MEINBERG
The Synchronization Experts.

Release Notes

LANTIME OS Firmware Version 7.06

and

LANTIME OS Firmware Version 7.06 light

English

Meinberg Funkuhren GmbH & Co. KG

Lange Wand 9, 31812 Bad Pyrmont, Germany

Telefon: + 49 (0) 52 81 / 93 09 – 0

Fax: + 49 (0) 52 81 / 93 09 - 230

Internet: https://www.meinbergglobal.com

Mail: info@meinberg.de

Date: July 25, 2022

1. Foreword

This document describes the changes & features of the new **LANTIME OS (LTOS) Firmware v7.06.004**. Please read these Release Notes carefully before installing the v7.06 firmware.

All Meinberg LANTIME servers (M series, SyncFire, IMS) shipped as of July 25, 2022 will include the new v7.06 firmware pre-installed. This firmware revision provides many new features and improvements for the LANTIME range of systems and their management tools. These include a variety of security-related improvements.

2. Software Versions

The LTOS Firmware v7.06.004 comprises several software components, some of which are provided by third parties. The most important third-party software packages included in LTOS v7.06.004 are listed below alongside their version numbers.

Linux	Linux kernel 4.14.281
SSL/TLS	OpenSSL 1.1.1q
SSH	OpenSSH 9.0p1
LDAP	OpenLDAP 2.4.58
NTP	NTP 4.2.8p15
NTS Client	Chrony 4.2
NTS TLS libraries	GnuTLS 3.7.2, Nettle 3.7.3, GMP 6.2.1

Table 1

3. Requirements

System Requirements: Standard-Version

The following requirements must be met in order to be able to install LANTIME OS Firmware v7.06.

Name of Firmware Revision	**LANTIME OS Firmware 7.06.004 Release Version**
Release Date	July 25, 2022
System Compatibility	
LANTIME Systems	M100
	M200
	M300
	M400
	M600
	M900
	SyncFire 1000
	SyncFire 1100
	SyncFire 1200
LANTIME IMS Systems	M500
	M1000
	M1000S
	M2000S
	M3000
	M3000S
	M4000
Modules	CPU-C05F1 [1]
	CPU-C15G2
	IMS Modules [2]
Installation Requirements	
CPU Module RAM:	Min. 256 MB
CPU Module Flash Memory:	Min. 512 MB

Table 2

[1] When using a CPU-C05F1 CPU module both the v6 and v7 LANTIME firmware branches will continue to be supported for 2022. However, due to the announced end-of-life of the v6 branch, users of LANTIME OS v6 are strongly recommended to migrate their systems to LANTIME Firmware v7 at their earliest convenience (or, for systems with 128 MB of RAM, to LANTIME Firmware "v7 light"). Please refer to the chapter "v7 light" for further information.

[2] Systems with LANTIME Firmware v7.06 installed support all current IMS clocks and I/O modules.

System Requirements: Light Version

To use the LANTIME OS Firmware “v7.06 light” the following requirements must be met. Please refer to the chapter “v7 light” for further information on the functional differences of the “light” version.

Name of Firmware Revision:	**LANTIME OS Firmware 7.06.004 “light” Release Version**
Release Date:	July 25, 2022
System Compatibility	
LANTIME Systems:	M100
	M200
	M300
	M400
	M600
	M900
LANTIME IMS Systems:	M500
	M1000
	M1000S
	M2000S
	M3000
	M3000S
	M4000
Modules:	CPU-C05F1 [1]
	CPU-C15G2
	IMS Modules [2]
Installation Requirements	
CPU Module RAM:	Min. 128 MB
CPU Module Flash Memory:	Min. 512 MB

Table 3

[1] When using a CPU-C05F1 CPU module both the v6 and v7 LANTIME firmware branches will continue to be supported for 2022. However, due to the announced end-of-life of the v6 branch, users of LANTIME OS v6 are strongly recommended to migrate their systems to LANTIME Firmware v7 at their earliest convenience (or, for systems with 128 MB of RAM, to LANTIME Firmware “v7 light”). Please refer to the chapter “v7 light“ for further information.

[2] Systems with LANTIME Firmware v7.06 installed support all current IMS clocks and I/O modules.

Connection Requirements

Cipher List

To be able to establish an **SSL/TLS connection** once your device is updated, your browser must support at least one of the listed cipher suites.

Web Server	
TLS Cipher Suites:	ECDHE-ECDSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-GCM-SHA256
	ECDHE-ECDSA-AES256-GCM-SHA384
	ECDHE-RSA-AES256-GCM-SHA384
	ECDHE-ECDSA-CHACHA20-POLY1305
	ECDHE-RSA-CHACHA20-POLY1305
	DHE-RSA-AES128-GCM-SHA256
	DHE-RSA-AES256-GCM-SHA384

Table 4

To be able to establish an **SSH connection** once your device is updated, your SSH client must support at least one of each of the cryptographic algorithms listed below (i.e., SSH cipher, key exchange algorithm, host key algorithm, message authentication code).

SSH	
Ciphers:	chacha20-poly1305@openssh.com
	aes256-gcm@openssh.com
	aes128-gcm@openssh.com
	aes256-ctr
	aes192-ctr
	aes128-ctr
Key Exchange Algorithms:	curve25519-sha256@libssh.org
	ecdh-sha2-nistp521
	ecdh-sha2-nistp384
	ecdh-sha2-nistp256
	diffie-hellman-group-exchange-sha256
Host Key Algorithms:	rsa-sha2-512
	rsa-sha2-256
	ecdsa-sha2-nistp521
	ssh-ed25519
MACs:	hmac-sha2-512-etm@openssh.com
	hmac-sha2-256-etm@openssh.com
	umac-128-etm@openssh.com
	hmac-sha2-512
	hmac-sha2-256
	umac-128@openssh.com

Table 5

4. New Features

syslog TLS Encryption *[mbgID 1303]*

As of v7.06, support has been added for external logging using *syslog* over an encrypted TLS connection to ensure that data is sent securely. This feature actively mitigates the risk of a would-be attacker 'eavesdropping' on or tampering with potentially sensitive data.

syslog Timezones *[mbgID 2640]*

It is now possible to specify the timezone in which *syslog* messages are sent to external servers. This allows local time information from logs to be displayed or processed, even if the external monitoring system does not support conversion from UTC to local time.

Display Carrier-to-Noise Ratio of Satellite Signals for GPS180 / GPS181 / GPS182 *[mbgID 1829]*

In the SyncMon section of the LANTIME OS WebUI, the signal quality is now also displayed for the GPS180, GPS181, and GPS182 receivers as the carrier-to-noise ratio of the received signal in dBHz, provided that the module is equipped with firmware V2.60.

Added Detection for Latest BPE8xxx Variants *[mbgID 11259]*

The latest BPE modules, including the BPE-80xx series, are now detected and supported as of LTOS v7.06.

Introduced *changes* Command in RESTful API to Show Pending Changes *[mbgID 10115]*

The global *lt_cli* command *changes*, which would allow unconfirmed, buffered changes to be displayed for review before being 'committed' or 'rolled back' is now also implemented in the RESTful API.

Include FDM Sync Status in Notifications *[mbgID 9806]*

FDM modules will now use the "**St**" status LED to signal not only frequency and time deviations but also sync status:

- "**St**" LED *green* FDM synchronized (PPS and 10 MHz are available)
- "**St**" LED *red* FDM not synchronized (PPS and 10 MHz reference signals disrupted)

"**FDM Error**" events are logged in the notifications and error messages are displayed in the "**Error**" field (see Figure 1).

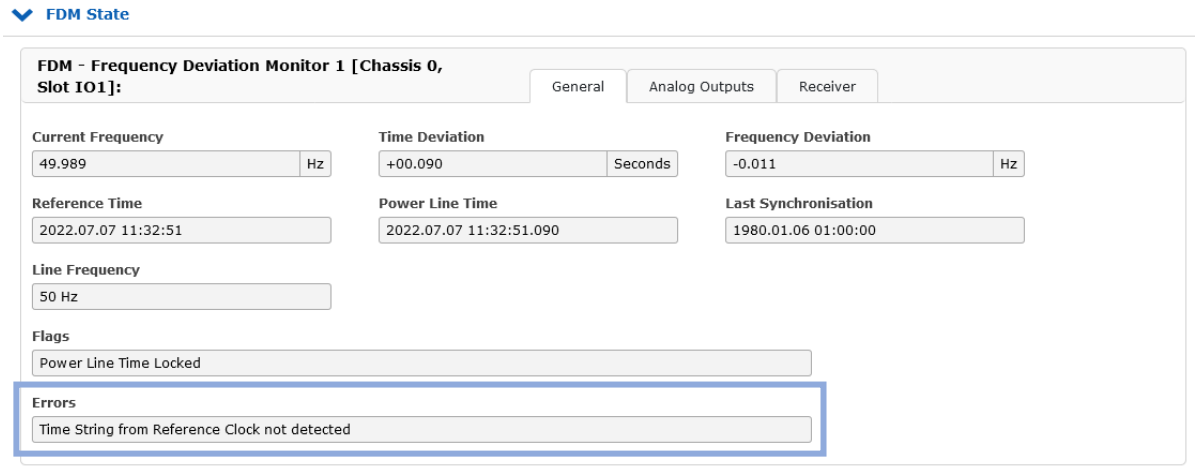

Figure 1

To use this feature, the FDM module must be equipped with FW Version 1.36 or newer.

Added Support for XHE Chassis in lt_cli and RESTful API *[mbgID 9718]*

Status information about a connected XHE chassis can now be accessed via both *lt_cli* and the RESTful API via the following routes:

```
/status/chassis-xhe/clk1
/status/chassis-xhe/clk2
```

Added Support for VSG Modules in *lt_cli* and RESTful API *[mbgID 6131 u. 6130]*

As of LTOS v7.06 the VSG180, VSG181, und VSG181H can be configured via *lt_cli* or the RESTful API.

Display Physical Location of Dedicated LAN Port of LNE Module via *lt_cli*, RESTful API, or WebUI *[mbgID 1328]*

A network port provided by an LNE module can now be physically located in *lt_cli* or via the RESTful API via the following route:

```
/status/network/ports
```

where "*slot-id*" shows the physical slot in which the network module is installed and "*port-id*" shows which physical port it relates to.

```
root:/ > view status/network/ports
ports
    lan0
        duplex                  "full [1]"
        operstate               "up [1]"
        speed                   "1000 [1000]"
        mac-address             ec:46:70:03:0e:df
        link                    "up [1]"
        slot-id                 7
        slot-name               cpu
        port-id                 0
        card-name               "ims-c15g2 [20004]"
    end #lan0
    lan1
        duplex                  "- [-1]"
        operstate               "down [0]"
        speed                   "- [0]"
        mac-address             ec:46:70:03:0e:e0
        link                    "down [0]"
        slot-id                 7
        slot-name               cpu
        port-id                 1
        card-name               "ims-c15g2 [20004]"
    end #lan1
```

Figure 2

The slot ID is also provided in the WebUI under "**Network → Physical Network Configuration**":

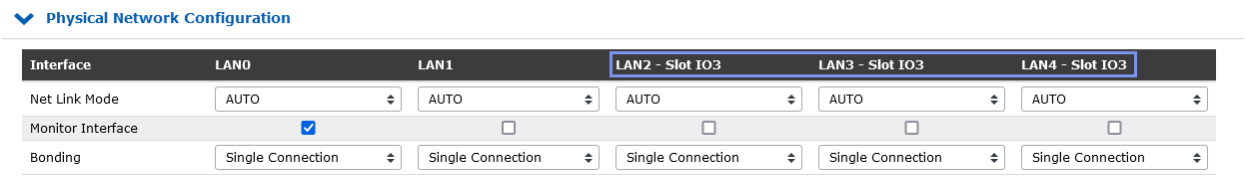

Figure 3

Support for Downloading SyncMon data via Web UI *[mbgID 1556]*

SyncMon data can now be downloaded as a ZIP file separately from the diagnostic file through the WebUI, for example if needed to send to Technical Support.

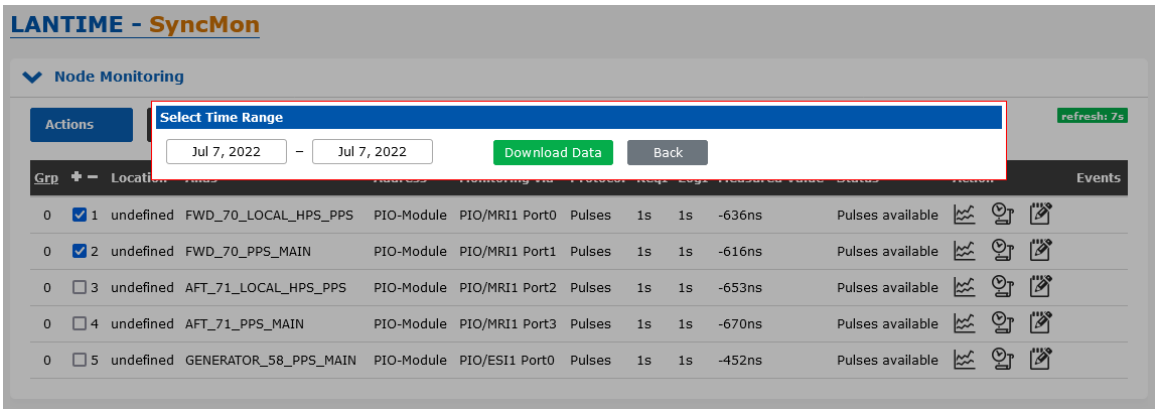

Figure 4

Procedure

1. First mark the nodes for which you wish to download the data.
2. Click on the "**Actions**" button, then select "**Download data files for selected nodes**".
3. Enter a time period for which the SyncMon data is to be downloaded.

The following prompt will appear:

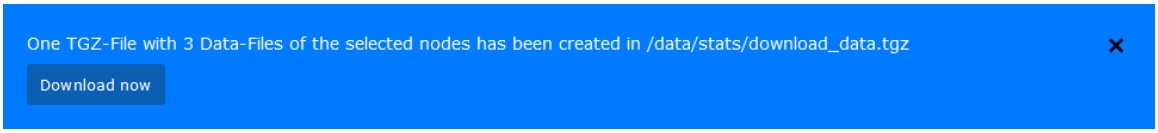

Figure 5

4. Click on **"Download now"** to launch the download.

IPv6 *syslog [mbgID 8115]*

An external *syslog* server can now also be configured via an IPv6 address. This can be entered in the address file. The system will automatically detect that it is an IPv6 address and modify the *syslog* configuration accordingly.

Brute Force Detection Using *faillock [mbgID 1825]*

Brute force attacks over SSH and the web interface can now be detected and prevented as of v7.06. By temporarily locking an account that is under attack, the time available for login attempts can be limited to such an extent that brute force attacks become essentially impossible. The number of failed login attempts and the time that an account is locked for can be configured. It is also possible to configure whether a notification is issued in the event of a user's account being locked.

NTP Key Autogenerator also Generates SHA-256/512 and AES-128-CMAC Keys *[mbgID 2569]*

The "**Auto-Generate Keys**" function now also generates AES-128-CMAC, SHA-256, and SHA-512 keys.

LDAP Connection Test *[mbgID 4539]*

To minimize problems with configuring LDAP, it is now possible to test a connection to an LDAP server. It is not necessary for all parameters to be set and correct in this case. The error codes of the LDAP client are also displayed in the Web Interface to enable fault diagnosis to be performed over the web.

LDAP Groups Lookup *[mbgID 5244]*

As of v7.06 *super*/*admin*/*info* groups can now be created in the directory service (e.g., Active Directory). Previously it was necessary to configure each user individually before they could be assigned to a group on the LANTIME. Group memberships in the directory service can now be represented in LANTIME OS' own group handling.

Improved Auditing (*saveconfig syslog*) *[mbgID 3336]*

Attempts to modify the start configuration using *saveconfig* are now additionally logged.

Link Status of Physical Interface Added *[mbgID 5678]*

The link status of the physical network interfaces has been added to the relevant page in the Web Interface. The status shows the negotiated speed for each interface. This enables the network connections to be easily monitored via the Web Interface.

Support for the RCG181 *[mbgID 6126]*

LANTIME OS v7.06 adds support for the RCG181, a generator for medium-wave carrier signals that outputs the generated signals through four BNC connectors.

Support for the GNS182 *[mbgID 10560]*

LANTIME OS v7.06 adds support for the GNS182, which is a 72-channel satellite receiver clock, like its predecessor, the GNS181.

Support for the FDM182 *[mbgID 11103]*

LANTIME OS v7.06 adds support for the FDM182, which is used to calculate power grid frequencies and monitor frequency deviations and drift in 50/60 Hz grids.

conntrack and *gc* Threshold Values Increased on SyncFire Systems *[mbgID 8080]*

To enable requests from an even larger number of different IP addresses on SyncFire systems, the values for the ARP and *conntrack* tables have been adjusted. The maximum number of entries is now 4,194,304.

TCR180 TFOM *[mbgID 8376]*

TFOM has been supported by the TCR180 since the Module Firmware Version 1.18. The IEEE1344 and C37.118 time codes specify a 4-bit extension for a “time figure of merit” (TFOM), a value that can be used to convey the anticipated accuracy of the reference system time to the receiving system.

SSM Value Selection in T1 Mode *[mbgID 6920]*

When outputting T1 signals from a LIU (Line Interface Unit), it is now possible to select between one of two modes, which dictate whether the reporting of the signal quality is divided into two or four quality levels.

Degradation Mode:	Simple (PRS or DNU)	Advanced (step-by-step degradation from PRS to DNU)
Quality Level:	1. PRS 2. DNU	1. PRC 2. Stratum 2 3. SMC 4. DNU
Explanation:	Only best and worst signal quality levels	Four signal quality levels

Table 6

Interface-Specific IPv6 Gateway *[mbgID 9607]*

As of LANTIME OS v7.06 it is now possible for interface-specific gateways to be configured when using IPv6 addressing.

NTS Client Support *[mbgID 10112]*

LANTIME OS v7.06 now supports Network Time Security in client mode on LANTIME devices with MRS support. NTS is a modern mechanism for cryptographically securing the NTP time protocol. NTS enables easy key distribution based on a PKI (Public Key Infrastructure). NTS can also be used to align the need for a high level of security and scalability with the natural and consistent demand to minimize loss of accuracy.

External NTS servers can therefore be configured as a trusted synchronization source on devices with MRS support. An extensive NTS server mode is planned for future releases.

SyncFire PTP syn1588PCI Card Support *[mbgID 6577]*

The Oregano PTP stack and drivers for the syn1588PCI card are now available on SyncFire systems as of LANTIME OS v7.06 to allow the *ntpd* service to be synchronized via PTP. The implementation at present requires configuration files to be edited manually. Support for configuration via the Web UI will follow in later versions.

Web Server Intermediate Certificates *[mbgID 9784]*

It is now possible to upload intermediate certificates that are part of certificate chains via the Web Interface. These certificates are recorded alongside the server certificate in a *pem* file and then uploaded.

Problems can arise on systems that already have intermediate certificates stored in a separate file. In this case the certificates will need to be moved manually from */etc/https_ca.pem* to */etc/https.pem* via the command line interface. When the web server is subsequently restarted with "*restart https*", the problem will be eliminated. Once you have verified that the web interface is functioning correctly, the change can be stored permanently in using "*saveconfig web*".

Programs Removed

The following programs are no longer present as of LTOS v7.06.

- Midnight Commander (*mc*, *mcedit*, *mcview*)
- *vim*
- *ar*
- *strings*
- *uuencode*, *uudecode*

v7 light

A scaled-back version of LTOS v7.06 referred to as **v7.06 light** will be available to download alongside the release of the full version of v7.06 itself. This version is intended for use with any older system with 128 MB RAM. The increasing demands placed by the software on the hardware mean that it is no longer possible to implement all functions and all security fixes in v6. This is why v7 light is being released for the older 128MB devices; while the feature set is reduced compared to the full version, it provides most of the security features of V7 and shares a common development basis with the full v7 OS.

The following functions are not available in v7 light:

- SyncMon
- NTS
- Bird

Discontinuation of LANTIME OS Version 6

Please refer to the link http://www.mbg.link/eol-ltos6_en for the official end-of-life announcement in relation to LANTIME OS Version 6.

5. Known Bugs & Issues

There are no known bugs in this version. Please report any bugs you may find to Meinberg Technical Support (techsupport@meinberg.de).

Compatibility with Meinberg Network Management System (mbgNMS)

Please note when scheduling an update for your LANTIME systems to LTOS v7.06 that this version is not compatible with mbgNMS v1.1.0 or lower due to incompatibilities with the RESTful API that mbgNMS utilizes as an interface. Support for the RESTful API v10.x that LTOS v7.06 provides will be introduced in mbgNMS v1.2.0.

LANTIME users are strongly encouraged to promptly update their time servers to minimize security risks as quickly as possible. However, if you are running mbgNMS v1.1.0 and do not wish to temporarily forego access to the service, you can temporarily postpone the update to LTOS v7.06 and continue to use v7.04 for the time being.

If you choose to postpone the LTOS update for this reason, please perform the update to v7.06 as soon as possible at such a time when mbgNMS v1.2.0 releases.

6. Download LTOS Version 7.06

Our download page is located at the following address:

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

You can access the download section by entering your system's serial number and your email address and accepting the Privacy Policy. The download section provides information about the most recent LTOS Firmware as well as a link to download it.

Meinberg Technical Support Page

Our support page is located at the following address:

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

7. Acknowledgments

Our thanks go to all those who have contributed to helping us improve the functionality and security of our LTOS Firmware. Each and every security issue that is reported and fixed is a benefit for everyone. So, thank you!