LOGmanager release notes version 2.6.2

Version:	2.6.2	**Date:**	15.01 2018

1 Content

2 Introduction

This document describes the following summary of enhancements, support information, installation instructions, list of bug fixes, and description of new features.

2.1.1 Supported models

2.1.2 Version 2.5.1, 2.6.1, 2.6.2

The following models are supported:

- LM-36 - 2U HP gen8 server with 12x 3TB HDD, 64GB RAM, 2x6core CPU
- LM-36B - 2U HP gen9 server with 12x 3TB HDD, 64GB RAM, 2x8core CPU
- LM-12B - 1U HP gen9 server with 4x 3TB HDD, 64GB RAM, 1x8core CPU
- LM-DEMO1 - Intel NUC, 480GB SSD, 16GB RAM, 1x2core CPU
- LOGM-48TB-D – 2U Dell R730xd with 12x 4TB HDD, 64GB RAM, 2x10core CPU
- LOGM-16TB-D – 1U Dell R430 with 4x 4TB HDD, 64GB RAM, 1x10core CPU
- LOGM-16TB-H – 1U HP gen9 with 4x 4TB HDD, 64GB RAM, 1x10core CPU
- LOGM-48TB-D – 2U HP gen9 server with 12x 4TB HDD, 64GB RAM, 2x10core CPU
- LOGM-120TB- D – 2U HP gen9 server with 12x 10TB HDD, 128GB RAM, 2x14core CPU
- LOGM-120TB-H – 2U HP gen9 server with 12x 10TB HDD, 128GB RAM, 2x14core CPU

2.1.3 Version 2.3.0, 2.4.0

The following models are supported:

- LM-36 - 2U HP gen8 server with 12x 3TB HDD, 64GB RAM, 2x6core CPU
- LM-36B - 2U HP gen9 server with 12x 3TB HDD, 64GB RAM, 2x8core CPU
- LM-12B - 1U HP gen9 server with 4x 3TB HDD, 64GB RAM, 1x8core CPU
- LM-DEMO1 - Intel NUC, 480GB SSD, 16GB RAM, 1x2core CPU
- LOGM-48TB-D – 2U Dell R730xd with 12x 4TB HDD, 64GB RAM, 2x10core CPU
- LOGM-16TB-D – 1U Dell R430 with 4x 4TB HDD, 64GB RAM, 1x10core CPU
- LOGM-16TB-H – 1U HP gen9 with 4x 4TB HDD, 64GB RAM, 1x10core CPU

2.1.4 Version 2.0.0, 2.1.0, 2.2.0

The following models are supported:

- LM-36 - 2U HP gen8 server with 12x 3TB HDD, 64GB RAM, 2x6core CPU
- LM-36B - 2U HP gen9 server with 12x 3TB HDD, 64GB RAM, 2x8core CPU
- LM-12B - 1U HP gen9 server with 4x 3TB HDD, 64GB RAM, 1x8core CPU
- LM-DEMO1 - Intel NUC, 480GB SSD, 16GB RAM, 1x2core CPU
- LOGM-48TB-D – 2U Dell R730xd with 12x 4TB HDD, 64GB RAM, 2x10core CPU
- LOGM-16TB-D – 1U Dell R430 with 4x 4TB HDD, 64GB RAM, 1x10core CPU

3 Release Notes

3.1.1 Version 2.6.2 - 15 Jan 2018

Fix added for 2 minor issues. No new features or parsers in this version.

3.1.2 Version 2.6.1 - 16 Dec 2017

Completely redesigned parsing engine, reduced memory demands and increased parser performance. Added support for forwarding to multiple external syslog servers and filtering forwarded messages.
Default Field describing alerted events "msg.alert@name" had been changed to "meta.alert".

3.1.3 Version 2.5.1 - 15 Sep 2017

Updating your operating system kernel and platform. Optimize system configuration. The system will only download updates from the server: up.logmanager.com, if you have rules limiting the LOGmanager communication on the firewall, please check that up.logmanager.com is enabled. Considerably redesigned parsers for CEF, LEEF and fortigate, see notes below.
The new system version requires updating of the components (SQL, VMWARE, CHECKPOINT), the update will be done automatically within ten minutes after the system is booted into the new version. The system must have access to the update server for this time.

3.1.4 Version 2.4.0 - 21 Apr 2017

Repair of serious memory leak, repair of internal monitoring system.
We recommend updating this version as soon as possible.

3.1.5 Version 2.3.0 - 31 Jan 2017

Small repairs, new parsers.
Improvement of the parser engine, increase performance.

3.1.6 Version 2.2.0 - 17 Jan 2017

Added support for forwarding parsed JSON messages to an external syslog server.
Small repairs, new parsers.

3.1.7 Version 2.1.0 - 23 Nov 2016

Restored support for database authorization management.
Added support for LOGmanager forwarders.

3.1.8 Version 2.0.1 - 7 Oct 2016

Small repairs, new parsers.

3.1.9 Version 2.0.0 - 14 Sep 2016

Most of the system has been overwritten. The main novelties include a new parsing engine that is fully customizable. It is user-friendly to create and modify parsers for different event sources.
Because of the ability to define custom parsers, the format of the saved data has been completely changed.
Autodetection of the type of received messages has been disabled, it is necessary to define the individual source device / subnets / message content in so-called classifiers. For common data sources used, a configuration is pre-configured in the system, to which it is sufficient to add IP subnets.
Warning: This option temporarily deletes the option to define access rights to the database, user permissions will be completely redesigned in version 2.1x

4 New Functions

4.1.1 Version 2.6.1

- Added support for forwarding events to multiple external syslog servers.
- Alerts let you define an action to forward a message to an external syslog server (filtering events to be forwarded to an external syslog server).
- Default Field describing alerted events. Field "msg.alert@name" had been changed to "meta.alert". Since version 2.6.1, all logs hit by one or more alerts will contain populated field "meta.alert" with alert names hitting.
- Redesigned parsing engine, 60% less memory usage, message parsing is about 20% faster (it's not a performance boost for the entire device).
    - New parser tests return to the internal states of error messages (attempts to set non-existent variables, etc.).
    - When using regular expressions, the new parsing engine automatically generates all the field names that were entered (in the original implementation, field names were not created if the value was empty).
- Reports - The LOGmanager header is newly added to the PDF with report name and report description.
- SQL Component newly logs successful connect to database events.

4.1.2 Version 2.5.1

- Added support for receiving events through syslog protocol on ports 51000 to 51100, TCP & UDP. Newly it is possible to make classification, followed by events parsing depending on the information on which port the event arrived.
- Redesigned component for reading data from SQL database:
    - Added support for reading data from PostgreSQL,
    - Added support for SQL database names. Added support for SQL tables, which contain special symbols (dots, Czech symbols, gaps, etc.),
    - Improved error messages.
- New version of VMWare's component:
    - VMWare updates SDK plus optimization,
    - Improved error messages.
- New version of Check Points's component:
    - Updates Check Point OPSEC SDK plus optimization,
    - Added support for connection through OPSEC protocol to Check Point version R80.x,
    - Improved error messages.
- Added support for XL Version LM.
- Kernel and operating system platform updates.
- Modifying the web query compression configuration.
- Optimization of RAID controller configuration.
- The Alerts / Parsers / Classification conditions newly takes into account **blockly** and accordingly create parentheses. Blocks were originally evaluated without brackets. Newly the brackets are automatically added according to the block connections. Example: if False and (False or True), originally written as if False and False or True.
- Newly Parsers are more resistant to Regular Expressions Catastrophic Backtracking (see http://www.regular-expressions.info/catastrophic.html).
- Newly the embedded dashboards searches for the last 12 hours (originally set to 24 hours).

4.1.3 Version 2.4.0

- Database groups are now encouraging to create rules with negation.

- Added support for backing up LM server configuration.
- Added support for reading SQL resources from the Oracle database.
- Added support for the upcoming version of Windows Agent 3.x.
- The internal disk queues of events waiting for processing are newly saved in compressed form.
  Warning: When the incoming events disk queue size increases to more than 10GB, newly an email notification to the system administrator is sent. When disk queues are used, the insertion speed of new events into the database is significantly slowed, and part of the disk subsystem performance is used to work with the event queue. At the moment the event queue exceeds the 50GB threshold, LM will automatically reject the received events.
    - In normal traffic incoming events don't use the disk queues. The disk queue is only used when a significantly higher volume of incoming events is sent to LM than the real-time system can process and store in the database.

4.1.4 Version 2.3.0

- An updated list of MAC address manufacturers.
- Added support for using schema when reading from Microsoft SQL database.
- Classifiers are newly sorted by alphabetical order for receiving messages. Once the message does not end in the classifier, it passes through the next classifier, which is in alphabetical order.
  This requires a minor explanation: *If you have multiple classifiers for the same data source (for example, Syslog or Windows), and in the first classifier (by alphabetical order) the event does not arrive to the exit rule "Pass to Parser", the system does not drop the event. It continues to process the event in the next classifier (by alphabet) for the given data source. If you do not create classifiers yourself, but just modify existing classifiers, this feature is not interesting to you.*
- Minor optimization of the parser engine - 50-100% increasing of parsing performance by type of report processed. Note - this is not about database performance increasing or increasing of total events per sec.

4.1.5 Version 2.2.0

- Added support for forwarding events to the parent syslog server.
- Added support for receiving and parsing events in LEEF format.
- Added button to test the connection to the update server (System > Software).
- Enhanced webserver configuration:
    - Only TLSv1.2 connection encryption is enabled.
    - Added HSTS security headers.
- Dashboards:
    - Fields for field names are enlarged.
    - Enhanced dashboard for viewing manipulation with Windows files, alerting, postfix / sendmail, and Windows Logons.
- Blockly - the zoom function on the mouse wheel was turned off.

4.1.6 Version 2.1.0

- Database permissions:
    - Added support for group definitions restricting access to the database. Access is tagged.
- Added support for LOGmanager forwarder.
- Reworked the internal queue system:
    - Split the queues into two levels (raw upon receipt and before saving the event to the database).
    - The memory is primarily used for the queue. At a heavy load, the system will automatically postpone events to temporary files on the hard drive and process them when the load decreases.

4.1.7 Version 2.0.0

- Own parsers:
    - It is necessary to define rules for classification of data and their subsequent parsing (classifier).
    - Classifiers let you use, for example, the IP prefix sheets, part of the hostname, etc. for easier configuration of the whole system.
    - Parsers can be customized to define their behavior.
    - The parser definition allows you to paste test events that are parsed live according to the current parser definition.
    - Parsers allow you to cast data to an IP address (automatic GEO IP, DNS PTR, etc.) to MAC address (automatic reformatting and adding MAC address manufacturer information), INT and FLOAT (number casting).
- Changed structure of saved data:
    - Added meta information.
    - Area msg - contains a user-defined field (scattered data).
    - Area raw - contains the original message in its unaltered form.
    - Raw_offset – contains information where raw data begins with parser data.
- Modified individual components to work with a new data format:
    - Checkpoint
    - VMware
    - SQL
    - SAP
- Edit GUI for better clarity and control:
    - The UID of the edited record has been added to the display URL.
    - After clicking Save, pages do not return to the report, but the view remains on the edited record.
    - Added ability to save a copy of the edited object (Parsers, Classifiers, IP prefixes, etc.).
    - Colorful highlighting of rows after hovering the mouse.
- New Version alert system, alerts newly allow a very detailed definition of rules for sending an alert.
- Support for lookup tables in parsers and alerts.
- Added support for defining the proxy server for downloading system updates.
- Added support for uploading and managing your own SSL certificates.
- JavaScript optimization, significantly faster GUI response.
- Added support for encrypted messaging from Windows agents (you need to create a second SRM log _logmanager-ssl in DNS! Detailed instructions are in the documentation).
- The Windows agent enables you to enable validation of the LM server certificate validity.
- Modify the minimum password for local users to 10 characters.

5 New parsers:

5.1.1 Version 2.6.1

- New parsers:
  - Samba audit log
- Updated Parsers:
  - CEF
    - Parser did not allow parsing messages that contained a dollar sign.
  - Kaspersky
  - Aruba – added support for instant AP
  - HP Comware
  - Kerio connect
  - Sophos
  - Ironport
  - Trapeeze
  - Freeradius
  - Postfix
  - Apache JSON

5.1.2 Version 2.5.1

- New parsers:
  - Amavis
  - Exchange mail log
  - Synology NAS DSM
- Updated Parsers:
  - CEF
    - Parsers are newly translating field names as recommended by LM (cf. https://doc.logmanager.cz/manual/lm/cs/standardized-variable-names.html) Existing custom parsers must be adjusted to the new behavior of the parsing engine.
  - LEEF
    - Parsers are newly translating field names as recommended by LM (cf. https://doc.logmanager.cz/manual/lm/cs/standardized-variable-names.html) Existing custom parsers must be adjusted to the new behavior of the parsing engine.
  - FortiGate
    - Parser has been completely redesigned, duplicate fields are not included in the parsing: dstcountry, srccountry, level, date, time. All of these fields are already stored in meta information.
  - Cisco ASA
  - Trapeze
  - Checkpoint
  - OpenSSH
  - Windows file access
  - HP ProCurve
  - HP Comware
  - Kerio connect
  - Cisco IOS

5.1.3 Version 2.4.0

- In this version, the old version of the parser was completely deleted, all parsers have been redesigned to a new format.
- List of old parsers updated to new format:
    - Trapeze
    - Kernun
    - Gama-web
    - E-Directory
    - AV Eset
    - Avast
    - MySQL
    - MicrosoftSQL
- New parsers:
    - JSON – a simple JSON parser that performs the standardization of commonly used fields.
    - Iron Port
    - Extreme networks
- Updated parsers:
    - Juniper
    - ISC DHCP server
    - Kerio connect
    - Checkpoint
    - Flowmon
    - SQL
    - SonicOS

5.1.4 Version 2.3.0

- Modify the built-in Syslog rating template - split into three linked templates for better clarity.
- These classification templates are sorted in the following order:
    1) Syslog-template-IP
    2) Syslog-template-program_name
    3) Syslog-template-guessing

- New parsers:
    - Discard – Special parser for discarding the events.
- Reworked parsers:
    - Apache Tomcat
    - Cisco ASA

5.1.5 Version 2.2.0

- New parsers:
    - Dell iDrac
    - LOGmanager - internal events
    - Mikrotik
    - Cisco FirePOWER
    - Palo Alto NGFW
    - Windows file access log
- Reworked parsers with standardized box names:
    - SAP
    - Kaspersky antivirus
    - FortiAuthenticator

- Brocade SAN
- MS SharePoint
- Force 10
- ISC DHCP server
- ISC Bind DNS server
- Postfix
- Windows firewall

5.1.6 Version 2.1.0

- Reworked parsers with standardized box names:
  - Kerio Connect
  - MySQL Windows/Linux audit log
  - UBNT rocket
  - UBNT Unifi
  - Dropbear SSH server
  - SonicOS
  - Flowmon CEF
  - CEF

5.1.7 Version 2.0.1

- Reworked parsers with standardized box names:
  - Cisco SMB
  - Cisco WLC
  - FortiDDoS
  - Kerio Control
  - HP ProCurve

5.1.8 Version 2.0.0

- Reworked parsers with standardized box names:
  - Aruba
  - Fortimail
  - Freeradius
  - JuniperSRX
  - Dell PowerConnect
  - SpamAssasin
  - Apache log JSON format / Apache log
  - Microsoft IIS
  - Nginx
  - Checkpoint
  - FortiGate
  - Kerio control
  - OpenSSH
  - Microsoft DHCP
  - Shorewall
  - Sophos
  - VMware

6 Corrected errors

6.1.1 Version 2.6.2

- Export to CSV failed if contain fields meta.field1@field2 or msg.field1@field2 with empty content.
- Under certain conditions, testing of alert with log source from WES did not provide correct test result.

6.1.2 Version 2.6.1

- An IPv6 address could not be entered into the IP address processing block.
- Fixed a Reports Generation Error - if the report name contained a space, the report was not sent.
- Repaired database crash on demo device (P/N: LM-DEMO1) which occurred due to lack of system memory.
- In particular cases LM System sent emails to non-existent domain **platform.sirwisa.cz**. Emails contained information that LOGmanager's hostname translation failed. This has been corrected and check was made that LM send all variants of operating and error states only to the internal syslog. (The LM system does not sent any information about its data or operation status to external systems.).
- SQL Component now correctly log DB hostname and IP address.

6.1.3 Version 2.5.1

- Repaired export of a large number of events. Data is newly exported in .CSV/GZIP format. Export has a newly implemented limit to the maximum number of exported messages = maximum of 100 million messages in one export.
- Repaired sorting of generated reports.
- Repaired internal NTP server status monitoring, new alerts will come only when all NTP servers are unfunctional.

6.1.4 Version 2.4.0

- **Correction of system bugs sending, added event queue size alert for events awaiting processing**
- Parsers:
    - Repaired memory leak that occurred during processing a large number of large messages (More than 80kB / message)
    - Repaired block Create text.
    - Repaired block if in, while using Windows.
    - Repaired block get last from list.
    - Repaired lookup tables using Czech characters.
    - Updated integrated regex for detection of IPv4 / IPv6 addresses.
    - Repaired block delete from variable message data.
- Repaired memory leak in RELP protocol. With a large number of large messages, the process for RELP events reception began to consume system memory.
- Repaired a typing error in the subject of the reports sent.
- Repaired deletion of unused Windows filters.

6.1.5 Version 2.3.0

- Some Windows systems do not support connection on TLS 1.2.
    - Editing the webserver configuration, the TLSv1.0, TLSv1.1, and TLSv1.2 ciphers are now enabled.
- Database groups – it was not possible to select Forwarder name for limitation access to data.

6.1.6 Version 2.2.0

- Repaired report sending.
- Repaired error mark for successful installation of new Version.
- Repaired button TEST at LDAP groups.

- Repaired clustering error – in some cases it was not possible to create new cluster.
- Repaired dashboards – it was not possible to add new rows.
- Repaired dashboards, it was not possible to save a dashboard with the same name in multiple database groups (when creating a report, the name of the database group to which the report will be generated is newly visible).
- User with limited rights had possibility to change his rights.
- Repaired error in JS at classificators (in case of using block "Contain text" it was not possible to go back from XML editing to block configuration).
- Changed limit for deletion of old data - if less than 35GB of disk space is available, deletes the oldest saved day data.

6.1.7 Version 2.1.0

- Repaired RELP Classifier. Messages sent to the LM server using RELP or RELP-SSL was not possible to send to any parser. All messages sent using syslog, RELP or RELP-SSL are newly referred to syslog. Additionally, to the message was added flag with information about the protocol that accepted it (meta.src.dialect).
- Repairs of the parsing engine - works with lists did not work correct.
- Mapping correction for field "meta.tags".

- Parser:
    - HP Aruba – parsing for messages from Wireless IPS. Newly parser does not create values that have a zero value.

6.1.8 Version 2.0.1

- Fixed bug in DNS PTR configuration. PTR for private IP subnets was not done.
- Fixed bug in GUI (CheckPoint and VMWare configuration) - it was not able to add tags.
- Fixed bug in syslog offset at Cisco appliance.
- Repaired Cisco appliance name detection (hostname).
- Dashboards repairs, global dashboard for traffic log was added.

Parsers - repairing and adding other messages types for parsing:

- Cisco IOS
- Cisco ASA
- Microsoft Windows
- HP Comware

6.1.9 Version 2.0.0

- Appearance of the reports was fixed. The results of the report are already located in the right place.

7 Known bugs

7.1.1 Version 2.6.2, 2.6.1, 2.5.1, 2.4.0, 2.3.0, 2.2.0

- Problem:
  - Editing database permissions sometimes does not load blocks. Appears primarily in Chrome.
- Workaround:
  - Reload the page.

- Problem:
  - Editing database permissions sometimes does not show translated tags name.
- Workaround:
  - Switch to xml view and back, tags will appear correctly.

7.1.2 Version 2.4.0, 2.3.0, 2.2.0

- Problem:
  - When installing a new Version of LOGmanager, the system may display a blue information field with text Error. However, installing the new LOGmanager Version will be successful.
- Workaround:
  - Repaired in version 2.5.1
  - Ignore a badly defined error message.

8 Security Advisory

8.1.1 LOGmanager and Meltdown/Spectre vulnerability - 15th of January 2018

3rd of January 2018 group of security researchers publish under Google's Project Zero description of possible vector attacks against features of modern CPU architecture. Those can lead to leak of information via virtual memory read vulnerabilities. More description of those vulnerabilities can be found on Project Zero webpage link: https://googleprojectzero.blogspot.cz/2018/01/reading-privileged-memory-with-side.html or under those CVE's: CVE-2017-5753; CVE-2017-5715 and CVE-2017-5754.

Developers from Sirwisa a.s. (vendor of LOGmanager) conduct deep analysis and impact assessment of those vulnerabilities on LOGmanager products. The outcome is that those vulnerabilities apply only on the products, where the untrusted code can execute on a given system.

LOGmanager does not allows execution of arbitrary code by an unauthorized or even authorized user. In order to exploit those vulnerabilities, an attacker would require that ability. (*Achieving code execution would require the presence of second, unrelated vulnerability, and it is likely that such a vulnerability would already allow compromise of the system without the need for further exploits.*)

Only place, where entering of untrusted code into LOGmanager is present are Dashboards and Blockly programming. Dashboard are properly sanitized against entering of untrusted tokens like JavaScript code. Blockly programs do not allow programming of timers, which is one of the pre-requisites to successfully launch the attack. Next to it, LOGmanager embedded database configuration does not permit user scripts.

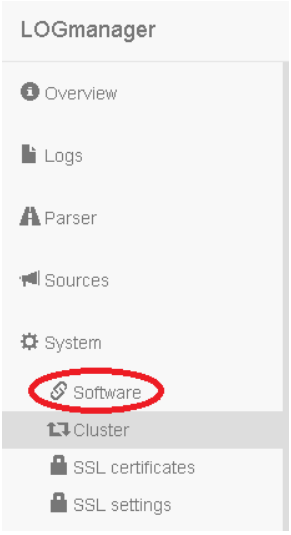
Therefore, LOGmanager is not vulnerable according to existing Meltdown/Spectre CVE's as of 15.01.2018.

However not being vulnerable, LOGmanager developers will add system patches to the LOGmanager components in next version of code consequently. According to our Security Software Development Life Cycle, we maintain our Security SDLC and vulnerability analytics of our products at high level all the time.

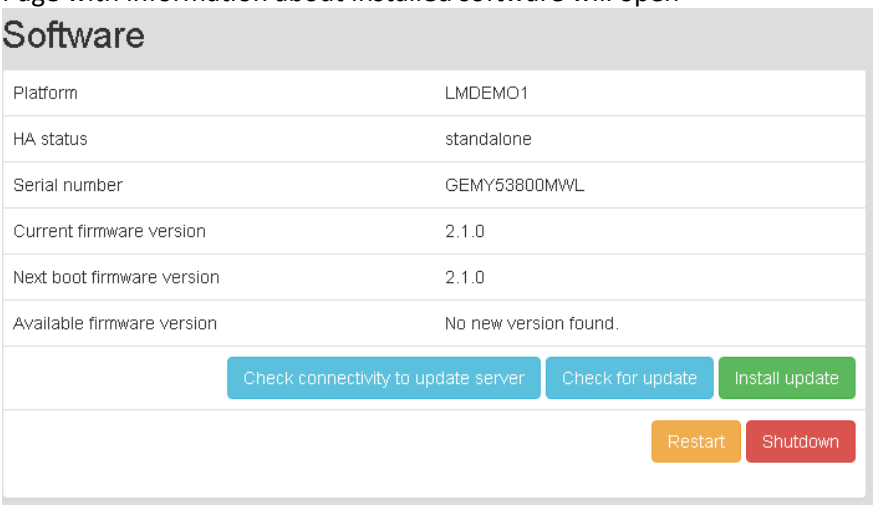
9 Update process

WARNING: Release 2.6.2 DOES NOT SUPPORT gradual cluster upgrades. You need to upgrade the cluster by installing a new SW on both boxes and restarting both cluster nodes at the same time.

For new version installation in WEB interface click on Settings > Software



Page with information about installed software will open



Upgrade process:

- Click the button “Check for update”.
- Available Version **2.6.2.** will be displayed
- Click the button “Install update”.
- Once the page is reloaded, in **next boot firmware** will be displayed **2.6.2.**
- In the last step, just click **Restart** and system will restart to the new Version.

9.1.1 After server restart

After restarting the server, it is necessary to delete the browser cache for the proper functioning of the web interface!

After each update, the database integrity check is performed. After the server restart, the status of the database is always in the red state and the check is performing, this is normal status after the upgrade - after the check is complete, the status returns to normal state.
No new data is stored in dB for the duration of the integrity check! However, the received events remain in the internal cache and are inserted into the dB as soon as the check is complete. The scan may take up to 30 minutes depending on the size and number of stored events.

End of document.