outer rails, and a **long bracket** to the rear side of each outer rail.
2. Adjust both the short, and the long brackets to the proper distance so that the rails fit snugly into the rack. Secure the short bracket to the front side of the outer rail with **two screws**, and the long bracket to the rear side of the outer rail with **three screws**.

Installing the server into the rack:

Once all the rails have been installed to the VelaSync chassis and the rack, the VelaSync unit can be installed into the rack.

Caution: The unit weighs approximately 24 lbs (11 kg). Depending on your chosen installation location, it may be advisable to lift the unit with two persons.

3. Line up the rear of the inner rails at the chassis with the front of the outer rails at the rack. Slide the server chassis into the rack, keeping the pressure even on both sides. Depress the locking tabs, if needed (they will click upon proper engagement).

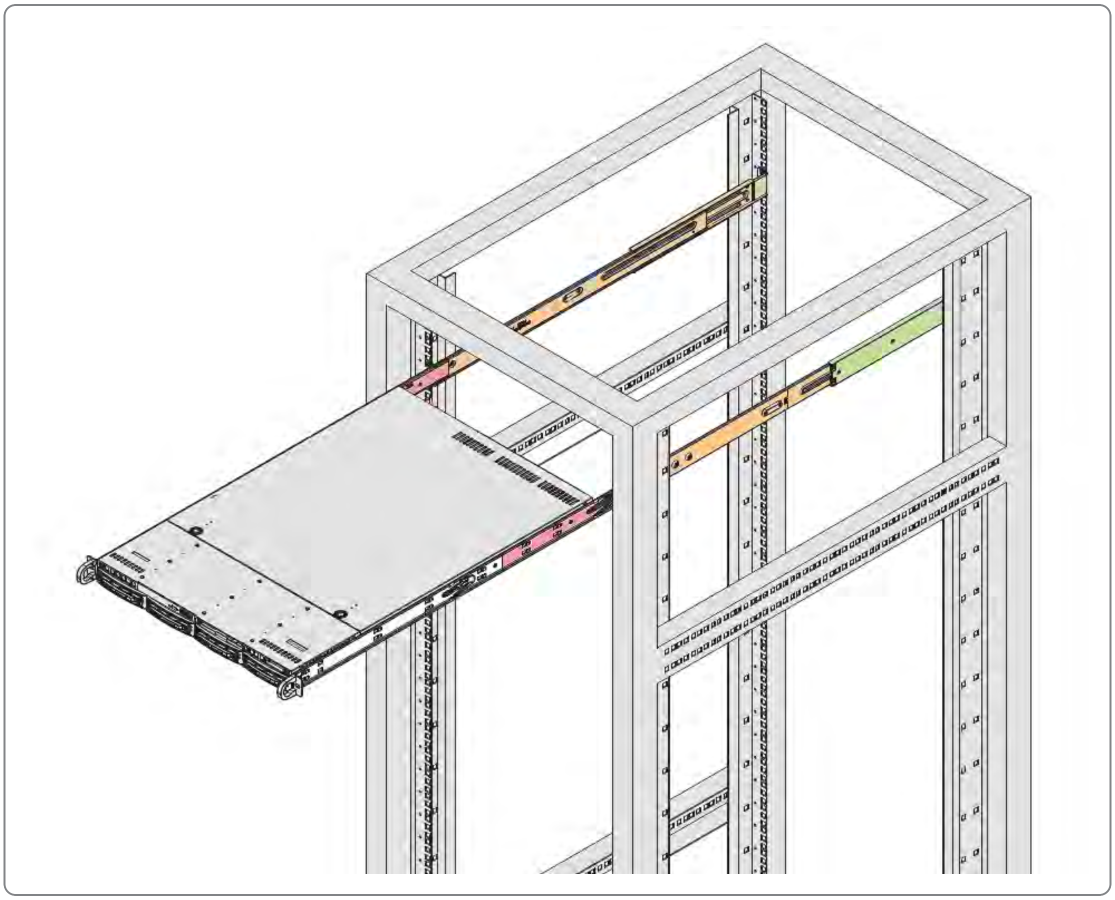


Figure 2-3: Rack installation

2.4.1 TELCO Rack Installation

To install the VelaSync unit in a Telco-type rack, use two L-shaped brackets on either side of the VelaSync chassis.

1. Determine how far forward the unit will extend out of the front of the rack. Determine a balanced front-to-back position of the chassis.
2. Remove the bezel from the VelaSync. Attach the two front brackets to each side of the chassis, then the two rear brackets, leaving just enough space to accommodate the width of the telco rack.
3. Slide the VelaSync into the rack, and tighten the brackets to the rack.

2.5 Connections

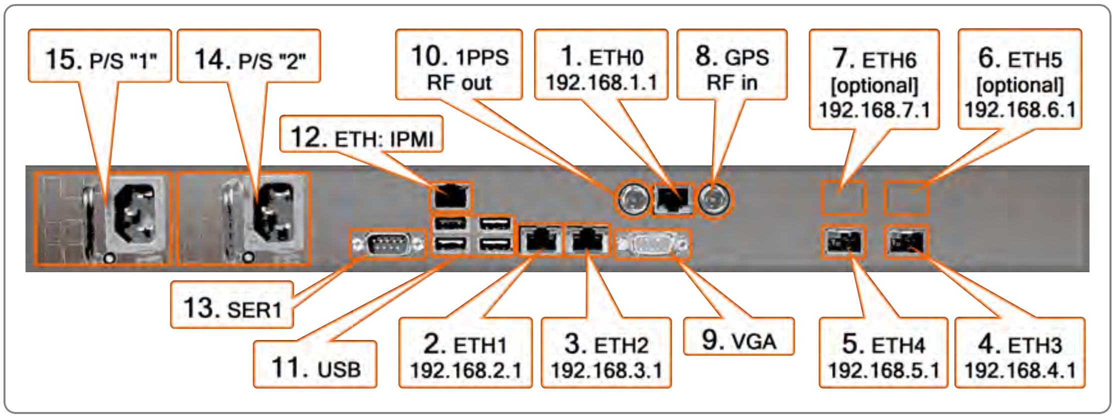


Figure 2-4: VelaSync rear panel

2.5.1 Connecting the GPS Antenna

For instructions on how to install a GPS/GNSS antenna, the signal cable, and accessories such as surge protectors, weatherproofing kits, or amplifiers, refer to the Installation Guide that came with the respective equipment.

For additional information regarding the GPS antenna location selection, see "GPS Antenna Location" on page 85.

1. Connect the GPS antenna to the GPS connector (see "Rear Panel Overview" on page 10, using the supplied Type-N adapter cable, and an LMR-400 equivalent cable with surge suppressor and active GPS L1 antenna, such as Spectracom model 8230.

   Note the GPS receiver connection provides $5V_{DC}$ power for the antenna.

2.5.2 Establishing a Network Connection

2. Connect a network cable to at least one of the Ethernet connectors ETH0 to ETH4 on the back panel of the unit. Take note of the ETH port you chose.

> **Note:** You'll likely want to change the default IP address of the ETH ports you plan on using. This procedure is described in the next topic . (You will need an Ethernet cable, or a serial null modem cable for this.)

2.5.3 Connecting Power

Before connecting power to the unit, make sure that you have read all safety information detailed in section "YOUR SAFETY" on page 11.

DANGER! When installing the product, use only the provided or designated power cables. Using any other cables and adaptors could cause a malfunction or a fire.

DANGER! This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 20 A.

3. Plug in power to both power supplies.

   As soon as at least one of the two power supplies has been connected to the mains voltage, you may hear **fan noise** from inside the VelaSync housing. However, note that the unit is not running yet (check the front indicator lamps: they will remain dark).

4. Switch the unit on by pressing the ON/OFF button on the front panel. Wait for the device to boot up.

   Note: If only one power supply is running, and the other one is inserted all the way, but not plugged in, or defect, VelaSync will emit a long BEEP, so as to alert you of a problem with the backup power.

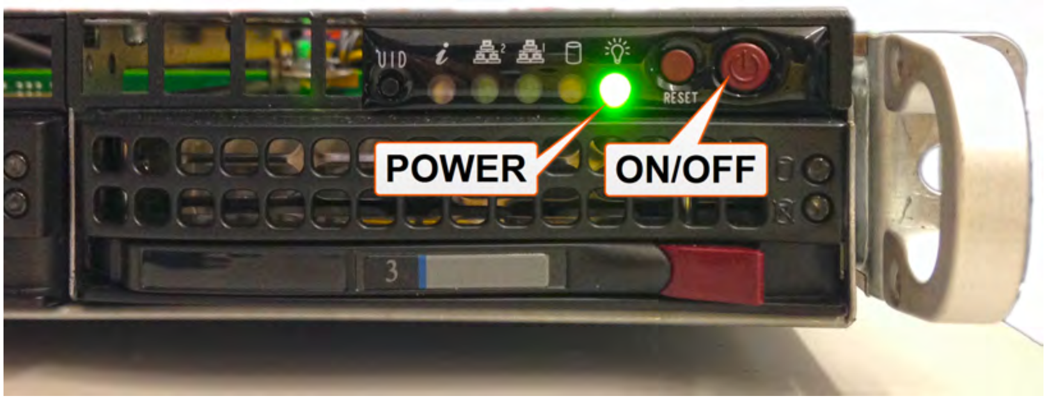


Figure 2-5: ON/OFF button

5. Once the boot process is completed, only the green POWER status LED should be lit.

   Proceed to the next topic below.

2.6 Configuring IP Address(es)

Each of VelaSync's network interface ports is configured with a unique static IP address when the unit is shipped (see the illustration under "Rear Panel Overview" on page 10 for details). If you need to change any of the IP addresses, proceed as follows.

> **Note:** The factory-programmed IP addresses can be found in the illustration: "Rear Panel Overview" on page 10.

There are two ways to change the IP address of a network interface:

1. Using an Ethernet cable, or hub/switch, via the Timekeeper web user interface ("Web UI"): Configuration > Networking: Interfaces: ethX
2. Or, by using `timekeeper_cli`, which can be opened also via IP, or by connecting a PC via null modem cable to the serial port. This is the preferred method if VelaSync has not yet been connected to a network.

The latter method is described below:

A. Connect the null modem cable between the serial ports of VelaSync, and your PC.

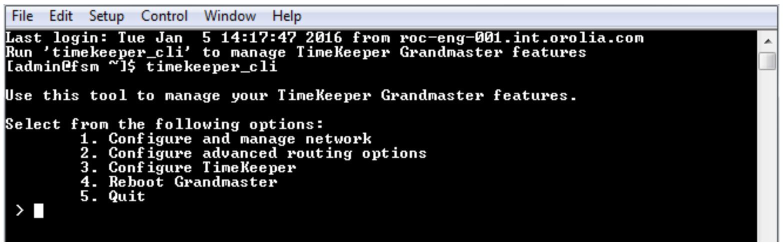
B. Start VelaSync by pressing the ON button on the upper right-hand corner of the front panel.

C. Start your PC, and open a terminal emulator program, such as PuTTY or Tera Term.

D. Configure your terminal emulator to use the serial port (COM1, typically), and a baud rate of 57400. If you are using SSH, you will need to provide your login credentials: The default user name is admin, the password is fsmlabs.

E. Once communication is established, in your CLI window, type: **timekeeper_cli**, and press **Enter**.

F. The first menu appears:



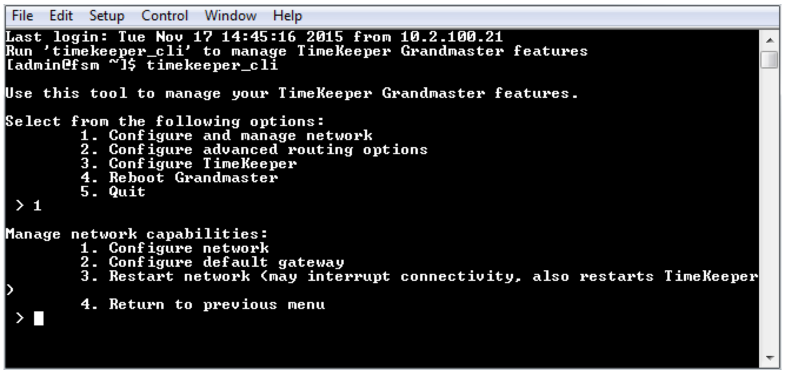
```
Last login: Tue Jan  5 14:17:47 2016 from roc-eng-001.int.orolia.com
Run 'timekeeper_cli' to manage TimeKeeper Grandmaster features
[admin@fsm ~]$ timekeeper_cli

Use this tool to manage your TimeKeeper Grandmaster features.

Select from the following options:
        1. Configure and manage network
        2. Configure advanced routing options
        3. Configure TimeKeeper
        4. Reboot Grandmaster
        5. Quit
 > █
```

Select option 1., **Configure and manage network**.

G. The next menu appears:



```
Last login: Tue Nov 17 14:45:16 2015 from 10.2.100.21
Run 'timekeeper_cli' to manage TimeKeeper Grandmaster features
[admin@fsm ~]$ timekeeper_cli

Use this tool to manage your TimeKeeper Grandmaster features.

Select from the following options:
        1. Configure and manage network
        2. Configure advanced routing options
        3. Configure TimeKeeper
        4. Reboot Grandmaster
        5. Quit
 > 1

Manage network capabilities:
        1. Configure network
        2. Configure default gateway
        3. Restart network (may interrupt connectivity, also restarts TimeKeeper
)
        4. Return to previous menu
 > █
```

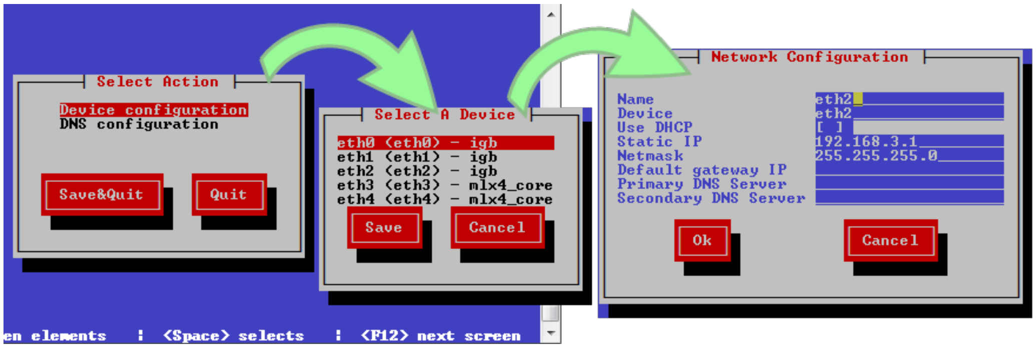
Select option 1., **Configure network**.

H. The following message appears:
Use this tool to configure the network, but do not rename or add devices. Please acknowledge this before configuring — Continue ? [y/n]

The purpose of this message is to inform you that these changes are not reversible via a reset. Acknowledge the message.

> **Caution:** Spectracom Technical Support is not obligated to providing support if such modifications had been made.

I. The network configuration menu will be displayed:



```
eth0 (eth0) - igb
eth1 (eth1) - igb
eth2 (eth2) - igb
eth3 (eth3) - mlx4_core
eth4 (eth4) - mlx4_core
```

```
Name                   eth2
Device                 eth2
Use DHCP               [ ]
Static IP              192.168.3.1
Netmask                255.255.255.0
Default gateway IP
Primary DNS Server
Secondary DNS Server
```

J. Press **Enter** to select the first menu option **Device Configuration**, and in the next menu, select the port (E0 thru E4) who you plan on using (see Step 2. under "Connections" on page 23). Enter your desired IP address, and subnet mask. (Normally, there is no need to change anything else.) Navigate by using the tab key, or arrow keys. Confirm selections by pressing Enter.

K. Repeat the previous step for other Ethernet ports, if required.

L. Leave the menus gracefully. Reboot the system to apply your changes.

M. To test your IP configuration, you may perform a Ping test from a network client computer .

You can now access the web user interface ("Web UI"): Using a web browser, enter the newly configured IP address of your VelaSync unit, and login into TimeKeeper. The user name is admin, the password is fsmlabs. (For security reason, change both immediately.) For more information, see "Logging into TimeKeeper" on page 64.

Note: If this is an upgrade and you have been using previous TimeKeeper versions, it is recommended that you force a full page reload (Ctrl-Shift-R on many browsers). This will make sure your browser loads the latest web interface from the grandmaster and provides all of the latest features.

Note: By default, SSH access is not enabled for VelaSync. To enable SSH, navigate to Configuration > Service & System Management, and under Manage Access, select the tab Enable SSH.

2.7 Verifying VelaSync Works

Between 1 to 5 minutes after turning on VelaSync, TimeKeeper should be active and running. Once synchronization is established, VelaSync will answer NTP queries and provide PTP service, as configured.

Note that initial GPS startup can take up to 15 minutes. You can monitor the progress via the **Status** tab.

Testing VelaSync's essential functionality encompasses two quick tests described below:

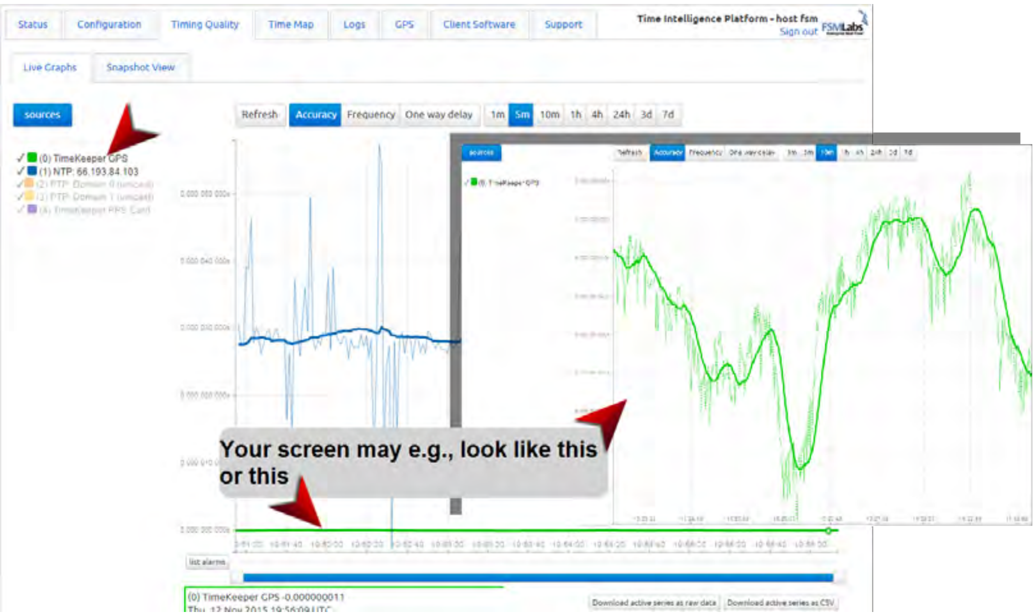
- Verify that TimeKeeper reports the presence of a GPS signal: See "Verifying the GPS Signal" below below.
- Test that NTP and/or PTP clients do, in fact, receive the time signal emitted by VelaSync: See "Verifying Network Configuration" on the next page below.

2.7.1 Verifying the GPS Signal

TimeKeeper's **Status** and **Timing Quality** tabs provide a clear summary of which source is being used, the current accuracy, and also details on the behavior of the various configured time sources over time.

To verify that a GPS signal is present:

1. In the TimeKeeper Web UI, navigate to **Timing Quality > Life Graphs**, and wait a few moments until enough data has been collected to build the graphical representation.
2. Verify that the **TimeKeeper GPS** line item is present and not grayed out under the Sources tab on the left.
3. Check for the presence of the **signal** (same color e.g., green) in the graph:


Status
Configuration
Timing Quality
Time Map
Logs
GPS
Client Software
Support
Time Intelligence Platform - host fsm
Sign out
FSMLabs
Live Graphs
Snapshot View
sources
Refresh
Accuracy
Frequency
One way delay
1m
5m
10m
1h
4h
24h
3d
7d
✓ 🟩 (0) TimeKeeper GPS
✓ 🟦 (1) NTP: 66.193.84.103
✓ (2) PTP: Domain 0 (unicast)
✓ (3) PTP: Domain 1 (unicast)
✓ (4) TimeKeeper PPS Card
list alarms
(0) TimeKeeper GPS -0.000000011
Download active series as raw data
Download active series as CSV

Your screen may e.g., look like this or this

Figure 2-6: Timing quality graphs

Another source of status information are the TimeKeeper logs, which are accessible under the **Logs** tab (see"The "Logs" Tab" on page 60 for more information). The log file contains a line for every update that TimeKeeper receives and how TimeKeeper is adjusting time for Source (0).

For more information on the log file contents, see "Creating an Audit Trail" on page 73.

2.7.2 Verifying Network Configuration

A Ping Test will tell you if VelaSync is accessible to clients.

For further testing ...

- …in an **NTP or Unicast PTP** environment, you have to go to the clients and configure them to use VelaSync as their timing server.
- …in a **Multicast PTP** environment, clients should see Multicast announce messages from your VelaSync unit, and will start synchronizing to VelaSync after a short while, if it is the best master.

CHAPTER 3

TimeKeeper

FSMLabs' TimeKeeper™ software is pre-installed on any VelaSync™ high-speed time server.

TimeKeeper's browser-based web user interface (referred to as "Web UI" throughout this manual) allows you to configure TimeKeeper and monitor your timing distribution network.

The following topics are included in this Chapter:

3.1 What is TimeKeeper?

TimeKeeper™ is a time synchronization software developed by FSMLabs, Inc. TimeKeeper leverages VelaSync's GPS-disciplined time and PPS, and distributes them over NTP and/or PTP, depending on how it is configured.

TimeKeeper is also capable of tracking other time sources, regardless of protocol, or type (e.g., NTP servers, PTP Grandmasters), cross-checks them against the onboard PPS and/or GPS source, and—if necessary—drives the system clock to match the configured source(s).

TimeKeeper will reject sources that disagree e.g., in offset or frequency in order to deliver accurate time to timing clients, and to use the approved sources for backup purposes, i.e. as a source for controlled failover.

This synchronization capability works across different protocols and also helps with the detection of network asymmetries, noisy clocks, or faulty hardware. Given time source(s) to track, TimeKeeper can deliver PTP, NTP, and more to thousands of clients.

TimeKeeper's advanced time tracking capabilities also can be utilized to centrally measure and log timing accuracies of all clients on the network. The results can be displayed in a network map, or logged for potential use with audit trails.

Because of its flexibility and sophisticated failover capability, TimeKeeper is very adaptable to different network topologies and resilient towards real-world network imperfections.

Please note that FSMLabs' TimeKeeper Software is licensed under the Software EULA, see:

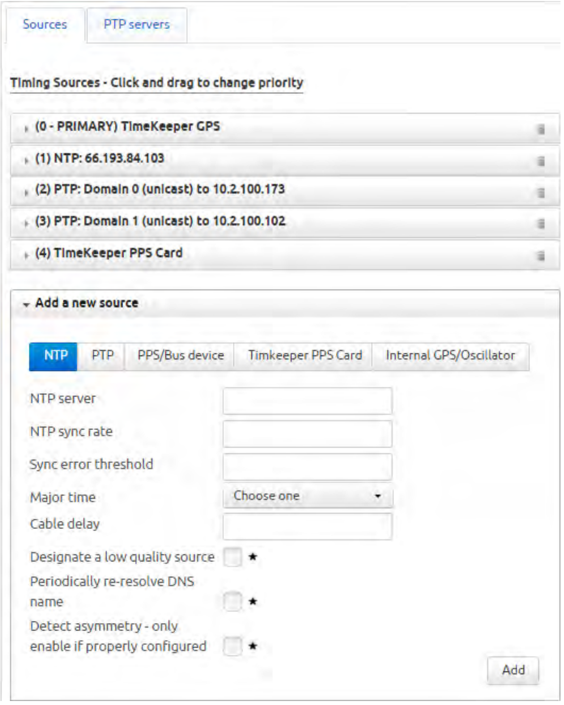
http://www.fsmlabs.com/Resources/tkeula/.

3.2 Why is TimeKeeper installed on VelaSync?

TimeKeeper is the software that ties VelaSync and the oscillator-disciplined GPS time it provides to the network and the NTP, PTP clients.

More specifically, TimeKeeper allows you to …

- … setup VelaSync to operate as an NTP server or PTP Grandmaster, or both.
- … reliably and accurately track and synchronize time from VelaSync's internal GPS receiver and other configured, external timing sources, and distribute time throughout networks, using NTP, and/or PTP.
- … interact with VelaSync, in order to configure:
  - Available time sources, including the on-board GPS receiver.
  - Standard network/event management tools, e.g. SNMP traps, syslog notifications, etc.
- … enable you to monitor timing performance across a network, using custom visualization tools.
- … alert you on quality issues with sources and clients with standard industry tools.
- … centrally log network-wide timing performance by building a consolidated audit trail.



Sources | PTP servers

Timing Sources - Click and drag to change priority

- (0 - PRIMARY) TimeKeeper GPS
- (1) NTP: 66.193.84.103
- (2) PTP: Domain 0 (unicast) to 10.2.100.173
- (3) PTP: Domain 1 (unicast) to 10.2.100.102
- (4) TimeKeeper PPS Card

Add a new source

NTP | PTP | PPS/Bus device | Timkeeper PPS Card | Internal GPS/Oscillator

NTP server

NTP sync rate

Sync error threshold

Major time: Choose one

Cable delay

Designate a low quality source □ *

Periodically re-resolve DNS name □ *

Detect asymmetry - only enable if properly configured □ *

Add

Figure 3-1: Adding a new timing source

3.3 How does TimeKeeper work?

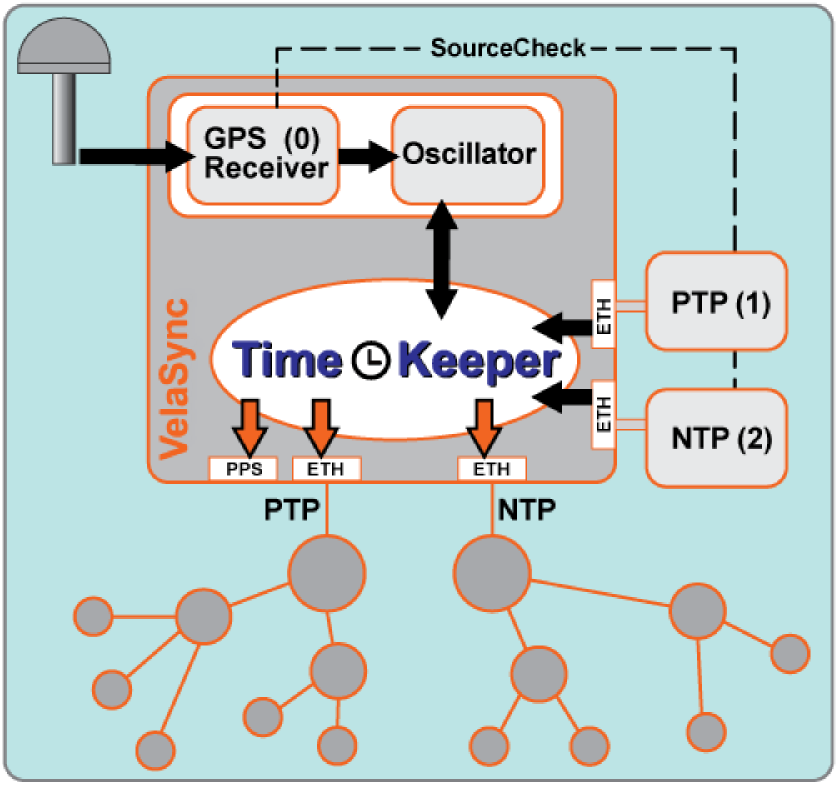


Figure 3-2: VelaSync/TimeKeeper system diagram

TimeKeeper synchronizes VelaSync's local clock to the highest priority source that is configured, i.e. typically GPS time. In the event this source is lost, TimeKeeper will then transparently and automatically failover to secondary, or tertiary sources as configured in advance.

TimeKeeper's integrated Sourcecheck feature will actively compare all time sources regardless of protocol, and proactively reject sources that have become invalid due to noise, a remote misconfiguration, or a spoof attack.

TimeKeeper then distributes this tightly synchronized local time via any of the used Ethernet connections, or the 1PPS line, respectively.

As a network administrator, you can interact with TimeKeeper and VelaSync by means of its web-based **user interface**:

The TimeKeeper "**Web UI**" is a versatile means to configure VelaSync without the need for command line interaction, and to centrally monitor timing performance for the entire network, using a timing network map, and other visualization features.

3.4 Protocols Supported by TimeKeeper

- NTP, versions 1,2,3, and 4
- PTP, IEEE 1588 versions 1 and 2
- TIME (RFC 868)
- 1PPS output

3.5 TimeKeeper Orientation Help

"Where to go from here?"

Now that you have read the TimeKeeper introduction above, you can …

a. …familiarize yourself with the web user interface ("**Web UI**") and its menus in the remainder of CHAPTER 3.

b. …browse through a collection of typical use cases ("**tasks**") system administrators face when setting up or using VelaSync in CHAPTER 4.

   Example tasks are:

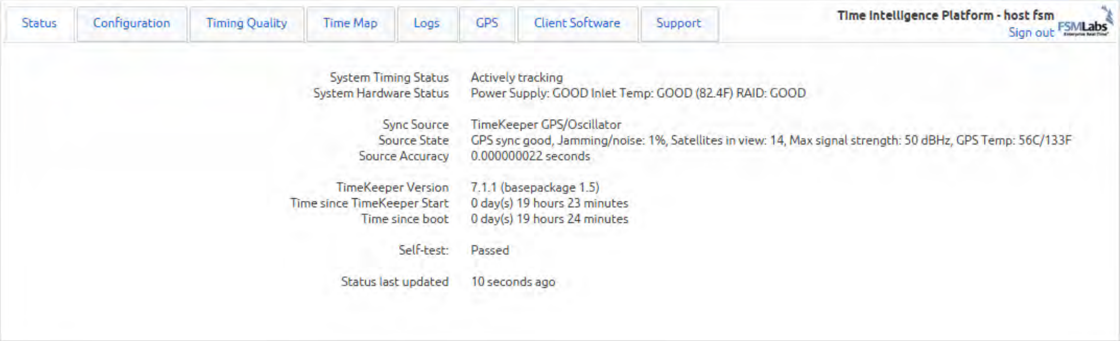
   - How to log into TimeKeeper?
   - How to monitor timing status?
   - How to use TimeKeeper's logging functionality (audit trail)?
   - How to configure Event Notifications?
   - How to replace a power supply or hard disk.

   For more information, see "Frequently Performed Tasks" on page 63.

c. Browse through additional **reference information** in the APPENDIX.

3.6 The "Status" Tab

VelaSync's default TimeKeeper configuration offers a set of web management tools that are accessible via the TimeKeeper Web UI. The initial screen displayed when pointing a web browser to the configured IP address will provide a status overview similar to this:



System Timing Status	Actively tracking
System Hardware Status	Power Supply: GOOD Inlet Temp: GOOD (82.4F) RAID: GOOD
Sync Source	TimeKeeper GPS/Oscillator
Source State	GPS sync good, Jamming/noise: 1%, Satellites in view: 14, Max signal strength: 50 dBHz, GPS Temp: 56C/133F
Source Accuracy	0.000000022 seconds
TimeKeeper Version	7.1.1 (basepackage 1.5)
Time since TimeKeeper Start	0 day(s) 19 hours 23 minutes
Time since boot	0 day(s) 19 hours 24 minutes
Self-test:	Passed
Status last updated	10 seconds ago

Figure 3-3: The Status screen

The items listed are:

System Timing Status

- Provides the tracking status e.g., "Actively tracking"

System Hardware Status

- Power Supply status
- Inlet Temperature [temperature in °F] (Note: Temperature data is not logged)
- RAID status

Sync Source

- TimeKeeper GPS/Oscillator

Source State

- GPS sync status (If the synchronization source is PTP, GPS data will not be shown here)
- Jamming/noise: x%
- Satellites in view: xx
- Max signal strength: xx dBHz
- GPS Temp: xx °C/ xxx °F

Source Accuracy

- [x] seconds

TimeKeeper Version

- version/package

Time since TimeKeeper Start

- [days] [hours] [minutes]

Time since boot

- [days] [hours] [minutes]

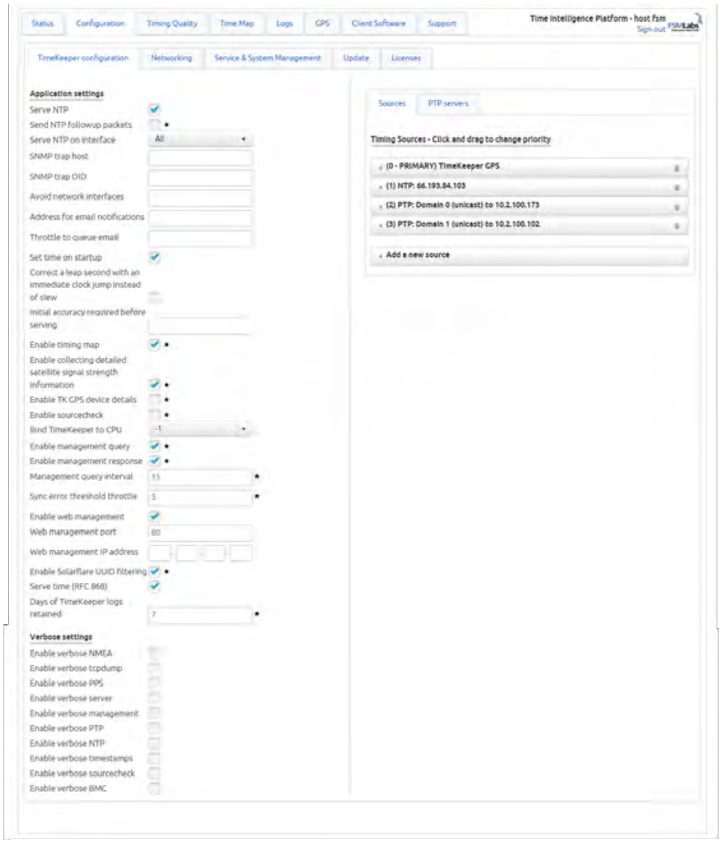
Self-test

- [Passed/Failed] Refers to state of VelaSync at the time of last boot. If a problem was reported, investigate the problem, and if resolve, if possible, or contact Technical Support.

Status last updated

- [x] seconds ago

3.7 The "Configuration" Tab



Application settings

Serve NTP	☑
Send NTP followup packets	□ *
Serve NTP on interface	All
SNMP trap host	
SNMP trap OID	
Avoid network interfaces	
Address for email notifications	
Throttle to queue email	
Set time on startup	☑
Correct a leap second with an immediate clock jump instead of slew	□
Initial accuracy required before serving	
Enable timing map	☑ *
Enable collecting detailed satellite signal strength information	☑ *
Enable TK GPS device details	□ *
Enable sourcecheck	□ *
Bind TimeKeeper to CPU	-1
Enable management query	☑ *
Enable management response	☑ *
Management query interval	15 *
Sync error threshold throttle	5 *
Enable web management	☑
Web management port	80
Web management IP address	
Enable Solarflare UUID filtering	☑ *
Serve time (RFC 868)	☑
Days of TimeKeeper logs retained	7 *

Verbose settings

Enable verbose NMEA	□
Enable verbose tcpdump	□
Enable verbose PPS	□
Enable verbose server	□
Enable verbose management	□
Enable verbose PTP	□
Enable verbose NTP	□
Enable verbose timestamps	□
Enable verbose sourcecheck	□
Enable verbose BMC	□

Timing Sources - Click and drag to change priority

- (0 - PRIMARY) TimeKeeper GPS
- (1) NTP: 66.193.84.103
- (2) PTP: Domain 0 (unicast) to 10.2.100.173
- (3) PTP: Domain 1 (unicast) to 10.2.100.102
- Add a new source

Figure 3-4: The Main Configuration Screen

What do the STARS mean?

The stars next to some of the menu items indicate that the corresponding setting/value is a TimeKeeper default value that will be written in the TimeKeeper configuration file, unless you change the setting/value.

If you mouseover it, a popup help text will appear in many cases. Once you edit a field, the star will disappear.

3.7.1 The "TimeKeeper Configuration" Subtab

This is the location where most of TimeKeeper's configuration settings are to be found.

The default TimeKeeper configuration will work well for many applications, i.e. the settings listed below need to be changed only if custom modifications have to be applied.

3.7.1.1 Application Settings

Serve NTP [checkbox; default = ON]

If ON, TimeKeeper will respond to NTP requests.

Send NTP followup packets [checkbox; default = OFF]

If enabled, TimeKeeper NTP server will also respond to NTP requests with a followup NTP packet. If VelaSync with TimeKeeper inside runs as a client, this allows processing of the followup to improve timing accuracy.

Serve NTP on interface [All, Eth0-4] (or, with option card: Eth0-6]

Determining the network interface that TimeKeeper should respond to NTP queries on. If TimeKeeper receives a request via that named interface, it will respond, but only on that interface. If set to "All", TimeKeeper listens and responds on all interfaces.

SNMP trap host [text field]

List of SNMP servers to send traps to.

In the field **SNMP trap host**, enter a host name or an IPv4 dotted notation address. TimeKeeper supports multiple SNMP trap destinations, to be entered in the following manner: host1, host2, host3.

SNMP trap OID

An OID string to use for sending all SNMP trap messages. If left unspecified, TimeKeeper will deliver traps as specified in the TimeKeeper MIB.

In the field **SNMP trap OID**, enter the OID to which all traps will be emitted e.g., “1.3.6.1.2.1.16.0.1”. Unless you need all traps sent to one OID, it is recommended you leave SNMPTRAPOID undefined in your configuration.

Avoid network interfaces

A comma separated list of network interface names. that TimeKeeper will not attempt to enable features on, e.g. timestamping capabilities.

Address for email notifications

List of email addresses (use comma to separate) to send alerts to [does currently not apply to TimeKeeper running on VelaSync].

Throttle to queue email

[Does currently not apply to TimeKeeper running on VelaSync]

A numeric value in seconds, to be used with email notification. If set, when an event occurs an initial email will be sent. Other emails that would be sent between then and the throttle timeout value will be queued.

Once the throttle timeout expires, any queued messages will be delivered as a single bundled email.

Set time on startup [checkbox]

If enabled, forcibly sets the time on startup regardless of offset, rather than trying to slew, for a faster sync on startup.

If disabled, TimeKeeper will slew in as long as the offset is less than ±5 seconds from the primary time source.

Correct a leap second with an immediate clock jump instead of slew [checkbox]

Per default, TimeKeeper introduces a leap second by "slewing". Alternatively, it is possible to introduce the leap second abruptly. For more information, see "Leap Seconds" on page 94.

Initial accuracy required before serving

Numeric value in seconds (i.e., 0.00001). If set, NTP/PTP/TIME protocols will not be served until the local clock accuracy meets this threshold.

Enable timing map [checkbox]

Enables the collection of information needed to build a map of the timing network.

Enable collecting detailed satellite signal strength information [checkbox]

Enables the collection of detailed GPS satellite angle/strength data.

Enable TK GPS device details [checkbox]

Enables the collection of detailed GPS states.

Enable sourcecheck [checkbox]

Will enable validity cross checks on timing sources. For more information, see "Validating a Timing Source" on page 73.

Bind TimeKeeper to CPU [Choose one, -1]

A numeric value indicating the CPU number that TimeKeeper should put all processes and threads on. A value of -1 will prevent TimeKeeper from applying affinities.

Enable management query [checkbox]

Enables the server to query PTP clients for their time sync quality data, which is stored on the server.

Enable management response [checkbox]

If enabled, allows the system to respond to incoming PTP management data requests.

Management query interval [15]

A numeric value in seconds that indicates how frequently to query PTP clients for their time sync quality data. Defaults to once every 15 seconds.

Sync error threshold throttle [5]

Numeric value in seconds that throttles the rate that TimeKeeper will send alerts about sync error threshold values being exceeded.

The default is 5, which will prevent TimeKeeper from sending alerts more often than every 5 seconds.

Enable web management [checkbox]

Enables the web management tools on the server.

Web management port [80]

A numeric value that indicates what port the web management should run on. If left unspecified, the web management tool will default to port 80.

Web management IP address [x.x.x.x]

By default, VelaSync will serve the Web UI (not the IPMI GUI) out any configured interface. You can restrict that if you want to by changing the **Web management IP address** option here: If you put an IP address in here, it will only serve the web out the interface with that IP address. If left blank VelaSync will serve the web out any configured interface.

Enable Solarflare UUID filtering [checkbox]

[Does not apply to VelaSync.]

Serve time (RFC 868) [checkbox]

If enabled, will cause TimeKeeper to respond to time requests (RFC 868) on all interfaces.

Days of TimeKeeper logs retained [7]

The default value is 7 days.

3.7.1.2 Verbose Settings

[All functions can be turned ON/OFF by means of a checkbox]

Enable verbose NMEA

Enables verbose logging of NMEA handling.

Enable verbose tcpdump

Enables tcpdump recording of PTP and NTP, kept alongside other TimeKeeper logs.

Enable verbose PPS

Enables verbose logging of PPS-based configurations.

Enable verbose server

Enables verbose logging of PTP behavior.

Enable verbose management

Enables verbose logging of management message behavior.

Enable verbose PTP

Enables verbose logging of PTP behavior.

Enable verbose NTP

Enables verbose logging of NTP behavior.

Enable verbose timestamps

Enables verbose logging of timestamping activity.

Enable verbose sourcecheck

Enables verbose logging of Sourcecheck-related activity.

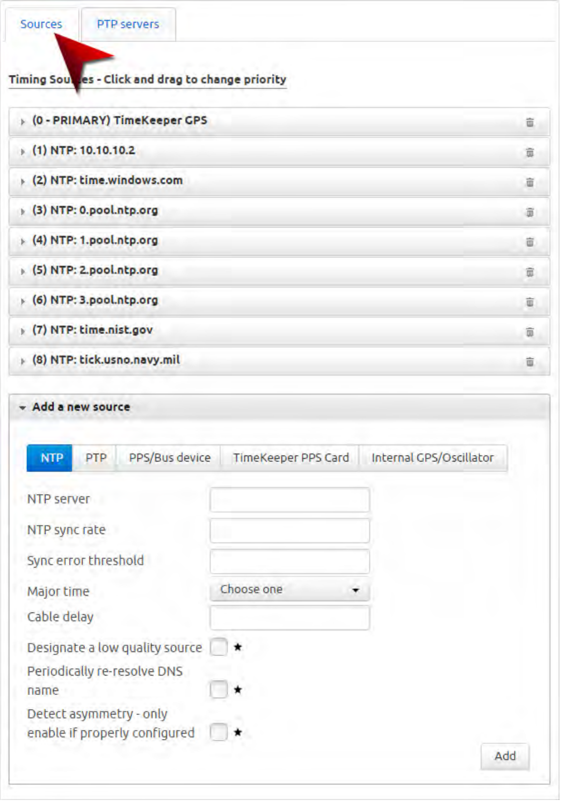
Enable verbose BMC

Enables verbose logging of any BMC algorithm activity when handling PTP data.

3.7.2 The Configuration Subtab "Sources"

The **Sources** subtab under **TimeKeeper Configuration** lists all sources currently configured. Here you can:

- change the priority order by dragging and dropping individual sources
- edit individual sources
- delete existing sources
- add new sources.



Timing Sources - Click and drag to change priority

- (0 - PRIMARY) TimeKeeper GPS
- (1) NTP: 10.10.10.2
- (2) NTP: time.windows.com
- (3) NTP: 0.pool.ntp.org
- (4) NTP: 1.pool.ntp.org
- (5) NTP: 2.pool.ntp.org
- (6) NTP: 3.pool.ntp.org
- (7) NTP: time.nist.gov
- (8) NTP: tick.usno.navy.mil

Add a new source

NTP server	
NTP sync rate	
Sync error threshold	
Major time	Choose one
Cable delay	
Designate a low quality source	☐ ★
Periodically re-resolve DNS name	☐ ★
Detect asymmetry - only enable if properly configured	☐ ★

Figure 3-5: The "Sources" subtab

3.7.2.1 Add an NTP Source

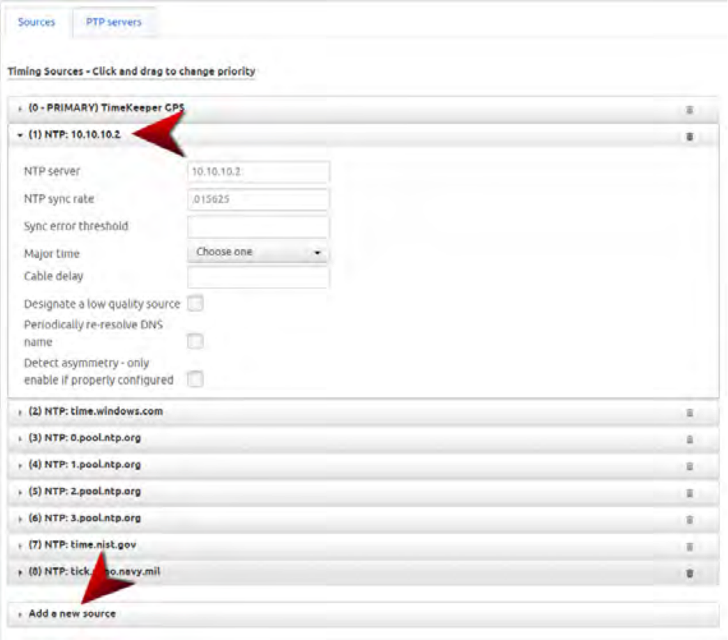
TimeKeeper supports nearly any form of NTP, and can achieve sub-microsecond accuracy with the protocol if the NTP implementation is adequate.

Typically, TimeKeeper running on VelaSync will be deployed as an NTP server, offering the following features:

- Accuracy in the low hundreds of nanoseconds
- Management capabilities to record the reported accuracy of NTP clients
- Support tens of thousands of clients per second from a single instance.

To change the configuration of an existing NTP source, or create a new NTP source:

- Navigate to **Configuration** > **TimeKeeper configuration**, and under the **Sources** tab, select the **NTP** source you would like to edit, or select **Add a new source** below.



Timing Sources - Click and drag to change priority

- (0 - PRIMARY) TimeKeeper GPS
- (1) NTP: 10.10.10.2

NTP server: 10.10.10.2
NTP sync rate: .015625
Sync error threshold:
Major time: Choose one
Cable delay:
Designate a low quality source □
Periodically re-resolve DNS name □
Detect asymmetry - only enable if properly configured □

- (2) NTP: time.windows.com
- (3) NTP: 0.pool.ntp.org
- (4) NTP: 1.pool.ntp.org
- (5) NTP: 2.pool.ntp.org
- (6) NTP: 3.pool.ntp.org
- (7) NTP: time.nist.gov
- (8) NTP: tick.[illegible]o.navy.mil
- Add a new source

Figure 3-6: Editing/Adding an NTP Source

The editable features are:

NTP server

The IP address or DNS name of the intended NTP server.

NTP sync rate

Rate at which to query the server, in packets/sec. A value of 0.9 would query every 1.1 seconds. A value of 0.5 stands for a query every 2 seconds. See also "NTP Query Rate" on page 98.

Sync error threshold

If the sync quality (offset) exceeds this floating point value, emit trap/syslog messages.

Major time

[Choose one: SOURCE0, 1, 2, etc.] Combine this source's second-scale time with time of day information from the source named here. [**Default**: unselect/Choose one]

Cable delay

Bias the clock to account for cable delays or asymmetries. With a long cable run that delays signal by 1ms, use a value of 0.001. TimeKeeper will subtract this value from the incoming timing signal.

Designate a low quality source

Assume source is very low quality and prioritize minimal changes to local oscillator to stabilize time.

Periodically re-resolve DNS name

If enabled, will cause the source to periodically re-resolve the DNS name specified for the NTP source.

Detect asymmetry

Enable to detect and measure network link asymmetry. Your network needs to be properly configured to test for asymmetries. For more information, see "Detecting Network Asymmetries" on page 76.

> **Note:** Do not forget to click Save TimeKeeper changes in the upper right corner, once you have applied your changes.

Additional information about adding sources can be found under "Setting Up Timing Sources" on page 70.

3.7.2.2 Add a New PTP Source

TimeKeeper on VelaSync can be deployed as an IEEE 1588 PTP Grandmaster and communicate with almost any PTP boundary clock and PTP client on the market, regardless whether it is a hardware appliance, a software instance, or a PTP-aware networking component.

TimeKeeper can serve IEEE 1588, Versions 1 and 2, in a number of ways. It can serve multiple domains via multiple interfaces, allowing traffic to be matched properly with the network. This avoids the introduction of link asymmetries that can cause clients to be unintentionally biased.

Key features of TimeKeeper running on VelaSync as a PTP Grandmaster include:

- Support for the Default, Telecom, and Hybrid PTP profiles
- Serves via many domains on many interfaces for link redundancy and managed PTP distribution
- Supports standard and extended management formats to collect client and Grandmaster information in one centralized location
- Can act solely as a management node on the network, collecting and analyzing timing data of discovered clients and Grandmasters.

PTP is very reliant on Multicast traffic, particularly in the default profile. In this mode, time is distributed from the Grandmaster via Multicast, and every client that requests information from the Grandmaster communicates via Multicast. Since every client will see every other client's

Grandmaster request, a lot of network and processor bandwidth will be consumed, which will likely cause problems in large networks (which may have thousands of nodes).

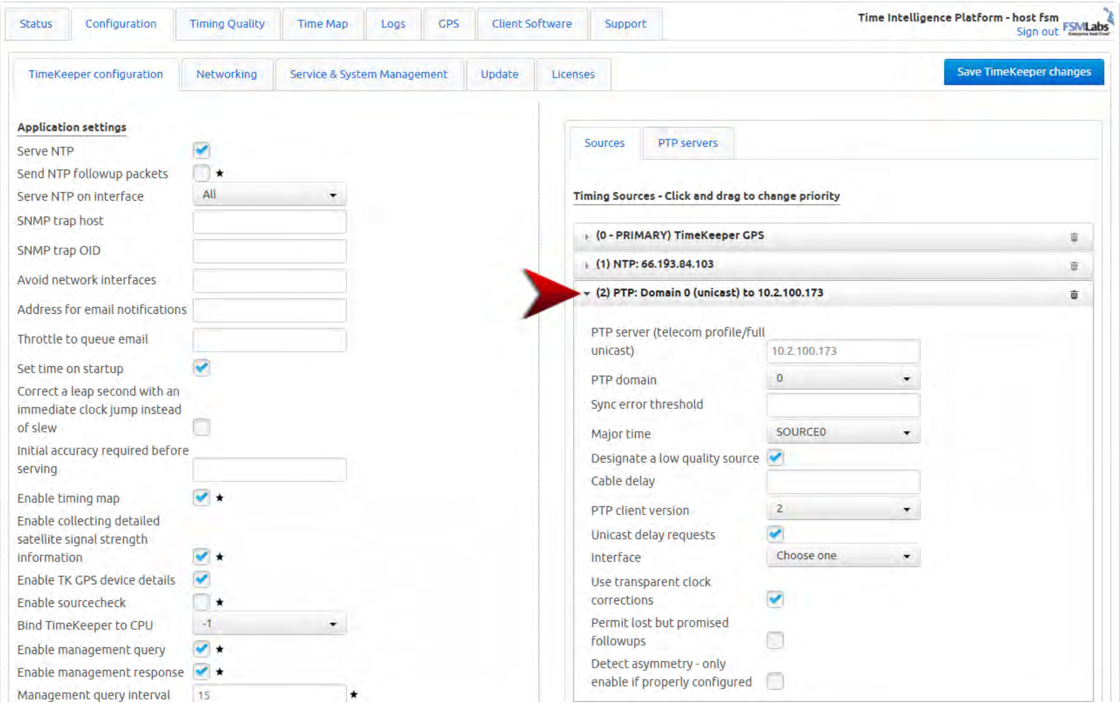
A hybrid mode helps to avoid creating extra Multicast traffic by allowing for the Grandmaster to distribute time via multicast to its clients, while the clients that need data from the Grandmaster (e.g., delay information) make direct Unicast queries.

Another option is full Unicast – also known as the Telecom profile. In this case, the client subscribes to unicast updates from the Grandmaster, and also exchanges all other information from the Grandmaster over a unicast connection. This can be ideal for longer links where multicast traffic is not an option.

Note that—contrary to NTP, where you just check the box **Serve NTP** under the **TimeKeeper Configuration** subtab—PTP requires you to configure each interface separately. This ensures e.g., that PTP for a 10 Gb network is being specifically delivered on a 10 Gb link. It also provides redundancy and a failover option for clients.

To change the configuration of an existing PTP source, or create a new PTP source:

» Navigate to **Configuration** > **TimeKeeper configuration**, and under the **Sources** tab, select the **PTP** source you would like to edit, or select **Add a new source** below.



Application settings

Serve NTP ☑
Send NTP followup packets ☐ ★
Serve NTP on interface: All
SNMP trap host:
SNMP trap OID:
Avoid network interfaces:
Address for email notifications:
Throttle to queue email:
Set time on startup ☑
Correct a leap second with an immediate clock jump instead of slew ☐
Initial accuracy required before serving:
Enable timing map ☑ ★
Enable collecting detailed satellite signal strength information ☑ ★
Enable TK GPS device details ☑
Enable sourcecheck ☐ ★
Bind TimeKeeper to CPU: -1
Enable management query ☑ ★
Enable management response ☑ ★
Management query interval: 15 ★

Timing Sources - Click and drag to change priority

(0 - PRIMARY) TimeKeeper GPS
(1) NTP: 66.193.84.103
(2) PTP: Domain 0 (unicast) to 10.2.100.173

PTP server (telecom profile/full unicast): 10.2.100.173
PTP domain: 0
Sync error threshold:
Major time: SOURCE0
Designate a low quality source ☑
Cable delay:
PTP client version: 2
Unicast delay requests ☑
Interface: Choose one
Use transparent clock corrections ☑
Permit lost but promised followups ☐
Detect asymmetry - only enable if properly configured ☐

Figure 3-7: Editing an existing NTP source

The editable features are:

PTP server (telecom profile/full unicast)

IP address or domain name of the PTP server to request a unicast lease from. If you enter an IP address or server name, TimeKeeper assumes your intent is to use Unicast. If you leave the field blank, TimeKeeper will use PTP multicast.

PTP domain

The numeric domain that TimeKeeper will watch for PTP data on.

Sync error threshold

If the sync quality (offset) exceeds this floating point value, emit trap/syslog messages.

Major time

[Choose one: SOURCE0, 1, 2, etc.] Combine this source's second-scale time with time of day information from the source named here. [**Default**: unselect/Choose one]

Designate a low quality source

Assume source is very low quality and prioritize minimal changes to local oscillator to stabilize time.

Cable delay

Bias the clock to account for cable delays or asymmetries. With a long cable run that delays signal by 1ms, use a value of 0.001. TimeKeeper will subtract this value from the incoming timing signal.

PTP client version

Version 1 refers to IEEE 1588-2002, and the preferred Version 2 refers to IEEE 1588-2008.

Unicast delay requests

If checked, unicast delay requests back to the server will be enabled.

Interface

This source should watch the named interface for PTP data. The interface name has to correspond with a valid Linux network device name.

Use transparent clock corrections

If **disabled**, this source will not make use of any transparent clock information provided in the PTP data, otherwise it will apply the correction to the timing data.

Permit lost but promised followups

If **disabled**, a PTP grandmaster that promises a followup message must deliver one in order for this source to use a given time update.

If **enabled**, a failed followup delivery will not prevent the sample from being updated.

The default (= disabled) is recommended in nearly all deployments, as missing followups indicate a problem with PTP delivery or the grandmaster.

Detect asymmetry – only enable if properly configured

Enable to detect and measure network link asymmetry. Your network needs to be properly configured to test for asymmetries. For more information, see "Detecting Network Asymmetries" on page 76.

> **Note:** Do not forget to click Save TimeKeeper changes in the upper right corner, once you have applied your changes.

Additional information about adding sources can be found under "Setting Up Timing Sources" on page 70.

3.7.2.3 Add PPS/Bus Device

This functionality does not apply to VelaSync.

3.7.2.4 Add TimeKeeper PPS Card

This functionality currently does not apply to VelaSync.

3.7.2.5 Add Internal GPS/Oscillator

In the standard configuration, TimeKeeper distributes the time provided by VelaSync's high-quality oscillator. The oscillator is disciplined by the GPS time. When no GPS is available e.g., because the signal is lost temporarily, the oscillator will be in Holdover mode (by default, for 7200 seconds [2 hours]), before TimeKeeper starts using other previously configured timing sources e.g., a PTP server.

Configuring the "Internal GPS/Oscillator" timing source may become relevant in the following situations:

a. If you accidentally deleted your GPS timing source (0)), and need to create a new one.

b. To add the oscillator to the list of permitted timing sources, using it as the **lowest** priority source. This will allow TimeKeeper to distribute the time and 1PPS signal provided by the un-disciplined oscillator in the event that the GPS and all other configured timing sources are lost.

c. To disable GPS steering for timing source (0), thereby allowing TimeKeeper to use the time provided by the oscillator, even if GPS is not available. In other words, the oscillator is not disciplined by any reference, i.e. it is in **Freerun** mode, and yet TimeKeeper is allowed to broadcast its time/1PPS signal. This may be useful for system testing (e.g., if no GPS antenna is yet installed), or for other, special use cases if the time distributed does not need to be linked to UTC.

See "Setting Up Timing Sources" on page 70 to learn how to configure these use cases.

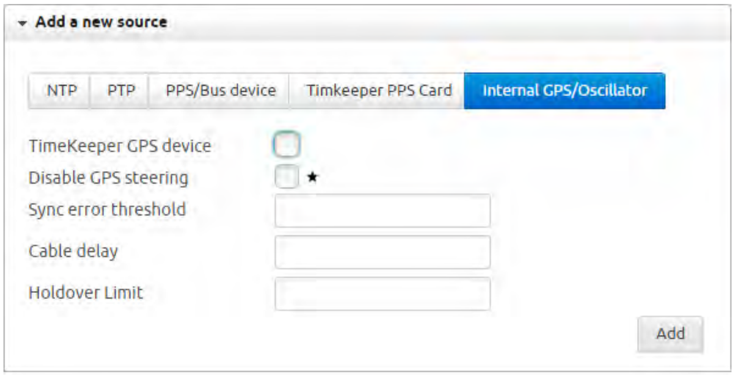


Figure 3-8: Window "Add a new Source: Internal GPS/Oscillator"

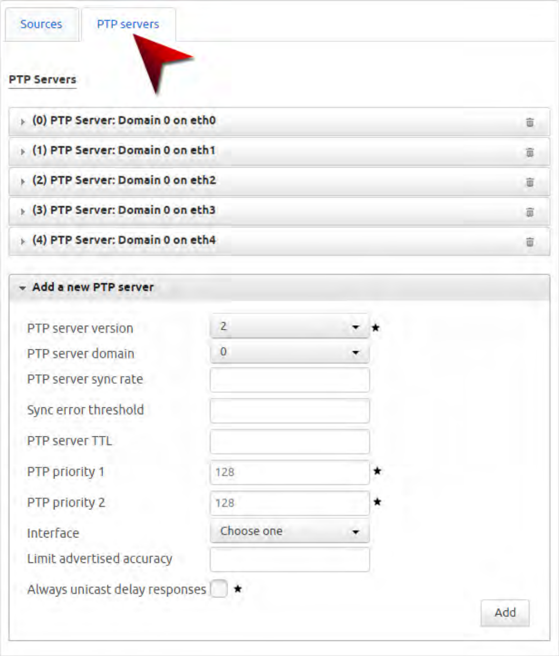
The menu items under **Internal GPS/Oscillator** are:

- **TimeKeeper GPS device**: [checkbox, default: checked] En-/Disable GPS input: This must be checked in order for TimeKeper to use VelaSync's GPS time. If unchecked, and **Disable GPS steering** checked, TimeKeeper will use the time and 1PPS signal provided by the oscillator indefinitely, even though the oscillator is at no point in time disciplined by a GPS signal.
- **Disable GPS steering**: [checkbox, default: unchecked] Only check this box in conjunction with the **TimeKeeper GPS device** disabled, so as to allow TimeKeeper to use the time and 1PPS signal provided by the free running oscillator, i.e. in the absence of a GPS signal.
- **Sync error threshold**: If the sync quality (offset) exceeds this floating point value, emit trap/syslog messages.
- **Cable delay**: Bias the clock to account for cable delays or asymmetries. With a long cable run that delays signal by 1ms, use a value of 0.001. TimeKeeper will subtract this value from the incoming timing signal.
- **Holdover Limit**: Determine for how long TimeKeeper is allowed to use the time and 1PPS signal provided by the free running oscillator, before TimeKeeper cross-checks time against other sources (in seconds). For more information on Holdover, see "Holdover" on page 91.

3.7.3 The Configuration Subtab "PTP Servers"

The **PTP Servers** subtab under **TimeKeeper Configuration** lists all PTP servers currently configured. Here you can:

- edit existing PTP servers
- delete existing PTP servers
- add new PTP servers.



PTP Servers

- (0) PTP Server: Domain 0 on eth0
- (1) PTP Server: Domain 0 on eth1
- (2) PTP Server: Domain 0 on eth2
- (3) PTP Server: Domain 0 on eth3
- (4) PTP Server: Domain 0 on eth4

Add a new PTP server

PTP server version: 2 ★
PTP server domain: 0
PTP server sync rate:
Sync error threshold:
PTP server TTL:
PTP priority 1: 128 ★
PTP priority 2: 128 ★
Interface: Choose one
Limit advertised accuracy:
Always unicast delay responses □ ★

Figure 3-9: "PTP Servers" subtab

When adding a new PTP server, or edit an existing server, the following fields need to be populated. When done, click **Add** (for adding a new PTP server), then **Save KimeKeeper changes**.

The editable fields are:

- **PTP server version**: [Version 1, or 2]
- **PTP server domain**: [1 – 255]]
- **PTP server sync rate**: Rate at which the server will send timing updates, in packets/sec. A value of 0.9 would send sync packets every 1.1 seconds.
- **Sync error threshold**: If the sync quality (offset) of any of the clients of this server exceed this floating point value, trap/syslog messages will be emitted.
- **PTP server TTL**: Numeric value indicating time to live for PTP packets.
- **PTP priority 1**: Numeric value from 0 to 255, with lower values taking precedence.
- **PTP priority 2**: Numeric value from 0 to 255, with lower values taking precedence.
- **Interface**: [Choose one: eth0, 1, 2, etc.] Bind communications to this network device.

- **Limit advertised accuracy**: If set, the server will limit the accuracy advertised in PTP announce messages to be no better than the value provided (in seconds). This is helpful when trying to prevent some clients from switching between grandmasters quickly.
- **Always unicast delay responses**: [checkbox Y/N] If set, the server will always respond to delay requests with unicast delay responses. Otherwise it will always respond in the form of the request.

3.7.4 The "Networking" Subtab

3.7.4.1 "Network settings"

The **Network settings** drop down menu options are:

- **Gateway**: The gateway (default router) address, if needed, to enable communication from outside of the local network. By default, the gateway is disabled.
- **Hostname**: Name assigned to the device.
- **DNS 0**: Default Domain Name Server.
- **DNS 1**: Alternate Domain Name Server.

3.7.4.2 Interfaces: "Network interfaces"

IPMI

The Intelligent Platform Management Interface (IPMI) is a protocol that allows for out-of-band management of computer systems, even when they are turned off. IPMI is active whenever the server is connected to power.

VelaSync has a dedicated IPMI Ethernet interface (see rear panel illlustration, item no. 12 under "Front Panel Overview" on page 8.) By default, the IPMI interface uses DHCP to obtain an IP address. A static IP address can also be set if DHCP is not desired.

To find out the IP address of the unit's IPMI interface:

- In TimeKeeper, navigate to **Configuration > Networking > Interfaces**.
- (The IPMI password is ADMIN and the login for IPMI is ADMIN.)

The **IPMI** drop down menu options are:

- **Status**: Link: [yes] [N/A]
- **Enabled**: [checkbox]
- **DHCP**: [checkbox] Dynamic Host Configuration Protocol enabled/disabled
- **IP address**: The unique static address assigned to this VelaSync unit by the network administrator. Make sure the chosen address is outside of the DHCP range of your DHCP server.

- **Gateway**: The gateway (default router) address is needed if communication to this VelaSync unit is made outside of the local network. By default, the gateway is disabled.
- **Netmask**: The subnet mask defines the number of bits taken from the IP address that are used in the network portion. The number of network bits used in the net mask can range from 8 to 30 bits.

eth[x]

The **eth[x]** drop down menu options are:

- **Status**: Link: N/A
- **Enabled**: [checkbox]
- **DHCP**: [checkbox] Dynamic Host Configuration Protocol enabled/disabled
- **IP address**: The unique static address assigned to this VelaSync unit by the network administrator. Make sure the chosen address is outside of the DHCP range of your DHCP server.
- **Netmask**: The subnet mask defines the number of bits taken from the IP address that are used in the network portion. The number of network bits used in the net mask can range from 8 to 30 bits.

Add a new VLAN

TimeKeeper supports VLAN interfaces. Once the device is present, TimeKeeper can use it just like any other network device.

The **VLAN** drop down menu options are:

Enabled: [checkbox]

- **Root Interface**: [Choose one/eth0 – 4/(6)]
- **VLAN Tag**: Specify a tag ID (number) for all messages sent through the VLAN [1 – 4095]
- **DHCP**: [checkbox] Dynamic Host Configuration Protocol enabled/disabled
- **IP address**: The subnet mask defines the number of bits taken from the IP address that are used in the network portion. The number of network bits used in the net mask can range from 8 to 30 bits.
- **Netmask**: The subnet mask defines the number of bits taken from the IP address that are used in the network portion. The number of network bits used in the net mask can range from 8 to 30 bits.

3.7.5 The Subtab "Service & System Management"

Manage TimeKeeper

Restart TimeKeeper: You will be asked to confirm this command. A counter will be displayed in the top right corner, stating when the restart will be completed. When completed, you will be asked to log back in.

Stop TimeKeeper: This button can be used to shut down TimeKeeper. It is recommended to use this only if advised by Technical Support, since re-starting TimeKeeper will require the CLI.

Set admin password: You need to login via https to create a new administrator password.

Set readonly password: You need to login via https to create a new readonly user password.

Set loguser password: You need to login via https to create a new loguser password.

Manage Access

Disable SSH: You will be asked to confirm your decision to turn off the (encrypted) Secure Shell protocol, which allows to login remotely/operate securely over an unsecured network.

Enable root login: Standard shell access as "root" is not normally permitted or recommended.

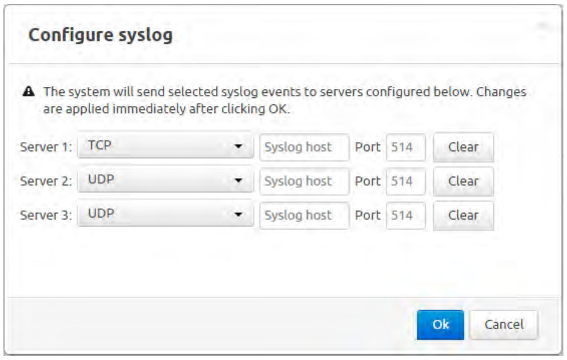
Caution: Please do not enable Enable root login, unless asked to by Spectracom Tech Support.

Enable loguser login: You will be asked to confirm that you want to enable loguser login access.

Enable readonly login: You will be asked to confirm that you want to enable readonly login access.

Manage Communication

Configure syslog: Log entries can be configured to be automatically sent to a Syslog Server for external log storage.



Configure syslog

The system will send selected syslog events to servers configured below. Changes are applied immediately after clicking OK.

Server 1: TCP Syslog host Port 514

Server 2: UDP Syslog host Port 514

Server 3: UDP Syslog host Port 514

For each server, determine:

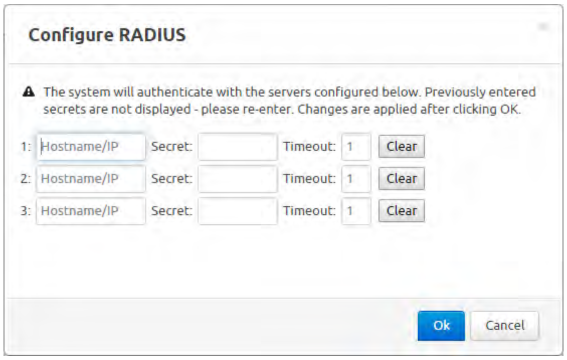
a. The transport layer protocol: [UDP: User Datagram Protocol], or [TCP: Transmission Control Protocol]

b. The host name

c. The Port number.

En-/Disable SNMP queries: Start authenticating

Configure RADIUS: RADIUS authentication provides the means to use an external RADIUS server to authenticate the user accounts when logging in to VelaSync. RADIUS allows the login password for user-created accounts to be stored and maintained in a central RADIUS or server on the network. This function greatly simplifies password management. Instead of having to change the password in many network appliances when a password needs to be changed, if a user password is changed in the RADIUS or RADIUS server, it automatically changes the login password for all of the appliances that are using the RADIUS server to authenticate a user login. In order to use the RADIUS authentication capability of the SecureSync, it needs to first be configured with the appropriate settings in order to be able to communicate with the RADIUS server(s) on the network.



Configure RADIUS

The system will authenticate with the servers configured below. Previously entered secrets are not displayed - please re-enter. Changes are applied after clicking OK.

1: Hostname/IP Secret: Timeout: 1 Clear

2: Hostname/IP Secret: Timeout: 1 Clear

3: Hostname/IP Secret: Timeout: 1 Clear

For each server, determine:

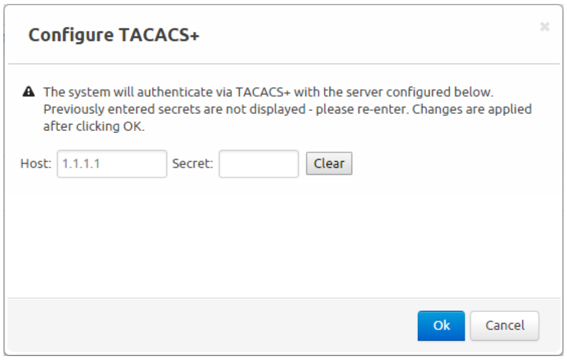
a. **The hostname/IP**: Enter either the hostname or IP address of the RADIUS server on the network with which you wish VelaSync to authenticate.

b. **The secret**: Enter the secret key which is shared by VelaSync and the RADIUS server (the key is used to generate an MD5 hash).

c. **The timeout**: Defines the Timeout that VelaSync will wait to communicate with the RADIUS server

Enable RADIUS: Start authenticating

Configure TACACS+: TACACS+ provides centralized authorization and accounting services of user access to VelaSync, and other routers and network access servers. Click **Configure TACACS+** to open the window shown below:



Configure TACACS+

The system will authenticate via TACACS+ with the server configured below. Previously entered secrets are not displayed - please re-enter. Changes are applied after clicking OK.

Host: 1.1.1.1 Secret:

Populate the following fields:

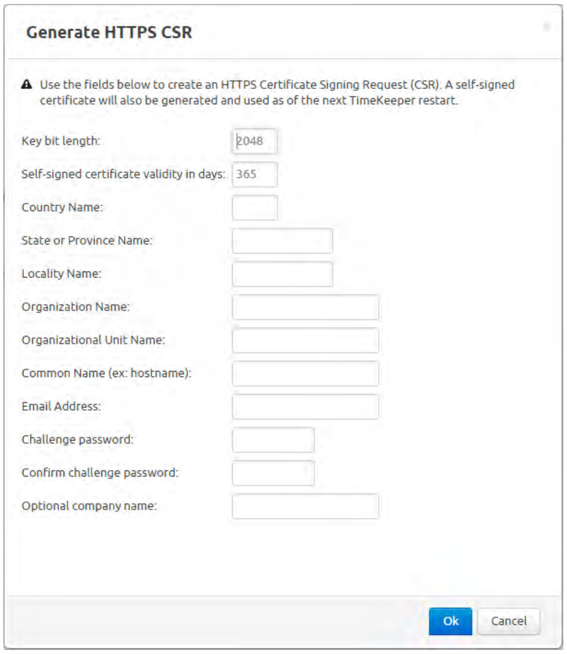
- **Host**: Specify the hostname of the TACACS+ server.
- **Secret**: Specify the encryption key for encrypting and decrypting all traffic between VelaSync and the TACACS+ daemon.

Enable TACACS+: Start authenticating

Generate HTTPS CSR: HTTPS provides secure/encrypted, web-based management and configuration of VelaSync from a PC. An SSL certificate is required to be stored in VelaSync in order to provide a secure HTTPS connection.

If using only self-signed certificates, you should choose values based on your company’s security policy.

For additional information about HTTPS see "HTTPS Support" on page 100.



Generate HTTPS CSR

Use the fields below to create an HTTPS Certificate Signing Request (CSR). A self-signed certificate will also be generated and used as of the next TimeKeeper restart.

Key bit length: 2048

Self-signed certificate validity in days: 365

Country Name:

State or Province Name:

Locality Name:

Organization Name:

Organizational Unit Name:

Common Name (ex: hostname):

Email Address:

Challenge password:

Confirm challenge password:

Optional company name:

Populate the following fields:

- **Key bit length**: The default key bit length is 2048. It is recommended that the RSA Private Key Bit Length be a power of 2 or multiple of 2. The key bit length chosen is typically 1024, but can range from 512 to 4096. Long key bit lengths of up to 4096 are not recommended because they can take hours to generate. The most common key bit length is the value 1024. Using a lower number may compromise security and is not recommended
- **Self-signed certificate validity in days:** How many days before the certificate expires. The default is 365.
- **Country Name**: This two-letter country code should match the ISO-3166-1 value for the country in question.
- **State or Province Name**: From the address of the organization creating up the certificate
- **Locality Name**: Locale of the organization creating the certificate
- **Organization Name**: The name of the organization creating the certificate
- **Organizational Unit Name**: The applicable subdivision of the organization creating the certificate
- **Common Name**: This is the name of the host being authenticated. The Common Name field in the X.509 certificate must match the hostname, IP address, or URL used to reach the host via HTTPS.
- **Email Address**: This is the email address of the organization creating the certificate.
- **Challenge password**: Valid response password to server challenge.
- **Confirm challenge password**: Re-enter password.
- **Optional company name**: An optional name for the organization creating the certificate.

Enter the information, and wait while the request is generated. It may take several minutes for VelaSync to create the certificate request and the private key. The larger the key, the longer amount of time is required. If a system is rebooted during this time, the certificate will not be created.

Once the key has been created, you can submit it to an external or corporate- internal Certificate Authority (CA) for the creation of a verifiable certificate.

Upload HTTPS Certificate: Choose a certificate file previously generated, and click to apply the authentication. (TimeKeeper will be restarted.)

Manage System

Restart system: Restart TimeKeeper and VelaSync.

Shutdown system: Use this button to gracefully shut down VelaSync. See also "Powering OFF VelaSync" on page 76.

Factory reset: The factory settings for network configuration and time service settings can be restored with a Factory reset. Once booted, the system defaults back to factory original settings.

Save GM config: The TimeKeeper Web UI can be used to save an existing configuration (GM = GrandMaster) as a downloadable file. This file can be used as a backup of the configuration, or a means of deploying the same configuration to multiple VelaSync easily.

> Note: You need to login via https to utilize this feature.

The configuration file generated represents the VelaSync configuration data only, and does not contain binary state, like the installed TimeKeeper version.

> Note: The generated file does contain potentially sensitive contents, like hashed system password files, RADIUS and TACACS+ secrets, etc. Please treat the file with care, and properly secure it.

Restore GM config: The configuration file generated under **Save GM config** can be uploaded via the **Restore GM config** button. (GM = Grandmaster).

3.7.6 The Subtab "Update"

Update TimeKeeper

Check TimeKeeper version and upgrade: Click to see which TimeKeeper version is installed on your VelaSync, and if a newer version is available. If a newer version is available, and you have been notified about it, paste the URL you have been provided with into the field.

Check Timekeeper version: Click to see which TimeKeeper version is installed on your VelaSync.

Update TimeKeeper install: Update TimeKeeper, using an installer file stored locally on the computer that is used to access VelaSync.

Update TimeKeeper base package: The base package includes operating system components which are required by TimeKeeper, and is maintained by FSMLabs.

> Note: See under the Status tab for information on the currently installed TimeKeeper and Basepackage version.

Update License

Upload new license file: VelaSync has a permanent license file that does not require regular maintenance updates, unless new features are being introduced.

Latest TimeKeeper Release

The latest TimeKeeper release is always available for download at:

- http://license.fsmlabs.com/timekeeper_release/.

3.7.7 The Subtab "Licenses"

Under this tab you can find license information on the currently installed version of TimeKeeper.

3.8 The "Timing Quality" Tab

The Web UI allows you to see how all of your time sources are behaving compared to each other. This includes offset information, one way delay data, and more.

3.8.1 Live Graphs view

The plotted sources and quality will vary by deployment. Here is an example:

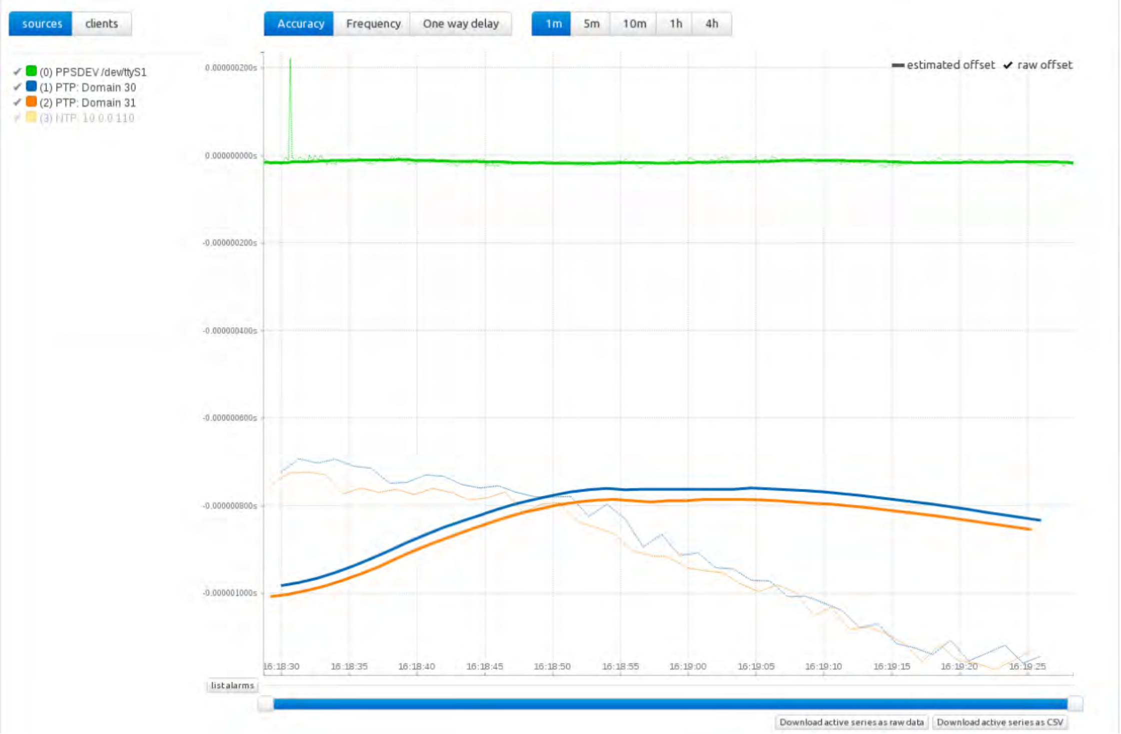
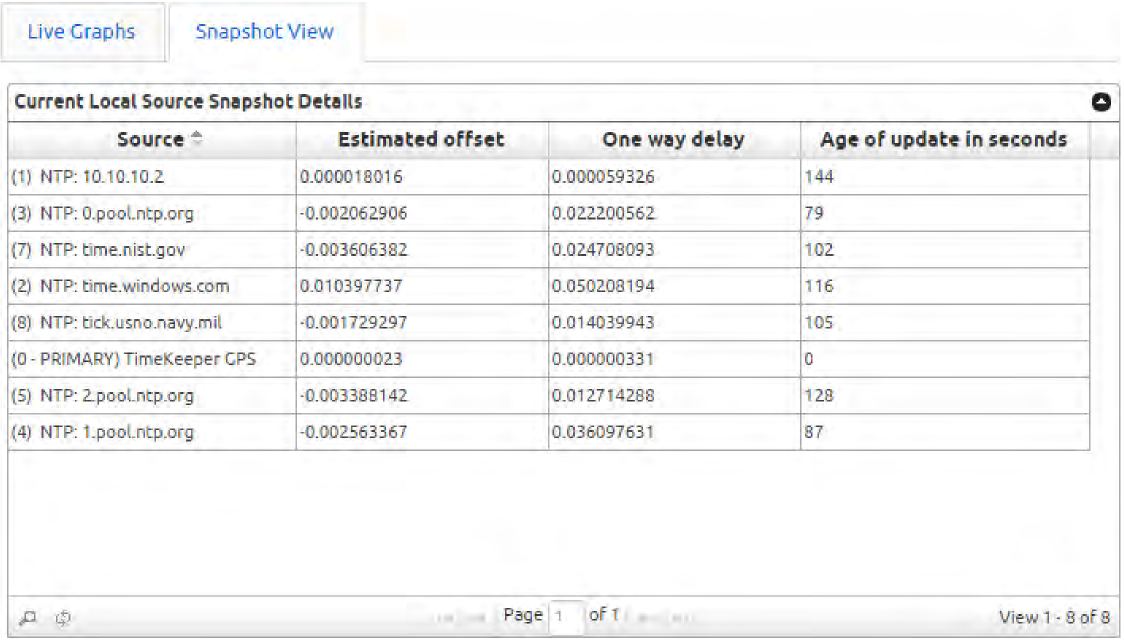


Figure 3-10: The "Live Graphs" timing quality screen

The plotted data can be downloaded in CSV format or as raw data. Click either button in the lower right corner of the screen to initiate the downloading process.

3.8.2 Snapshot View

The Snapshot view offers not only a means to check the presense of all sources (the illustration below suggests that there is a problem with Source (6), for example), but also provides specific current data for each of the present sources. Note that NTP sources are generally not updated as often as other sources.



Current Local Source Snapshot Details

Source	Estimated offset	One way delay	Age of update in seconds
(1) NTP: 10.10.10.2	0.000018016	0.000059326	144
(3) NTP: 0.pool.ntp.org	-0.002062906	0.022200562	79
(7) NTP: time.nist.gov	-0.003606382	0.024708093	102
(2) NTP: time.windows.com	0.010397737	0.050208194	116
(8) NTP: tick.usno.navy.mil	-0.001729297	0.014039943	105
(0 - PRIMARY) TimeKeeper GPS	0.000000023	0.000000331	0
(5) NTP: 2.pool.ntp.org	-0.003388142	0.012714288	128
(4) NTP: 1.pool.ntp.org	-0.002563367	0.036097631	87

Figure 3-11: Snapshot view of current sources

3.9 The "Time Map" Tab

TimeKeeper also builds a map of the timing network, from all accessible sources to all clients, as far as can be reached. It also includes any other clients found on the network, and other time sources even if a source is not a configured on the local host.

These maps can be very extensive and in some cases point out issues with the current timing systems in place.

Here is a snapshot of a time map generated with TimeKeeper:

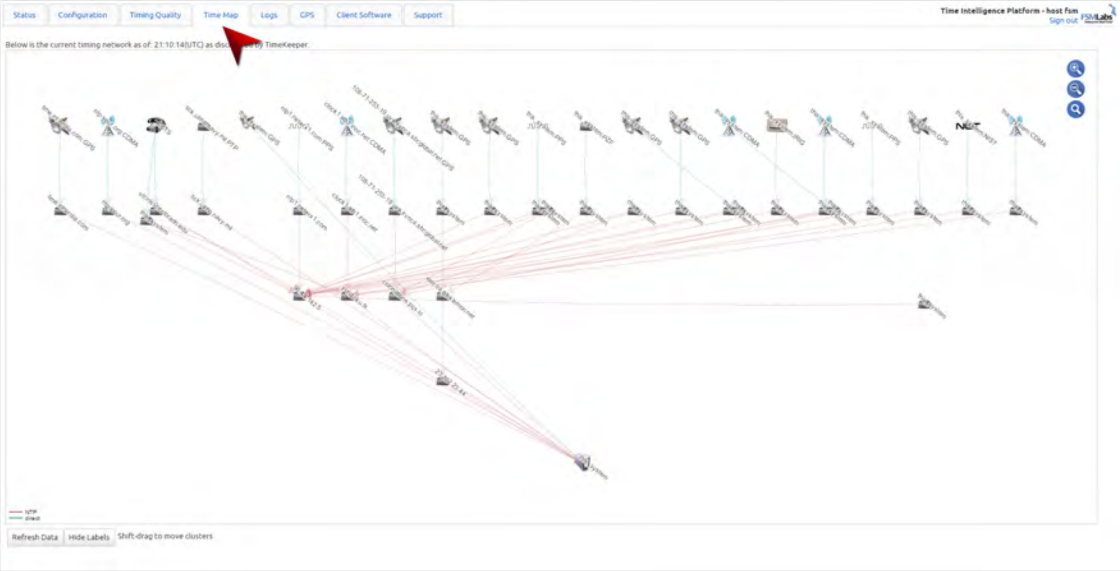


Figure 3-12: The "Time Map" screen

The connecting lines are color-coded:

- Red: NTP
- Green: PTP
- Blue: direct

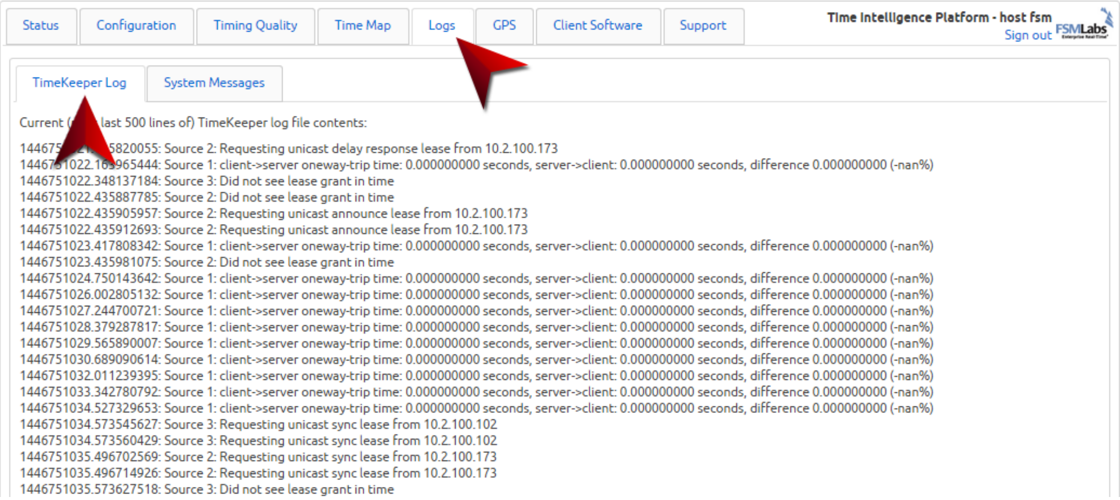
Drag any node or time source with your computer mouse to adjust the graph.

Use the mouse wheel to zoom in or out.

Scroll to the bottom of the page to see additional features, such as **static display** and **hiding labels**.

3.10 The "Logs" Tab

TimeKeeper's logs can be inspected under the **Logs** tab. They can also be downloaded, see "Downloading Log Files" on page 75 for more information.



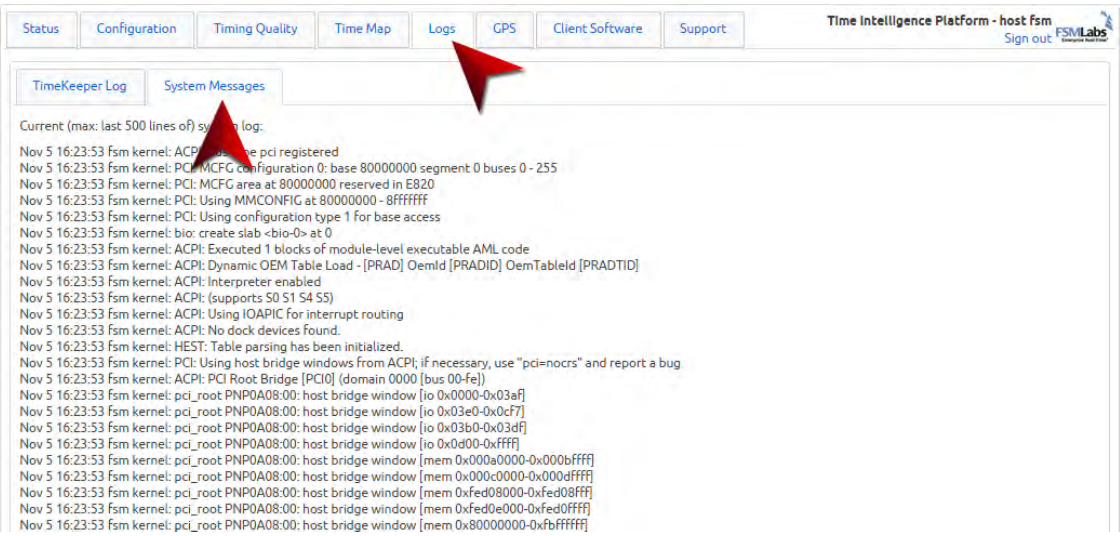
Current (max: last 500 lines of) TimeKeeper log file contents:

```
144675[illegible]5820055: Source 2: Requesting unicast delay response lease from 10.2.100.173
1446751022.16[illegible]965444: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751022.348137184: Source 3: Did not see lease grant in time
1446751022.435887785: Source 2: Did not see lease grant in time
1446751022.435905957: Source 2: Requesting unicast announce lease from 10.2.100.173
1446751022.435912693: Source 2: Requesting unicast announce lease from 10.2.100.173
1446751023.417808342: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751023.435981075: Source 2: Did not see lease grant in time
1446751024.750143642: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751026.002805132: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751027.244700721: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751028.379287817: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751029.565890007: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751030.689090614: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751032.011239395: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751033.342780792: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751034.527329653: Source 1: client->server oneway-trip time: 0.000000000 seconds, server->client: 0.000000000 seconds, difference 0.000000000 (-nan%)
1446751034.573545627: Source 3: Requesting unicast sync lease from 10.2.100.102
1446751034.573560429: Source 3: Requesting unicast sync lease from 10.2.100.102
1446751035.496702569: Source 2: Requesting unicast sync lease from 10.2.100.173
1446751035.496714926: Source 2: Requesting unicast sync lease from 10.2.100.173
1446751035.573627518: Source 3: Did not see lease grant in time
```

Figure 3-13: The "TimeKeeper Log" screen

3.10.1 "System Messages" Tab

The **System Messages** log captures information pertaining to the underlying Linux operating system.



Current (max: last 500 lines of) system log:

```
Nov 5 16:23:53 fsm kernel: ACPI: bus type pci registered
Nov 5 16:23:53 fsm kernel: PCI: MCFG configuration 0: base 80000000 segment 0 buses 0 - 255
Nov 5 16:23:53 fsm kernel: PCI: MCFG area at 80000000 reserved in E820
Nov 5 16:23:53 fsm kernel: PCI: Using MMCONFIG at 80000000 - 8fffffff
Nov 5 16:23:53 fsm kernel: PCI: Using configuration type 1 for base access
Nov 5 16:23:53 fsm kernel: bio: create slab <bio-0> at 0
Nov 5 16:23:53 fsm kernel: ACPI: Executed 1 blocks of module-level executable AML code
Nov 5 16:23:53 fsm kernel: ACPI: Dynamic OEM Table Load - [PRAD] OemId [PRADID] OemTableId [PRADTID]
Nov 5 16:23:53 fsm kernel: ACPI: Interpreter enabled
Nov 5 16:23:53 fsm kernel: ACPI: (supports S0 S1 S4 S5)
Nov 5 16:23:53 fsm kernel: ACPI: Using IOAPIC for interrupt routing
Nov 5 16:23:53 fsm kernel: ACPI: No dock devices found.
Nov 5 16:23:53 fsm kernel: HEST: Table parsing has been initialized.
Nov 5 16:23:53 fsm kernel: PCI: Using host bridge windows from ACPI; if necessary, use "pci=nocrs" and report a bug
Nov 5 16:23:53 fsm kernel: ACPI: PCI Root Bridge [PCI0] (domain 0000 [bus 00-fe])
Nov 5 16:23:53 fsm kernel: pci_root PNP0A08:00: host bridge window [io 0x0000-0x03af]
Nov 5 16:23:53 fsm kernel: pci_root PNP0A08:00: host bridge window [io 0x03e0-0x0cf7]
Nov 5 16:23:53 fsm kernel: pci_root PNP0A08:00: host bridge window [io 0x03b0-0x03df]
Nov 5 16:23:53 fsm kernel: pci_root PNP0A08:00: host bridge window [io 0x0d00-0xffff]
Nov 5 16:23:53 fsm kernel: pci_root PNP0A08:00: host bridge window [mem 0x000a0000-0x000bffff]
Nov 5 16:23:53 fsm kernel: pci_root PNP0A08:00: host bridge window [mem 0x000c0000-0x000dffff]
Nov 5 16:23:53 fsm kernel: pci_root PNP0A08:00: host bridge window [mem 0xfed08000-0xfed08fff]
Nov 5 16:23:53 fsm kernel: pci_root PNP0A08:00: host bridge window [mem 0xfed0e000-0xfed0ffff]
Nov 5 16:23:53 fsm kernel: pci_root PNP0A08:00: host bridge window [mem 0x80000000-0xfbffffff]
```

Figure 3-14: The "System Messages" tab

3.11 The "GPS" Tab

3.11.1 Signal Strength – Sky Map

TimeKeeper's **Sky Map** is a graphic representation of the sky above your GPS antenna, illustrating GPS signal strength and quality. It is useful for assisting with GPS antenna installation problems, interference, jamming, etc.

To display the Sky Map, navigate to **GPS** > **Signal Strength**:

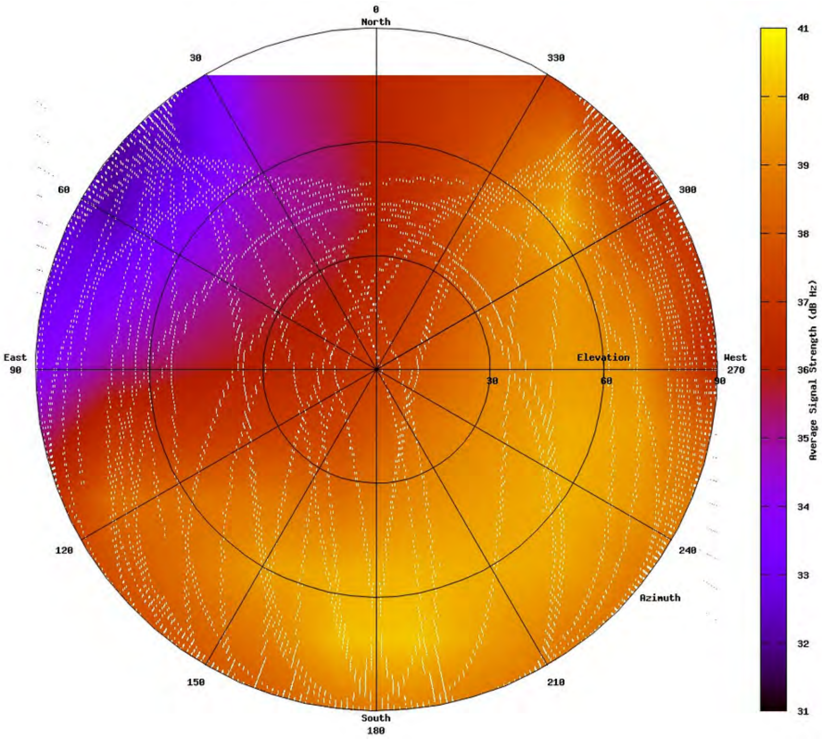


Figure 3-15: Sky Map

Note: It may take some time for the illustration to appear. Note also that it will take TimeKeeper at least 12 hours after commissioning to collect all relevant data.

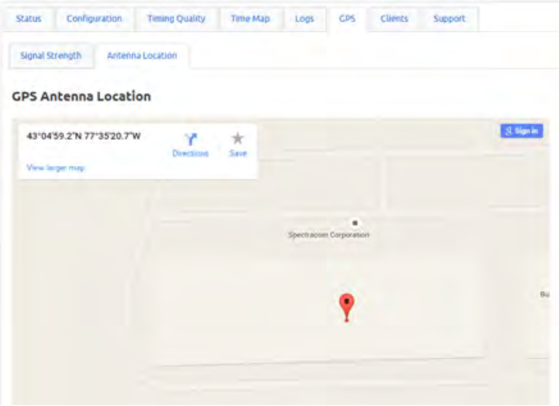
The illustration represents what you would see if you were looking straight up at the sky at the location of your GPS antenna, hence West and East seem reversed. Darker colors indicate a lower signal strength. Dotted lines show satellite trajectories. White segments show areas without reception, i.e. the sky view is likely to be obstructed by an object, such as a building, an A/C unit, or similar.

> **Note:** Minor changes in reception throughout the day are normal, as they are likely caused by cyclic atmospheric changes.

3.11.2 Antenna Location – Map

> **Note:** An Internet connection is required.

Under the **Antenna Location** tab, a map is shown (provided by Google Maps™) that illustrates the antenna location. You can zoom out the map, or display a satellite view, by clicking on the icons at the lower side of the map.



GPS Antenna Location

43°04'59.2"N 77°35'20.7"W

Figure 3-16: Antenna Location map

This feature helps to assess the GPS antenna installation location, e.g., by detecting objects that may block reception, such as buildings or trees.

3.12 The "Support" Tab

The **Support** tab allows you to:

- download user documentation
- download your TimeKeeper MIB file
- download your TimeKeeper log files
- upload your TimeKeeper log files to Technical Support.

CHAPTER 4

Frequently Performed Tasks

In this CHAPTER you will find descriptions of typical **use cases** for TimeKeeper and VelaSync that we compiled for your convenience.

Should you miss a task description, please feel free to send us a note:

» techpubs@spectracom.com — Thank You!

The following topics are included in this Chapter:

4.1 TimeKeeper Tasks

4.1.1 Logging into TimeKeeper

In order to login into the TimeKeeper Web UI, you will need to know the **IP address**, as well as your **Username**, and **Password** (defaults are provided below).

Network scenario

If VelaSync is connected to your network, the unit will likely have been assigned a static IP address by you or a co-worker (see "Configuring IP Address(es)" on page 25).

Standalone scenario

If VelaSync is NOT yet connected to a network, and you want to access TimeKeeper in order to change the IP address, you can use the unit's factory default IP address for the Ethernet port you have chosen. The IP address for ETH0, for example, is 192.168.1.1. (For the other IP addresses, see "Rear Panel Overview" on page 10.)

Procedure

1. Using a computer that is connected to your VelaSync unit, open a web browser, and enter the IP address of your VelaSync unit into the address field. The TimeKeeper Login window will appear:

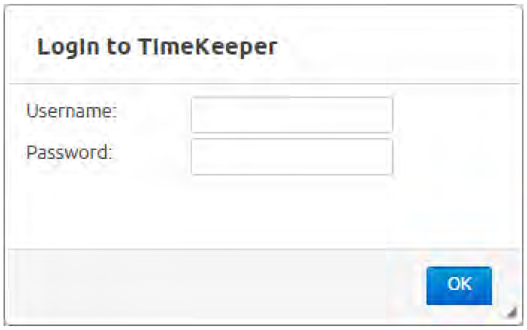
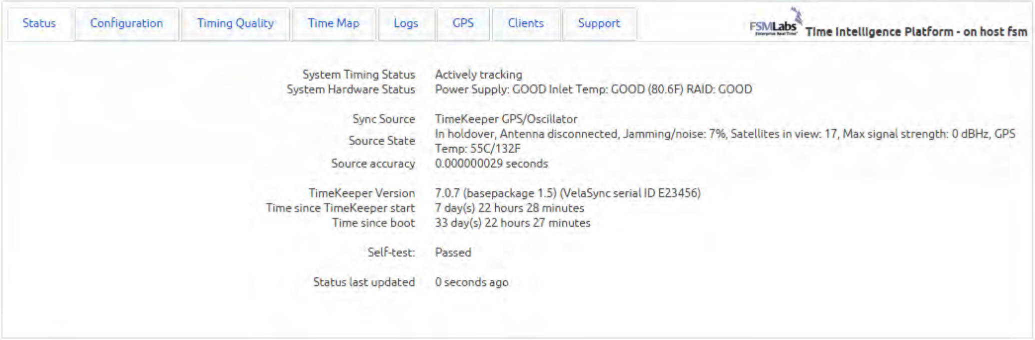


Figure 4-1: Login window

2. Enter **Username** and **Password** (the default Admin Username is "admin", the password is "fsmlabs").

> **Note:** For safety reasons, it is recommended to change the default Username and Password immediately (login via https, then navigate to Configuration > Service & System Management: Manage TimeKeeper).

The TimeKeeper Status page will be displayed:



System Timing Status	Actively tracking
System Hardware Status	Power Supply: GOOD Inlet Temp: GOOD (80.6F) RAID: GOOD
Sync Source	TimeKeeper GPS/Oscillator
Source State	In holdover, Antenna disconnected, Jamming/noise: 7%, Satellites in view: 17, Max signal strength: 0 dBHz, GPS Temp: 55C/132F
Source accuracy	0.000000029 seconds
TimeKeeper Version	7.0.7 (basepackage 1.5) (VelaSync serial ID E23456)
Time since TimeKeeper start	7 day(s) 22 hours 28 minutes
Time since boot	33 day(s) 22 hours 27 minutes
Self-test:	Passed
Status last updated	0 seconds ago

For more information on https support, see "HTTPS Support" on page 100.

4.1.1.1 The "Admin" Web User Account

Logging in as **Admin** will allow you to manage all aspects of the system, including visualization, service management, configuration, and other supported options. For a more limited login, refer to the next section on the **Readonly** and **Loguser** users.

Authentication of the web login is handled based on how the unit is configured:

- Since VelaSync is used as a server—rather than a client—, by default the TimeKeeper authentication and password control is local to the **system** "admin" account.

> **Note:** TimeKeeper can also be run as a client, when installed on NTP/PTP client computers. In these cases authentication is internal to TimeKeeper.

- If RADIUS or TACACS+ is enabled, authentication is handled by the configured servers. Should authentication via TACACS+ or RADIUS fail (such as during a network outage), the provided password will be tested against the local system account.

> **Note:** For "admin" to be authenticated via RADIUS or TACACS+, the authentication server must have an account named "admin" with matching credentials.

A VelaSync TimeKeeper **upgrade** will detect that there is a need for a local system "admin" account for authentication, and consequently will add this account. As a precautionary measure SSH will be disabled, so as to prevent unauthorized logins with the default "admin" password, until this password can be changed to something unique. SSH access can then be re-enabled via the Web UI.

> **Note:** Upgrading from TimeKeeper Version 6.3.12 will require web login with the default credentials of “admin” and “fsmlabs”. The password can be set as before via the Web UI.

4.1.1.2 The Accounts "Readonly" and "Loguser"

More limited user accounts are also available with the **Readonly** and **Loguser** accounts. Both can be configured by the **Admin** user via the Web UI. Both types of accounts can log in and review TimeKeeper data, but cannot reconfigure or manage the system. On VelaSync, both accounts are identical.

If RADIUS or TACACS+ is enabled, any user that can authenticate with the configured server that is not named **Admin** will be logged in as the **Readonly** role with reduced capabilities.

By default, the **Readonly** and **Loguser** accounts are present but not configured and cannot be used.

To configure either account:

1. Log in as **Admin**.
2. Navigate to **Configuration** > **Service & System Management**. The **Set readonly [loguser] password** button will allow you to configure a password, which will be named “readonly” or "loguser", respectively.

4.1.2 Verifying TimeKeeper is Working

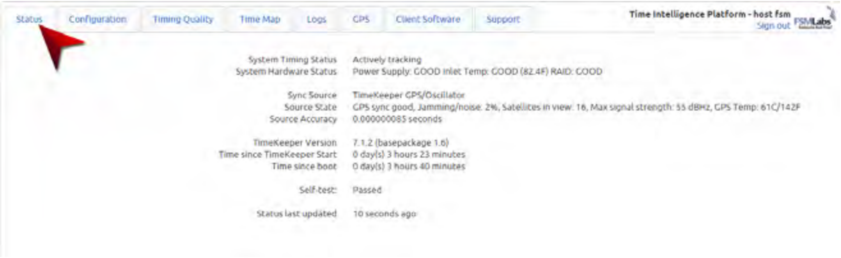
This is covered under Installation & Setup, see "Verifying VelaSync Works" on page 27.

4.1.3 Status Monitoring with TimeKeeper

TimeKeeper offers several ways to monitor the status of VelaSync, the time distributed over the network, and other aspects of network administration:

4.1.3.1 "Status" Tab

The Status tab provides information on the source currently tracked, as well as TimeKeeper system data, and system tracking information.



System Timing Status Actively tracking
System Hardware Status Power Supply: GOOD Inlet Temp: GOOD (82.4F) RAID: GOOD

Sync Source TimeKeeper GPS/Oscillator
Source State GPS sync good, Jamming/noise: 2%, Satellites in view: 16, Max signal strength: 55 dBHz, GPS Temp: 61C/142F
Source Accuracy 0.000000085 seconds

TimeKeeper Version 7.1.2 (basepackage 1.6)
Time since TimeKeeper Start 0 day(s) 3 hours 23 minutes
Time since boot 0 day(s) 3 hours 40 minutes

Self-test: Passed

Status last updated 10 seconds ago

Figure 4-2: TimeKeeper Status tab

4.1.3.2 "Timing Quality" Tab

Under the **Timing Quality** tab, you can access graphical representations of accuracy data:

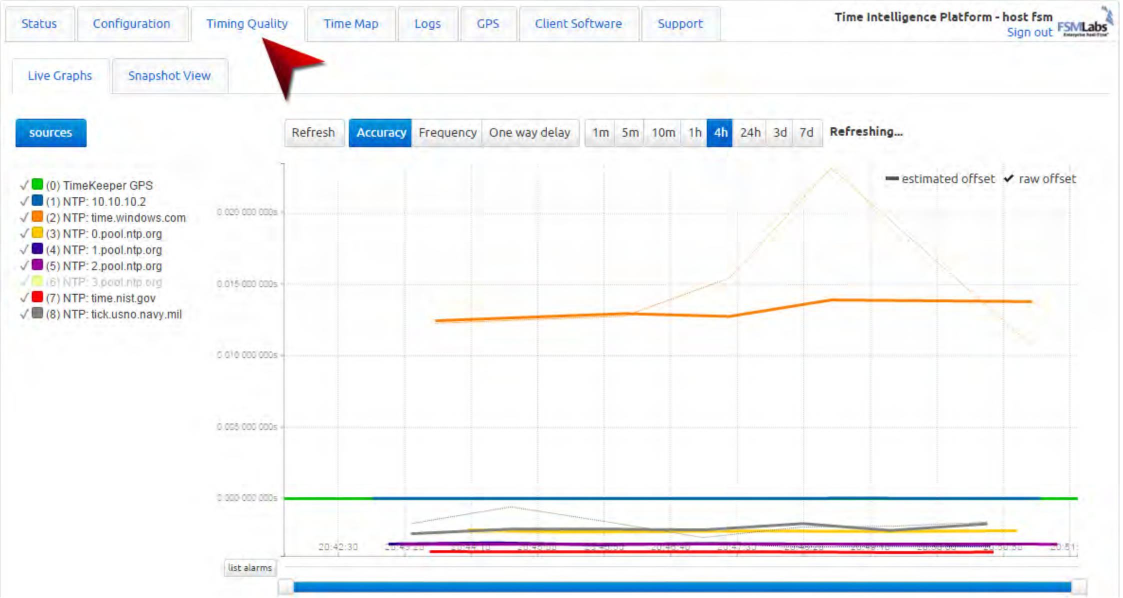
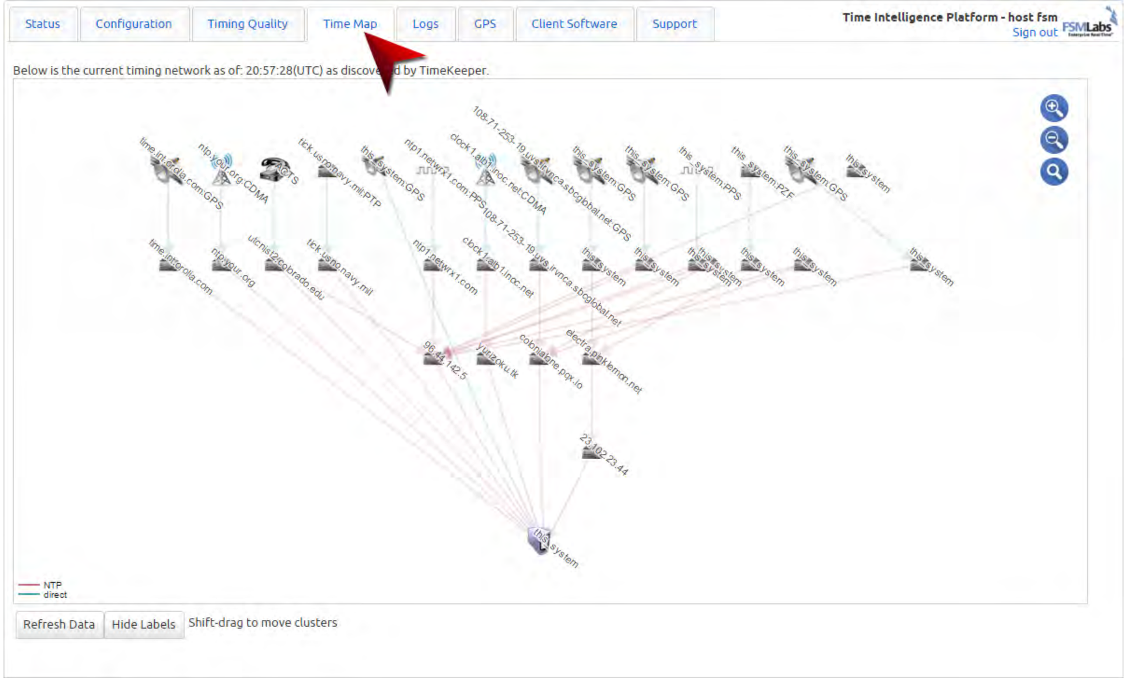


Figure 4-3: TimeKeeper Timing Quality tab

4.1.3.3 "Time Map" Tab

Under the Time Map tab, TimeKeeper TKL visualizes the structure of the timing network environment, including all time sources, and other clients found on the network. Espcially with complex networks, this visualization tool can be of assistance when it comes to identifying architectural or accuracy problems.



Below is the current timing network as of: 20:57:28(UTC) as discovered by TimeKeeper.

Figure 4-4: TimeKeeper Time Map tab

The connecting lines are color-coded:

- Red: NTP
- Green: PTP
- Blue: direct

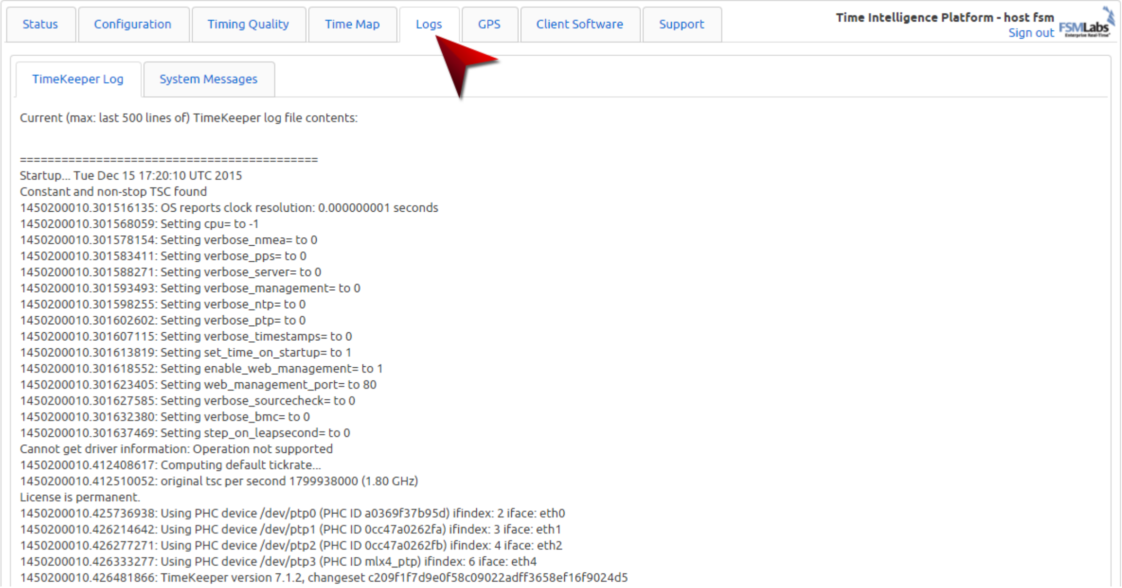
Drag any node or time source with your computer mouse to adjust the graph.

Use the mouse wheel to zoom in or out.

Scroll to the bottom of the page to see additional features, such as **static display** and **hiding labels**.

4.1.3.4 "Logs" Tab

TimeKeeper maintains log files that can be conveniently reviewed under the **Logs** tab.



Current (max: last 500 lines of) TimeKeeper log file contents:

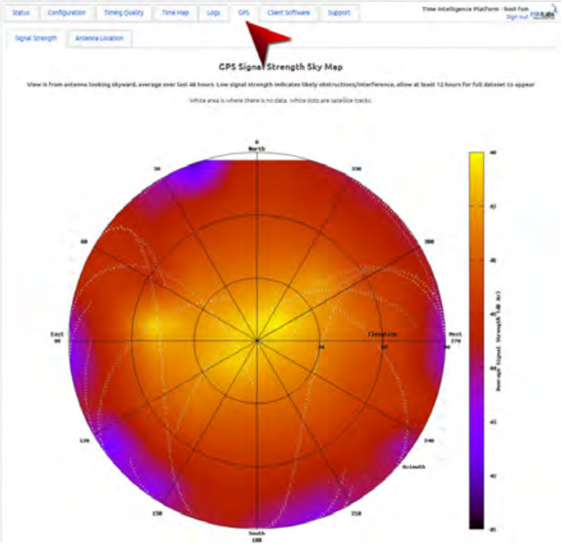
```
==========================================
Startup... Tue Dec 15 17:20:10 UTC 2015
Constant and non-stop TSC found
1450200010.301516135: OS reports clock resolution: 0.000000001 seconds
1450200010.301568059: Setting cpu= to -1
1450200010.301578154: Setting verbose_nmea= to 0
1450200010.301583411: Setting verbose_pps= to 0
1450200010.301588271: Setting verbose_server= to 0
1450200010.301593493: Setting verbose_management= to 0
1450200010.301598255: Setting verbose_ntp= to 0
1450200010.301602602: Setting verbose_ptp= to 0
1450200010.301607115: Setting verbose_timestamps= to 0
1450200010.301613819: Setting set_time_on_startup= to 1
1450200010.301618552: Setting enable_web_management= to 1
1450200010.301623405: Setting web_management_port= to 80
1450200010.301627585: Setting verbose_sourcecheck= to 0
1450200010.301632380: Setting verbose_bmc= to 0
1450200010.301637469: Setting step_on_leapsecond= to 0
Cannot get driver information: Operation not supported
1450200010.412408617: Computing default tickrate...
1450200010.412510052: original tsc per second 1799938000 (1.80 GHz)
License is permanent.
1450200010.425736938: Using PHC device /dev/ptp0 (PHC ID a0369f37b95d) ifindex: 2 iface: eth0
1450200010.426214642: Using PHC device /dev/ptp1 (PHC ID 0cc47a0262fa) ifindex: 3 iface: eth1
1450200010.426277271: Using PHC device /dev/ptp2 (PHC ID 0cc47a0262fb) ifindex: 4 iface: eth2
1450200010.426333277: Using PHC device /dev/ptp3 (PHC ID mlx4_ptp) ifindex: 6 iface: eth4
1450200010.426481866: TimeKeeper version 7.1.2, changeset c209f1f7d9e0f58c09022adff3658ef16f9024d5
```

Figure 4-5: Logs tab

Logs can also be downloaded: Navigate to **Support**, and click **Collect TimeKeeper Logs**.

4.1.3.5 "GPS" Tab

Since GPS reception is critical for VelaSync, TimeKeeper has two integrated monitoring tools that help with assessing GPS signal strength-related status.



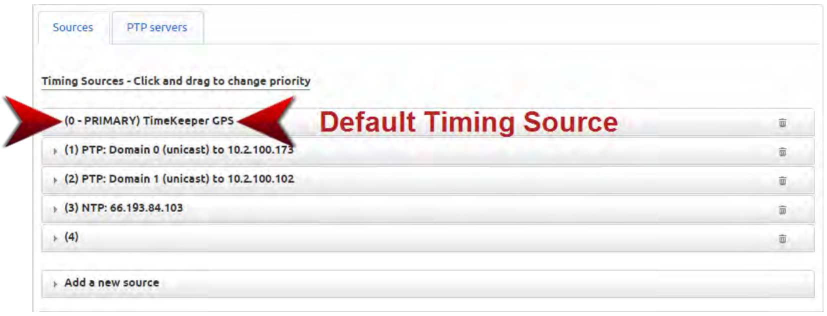
View is from antenna looking skyward, average over last 48 hours. Low signal strength indicates likely obstructions/interference, allow at least 12 hours for full dataset to appear

White area is where there is no data. White dots are satellite tracks.

Figure 4-6: TimeKeeper's Sky Map

In addition to this, under the **Antenna Location** tab, you can display a Google Maps® window, showing the antenna location.

4.1.4 Setting Up Timing Sources



Sources | PTP servers

Timing Sources - Click and drag to change priority

(0 - PRIMARY) TimeKeeper GPS

(1) PTP: Domain 0 (unicast) to 10.2.100.173

(2) PTP: Domain 1 (unicast) to 10.2.100.102

(3) NTP: 66.193.84.103

(4)

Add a new source

Figure 4-7: Configuration > TimeKeeper configuration: Timing Sources

Out of the box, VelaSync comes with only one timing source pre-configured: **TimeKeeper GPS**. While this configuration will suffice for basic operation, it is advisable to add other timing sources for improved failover performance. Below are some general recommendations:

> Note: When filling out the menu forms for a newly added source, many if not most of the fields can be left blank. There are very few fields that must be populated e.g., NTP server.

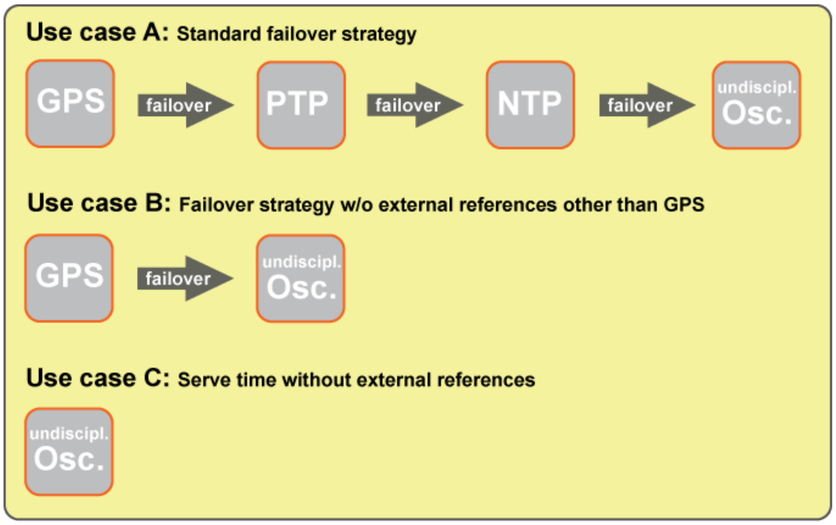

Use case A: Standard failover strategy
GPS
failover
PTP
failover
NTP
failover
undiscipl. Osc.
Use case B: Failover strategy w/o external references other than GPS
GPS
failover
undiscipl. Osc.
Use case C: Serve time without external references
undiscipl. Osc.

Figure 4-8: Timing sources failover strategies

1. **Add timing sources**: In order to allow VelaSync to failover to another timing source in the event the GPS signal will be lost temporarily, it is advisable to create at least one additional timing source e.g., a PTP or NTP server. While TimeKeeper will continue to

provide time to VelaSync's network clients after loss of a GPS signal and expiration of the holdover period, it will do so without its internal clock being steered by an external reference. As a consequence, the time served will be:

- less stable (+/- variation)
- likely drift over time
- not be traceable.

It is noteworthy to mention that, while there is no valid GPS signal present, TimeKeeper's internal clock will NOT be steered by VelaSync's high-precision oscillator, once the hold-over time has expired.

To add a PTP or NTP timing source:

- See "Add an NTP Source" on page 41 , or see "Add a New PTP Source" on page 43.

2. **Utilize VelaSync's oscillator for failover handling**: The fewer timing sources you have configured, the more arises the need to utilize VelaSync's oscillator as the last failover timing source: It is possible and useful to configure TimeKeeper such that it will accept the time and PPS signal generated by the oscillator, even if the oscillator is temporarily not steered ("disciplined") by the GPS timing source.
   In fact, the oscillator's accuracy tends to be significantly better than the timing signal obtained from a typical NTP server. Which raises the question why not use it in the first place, i.e. *instead* of an NTP server? The answer is: Because without external references such as NTP or PTP servers VelaSync operates in "freerun" mode, and while the time served by VelaSync may be very accurate, it is not traceable.

   Hence, allowing the un-disciplined oscillator to steer TimeKeeper's internal clock as a primary failover source is only advisable if there is no need for an auditing trail, and it is permissible to serve a time that has no direct reference to UTC. However, for most applications it is generally advisable to add the oscillator as the *lowest* priority timing source.

   To configure TimeKeeper such that it will accept the non-disciplined oscillator as a valid failover timing source:

   I. Navigate to **Configuration > TimeKeeper configuration > Sources: Add a new source: Internal GPS/Oscillator**.

   II. Uncheck **TimeKeeper GPS device**, and check Disable GPS steering.

   III. **Add** the newly created source, and leave it at its default lowest-priority position. (Or, drag&drop it to position **(1)** right below **TimeKeeper GPS**, in order to use the un-disciplined oscillator as the *primary* failover source.

   IV. Click **Save TimeKeeper changes**.

Note: Another option to allow the un-disciplined oscillator to steer TimeKeeper's internal clock for an extended period of time, before failing over to e.g., a PTP or NTP server, is to increase the Holdover Time under Application Settings from 7200 seconds to a longer period.

3. **Utilize Sourcecheck**: Even if no NTP or PTP servers are available, it may be advisable to add two public time servers (such as NIST and pool.ntp). While these normally will be not accurate enough to act as as a quality failover timing source, they can be used by TimeKeeper's Sourcecheck feature.
   Sourcecheck utilizes standby timing sources to verify the validity of an incoming GPS signal, thus enabling the detection of accidental or intentional spoofing of the satellite timing signal.

   To use Sourcecheck:

   » Designate the newly added public time servers as a **low quality source** so as to limit their permission to discipline the oscillator.

   » Under **Application Settings**, enable **Source Check**.

4. **Special use case: No GPS available at all**: Even in the case of complete absence of a GPS source e.g.,

   » during initial installation of VelaSync while the GPS antenna has yet to be installed,

   » or if for other reasons the time to be distributed by VelaSync does not need to be linked to UTC,

   ... it is also possible to use the internal oscillator as the primary timing source, i.e. *instead* of the **TimeKeeper GPS** source.

   Please note, however, that while the time distributed by TimeKeeper will be very stable, it most likely will differ from UTC, because of the lack of any external steering.

   To configure VelaSync's oscillator to become TimeKeeper's primary timing source:

   » Open the PRIMARY (0) **TimeKeeper GPS** source, uncheck **TimeKeeper GPS device**, and check **Disable GPS steering**. Click Save TimeKeeper changes and wait for TimeKeeper to restart.

Note: Should you accidentally delete the TimeKeeper GPS timing source, create a new one by navigating to Add a new source > Internal GPS/Oscillator. Leave the default settings for TimeKeeper GPS device (checked) and Disable GPS steering (unchecked), and drag&drop the newly added source to list position (0).

4.1.5 Validating a Timing Source

To check if a timing source is present and valid:

1. Navigate to **Timing Quality > Live Graphs**: If under the **sources** tab a source is grayed out, it is not present.
2. You can also check under **Snapshot View** if a given source is listed/present.
3. Click on one of the present sources to exclusively display its accuracy graph.

4.1.6 Creating an Audit Trail

TimeKeeper maintains all logging data in clear text formats for easy analysis and management. This includes logging parameters of each configured timing source, client timing quality information, network map data, and more.

To access the logs, either see under the **Logs** tab, or download the logs under the **Support** tab (see "Downloading Log Files" on page 75).

4.1.6.1 Log Format Description

TimeKeeper logs information in multiple files, maintaining data on alarms, general messages, state change information, administrative information, and source sync information. All sources have the same log format regardless of source type.

Every update that TimeKeeper receives is recorded, one line per update.

Below is some information on the log file format:

`timekeeper_0.data` in the folder `tk_report\var\log` is a running list of every update that TimeKeeper receives and how TimeKeeper is adjusting time for Source (0). It is the best way to see how TimeKeeper is performing. This file contains a line for every update received from the time source. If it is growing then TimeKeeper is receiving time updates.

In most installations, the first two fields – the absolute timestamp and the offset from the time source — are all that is of interest. Once started and running properly this file should be growing as updates are received.

- **Column 1**: Absolute timestamp of the update, seconds since midnight January 1 1970 (also known as UNIX time)
- **Column 2**: Offset (in seconds) from the remote server or time source
- **Column 3**: Raw offset from remote side – pre-smoothing and adjustments
- **Column 4**: Internal testing use
- **Column 5**: Clock correction factor for the TimeKeeper managed clock
- **Column 6**: Used to provide additional data with TimeKeeper GPS devices
- **Column 7**: Used to provide additional data with TimeKeeper GPS devices
- **Column 8**: A predictive indicator for internal use
- **Column 9**: Timestamp type – hardware/software/other timestamp source

- **Column 10**: Network delay – meaning depends on type of source
- **Column 11**: Raw network delay – meaning depends on type of source (for NTP/PTP this is the oneway trip time)
- **Column 12**: Time source, PTP, NTP, PPS or other
- **Column 13**: “Ideal” clock correction that if used would have minimized offsets over the previous few minutes
- **Column 14**: Model error over the model interval period
- **Column 15**: “Ideal” clock correction from sourcecheck calculations if applicable

If this file is not being updated, it is likely that firewalls are preventing receipt of network data, or there is some configuration issue reported in the timekeeper file.

The directory `\var\log\timekeeperclients` contains clock quality about client machines that TimeKeeper is either directly serving time to or otherwise able to retrieve information from. The files in this directory contain data in the same format as described above for `timekeeper_$SOURCE.data`. The amount of detail available in each file will vary depending on the client. For some remote client types, the data available is limited. If the client is a TimeKeeper client, the data provided in that file will be more fully populated, giving you a better understanding of timing quality across the network.

Log Rotation

TimeKeeper is provided with a default log rotate recipe that rotates all of the relevant TimeKeeper log files. By default, this will retain 7 days worth of log files. If you have specific log storage needs this value can be modified via the TimeKeeper Web UI: Navigate to **Configuration > TimeKeeper configuration**, and scroll down to **Days of TimeKeeper logs retained**.

4.1.6.2 FINRA OATS Compliance

TimeKeeper’s multisource feature allows for easy compliance with the FINRA OATS specification. For complete details, refer to the OATS Reporting Technical Specifications.

Accuracy to within one second of NIST time is required. However, if there is a very precise local time source, it is unlikely that a public NIST server is being used to drive the clock. By pointing to a NIST server as a secondary source, accurate logs can be maintained that provide continuous system time offsets from NIST time.

To configure for this scenario, the TimeKeeper configuration should specify a NIST server as a secondary (or even lower priority) time source.

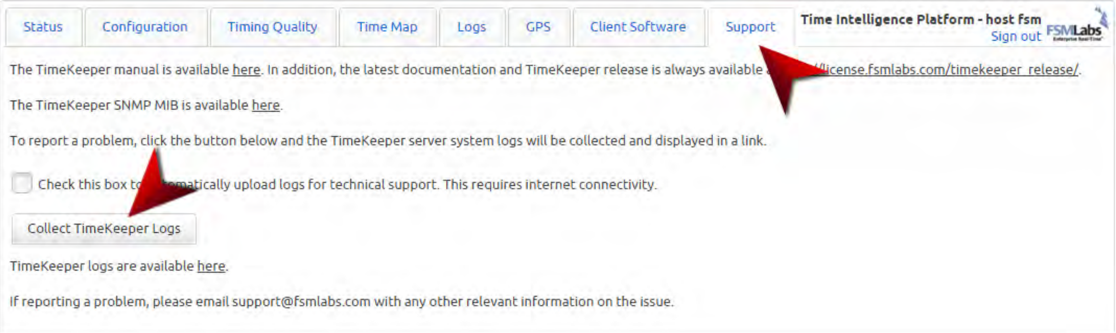
The display compliance inside the Web UI, obtain a list of all the timing sources (**Configuration > TimeKeeper configuration > Sources**), and then check for their timing accuracy under **Timing Quality > Live Graphs** , where you can trace presence and accuracy over the log duration.

Note: The default log duration retainment period is 7 days. This can be changed under Configuration > TimeKeeper configuration.

For permanent tracing, establish a process to pull logs regularly, and store them in a safe location. VelaSync supports setting up cron jobs to transfer relevant logs from the unit to a storage system via standard protocols like FTP or SCP.

4.1.7 Downloading Log Files

To download the current TimeKeeper logs, navigate to **Support**, and click **Collect TimeKeeper Logs**.



The TimeKeeper manual is available here. In addition, the latest documentation and TimeKeeper release is always available a //license.fsmlabs.com/timekeeper_release/.

The TimeKeeper SNMP MIB is available here.

To report a problem, click the button below and the TimeKeeper server system logs will be collected and displayed in a link.

□ Check this box to matically upload logs for technical support. This requires internet connectivity.

TimeKeeper logs are available here.

If reporting a problem, please email support@fsmlabs.com with any other relevant information on the issue.

Figure 4-9: Downloading logs

The compressed file contains several folders and files; the main TimeKeeper logs are located under `\var\log`.

The log file contains a line for every update that TimeKeeper receives and how TimeKeeper is adjusting time for Source (0).

In the file, column 1 is the absolute UTC timestamp from the time source in seconds since midnight January 1 1970.

Column 2 is the estimated local time offset as of that update. The second column gives a good indication as to the quality of the sync that TimeKeeper has, and will converge shortly after TimeKeeper starts.

For additional information on the log file contents, see "Creating an Audit Trail" on page 73.

4.1.8 Upgrading TimeKeeper

To upgrade TimeKeeper, navigate to **Configuration > Update** and follow the instructions.

For additional information on the tabs provided on this page, see."The Subtab "Update"" on page 55.

After completion of the install, make sure to force a full page reload (Ctrl-Shift-R in most web browsers) once you logged into the TimeKeeper Web UI again to ensure changes will actually be displayed.

4.1.9 Detecting Network Asymmetries

When properly configured, TimeKeeper is able to detect and measure a network route asymmetry.

To setup a network to test for an asymmetry:

1. Setup a TimeKeeper instance on a system configured to be a PTP or NTP client to a local VelaSync server/Grandmaster (via LAN). This will be Source (0).
2. At the other end of the network route that you wish to measure, you must have another PTP or NTP server with a GPS reference.

To enable measuring a network route for asymmetry:

» Navigate to **Configuration > TimeKeeper Configuration > Sources**, and check the box **Detect asymmetry** for the NTP or PTP sources you want to measure.

4.1.10 Powering OFF VelaSync

To power off VelaSync, in TimeKeeper navigate to the **Service & System Management** tab, and then, under **Manage System**, select **Shutdown system** to gracefully shutdown TimeKeeper, and power down VelaSync.

DANGER! The power supplies, and the IPMI interface will remain energized as long as a power supply cord is connected to the mains supply.

Note: Avoid shutting down VelaSync using the ON/OFF switch on the front of the unit.

4.2 Configuration Tasks

4.2.1 Changing an IP address

… by using the Web UI

To change network interface addresses, navigate to **Configuration > Networking**, then select the options you would like.

When done, click **Save network changes**, and then **Restart Network** to apply the updates.

The changes will take a moment to apply after which you can reconnect to the newly configured address.

… without using the Web UI

If the TimeKeeper Web UI is not available (yet) e.g., during initial setup, and you need to change the default IP addresses (see "Rear Panel Overview" on page 10), follow the procedure outlined under "Configuring IP Address(es)" on page 25.

4.2.2 Configuring Event Notifications

TimeKeeper provides several methods of delivering notifications of significant events. They can be delivered via syslog, and/or SNMP.

Each event is also logged locally, no matter what delivery options may or may not be set. Below a brief overview is given for each type of delivery mechanism

For specifics about the messages TimeKeeper will emit, see "TimeKeeper Event Notifications" on page 86.

4.2.2.1 Configuring SNMP

TimeKeeper can generate SNMP traps. To configure TimeKeeper to generate SNMP traps and deliver them to the host “host1”:

1. Navigate to **Configuration** > **TimeKeeper Configuration**.
2. In the field **SNMP trap host**, enter a host name (e.g., "host1") or an IPv4 dotted notation address. TimeKeeper supports multiple SNMP trap destinations, to be entered in the following manner: host1,host2,hostr3.
3. In the field **SNMP trap OID**, enter the OID to which all traps will be emitted e.g., “1.3.6.1.2.1.16.0.1”. Unless you need all traps sent to one OID, it is recommended you leave SNMPTRAPOID undefined in your configuration.

By default, TimeKeeper delivers traps according to the provided MIB file, which can be accessed under the **Support** tab.

TimeKeeper also allows users to walk the SNMP tree on the appliance. To enable this feature:

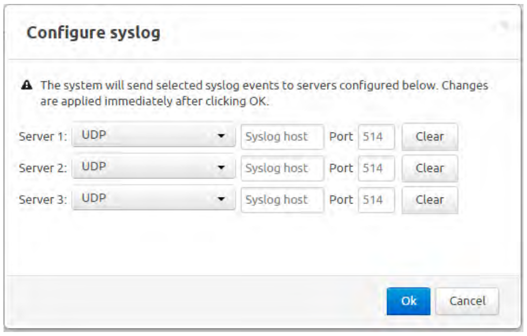
- » Navigate to **Configuration > Service & System Management**, and under **Manage Communication**, click **Enable SNMP queries**.

4.2.2.2 Configuring Syslog

Events that are sent over SNMP can also be delivered via syslog. TimeKeeper automatically emits syslog messages, so TimeKeeper clients can be configured to send data to a syslog server just like any other application, using whichever syslog daemon is in use on the client.

To change the configuration:

1. Navigate to **Configuration** > **Service & System Management**: Under **Manage Communication**, select **Configure Syslog**.



Configure syslog

The system will send selected syslog events to servers configured below. Changes are applied immediately after clicking OK.

Server 1: UDP | Syslog host | Port 514 | Clear

Server 2: UDP | Syslog host | Port 514 | Clear

Server 3: UDP | Syslog host | Port 514 | Clear

Figure 4-10: Syslog configuration window

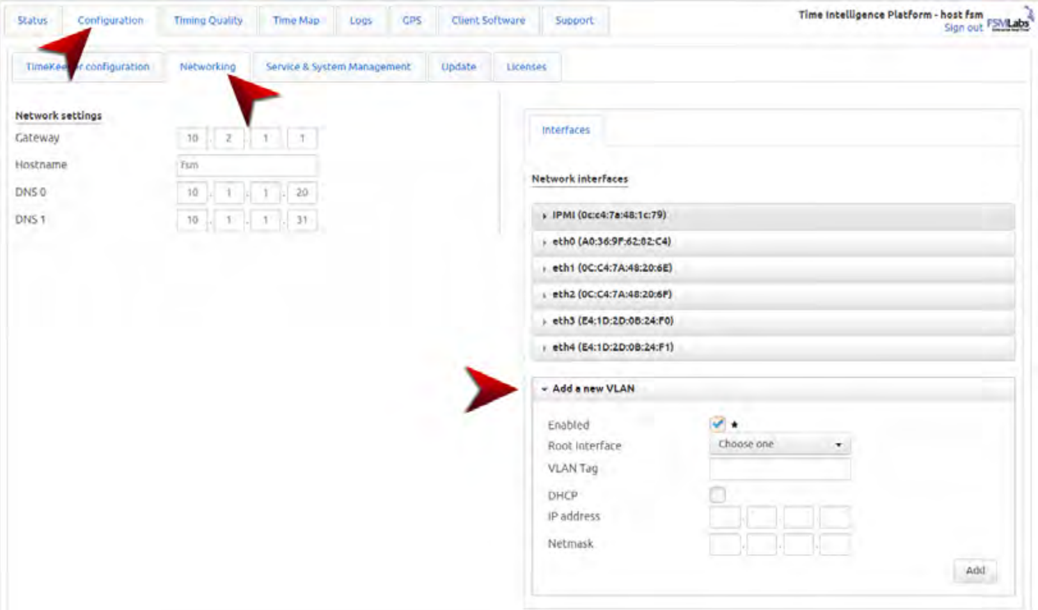
From this interface, three separate syslog servers can be configured. Once applied, the change is immediate and syslog messages will be delivered to those hosts without having to restart VelaSync or TimeKeeper.

4.2.3 Adding a New VLAN

TimeKeeper supports VLAN interfaces and bonded interfaces. Both are configured as normal for your distribution using the normal Linux tools.

To configure a new VLAN in TimeKeeper:

» Navigate to **Configuration > Networking > Interfaces: Add a new VLAN**.



Network settings

Gateway: 10.2.1.1

Hostname: fsm

DNS 0: 10.1.1.20

DNS 1: 10.1.1.31

Network interfaces

- IPMI (0c:c4:7a:48:1c:79)
- eth0 (A0:36:9F:62:82:C4)
- eth1 (0C:C4:7A:48:20:6E)
- eth2 (0C:C4:7A:48:20:6F)
- eth3 (E4:1D:2D:08:24:F0)
- eth4 (E4:1D:2D:08:24:F1)

Add a new VLAN

Enabled ☑ *

Root interface: Choose one

VLAN Tag

DHCP ☐

IP address

Netmask

Figure 4-11: VLAN configuration menu

Once the device is present, TimeKeeper can use it just like any other network device.

4.2.4 Saving and Restoring Current Configuration

Note: You need to login to TimeKeeper via https to create a configuration file.

The TimeKeeper Web UI can be used to save an existing configuration state as a downloadable file. This file can be used as a backup of the configuration, or a means of deploying the same configuration to multiple VelaSync units easily.

The configuration file generated represents the VelaSync configuration data only, and does not contain binary state, like the installed TimeKeeper version.

Note: The generated file does contain potentially sensitive contents, like hashed system password files, RADIUS and TACACS+ secrets, etc. Please treat the file with care, and properly secure it.

To save a VelaSync configuration, navigate via https to **Configuration > Service & System Management**.

The screen will look similar to this:

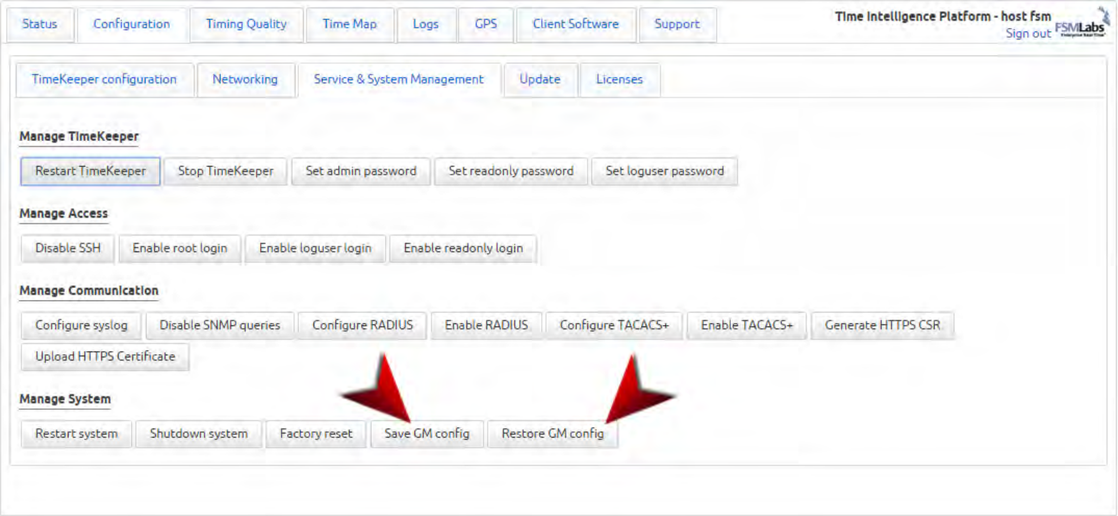


Figure 4-12: Service & System Management screen

Under Manage System, click **Save GM Config** (GM = Grandmaster) to download a file with the current configuration data. That same file can be uploaded via the **Restore GM config** button.

4.3 Hardware Tasks

4.3.1 Replacing a Power Supply

For redundancy purposes, the server is equipped with two hot-swap power supply modules. Should either of the modules fail, the other will take the full load, and supply power without interruption to the server.

Since the power supplies can be hot-swapped, the VelaSync unit does not have to be shut down, in order to replace the defective power supply.

Caution: Allow the power supply modules to cool before touching.

1. To determine which of the two power supplies failed, on the back side of the server check the LED located on either power supply. The LED of a failed power supply will not light up.
2. Unplug the power cord of the defective power supply.
3. To remove the power supply module from the VelaSync unit, push the release tab to the side, and then pull the module straight out.

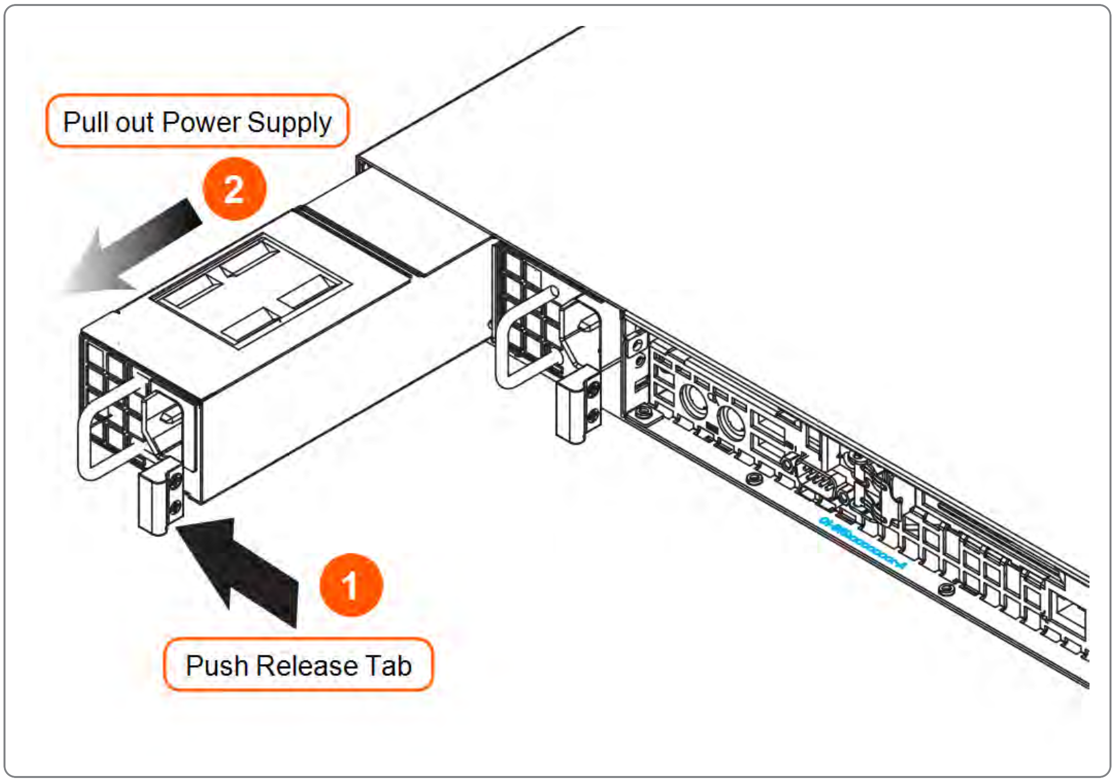


Figure 4-13: Power supply removal

4. Replace the failed power supply module with a replacement unit.

   Note: Only use the approved type of power supply, for more information, see "Maintenance and Service" on page 104.

   Simply push the new power supply module into the empty bay until you hear a click.

5. Plug the AC power cord back into the new power supply.

Note: For additional information on the power supplies, see http://www.supermicro.com.tw/manuals/superserver/1U/MNL-1328.pdf, Chapter 2 on page 2-1.

4.3.2 Removing/Installing a Hard Disk Drive

Since the SATA Hard Disk Drives (HDDs) are hot-swappable, and they are RAID configured, either of the two drives can be removed from the front of the VelaSync chassis, without the need to open the chassis, or shut down VelaSync.

Caution: Allow the hard disk drives to cool before touching.

Proceed as follows:

Removing the bezel

» Remove the front bezel from the chassis, by unlocking it with the key, then pressing the red release knob, then removing the bezel with both hands. While the bezel is removed, check if the filter requires cleaning or replacement.

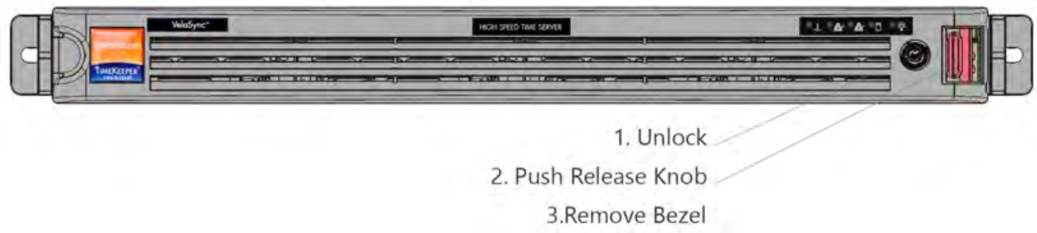


Figure 4-14: Removing the front bezel

Removing the HDD carrier

1. The HDDs are installed in carriers. To release a carrier, press down its red release button next to the drive LEDs. The handle will be released.

2. Swing the handle out all the way.
3. Pull out the carrier from the chassis, using the handle.

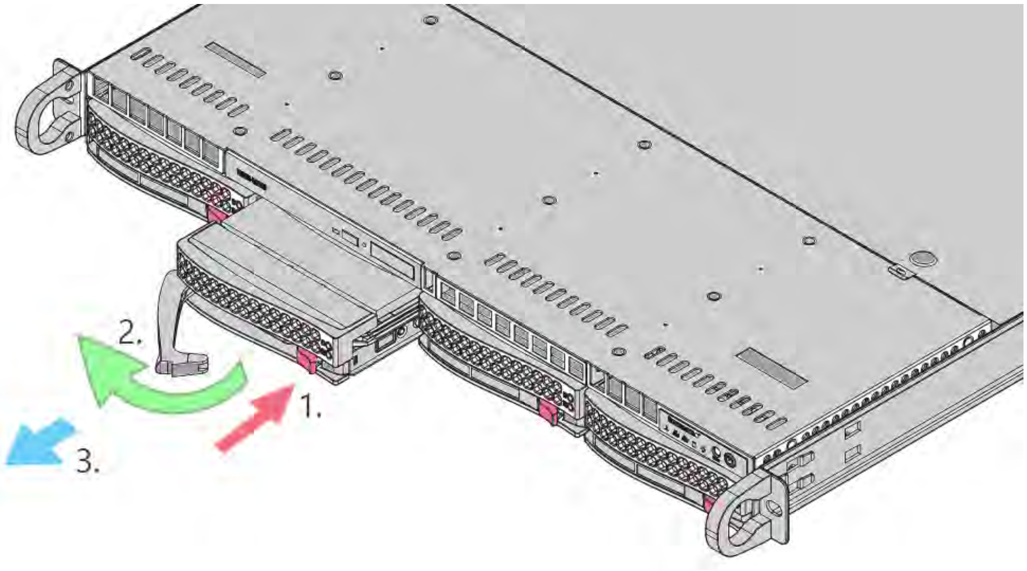


Figure 4-15: Removing a HDD carrier

Caution: In order to maintain proper airflow, each HDD carrier must always be re-installed into the unit, even if empty.

To **remove a HDD from its carrier**, loosen the three screws on either side.

To **install a HDD into a carrier**, insert it into the carrier with its PCB facing down. Check alignment, then use the three screws on either side to assemble the two components.

To **install a carrier** into VelaSync, follow the instructions shown above Removing the HDD carrier in reverse order.

For additional information on HDD installation, see the user documentation provided by the Original Equipment Manufacturers: Supermicro™ SuperO® SuperServer 5017R-WRF under http://www.supermicro.com.tw/manuals/superserver/1U/MNL-1328.pdf.

APPENDIX

Appendix

The following topics are included in this Chapter:

5.1 Troubleshooting

This section is intended to assist you with troubleshooting VelaSync. Please also consult the OEM documentation for Supermicro™ SuperO® SuperServer 5017R-WRF which can be found online under:

http://www.supermicro.com.tw/manuals/superserver/1U/MNL-1328.pdf

For Technical Support contact information see "Technical Support" on page 102.

5.1.1 Troubleshooting Hardware Issues

Failure Mode Symptom	Failure Mode Diagnosis	Failure Mode Resolution
Info LED on front panel blinks slowly	One of the two redundant power supplies is defective.	Replace defect power supply. See "Replacing a Power Supply" on page 80.
TimeKeeper log and Status page report HD failure	One of the two RAID harddisks is defect.	Replace harddisk. See "Removing/Installing a Hard Disk Drive" on page 81.

5.1.1.1 Power Supply Failure

If either of the two redundant power supply modules fail, the other module will take over without service interruption. The UID LED on the front panel (see "Front Panel Overview" on page 8) will blink slowly until the failed module has been replaced.

Do not user power supplies other than the original model installed in the unit. Replacement power supplies can be procured directly from Spectracom (part no. PS09R-070J-SL01), or from the OEM manufacturer, Supermicro Computer (model PWS-651-1R).

To find out how to replace a power supply, see "Replacing a Power Supply" on page 80.

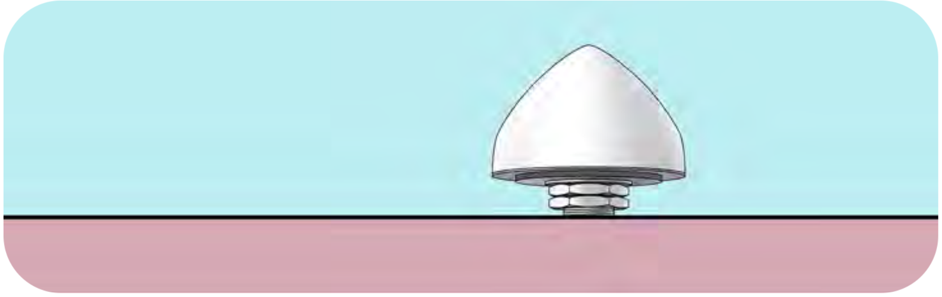
5.1.2 Identifying Accuracy Problems

5.1.2.1 Firewalls

Although uncommon, occasionally firewalls are used between timing clients and servers. While the clients can still sync through the firewall, generally this reduces the potential accuracy of the client greatly.

5.2 GPS Antenna Location

For instructions on how to install a GPS/GNSS antenna, the signal cable, and accessories such as surge protectors, weatherproofing kits, or amplifiers, refer to the Installation Guide that came with the respective equipment.



Regarding the selection of a suitable antenna location, the following recommendations generally apply:

- A **clear view of the sky down to the horizon** in all directions is recommended for the most optimal satellite reception.
- GPS antennas need to be separated from surrounding **metallic materials**. Any metal in the area changes the shape of the reception pattern of the antenna. Any buildings or metallic materials close to the antenna can create shadows which can shield the antenna from receiving in that particular direction.
- **Separation between multiple antennas**: If the antennas are installed too close together there could potentially be interaction between the antennas and a resulting loss of sensitivity. This could also adversely affect the search pattern of the antennas, resulting in fewer satellites being tracked.
    - Ideally, antennas should be separated as much as physically possible, so as to help isolate them from being simultaneously affected by the same anomaly (such as a nearby lightning strike or a falling object, for example).
    - GPS antennas are receive-only antennas which do not intentionally transmit any signals. Even though this reduces the amount of separation needed between multiple antennas, a few meters of separation are recommended to isolate the antennas from each other, in order to limit any possible EMI interference caused by the active components inside the antennas.
    - If a noticeable decrease in sensitivity (resulting in weak signal strengths) and/or very few satellites being tracked is noted, try repositioning the antennas to improve the satellite reception.

5.3 About RAID Support

TimeKeeper supports VelaSync's RAID configuration. TimeKeeper will send alarms about disk failure and recovery through the normal configured alerting methods – syslog and SNMP, as detailed under "TimeKeeper Event Notifications" below.

In the event of a disk failure, the failure will be logged in the TimeKeeper log, as well as displayed on the status page until the failed component is replaced, but VelaSync will continue operating.

Once the failed component is replaced, a reboot is required in order to initiate reconstruction of the RAID array.

5.4 Configuration via Command Line

Some of VelaSync's and TimeKeeper's capabilities may be configured via a Command Line Interpreter (CLI) running on a remote computer/console. An example would be the configuration of IP addresses during initial setup.

In standard configuration scenarios, however, all of the remaining network configuration settings can be done via the Web UI, either over http or https.

The procedure how to connect a remote computer and use a CLI is outlined in the topic "Configuring IP Address(es)" on page 25.

TimeKeeper requires all of the network interfaces to be present in the proper order. When using TimeKeeper CLI, take care to not delete or move any interfaces.

5.5 TimeKeeper: Additional Information

This Chapter contains additional information about TimeKeeper- specific features and resources, such as event notifications, licensing, and other reference information not covered elsewhere.

5.5.1 TimeKeeper Event Notifications

5.5.1.1 SNMP, or Syslog Messages

Below are the specific messages that TimeKeeper will emit via SNMP, or syslog. Variable components of each message are replaced with the string VALUE below – depending on the specific value found, the message will vary here.

Each trap is followed by a brief explanation of the cause, and are grouped by function.

Client Sync Quality

» `Client sync quality error on PTP server VALUE, client VALUE, source VALUE: absolute value of offset VALUE > VALUE`

VelaSync collects client sync accuracy information from clients - and will emit the above trap when one of the clients exceeds the server- specified accuracy threshold. (See the SYNCERRORTHRESHOLD configuration variable.)

These messages can be throttled by setting the "SYNC_ ERROR_ THRESHOLD_ THROTTLE" variable.

When configured to send SNMP traps, this event will be delivered using the clientQualityTrap.

Invalid Sources

1. `Source VALUE: source appears to be valid again - re-enabling`
2. `Source VALUE declared invalid/insecure`
3. `Source VALUE declared invalid/insecure because of tickrate`
4. `Source VALUE declared invalid/insecure because of offset`
5. `Source VALUE declared invalid/insecure because of large time jump`
6. `Source VALUE: TimeKeeper GPS/Oscillator detected moderate jamming`
7. `Source VALUE: TimeKeeper GPS/Oscillator detected critical jamming level`
8. `Source VALUE: TimeKeeper GPS device reports overheating, Temp: VALUEC/VALUEF`
9. `Source VALUE: TimeKeeper GPS/Oscillator detected VALUE% jamming/noise`

If TimeKeeper is crosschecking sources with the SOURCECHECK feature, some sources may be found to be invalid and rejected for a time. If a source has been rejected but is now found to be valid again, the **first message** will be sent. This is a clearing trap for the remainder of the list.

Similarly, TimeKeeper will send **traps 2-5** above when a source is rejected. The second trap will be sent in every case, with one of the following traps 3-5 depending on the reason the source is being rejected.

The **last four messages** indicate there is an issue with the GPS device provided in TimeKeeper Grandmasters. These messages do not have clearing equivalents.

When configured to send SNMP traps, this event will be delivered using the sourceStateTrap.

Other Source-Related Messages

1. `Time source change VALUE -> VALUE`
2. `Unable to find any valid time source.`
3. `Previously unable to find any valid time source, now using source VALUE.`

The **first message** above will be sent whenever TimeKeeper changes source for any reason - such as when one source stops providing timing data for more than 3 minutes. This will also occur in situations where the source TimeKeeper is tracking changes where it is getting time from, such as when an NTP server switches to another upstream source.

The **second message** will only be sent if TimeKeeper has failed over to the last configured source and even that has stopped responding. At this point, TimeKeeper is unable to track any sources and is driving the clock based on its best known clock rate.

The **third message** is a clearing trap for the second - if TimeKeeper previously lost all sources but one was found to be usable again, this message provides notification of the change.

When configured to send SNMP traps, this event will be delivered using the changedSourceTrap.

Sync Quality

1. `Sync quality error on source VALUE, absolute value of offset VALUE > VALUE`
2. `Sync quality restored on source VALUE, absolute value of offset VALUE < VALUE`

When a client has the SYNCERRORTHRESHOLD configuration option defined on a source, it will emit the **first trap** above whenever the sync offset exceeds that threshold.

When the sync comes back into the SYNCERRORTHRESHOLD range, the **second trap** above will be sent as a means of clearing state.

When configured to send SNMP traps, this event will be delivered using the sourceQualityTrap.

Grandmaster Issues

1. `Grandmaster unable to collect system chassis version information.*`
2. `Grandmaster unable to collect system chassis information from pipe.*`
3. `Grandmaster power supply 1 failure`
4. `Grandmaster power supply 2 failure`
5. `Inlet temperature failure`

A "*" above indicates there may be further information provided in the data. These messages are specific to TimeKeeper Grandmasters, and indicate issues with the appliance.

Contact Spectracom Technical Support for assistance (see "Technical Support" on page 102). These messages do not have clearing equivalents.

When configured to send SNMP traps, this event will be delivered using the grandMasterFaultTrap.

Web Management IP Mismatch

- `Address VALUE specified for WEB_MANAGEMENT_IP but was not matched to a device. Ignoring parameter.`

On startup, if the WEB_MANAGEMENT_IP parameter is used to limit access to the web tools, TimeKeeper makes sure that matches a configured interface. If it does not, this trap will be sent out and TimeKeeper will allow the web interface to be used on all interfaces so the issue can be resolved.

When configured to send SNMP traps, this event will be delivered using the startupFaultTrap.

Miscellaneous Issues at Startup

1. `Cannot open socket: VALUE`
2. `Source VALUE: Cannot open socket: VALUE`
3. `Source VALUE: Unable to prepare server socket descriptors for PTP`
4. `Unable to prepare server socket descriptors for PTP`
5. `Invalid MAJORTIME reference specified for source`
6. `No time sources found. Make sure at least one time source is declared in /etc/timekeeper.conf`
7. `Invalid CPU value specified: VALUE`

This is a subset of the number of possible traps, sent on startup if TimeKeeper is unable to prepare internal resources as needed based on the current configuration, or if it is unable to start for other reasons, like an invalid configuration.

Regardless of the specific message, a startupFaultTrap indicates TimeKeeper is not operating normally and requires investigation — generally this is due to a misconfiguration. However, despite these messages thrown at startup, VelaSync will allow you to reconfigure TimeKeeper via the Web UI, in order to resolve the detected issue.

When configured to send SNMP traps, this event will be delivered using the startupFaultTrap.

5.5.1.2 Locating the MIB

For more details on the SNMP trap/Event types referenced below, refer to the MIB, which can be found in the Web UI under the **Support** tab.

5.5.2 TimeKeeper: Included Tools

VelaSync's TimeKeeper installation includes several tools, some of which are not covered elsewhere in this document. These helpful additional resources include:

» baddate — This is a (Linux) test utility for moving the time away from the current value. The argument to baddate is a floating point number of seconds to move time either forwards or backwards. This can be used before TimeKeeper starts, in order to move the system time around for testing.

» timetests.* — These provide system call overhead information for static, dynamic, and 32 bit binaries on a given host.

» timekeeper_uninstaller, timekeeper_uninstaller.bat — This is an uninstall script to remove a TimeKeeper installation. Use timekeeper_uninstaller.bat on Windows.

» report_problem.sh and report_problem.bat (also available on Linux as /usr/bin/report_problem.sh) — This script collects system information to be emailed in case of a problem. Please provide the results of this script with the description of any product issue. Running "report_problem.sh -u" ("report_problem.bat -u" onWindows) will try to automatically upload the generated report to FSMLabs. Both of these scripts can be more easily run from the "Support" tab on TimeKeeper's web interface.

» tkstatus.sh (also available as /usr/bin/tkstatus on Linux) — This script on Linux gives a short overview of the current TimeKeeper status, including a license overview, current source accuracy, and the age of any recent updates.

» stats — This Linux tool summarizes TimeKeeper source files to give offset and frequency data. It can be run as "./stats timekeeperdata=/var/log/timekeeper_0.data" to provide a summary of the primary source's behavior over time.

- timekeeper_cli — This is a tool that allows for some command-line based configuration ability on VelaSync.

5.5.3 Holdover

VelaSync is equipped with a high-quality oscillator which is capable of providing good time, even while not actively receiving time updates via GPS.

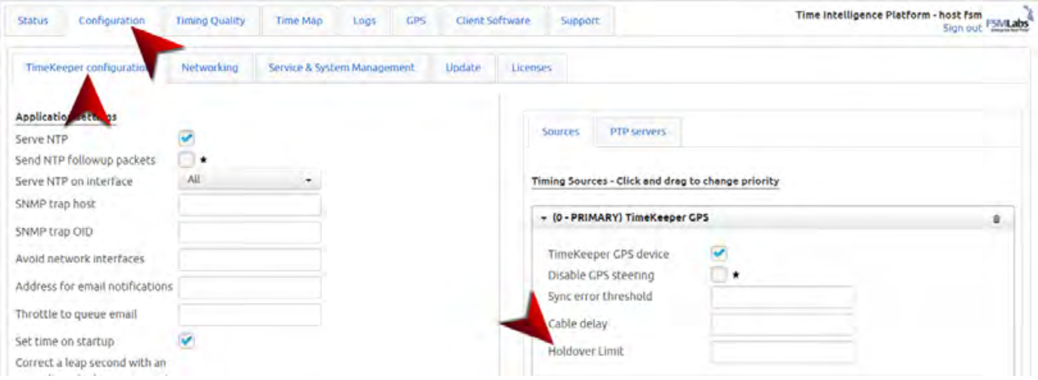
TimeKeeper utilizes this feature and hence will remain in **holdover** for 2 hours (7200 seconds) by default, i.e. continues to use the GPS timing source, even when it reports no GPS signal.

Once the 2 hours expire without the GPS time becoming available again, TimeKeeper will begin comparing all available time sources to determine if the holdover time is out of range with other time sources by using the **Sourcecheck** algorithm (even if Sourcecheck is disabled). For more information, see "Validating a Timing Source" on page 73.

If Sourcecheck determines that a different time source previously configured by you (e.g., a PTP server) provides a better quality time than the oscillator, TimeKeeper will automatically switch over to that time source until the GPS source becomes available again. This concept is referred to as **Failover**; for more information, see "Failover" on the next page.)

The 2-hour holdover time can be changed:

1. Navigate to **Configuration > TimeKeeper configuration: Sources**, and open the **TimeKeeper GPS** pull-down menu.
2. Enter a number in seconds into the **Holdover Limit** field.



Application Settings

Serve NTP ☑
Send NTP followup packets □ *
Serve NTP on interface: All
SNMP trap host
SNMP trap OID
Avoid network interfaces
Address for email notifications
Throttle to queue email
Set time on startup ☑
Correct a leap second with an

Timing Sources - Click and drag to change priority

(0 - PRIMARY) TimeKeeper GPS

TimeKeeper GPS device ☑
Disable GPS steering □ *
Sync error threshold
Cable delay
Holdover Limit

Figure 5-1: Configuring the Holdover Limit

> **Note:** If left blank, the Holdover Limit defaults to 7200 seconds.

5.5.3.1 Disciplining

The above-mentioned oscillator integrated into VelaSync is, in fact, the device that under normal operating conditions provides TimeKeeper with the time signal and the 1PPS signal to be distributed over the network. The GPS source only **steers** the oscillator, in order to counteract the unavoidable (albeit miniscule) drift of OCXO or even Rubidium oscillators. This process is called **Disciplining**.

In its standard configuration, TimeKeeper uses the time and 1PPS signal provided by the oscillator, steered by the GPS time, since this is by far the most accurate time source commercially available. If the GPS signal is temporarily lost, however, the oscillator will freerun for the duration of the holdover time, before TimeKeeper selects the next-best timing source e.g., a PTP- or NTP-server until the GPS source becomes available again to discipline the oscillator which will then again take over the role as primary timing source.

This standard configuration can be changed: see "Setting Up Timing Sources" on page 70 to learn more.

5.5.4 Failover

Failover refers to the concept of TimeKeeper automatically switching to a lower-priority time source if a higher-priority time source becomes unavailable e.g., in the case of GPS if reception quality fluctuates.

TimeKeeper utilizes timing sources in the order defined. This means, VelaSync's system clock will be driven to match Source (0) (or the lowest numbered source) as long as that Source is delivering timing data. Should Source (0) stop to provide data, TimeKeeper will fail over to Source (1), (2), and so on.

In the event of a source failure, TimeKeeper will start using Source (1), and it will continue to use Source (1) until either it fails, or Source (0) begins responding again.

If Source (0) returns, TimeKeeper will begin tracking it again. All of this occurs regardless of what protocol or type of Source is in use.

TimeKeeper can also actively compare each time source, and proactively reject bad sources using the **Sourcecheck** feature. For details on enabling and using Sourcecheck, please see below.

Note that before failing over to a lower-grade timing source, the VelaSync internal oscillator will be used for a period of time (the default is 2 hours) to provide the timing signal and the 1PPS signal. This is referred to as **Holdover**.

5.5.4.1 Failover Without Sourcecheck

In its default configuration (i.e. Sourcecheck = DISABLED), TimeKeeper will allow for automatic failover from higher priority sources to lower priority sources, in the event that the higher priority sources stop providing time. This means that if you have configured Source (0) and Source (1), TimeKeeper will use Source (0) as long as it is providing time.

Even if Source (0) provides incorrect time e.g., due to faulty hardware, a spoofing attack, or a misconfiguration, TimeKeeper will continue to use it. When configured, alarms will be sent out because Source (1) will disagree with Source (0), but Source (0) will continue to be used.

5.5.4.2 Failover With Sourcecheck

Sourcecheck provides an additional failover model that includes checks on the validity of time and not just whether or not time is being provided. With Sourcecheck enabled, in addition to tracking sources based on the configured priority, TimeKeeper will actively compare each source against the others and proactively reject a source based on its behavior, even if it is continuing to provide data. Source (0) could be rejected for Source (1) if Source (0) disagrees with Sources (1), (2), and (3). This detects and avoids timing issues based on faulty hardware, false leap seconds, misconfigurations, spoof attacks, and so on.

To take advantage of Sourcecheck, you must have at least two time sources configured. Three or more time sources is preferred since more advanced checks can be performed. More sources is better than fewer. More accurate sources allow for more accurate checks and faster problem detection. For example, even multiple public NTP servers over the internet can be useful for cross-checking a good local GPS clock source.

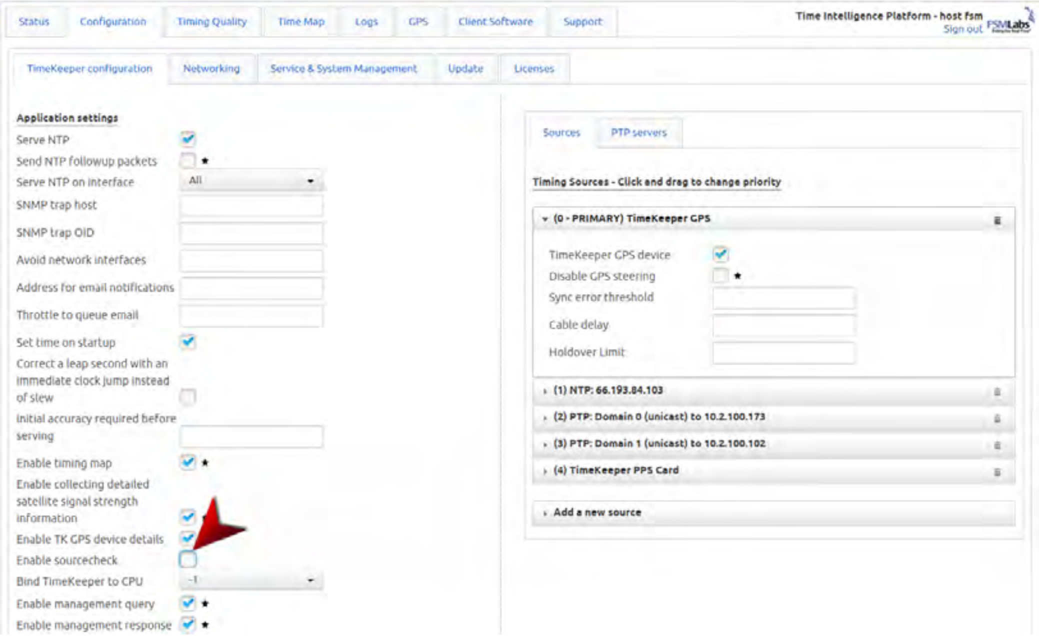
TimeKeeper watches all of the sources for their trending behavior, and reports in the TimeKeeper log file if it detects that a source is out of agreement or behaving erratically. Should that be the case, then information about the behavior of the primary and the current source will provide information about why the clock is unacceptable.

Note that TimeKeeper distrusts all sources in this configuration — if the primary time source is moving in a different direction than the majority of the sources, TimeKeeper will reject the primary source and move to the next highest priority source that is in agreement with the majority and send alerts about the change. Alerts will be sent out based on the configuration, i.e. via SNMP, or syslog.

The Sourcecheck feature can be used to provide logging data for the behavior of available time sources on the network (including local devices). It can also act as an alarm to detect any freewheeling or compromised time servers. If VelaSync is used as a server, it can ensure that clients retain a good quality sync regardless of network issues or timing attacks. If a source goes away or acts erratically, TimeKeeper will decide what the next best source is and choose it, without interrupting service to any clients.

To enable Sourcecheck:

» Navigate to **Configuration > TimeKeeper configuration: Enable Sourcecheck**.



Application settings

- Serve NTP ☑
- Send NTP followup packets ☐ ★
- Serve NTP on interface: All
- SNMP trap host
- SNMP trap OID
- Avoid network interfaces
- Address for email notifications
- Throttle to queue email
- Set time on startup ☑
- Correct a leap second with an immediate clock jump instead of slew ☐
- Initial accuracy required before serving
- Enable timing map ☑ ★
- Enable collecting detailed satellite signal strength information ☑
- Enable TK GPS device details ☑
- Enable sourcecheck ☐
- Bind TimeKeeper to CPU: -1
- Enable management query ☑ ★
- Enable management response ☑ ★

Timing Sources - Click and drag to change priority

- (0 - PRIMARY) TimeKeeper GPS
  - TimeKeeper GPS device ☑
  - Disable GPS steering ☐ ★
  - Sync error threshold
  - Cable delay
  - Holdover Limit
- (1) NTP: 66.193.84.103
- (2) PTP: Domain 0 (unicast) to 10.2.100.173
- (3) PTP: Domain 1 (unicast) to 10.2.100.102
- (4) TimeKeeper PPS Card
- Add a new source

Figure 5-2: Configuring Sourcecheck

For more information on Failover, see "Setting Up Timing Sources" on page 70.

For more information on Holdover, see "Holdover" on page 91.

5.5.5 Leap Seconds

Per default, TimeKeeper handles leap seconds by “slewing”, rather than introducing discontinuities, “jumps” or pauses in time to correct them. It will smoothly adjust any offset introduced by a leap second to ensure monotonically increasing time.

Some time keeping methods and time reference sources do pause the clock and TimeKeeper will deal with them gracefully. This will initially show up as about a 10 second offset of the time which will be smoothly corrected out over the next three to eight minutes.

TimeKeeper does offer a mode to “jump” the clock or perform a “step” when the leap second occurs in order to reduce the amount of time needed to correct out the time offset introduced by the leap second. To enable this feature:

» Navigate to **Configuration > TimeKeeper configuration**, and click the field next to the Application Setting "**Correct a leap second with an immediate clock jump instead of slew**".

In this mode, when TimeKeeper detects a 1 second offset within a 15 second window of when a leap second is introduced (either midnight UTC of June 30, or December 31 of a year) it will immediately correct the clock by 1 second. Note that depending on how leap seconds are propagated within your time environment, this may not occur exactly when the leap second occurs.

We recommend testing how a leap second is handled in your specific environment by simulating one if very fast correction of a leap second is important to you. Please contact Spectracom Technical Support for assistance, see "Technical Support" on page 102.

5.5.5.1 GPS-Induced Leap Second

VelaSync's GPS source (and any other GPS time source) provides time via a UTC broken down format. This means that normally an additional second will be sent to TimeKeeper at the 23rd hour, 59th minute and 60th second of the day when the leap second happens.

This will show up on the server as 1 second after the 23rd hour, 59th minute and 59th second of the day. When the new day starts in the next second – 0th hour, 0th minute and 0th second – TimeKeeper will calculate this as the same second as was previously reported by the time source. This will mean TimeKeeper will calculate an error of 1 second at that time.

Over the next few seconds TimeKeeper will work to remove that error through slewing. Normally this takes 5 to 10 seconds to do. It should be noted that an offset will be expected when leap seconds are introduced and will take 5 to 10 seconds to eliminate. During the time that this offset is being reduced TimeKeeper will not slow down the clock by more than 25% of its original value.

5.5.5.2 TimeKeeper as an NTP Client/Server

Most NTP protocol implementations will handle leap seconds by pausing the clock at some point in the last second of the day. TimeKeeper does not do this. Below is an example of querying a typical non-TimeKeeper NTP server at 0.25 second intervals during a leap second.

```
Response from some non-TimeKeeper NTP servers:

23:59:58.50

23:59:58.75

23:59:59.00
```

```
23:59:59.25
23:59:59.50
23:59:59.75
23:59:59.75
23:59:59.75
23:59:59.75
23:59:59.75
00:00:00.00
00:00:00.25
```

If a TimeKeeper instance is configured to act as a **client** to one of these non-TimeKeeper NTP servers, TimeKeeper will slow it's own clock down slightly so that it can match the remote clock that is paused until the 1 second offset that was introduced by the leap second is corrected. This offset removal should take a few seconds.

TimeKeeper acting as an NTP **server** will not set the “leap second indicator” flag in responses that it sends. It will track the time of any source that it is configured to use and will send that time out to any requesting NTP clients. It will not pause the clock at any point and any offsets introduced by the leap second will be corrected through slewing without introducing pauses or jumps.

5.5.5.3 TimeKeeper as a PTP Client/Server

TimeKeeper as a **PTP client** will see a leap second occur when a PTP Announce message sent by the server shows a change in the UTC offset field. At that point, TimeKeeper will begin to correct the offset introduced by the change in TAI to UTC offset values. This occurs whenever the server sends the new UTC offset in an announce message and that can vary depending on the server. This could be quite some time after the actual leap second.

TimeKeeper acting as a **PTP server** will not set the “leap second indicator” bit in announce messages to clients. When the leap second occurs according to the source feeding the server, TimeKeeper will slew to match the source and will provide that time to the client without introducing a discontinuity.

5.5.5.4 Reasons for a Leap Second Correction

A Leap Second is an intercalary[1] one-second adjustment that keeps broadcast standards for time of day close to mean solar time. Leap seconds are required to synchronize time standards with civil calendars, thus keeping UTC time in sync with the earth's rotation.

If it has been determined by the International Earth Rotation and Reference Systems Service (IERS) that a Leap Second needs to applied, this time correction occurs only at the end of a UTC month, and has only ever been inserted at the end of June 30 or December 31. A Leap Second may be either added or removed, but in the past, the leap seconds have always been added because the earth's rotation is slowing down.

Historically, Leap seconds have been inserted about every 18 months. However, the Earth's rotation rate is unpredictable in the long term, so it is not possible to predict the need for them more than six months in advance.

Note: Leap seconds only apply to the "UTC" and "Local" timescales. Leap seconds do not affect the "GPS" and "TAI" timescales. However, a leap second event will change the GPS to UTC and TAI to UTC offsets. When a leap second occurs, VelaSync will automatically change these offsets by the proper amount, no matter which timescale is currently being used by the system.

5.5.6 Simulating a Time in the Past

When receiving time from any time source, TimeKeeper will validate that time to make sure that it can be trusted. One of these checks includes making sure the time is not earlier than the release date of the TimeKeeper version being used. This can catch problems with time sources that are reporting erroneous time but it also means that it is not possible to run simulations with time in the past. If you need to be able to use simulated time that is in the past please contact Spectracom Technical Support (see "Technical Support" on page 102).

5.5.7 PTP Sync Rate

A PTP sync message rate of roughly 1 packet/second is a good tradeoff between network traffic and synchronization accuracy. A faster sync rate can reduce the accuracy of the synchronization rather than improve it. Even though TimeKeeper supports a rate of 64 sync messages per second it is not recommended to set the rate that high it since it can reduce the synchronization accuracy a great deal.

[1] Intercalary: (of a day or a month) inserted in the calendar to harmonize it with the solar year, e.g., February 29 in leap years.

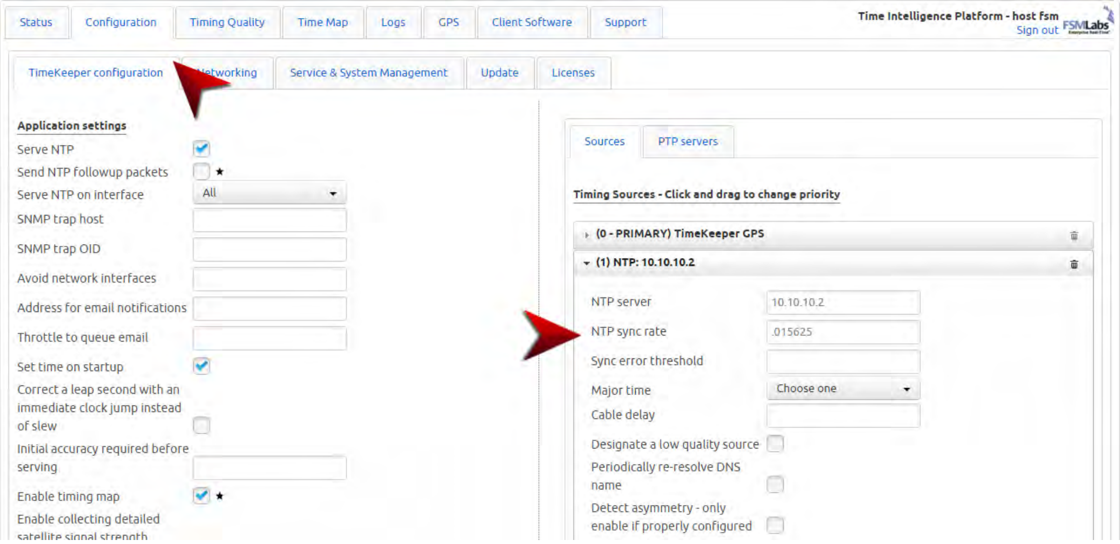
5.5.8 NTP Query Rate

By default as an NTP client TimeKeeper will query the server at 1.1 second intervals. Faster and slower query rates are supported but the default rate is generally recommended as it achieves the best performance while using little bandwidth.

When acting as a NTP client, TimeKeeper will wait for many milliseconds for a response. If there is no response from the server in that time, the server is assumed to not be responding and no time synchronization will occur during that query of the server. This could be a problem for synchronization of a very slow WAN connection. If your installation requires a very long interval please contact Spectracom Tech Support for configuration information. (See "Technical Support" on page 102.)

To set the sync rate for an NTP time source:

1. Navigate to **Configuration > TimeKeeper Configuration > Sources**.
2. Open the pulldown menu for the desired NTP source, and edit the second line item.



Application settings

Serve NTP ☑
Send NTP followup packets □ *
Serve NTP on interface: All
SNMP trap host
SNMP trap OID
Avoid network interfaces
Address for email notifications
Throttle to queue email
Set time on startup ☑
Correct a leap second with an immediate clock jump instead of slew □
Initial accuracy required before serving
Enable timing map ☑ *
Enable collecting detailed satellite signal strength

Timing Sources - Click and drag to change priority

(0 - PRIMARY) TimeKeeper GPS
(1) NTP: 10.10.10.2

NTP server: 10.10.10.2
NTP sync rate: .015625
Sync error threshold
Major time: Choose one
Cable delay
Designate a low quality source □
Periodically re-resolve DNS name □
Detect asymmetry - only enable if properly configured □

Figure 5-3: Setting the NTP sync rate

Specify the rate at which the server is to be queried, in packets/sec, for example:

- A value of 0.9 would query every 1.1 seconds (1/0.9 = 1.1)
- A value of 0.5 represents a query every 2 seconds.
- A value of 0.015625 will generate a query every 64 seconds.

5.5.9 Logging in via SSH, Console, or Keyboard

TimeKeeper supports several login and authentication protocols.

A TimeKeeper instance running on VelaSync utilizes local system accounts forweb, SSH and console logins. These accounts can be configured to authenticate with remote tools like RADIUS and TACACS+. This topic covers the specifics of each of these types of logins and how they are authenticated.

As per default, TimeKeeper running on VelaSync permits RS232 console login, and keyboard/monitor access for enabled accounts, but not SSH access.

To enable SSH access:

- Login to the Web UI as “admin”. Then navigate to **Configuration** > **Service & System Management**, and under Manage Access, click the **Enable SSH** button. (If you only see a button **Disable SSH**, then SSH is already enabled.)

Once this is enabled, logs can be retrieved via SCP, SFTP and similar tools with the ’loguser’ user. It is also possible to SSH into the device and run system monitor tools like ’top’, ’ps’ and other Linux programs.

Users “admin” and “readonly” can also be used on the console or via SSH in addition to the “loguser” user. However, “readonly” and “loguser” accounts must be enabled via the Web UI before they can be used.

To enable the accounts “readonly” and “loguser”:

- Navigate to **Configuration** > **Service & System Management**, and under Manage Access, click either corresponding button. This will permit RS232 and keyboard/monitor access but not SSH, unless SSH access is enabled.

All console and SSH logins will authenticate via RADIUS or TACACS+ if TimeKeeper is configured to use those protocols.

Note: For safety reasons, it is strongly recommended that you change the default password for “loguser” immediately.

The default password for "loguser" is: “**logaccess**”. This applies even if RADIUS or TACACS+ is in use, as TimeKeeper will still fall back to login against the local account if possible when logging in.

The “readonly” and “loguser” accounts are intended for easy log collection via SSH, so that logs can be archived as needed for audit trails.

5.5.9.1 "Root" Access

Standard shell access as “root” is not normally permitted or recommended. Please do **NOT** enable **Enable root login** via the Web UI menu **Configuration** > **Service & System Management**, unless asked to by Spectracom Technical Support.

> **Caution:** Modifying the configuration by changing console ports, otherwise modifying the Linux kernel, BIOS settings, installed devices or installed software applications may cause problems in performance or correctness. Spectracom Technical Support is not obligated to providing support if such modifications had been made.

5.5.10 HTTPS Support

HTTPS provides secure/encrypted, web-based management and configuration of VelaSync from a PC. An SSL certificate is required to be stored in VelaSync in order to establish this secure HTTPS connection.

VelaSync uses OpenSSL library with a basic user interface to create a certificate request or self-signed certificate. The certificate request must be submitted to an external Certificate Authority (CA) for the creation of a third party verifiable certificate or use an internal corporate Certificate Authority. If a Certificate Authority is not available you can use the default self-signed certificate that comes with the unit until it expires, or create your own self-signed certificate to allow the use of HTTPS. Please note that the default certificate is empty—you may need to create a new one in order to comply with your company's internal policies, or just to simplify systems management.

Out of the box, VelaSync will use the above-mentioned unique self-signed certificate, when accessed via https. This means that browsers may, on initial connection, ask you to confirm that the certificate is acceptable. This is normal and expected when using a self-signed certificate. This warning will only occur when using https, and with most browsers will only need to be viewed once.

> **Note:** If deleted, the HTTPS certificate cannot be restored. A new certificate will need to be generated.

Note: If the IP Address or Common Name (Host Name) is changed, you may wish to regenerate the security certificate. Otherwise you may receive security warnings from your web browser each time you login.

The OpenSSL library provides the encryption algorithms used for secure HTTP (HTTPS). The OpenSSL package also provides tools and software for creating X.509 Certificate Requests, Self Signed Certificates and Private/Public Keys. For more information on OpenSSL, please see www.openssl.org.

To access VelaSync's https functionality under the **Configuration > Service & System Management** tab, you need to login via https. An example login address would be the following URL:

» `https://192.168.1.1`

The **Generate HTTPS CSR** button is located under **Manage Communication** in the **Service & System Management** tab.

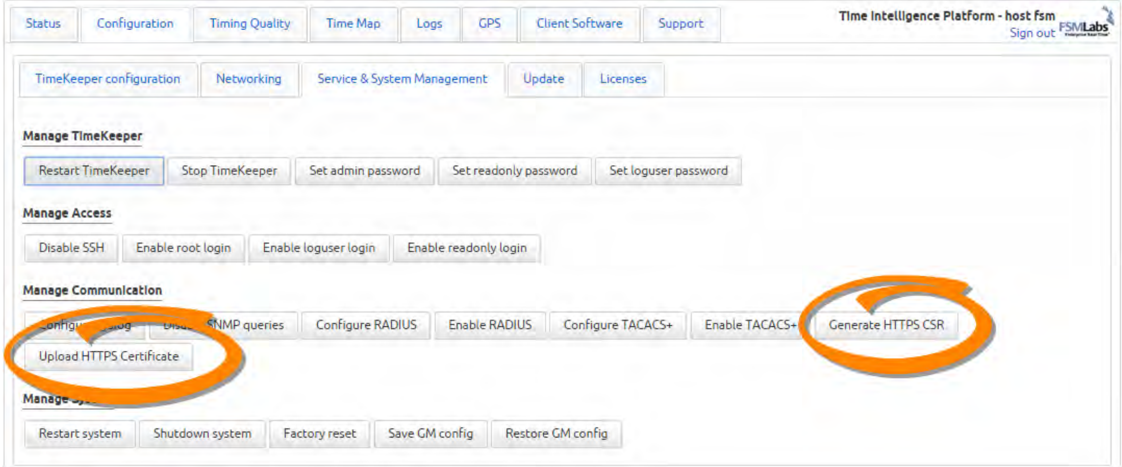


Figure 5-4: HTTPS controls

Click Generate HTTPS CSR to open the corresponding menu. Information on how to populate the fields can be found under "The Subtab "Service & System Management"" on page 50.

Once the request is generated, the dialog will be updated with the CSR data. This text can be copied and delivered to the appropriate certificate authority for validation. As part of this process, a new certificate and key will be generated on the appliance. TimeKeeper must be restarted in order for the new key to be used. (Note that since VelaSync now has a new self-signed certificate, client browsers may again present the initial certificate warning after the next appliance restart.)

Once a signed certificate has been generated based on the CSR, it can be uploaded by clicking **Upload HTTPS Certificate** at the same Web UI location. This will initiate a file upload dialog that can be used to upload the newly generated certificate. This step will cause TimeKeeper to restart immediately in order to apply the certificate.

5.6 Links to External Information

To learn more about the following **hardware**-related subjects, see the Server OEM User's Manual at http://www.supermicro.com.tw/manuals/superserver/1U/MNL-1328.pdf:

- System safety
- Server setup
- Rack mounting
- System Interface
- Motherboard
- Chassis
- System fans
- Hard disks
- Power supplies
- Advanced setup
- BIOS setup
- BIOS error beep codes
- Chipset
- Server management
- System specifications

5.7 Technical Support

To request technical support, please go to the "Support" page of the Spectracom Corporate website, where you can not only submit a support request, but also find additional technical documentation.

Phone support is available during regular office hours under the telephone numbers listed below.

To speed up the diagnosis of your VelaSync unit, please send us:

- the current **product configuration**, and
- the **events log**.

Thank you for your cooperation.

5.7.1 Regional Contact

Spectracom operates globally and has offices in several locations around the world. Our main offices are listed below:

Country	Location	Phone
China	Beijing	+86-10-8231 9601
France	Les Ulis, Cedex	+33 (0)1 6453 3980
USA	Rochester, NY	+1.585.321.5800

Table 5-1: Spectracom contact information

Additional regional contact information can be found on the Contact page of the Spectracom corporate website.

5.8 Return Shipments

Please contact Spectracom Technical Support before returning any equipment to Spectracom. Technical Support must provide you with a Return Material Authorization Number (RMA#) prior to shipment.

When contacting Technical Support, please be prepared to provide your equipment serial number(s) and a description of the failure symptoms or issues you would like resolved.

Freight to Spectracom is to be prepaid by the customer.

Note: Should there be a need to return equipment to Spectracom, it must be shipped in its original packing material. Save all packaging material for this purpose.

5.9 Maintenance and Service

We recommend to clean the front **bezel filter** regularly:

» Remove the front bezel by unlocking it with the key, then pressing the red release knob, then removing the bezel with both hands. While the bezel is removed, check if the filter requires cleaning.

It is recommended that you keep a maintenance log of filter cleaning/replacement, since its condition will affect the airflow throughout the whole system.

Note: When using a cabinet-style rack, close the cabinet doors after completion of the maintenance work, to maintain proper cooling.

5.10 License Notices

TimeKeeper Software is licensed under the Software EULA, provided here:

http://www.fsmlabs.com/resources/tkeula

TimeKeeper, and some of its components are licensed under the terms granted by the copyright holders. Licenses used are listed in the file `licenses.pdf` that can be found either in the folder `/opt/timekeeper/doc`, or is available upon request from Spectracom or FSMLabs.

5.11 List of Tables

5.12 List of Images

5.13 Document Revision History

Rev	ECO	Description	Date
1.0	735	First-generation product manual.	Jan 2016

INDEX