Release Notes

LANTIME Firmware V7

1. Introduction

This document describes the features of Meinberg´s new firmware V7. Please read these release notes thoroughly before you install the V7 firmware, as they contain information you need to successfully install the software onto your Meinberg system.

Starting on the 15th of October 2019, all Meinberg LANTIME timeservers (M-series, SyncFire, IMS) will be delivered with the new V7 firmware. The V7 firmware comes with numerous new features and improvements for the LANTIME family systems and their management tools. This includes a comprehensive redesign of the web interface, as well as various security-relevant innovations.

2. V7 Release Notes Categories

2.1. Firmware

The LTOS Firmware V7 consists of several software components. The main third-party software packages included in LTOS are listed below with their version information.

Linux	Linux kernel 4.14.58
SSL	OpenSSL 1.0.2t and 1.1.1d
SSH	OpenSSH 8.1P1
Libssh	Libssh libssh-0.9.0
Web server	Web server lighttpd 1.4.53
Net-snmp	Net-snmp 5.8
Syslog-ng	Syslog-ng 3.20.1
NTP	NTP 4.2.8p13
Bash	Bash 4.4.18

2.2. Security

Due to the increased security requirements of computer systems, which are partly implemented in particularly worth-protecting environments, some of the security relevant settings have changed. As a result, it might be possible that regressions in terms of usage arise. The following chapters will clarify the changes and possible regressions.

2.3. Web Interface

The Web interface is the main management tool to configure the Meinberg LANTIME systems as well as LANTIME IMS systems and comes with the firmware V7 in a completely new look. All relevant changes will be described in this release notes.

2.4. SyncMon

The SyncMon is a new web-based application for the management of LANTIME as well as IMS models which are running with the new LTOS7. It has been developed for the LANTIME firmware V7 to provide end users with a multifunctional monitoring tool by allowing to measure NTP and PTP clients instead of relying on self- reported sync accuracy.

The re-design of the web interface also gives the SyncMon a completely new look. Added and improved features are explained in this release notes.

2.5. LANTIME Command Line Interface (LT_CLI)

The LT_CLI is now additionally available to the CLI you know since the LTOS 6. It offers a completely new management option for LANTIME products and allow the user a configuration with simplified handling as well as an easier access to (almost) all status information.

To reach the download page of the lt_cli manual go to:

English https://www.meinbergglobal.com/download/docs/manuals/english/ltos7-cli.pdf

German https://www.meinberg.de/download/docs/manuals/german/ltos7-cli.pdf

Here you can get information about how to get access to the lt_cli and detailed description of most of the popular commands.

3. Requirements

3.1. System Requirements

For the LANTIME Firmware V7 deployment, V7 needs the following requirements.

Name of Firmware release	Initial release Version LTOS 7.00 Build (7.00.002)
Date of release	11.10.2019
System Compatibility	
LANTIME Systems	M100
	M200
	M300
	M400
	M600
	M900
	SyncFire1000
	SyncFire1010
	SyncFire1100
LANTIME IMS Systems	M500
	M1000
	M1000S
	M3000
	M3000S
	M4000
Modules	[1]CPU-C05F1
	[2]CPU-C15G2
	[3]IMS Modules
Installation Requirements	CPU Module RAM: min 256MB
	CPU Module Flash: min 512 MB

[1] When using the CPU module - CPU-C05F1, the LANTIME Firmware V6 and V7 is supported

[2] When using the CPU module - CPU-C15G2 (Q7), only the Lantime firmware V7 is supported

[3] All current IMS clock and I/O modules are running in systems with installed LANTIME Firmware V7.

3.2. Connection Requirements

Cipher List

To be able to establish an ***SSL/TLS connection*** after updating your device, your browser has to support at least one of the listed cipher suites.

To be able to establish an ***SSH connection*** after updating your device, your SSH client has to support at least one of each of the listed cryptographic algorithms (e.g. SSH cipher, key exchange algorithm and message authentication code).

SSL	
Cipher suites:	ECDHE-ECDSA-AES256-GCM-SHA384
	ECDHE-RSA-AES256-GCM-SHA384
	ECDHE-ECDSA-CHACHA20-POLY1305
	ECDHE-RSA-CHACHA20-POLY1305
	ECDHE-ECDSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-GCM-SHA256
	ECDHE-ECDSA-AES256-SHA384
	ECDHE-RSA-AES256-SHA384
	ECDHE-ECDSA-AES128-SHA256
	ECDHE-RSA-AES128-SHA256
SSH	
Ciphers:	chacha20-poly1305@openssh.com
	aes256-gcm@openssh.com
	aes128-gcm@openssh.com
	aes256-ctr
	aes192-ctr
	aes128-ctr
Key Algorithms:	curve25519-sha256@libssh.org
	ecdh-sha2-nistp521
	ecdh-sha2-nistp384
	ecdh-sha2-nistp256
	diffie-hellman-group-exchange-sha256
MACs	hmac-sha2-512-etm@openssh.com
	hmac-sha2-256-etm@openssh.com
	umac-128-etm@openssh.com
	hmac-sha2-512
	hmac-sha2-256
	wumac-128@openssh.com

4. Changes

This chapter gives you detailed information about added or improved as well as removed functions of all relevant categories of Meinberg LANTIME Firmware V7.

4.1. Security

4.1.1. Security relevant settings and functions

- **SSH and web server configuration are overwritten with firmware defaults when updating V6 to V7**

  With an update of V6 to V7, all individual settings in the ssh and web server configuration are overwritten. Certificates or SSH keys are not affected. Subsequent updates will not change the settings made by the customer. This is necessary, because the update process of these configuration files has changed completely. Thus, the customer can specify individual configuration settings in a more comfortable manner in the future. The setup and location of some configurations have changed. Due to this fact, it is recommended to check the functionality of the scripts, cron jobs, settings or other deviations from the Meinberg firmware. This task has only to be performed, if any changes have been made by the customer, manually.

- **SSH has new cipher algorithms**

  Due to stronger cryptographic functions, it is possible that older ssh clients cannot connect to the LANTIME. In such a case, the clients should get an update. If this is not possible, the SSH service configuration must be adjusted using at least one updated SSH client. Using unsafe ciphers is not recommended.

- **Web server has new cipher algorithms**

  Due to stronger cryptographic functions, it may happen that older browsers can not establish a connection to a LANTIME. In such a case, the browser should be updated. If this is not possible, use a ssh connection and customize the web server configuration to use older unsafe algorithms. Using unsafe ciphers is not recommended.

- **Blocked SSH access on TSU cards**

  An SSH connection to the TSU cards T20 V1.2A GB and PXA 270 V2.4A via network is not possible anymore.

- **Resetting to factory defaults will activate the services HTTPS, SSH and NTP only**

  When setting factory defaults via front panel or via command line, only the most important services are activated. These services are HTTPS, SSH and NTP. NTP is not secure by default. Reconfigure it, if authenticated ntp timestamps are needed. In addition, the web server uses a HTTP redirect to HTTPS in the factory defaults. Resetting the factory defaults by web interface does not change the activated services in the network tab.

- **Display of changes made to the configurations**

  Security-relevant entries made to the configurations, such as passwd, are not displayed anymore in the web interface ***Main → "Last messages*** and ***"Show system messages"***.

- **Edit of default settings in the web interface**

  The choices of security relevant settings in the web interface are selected to the most secure value by default.

- **Active session timeout**

  After a session timeout has expired, the session will be deleted actively. This happens always on server side and also at client side when the browser is still opened. Please note that a web site which refreshes automatically does not have a timeout.

- **Predefined password length**

  The default password length of new passwords consists of eight characters.

- **Unique default self-signed certificates**

  Delivered web server certificates are uniquely created for each device. However, the customer should change the self-signed certificate into a certificate which is generated for usage in a public key infrastructure.

- **Syslog logfiles**

  According to the facility, syslog messages will be stored separately. With V7 it exists an auth, kern, messages, cron and syslog log file.

- **Automatic refresh of the main site**

  The main page will no longer be automatically refreshed.

4.1.2. Changed admin functions

The following functions are now allowed to super users only. An admin user was able to use them to do malicious activities. Because these changes are extensive, check carefully if admin users must get higher privileges or if affected tasks can be done by another super user.

- **Security → HTTPS Certificate**
  An admin user is not allowed to upload or change certificates. In addition, the private key is not displayed anymore.

- **NTP → NTP Leap Second → Upload Leap Second File Manually**
  An admin user is not allowed to upload a leap second file.

- **System → Services and Functions → Reset Factory Defaults**
  An admin user is not allowed to reset the system to factory defaults

- **System → Services and Functions → Manual Configuration**
  An admin user is not allowed to do changes in the “manual configurations” section.

- **System → User Management → External Authentication Options**
  An admin user is not allowed to enable or disable external authentication.

- **System → User Management → Add External Authentication Server**
  An admin user is not allowed to add or delete an external authentication server.

- **System → Firmware/Software Update → Start Update**
  An admin user is not allowed to start a firmware/software update.

- **System → Diagnostics → Download Diagnostic File**
  An admin user is not allowed to download a diagnostic file.

- **System → Configuration & Firmware Management → Upload Configuration**

  An admin user is not allowed to upload a configuration.

- **System → Configuration & Firmware Management → Configuration Management → Available Configurations → Download**

  An admin user is not allowed to download configurations.

- **System → Configuration & Firmware Management → Firmware Management → Available Firmwares Files → Activate**

  An admin user is not allowed to activate a firmware before V7.

- **System → Display → Edit Time Zone Table**

  An admin user is not allowed to edit the time zone table.

- **SyncMon**

  The changing of SyncMon settings is allowed to super users, only. The view is only filled, if a node or system monitoring was configured by a super user before.

4.1.3. Improved

Hardening measures that are listed in this section, are integrated in the firmware V7. The list relates to settings that are chosen by Meinberg and cannot be customized in most cases. Furthermore, only measures that affect public interfaces are listed. Customers should be aware that instructions about a secure configuration of a LANTIME is to be found in the LTOS 7 user manual in chapter "Security User Guide / Security Advisories".

English https://www.meinberg.de/download/docs/manuals/english/ltos_7-00.pdf

German https://www.meinberg.de/download/docs/manuals/german/ltos_7-00.pdf

System	
	▪ „Samba/Jquery removed because no longer required/supported.”
	▪ Firewall policy converted into a whitelisting policy
	▪ Firewall rules against SACK attacks added
	▪ Verification of the digital Meinberg firmware signature during firmware update added
	▪ LANTIME network footprint minimized
SSH	
	▪ Usage of Diffie-Hellmann parameters >= 3071bits
	▪ Modern cipher configuration recommended by Mozilla
Web server	
	▪ HTTP redirect added
	▪ Certificates will be generated with sha 256 and 2048bit during first boot
	▪ Diffie-Hellmann parameter >= 2048bit if a customer wants to use DHE cipher
	▪ Anti-Cache header added
	▪ Content-Security-Policy header added
	▪ Strict-Transport-Security header added
	▪ X-Frame-Options header added
	▪ X-Content-Type-Options header added
	▪ Intermediate certificates are easier to configure now
Web interface	
	▪ Anti-Cross-Site-Scripting OWASP guidelines implemented
	▪ Anti-Command-Line-Injection OWASP guidelines implemented
	▪ Privilege-Escalation vulnerabilities removed
	▪ Information-Leakage vulnerabilities removed
	▪ HTML-Noreferrer tag added to links, to prevent Cross-Domain-Referrer-Leakage
	▪ Password field auto completion disabled by default
	▪ Meinberg leap second file download only via HTTPS
	▪ Hiding security-relevant configuration settings
	▪ Warning, that a self-signed certificate is in use
	▪ Edit of the web logout mechanism to force timeouts
TSU	
	▪ Firewall policy converted into a whitelisting policy
	▪ SSH connection via network disabled

4.2. Web Interface

With the release of the LANTIME Firmware V7, the web interface was re-designed.

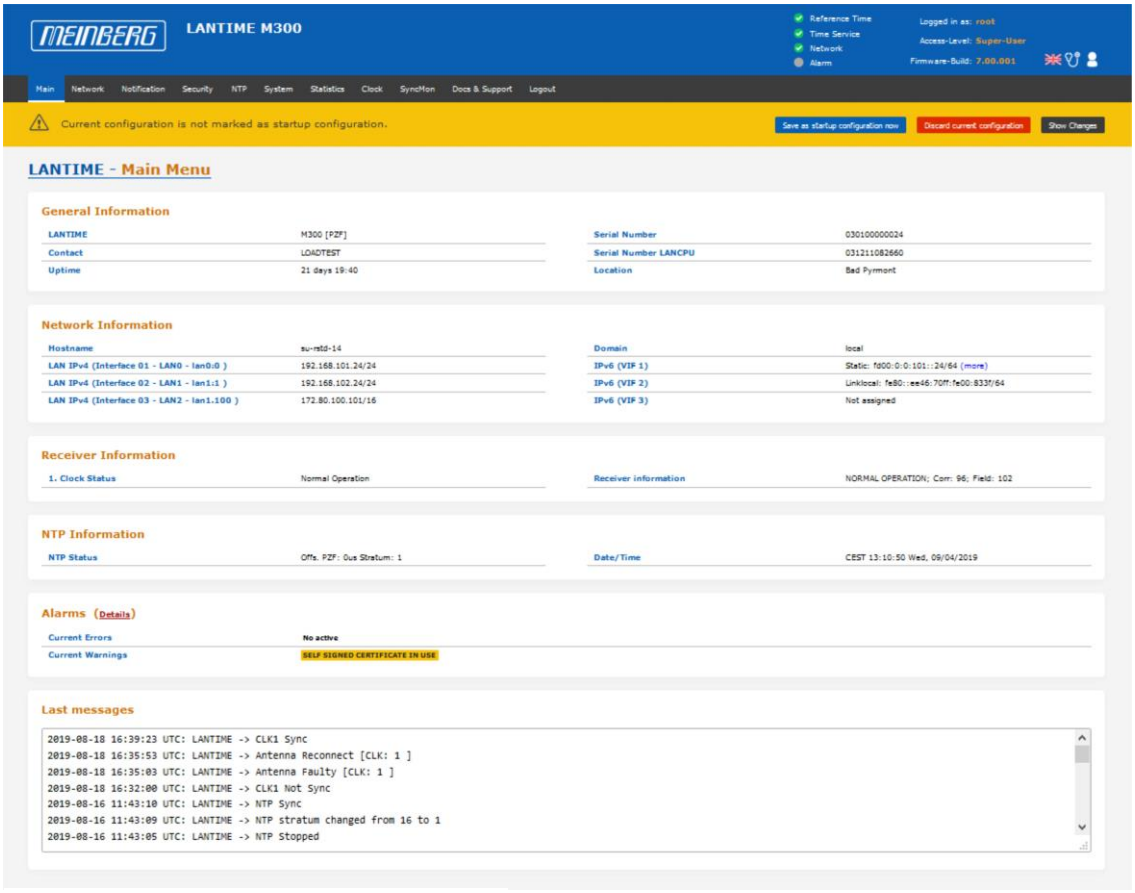


Figure 1: Main page of the web interface

4.2.1. Added

- Additional info in /xmr_info and WEB interface in case of MRS is waiting for TimeOfDay or Phase Reference
- New refclock parameter 'PTP Min Clock Class' to disable PTP reference if clock-class is degraded
- Up to 4 external Syslog servers with different log levels and formats
- Feature - Automatic save and apply of configurations uploaded via USB interface
- Feature - Automatic activation of firmware installed via USB interface
- Notification event “self-signed certificate in use”
- Network link status visible at main page
- For MRS systems it’s possible to specify a different symmetric key for each server
- PRP (Parallel Redundancy Protocol IEC 62439-3) can be configured

  (“Network” → “Physical Network Configuration” → “Bonding”)

4.2.2. Improved

- Login and Timeout behavior
- Redesign of “Clock” menu navigation

4.2.3. Changed

- System → General Settings → Web Timeout moved to Security → Login/Access
- Changed menu - Statistics → NTP Access Graph replaced by SyncMon → System Monitoring → Local NTP Counter
- Changed menu - “Ignore NTP mode 6 and 7 packets” and “Activate access restriction”

  moved from NTP → “General Settings” to NTP → “NTP Restrictions”

4.2.4. Removed

- Utilities for Windows Popup Notifications support (smbblient)
- XtraStats removed “(functionality now provided by SyncMon)”

4.3. SyncMon

The re-design of the web interface also gives the SyncMon a completely new look and it became more powerful with the firmware V7. Lots of new functions e.g. more internal system parameters have been added. The Xtrastats menu has been removed as the Xtrastats functionality is now provided by SyncMon. Added and improved features are explained below.

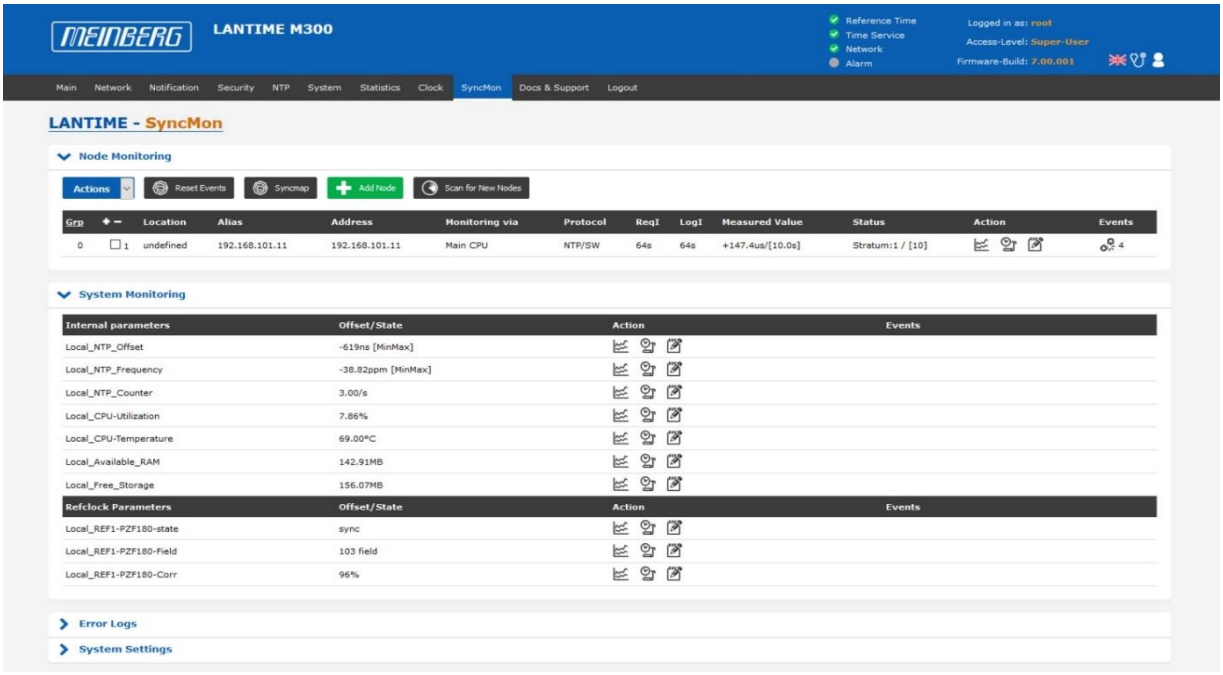


Figure 2:SyncMon

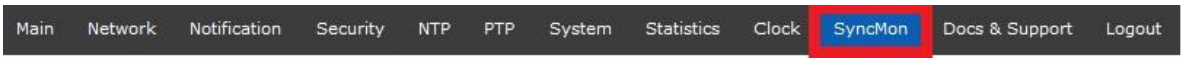
Please Note:

The changing of SyncMon settings is allowed to super users, only. The view is only filled, if a node or system monitoring was configured by a super user before.

4.3.1. Activate System Monitoring

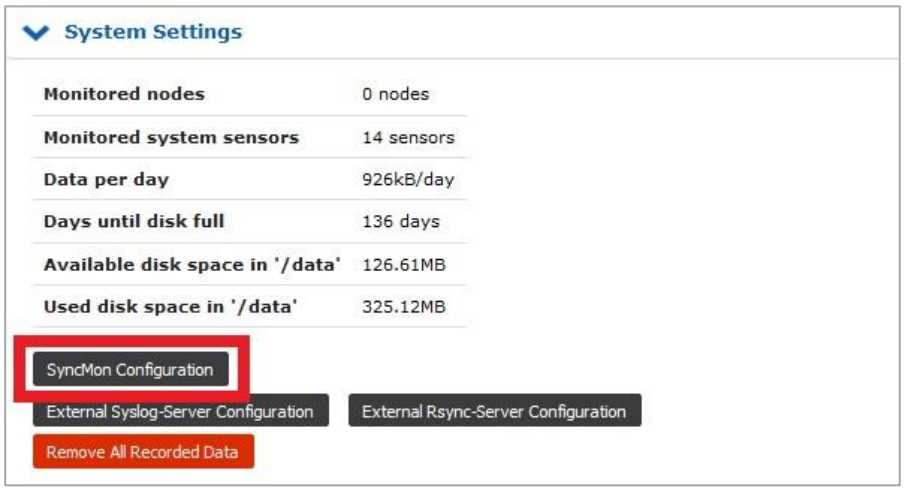
In the default settings the menu “System Monitoring” is disabled. It must be enabled manually if you want to monitor internal system parameters.

1. Select the menu “SyncMon” in the main bar of your web interface

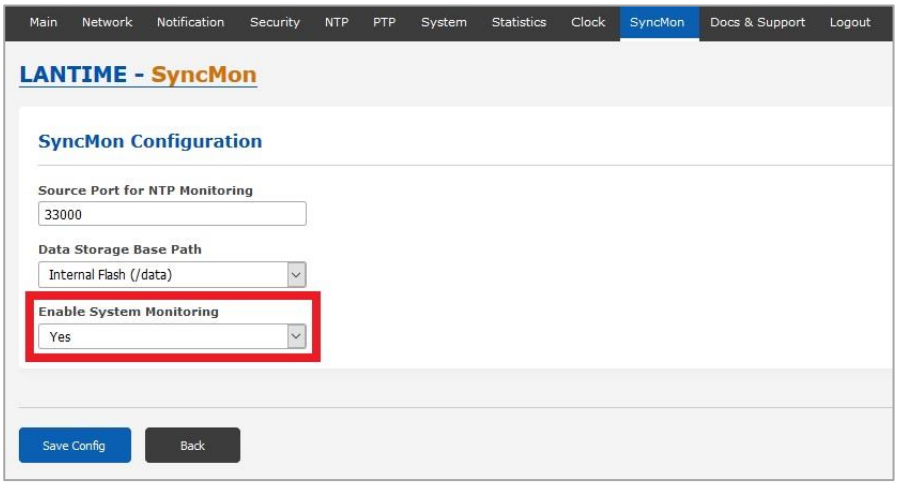


2. Select the sub menu “System Settings”

3. Select the menu “SyncMon Configuration”



4. Select ***Yes*** in the drop-down menu and click “Save Config” to enable “System Monitoring”



4.3.2. Added

- You can send measured data to external database
- New sensors for CPU temperature, NTP counter and Memory Usage
- Status file in JSON format for each node
- Location string to Splunk and JSON output
- FDM with Frequency and Time Deviation support
- External SyncMon as node to monitor

4.3.3. Improved

All graphs of the “SyncMon” are based on Java Script:

- More powerful by using the performance of the client’s pc web browser to generate the graph
- More flexible by selecting time range and scalability of the recorded graph
- More parameters can be monitored and visualized in a graph

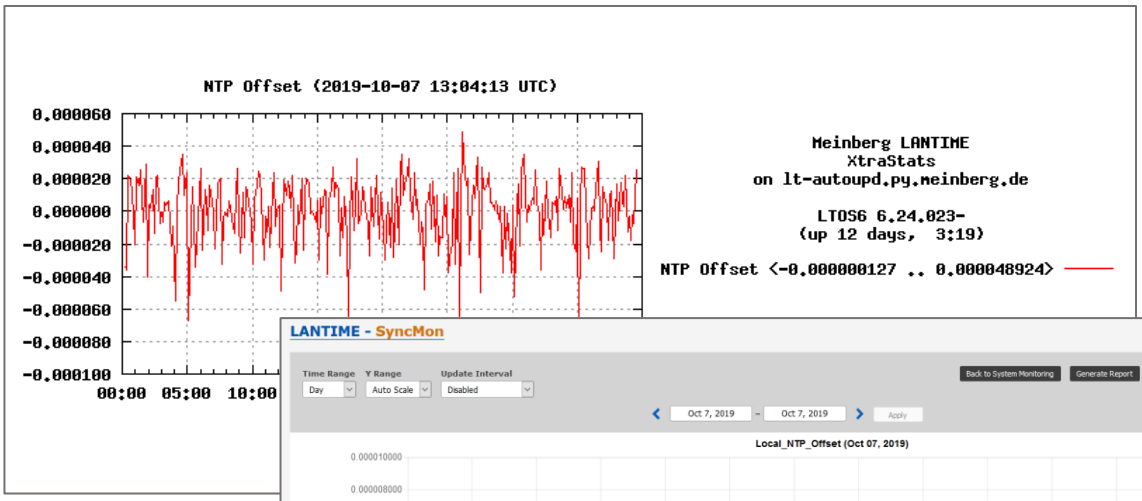


Figure 3: XtraStats in V6

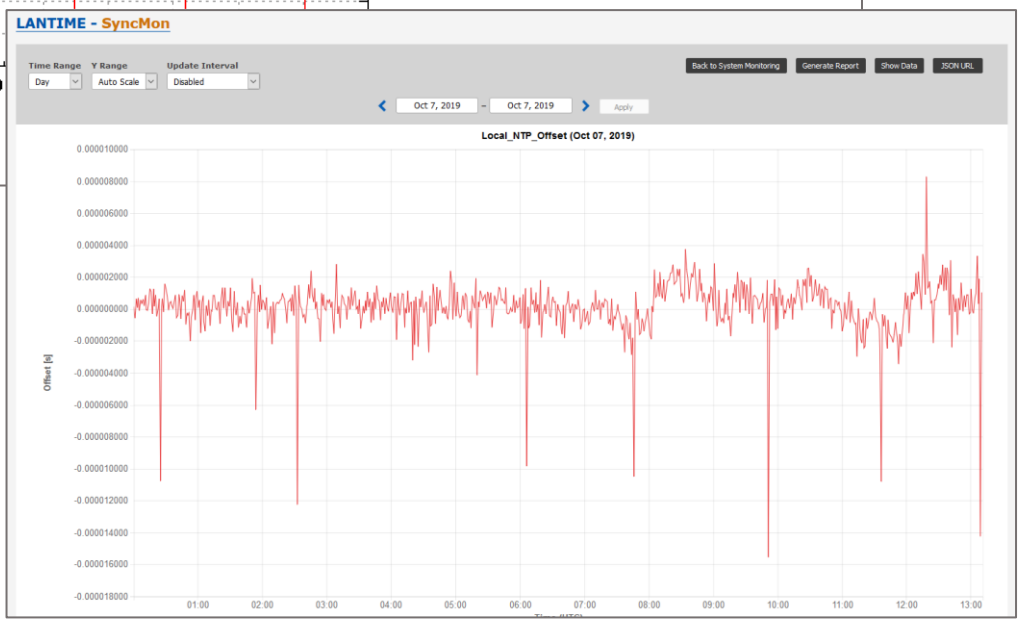


Figure 4: SyncMon in V7

4.3.4. Newly supported

- Monitoring HPS cards as PTP-slave on all slots (including IO slots). It is now possible to monitor up to 10 PTP networks also with different PTP profiles configured
- Group nodes to get a better arranged overview
- Select one of multiple USB storages
- NTP with IPv6 on HPS100
- New CPU with dual core, 2GB RAM, 4GB flash and 2xGBit Ethernet (Copper and SFP)

4.4. LANTIME Command Line Interface (lt_cli)

The V7 command line interface offers a completely new management option for LANTIME products. The new functionalities of this interface allow to automate processes and configurations by using small scripts. In addition, the JSON structure of the configuration parameters and status information to easily integrate the LANTIME to own web pages or management systems.

5. Known Bugs and Limitations

There are no known bugs in this release. Please report any bugs to your Meinberg technical support team (techsupport@meinberg.de).

6. Download LANTIME Firmware V7

To reach our download page go to:

English https://www.meinbergglobal.com/english/sw/firmware.htm

German https://www.meinberg.de/german/sw/firmware.htm

By entering the serial number of your device and your e-mail address, as well as accepting the data protection declaration, you can enter the download area of the selected firmware here and get information about the specifications of the current Meinberg LANTIME firmware.

Please Note:

A few devices show a message, that they will not support the update to V7 firmware during an update attempt. If this error message appears or you face any other problems, do not hesitate to contact your Meinberg support service.

Meinberg Support Services

To reach our support page go to:

English https://www.meinbergglobal.com/english/support/tech-support.htm

German https://www.meinberg.de/german/support/tech-support.htm

7. Acknowledgment

We want to thank everyone who has helped us to improve the security of our LANTIME-Firmware. Each reported and fixed vulnerability is a benefit for all of us. Thank you very much!