

# LOGmanager

- > Central Log Repository
- > Affordable SIEM



HELP TO RESOLVE  
CRITICAL IT INCIDENT

## LOGmanager release notes version 3.8.3 and 3.9.6

|                 |                 |              |               |
|-----------------|-----------------|--------------|---------------|
| <b>Version:</b> | 3.8.3 and 3.9.6 | <b>Date:</b> | June 24, 2022 |
|-----------------|-----------------|--------------|---------------|

**Restrictive conditions for publication:**

*This document is copyrighted and as such may not be copied or forwarded to a third person or legal entity without the prior consent of the author.*

**Notice:**

*All trademarks and product names listed in this material are or may be registered trademarks, trademarks or trademarks of their respective owners.*

---

[www.logmanager.cz](http://www.logmanager.cz)

**Sirwisa a.s.**

Zubatého 295/5, 150 00 Praha 5, IČ: 04667115, DIČ: CZ04667115

# 1 Content

|   |    |
|---|----|
| LOGmanager release notes version 3.8.3 and 3.9.6..... | 1  |
| 2 Introduction.....                                   | 3  |
| 2.1 Supported models.....                             | 3  |
| 2.1.1 Version 3.7.0, 3.8.2, 3.8.3.....                | 3  |
| 2.1.2 Versions 3.9.5 and 3.9.6.....                   | 3  |
| 3 New features overview.....                          | 4  |
| 3.1.1 Version 3.8.3 a 3.9.6.....                      | 4  |
| 3.1.2 Version 3.8.2 and 3.9.5.....                    | 4  |
| 3.1.3 Version 3.7.0.....                              | 4  |
| 3.1.4 Version 3.6.2.....                              | 4  |
| 3.1.5 Version 3.6.1.....                              | 4  |
| 3.1.6 Version 3.5.2.....                              | 5  |
| 3.1.7 Version 3.5.0.....                              | 5  |
| 3.1.8 Version 3.4.0.....                              | 5  |
| 4 New Functions.....                                  | 6  |
| 4.1.1 Version 3.8.3 a 3.9.6.....                      | 6  |
| 4.1.2 Version 3.8.2 and 3.9.5.....                    | 6  |
| 4.1.3 Version 3.7.0.....                              | 7  |
| 4.1.4 Version 3.6.2.....                              | 9  |
| 4.1.5 Version 3.6.1.....                              | 9  |
| 4.1.6 Version 3.5.0.....                              | 10 |
| 4.1.7 Version 3.4.0.....                              | 11 |
| 4.1.8 Version 3.3.0.....                              | 12 |
| 5 New parsers:.....                                   | 13 |
| 5.1.1 Version 3.8.3 a 3.9.6.....                      | 13 |
| 5.1.2 Version 3.8.2 and 3.9.5.....                    | 13 |
| 5.1.3 Version 3.7.0.....                              | 14 |
| 5.1.4 Version 3.6.2.....                              | 15 |
| 5.1.5 Version 3.6.1.....                              | 15 |
| 5.1.6 Version 3.5.0.....                              | 15 |
| 5.1.7 Version 3.4.0.....                              | 16 |
| 5.1.8 Version 3.3.0.....                              | 16 |
| 6 Corrected errors.....                               | 17 |
| 6.1.1 Version 3.8.3 a 3.9.6.....                      | 17 |
| 6.1.2 Version 3.8.2 and 3.9.5.....                    | 17 |
| 6.1.3 Version 3.7.0.....                              | 17 |
| 6.1.4 Version 3.6.2.....                              | 17 |
| 6.1.5 Version 3.6.1.....                              | 17 |
| 6.1.6 Version 3.5.2.....                              | 18 |
| 6.1.7 Version 3.5.0.....                              | 18 |
| 6.1.8 Version 3.4.0.....                              | 18 |
| 6.1.9 Version 3.3.0.....                              | 18 |
| 7 Known bugs.....                                     | 19 |
| 7.1.1 Version 3.8.3 a 3.9.6.....                      | 19 |
| 7.1.2 Versions 3.2.4 to 3.8.3 and 3.9.6.....          | 19 |
| 8 Update process.....                                 | 20 |
| 8.1.1 After server restart.....                       | 20 |

## 2 Introduction

This document describes the following summary of enhancements, support information, installation instructions, list of bug fixes, and description of new features for LOGmanager software version 3.X.X. If you need a detailed description of previous versions of 2.X.X and 1.X.X, see the LOGmanager documentation in the release notes menu or in the LOGmanager user forum here:

<https://forum.logmanager.com/viewforum.php?f=4>

### 2.1 Supported models

#### 2.1.1 Version 3.7.0, 3.8.2, 3.8.3

The following SKU models are supported:

- LM-36 (2U HP 380 gen8, 12x 3TB HDD, 64GB RAM, 2x6core CPU)
- LM-36B (2U HP 380 gen9, 12x 3TB HDD, 64GB RAM, 2x8core CPU)
- LM-12B (1U HP 360 gen9, 4x 3TB HDD, 64GB RAM, 1x8core CPU)
- LM-DEMO1 (Mini ITX Intel NUC, 1x 500GB SSD, 16GB RAM, 1x2core CPU)
- LM-DEMO-G2 (Mini ITX Intel NUC, 1x 500GB SSD, 32GB RAM, 1x2core CPU)
- LOGM-120TB-D (2U Dell R730xd, 12x 10TB HDD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-D (2U Dell R730xd, 12x 4TB HDD, 64GB RAM, 2x10core CPU)
- LOGM-16TB-D (1U Dell R430, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-H (2U HPE 380 gen9, 12x 10TB HDD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-H (2U HPE 380 gen9, 12x 4TB HDD, 64GB RAM, 2x10core CPU)
- LOGM-16TB-H (1U HPE 360 gen9, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-D-G2 (2U Dell R740xd, 12x 10TB HDD, 3.2TB SSD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-D-G2 (2U Dell R740xd, 12x 4TB HDD, 128GB RAM, 2x10core CPU)
- LOGM-16TB-D-G2 (1U Dell R440, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-120TB-H-G2 (2U HPE 380 gen10, 12x 10TB HDD, 3.2TB SSD, 128GB RAM, 2x14core CPU)
- LOGM-48TB-H-G2 (2U HPE 380 gen10, 12x 4TB HDD, 128GB RAM, 2x10core CPU)
- LOGM-16TB-H-G2 (1U HPE 360 gen10, 4x 4TB HDD, 64GB RAM, 1x10core CPU)
- LOGM-8TB-D (Tower Dell T140, 2x 4TB HDD, 32GB RAM, 1x2core CPU)
- LOGM-48TB-H-G3 (2U HPE 380 gen10, 12x 4TB HDD, 128GB RAM, 2x12core CPU)
- LOGM-16TB-H-G3 (1U HPE 360 gen10, 4x 4TB HDD, 64GB RAM, 1x12core CPU)
- LOGM-48TB-D-G3 (2U Dell R740xd, 12x 4TB HDD, 128GB RAM, 2x12core CPU)
- LOGM-16TB-D-G3 (1U Dell R440, 4x 4TB HDD, 64GB RAM, 1x12core CPU)
- LOGM-144TB-D-G3 (2U Dell R740xd, 12x 12TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-144TB-H-G3 (2U HPE 380 gen 10, 12x 12TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-192TB-D-G3 (2U Dell R740xd, 12x 16TB HDD, 128GB RAM, 2x16core CPU)

#### 2.1.2 Versions 3.9.5 and 3.9.6

- LMDEMO-G3 (Asus MiniPC, 1x 500GB SSD, 32GB RAM, 1x8core CPU)
- LOGM-16TB-D-G4 (1U Dell R6515, 4x 4TB HDD, 64GB RAM, 1x16core CPU)
- LOGM-48TB-D-G4 (2U Dell R7525, 12x 4TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-96TB-D-G4 (2U Dell R7525, 12x 8TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-144TB-D-G4 (2U Dell R7525, 12x 12TB HDD, 128GB RAM, 2x16core CPU)
- LOGM-192TB-D-G4 (2U Dell R7525, 12x 16TB HDD, 192GB RAM, 2x16core CPU)

## 3 New features overview

### 3.1.1 Version 3.8.3 a 3.9.6

This is service build and brings fixes and minor improvements. Upgrade from previous version is necessary. Contains fix for CVE-2022-24903 Rsyslog vulnerability.

### 3.1.2 Version 3.8.2 and 3.9.5

The main novelty of this version is a new system for collecting logs from the Windows environment via a new Beats agents built on open-source Elastic Beats (winlogbeat/filebeat). Increased performance, interoperability and stability while maintaining capabilities of previous LOGmanager WES agent.

Added support for source tracking. LOGmanager administrators can create source tracking rules which will notify via email when log source will not send any data in defined interval.

Replaced and improved internal task management system.

As announced previously with version 3.6.1 release notes, termination of the CheckPoint component using OPSEC protocol is applied in version 3.8.2 and 3.9.5.

Version 3.8.2 runs on the original version of the operating system.

Version 3.9.5 runs on the new version of the operating system with improved support for virtualization.

*Note: Both versions are identical from the user experience perspective. Only difference is that version 3.9.5 will be offered during the upgrade on new hardware platform as described in table 2.1.2 of this release notes. In next version of the software, the versions will be reunified for all the hardware models.*

### 3.1.3 Version 3.7.0

Added support for receiving and parsing data from winlogbeat and filebeat.

Redesigned and modified default dashboards.

Replacement of internal monitoring system.

Added support for incremental cluster upgrade.

Completely redesigned manual "Microsoft Security Auditing for LOGmanager".

### 3.1.4 Version 3.6.2

Reworked contexts, fixed bug in mathematical operations inside contexts.

### 3.1.5 Version 3.6.1

**CAUTION - This release contains a notice about the planned termination of support for the CheckPoint component for getting CheckPoint logs via the OPSEC protocol.** For information on how to set up CheckPoint Firewalls to use the CheckPoint log export instead, see our documentation. We kindly ask customers who use CheckPoint to collect logs via the settings in the Resources / CheckPoint menu, to change their configuration till the next version of the LOGmanager software.

Lightweight parsers. It is now possible to easily enable "Lite" parsers without having to modify the data classification. For loaded boxes (CPU utilization constantly over 70%), it is advisable to start using these lightweight parsers. This is because they generate fewer fields during data processing, which reduces CPU, disk array and system memory utilization.

Test window (known from parsers and alerts) now also in the classification of input data.

The IP address field now contains a sub-field with the number and name of the AS (autonomous system).

Digital signing of backups.

Enhancements to the Role-Base Access Control (RBAC) feature to increase the number of concurrent system operators.

Optimization of work of internal balancing queues.

Optimization and acceleration of data processing in the cluster - increase of performance by 30-40% and data replication by 75%.

6 new and 9 modified parsers, 6 new dashboards.

Added complete support for new generations of servers (G3).

### 3.1.6 Version 3.5.2

**CAUTION - This release contains version 3.5.0 bug fixes. If you are using version 3.5.0, we recommend that you update as soon as possible!**

This release fixes a bug that could, under certain rare circumstances, cause system-wide services to crash.

### 3.1.7 Version 3.5.0

**Caution - a significant change in the behavior of classifiers.**

The upgrade simplifies the classification parameters. For more details, see the detailed description of new features in this release notes section 4.1.1.

**Attention - possible upgrade of Dell PERC firmware**

The upgrade automatically detects and updates the Dell PowerEdge Raid Controller firmware on LOGmanager models, where needed.

Improvements to VMWARE and SQL components.

New blockly block.

WES (LOGmanager Windows Event Sender) now uses the cryptographic protocol TLS 1.2.

New dashboards and alert templates

### 3.1.8 Version 3.4.0

Correlations and Alerts with Thresholds - Maximum context time increased from 15 to 30 minutes.

Added possibility to reduce DNS PTR only to a given IP prefix list.

New blockly blocks.

## 4 New Functions

### 4.1.1 Version 3.8.3 a 3.9.6

- Added the ability to bulk delete Beats and WES agents from the LOGmanager GUI using checkboxes.
- Redesigned internal task management system.
- Added new dashboard for SecureAnyBox.

### 4.1.2 Version 3.8.2 and 3.9.5

- **New Beats agents** for the log collection from the Microsoft Windows environment. It is based on Elastic Beats with complete support at least at the level of the previous WES agent.
  - o Old version of WES agent is still usable, only the GUI menu name is supplemented by "legacy".
  - o New MSI for collecting logs from Windows environment - LOGmanager Orchestrator. Available in two versions, with automatic update support and without automatic update support. LOGmanager Orchestrator manages Elastic Beats agents state, updates, component registration etc.
  - o API communication between Beats agents and LOGmanager is protected with TLS 1.2 or TLS 1.3, if supported by source operating system. Logs from Beats agents are sent over TLS 1.3 by default.
  - o Beats agents use certificate validation, therefore communication requires strict use of DNS name in SRV Type record for automatic agent configuration service.
  - o Added complete configuration in the following menus: Sources > Beats agents / Beats filters / Beats global config.
  - o LOGmanager will automatically trunk all incoming Beats file messages that exceed size limit of 64 000 bytes. Every truncated message will be automatically marked as truncated. You can find more information in the documentation.
  - o Added enhanced log filtering capabilities to new Beats Agents.
  - o Support for manual configuration of DNS name of LOGmanager for sending logs from sources outside the domain. Requires manual or automated configuration of the registry.
  - o New documentation, including a description of registry settings on Beats Agents.
  - o Created/updated 8 parsers for processing logs from the Microsoft environment for logs sent by the Beats Agent. Improved and simplified classification template for logs from Beats Agents.

*Note: Automatic update WES agent -> Beats agents: Due to the large number of changes, the new version of the Beats agents does not yet allow automatic update and migration of the configuration. At this point, we recommend that you gradually migrate to the new version of the Beats agents, at least for selected systems with a heavy load, or systems that are outside the domain and require manual configuration of the LOGmanager address.*

*Important note: Automatic configuration of the Beats agents and DNS record: Before installing LOGmanager Orchestrator, please make sure that you are using DNS A record of LOGmanager in the DNS SRV record, not its IP address. If an IP address is used in DNS SRV record for LOGmanager,*

*Beats agents will refuse to send logs. Reason - use of certificates for authentication does not allow use of IP addresses.*

Note: *Beats Agents does not yet support central configuration and log forwarding via LOGmanager Forwarder. Support will be added soon in the new version of Forwarder.*

- Added support for source tracking functionality.
  - o Source tracking allows detection and notification of log sources which suspended data delivery to LOGmanager. New GUI for Source tracking is present in menu Logs > Source tracking.
  
- Replace of the internal task manager and added task monitoring GUI.
  - o New GUI for monitoring current and scheduled tasks is present in menu System > Task status.
  - o Displays database export tasks and its actual state.
  - o Added automated alerts when certain tasks cannot be completed or failed.
  - o Changed flow for database exports. LOGmanager will first query availability of SMB server, its free space for scheduled backup data and then starts export.
  
- Added feature of automated error reporting to vendor. Disabled by default.
- LOGmanager internal components virtualized.
- New version of embedded Rsyslog.
- Added IP address of iLO/iDrac of LOGmanager server in menu Overview > System status.
- New Dashboards:
  - o ISO Access Provisioning
  - o Microsoft Exchange
  - o DNS overview
  - o Zyxel DHCP log
  - o Zyxel Interface statistics log
  - o Zyxel Performance log
  - o Zyxel SSL VPN log
  - o Zyxel System log
  - o Zyxel Traffic log
  - o Zyxel Webfilter log
  - o Zyxel WLAN log
- Updated dashboards:
  - o Dell servers iDRAC
  - o Windows DHCP
  - o Windows DNS

#### **4.1.3 Version 3.7.0**

- Added support for receiving logs from winlogbeat and filebeat
  - o Encrypted data reception using TLS1.3 only.
  - o JSON Data received from beats is automatically expanded to the variable msg ["structured\_data"]. Data can be used directly in the classification. This version adds test windows support data from beats.
- Replaced internal monitoring system

- The GUI displays graphs of CPU usage
  - Improved display of network interfaces and link aggregations
- Added support for several other syslog output formats to simplify integration with the qradar solution.
- Added support for incremental cluster upgrades.
- Completely redesigned manual "Microsoft Security Auditing for LOGmanager".
- Updated alert correlation examples with new correlation options added in version 3.6.2
- Added support for reading logs from vmware version 7.0.2
- Redesigned home dashboard page.
- New predefined dashboards:
  - ISO Access Provisioning
  - ISO Authentication
  - ISO File Access
  - ISO Network Monitoring
  - ISO User Accounts
  - ClearPass audit log
  - ClearPass endpoint log
  - ClearPass radius and accounting log
  - ClearPass radius log
  - ClearPass system log
  - ClearPass TACACS+ log
  - FortiGate DoS policy
  - FortiGate Antivirus
  - FortiGate DLP
  - FortiGate WAF
  - FortiGate users report
  - FortiADC attack log
  - FortiADC system log
  - FortiADC traffic log
  - FortiAuthenticator auth log
  - FortiAuthenticator config changes
  - FortiSandbox alert events
  - FortiSandbox debug events
  - FortiSandbox system events
  - FortiWeb attack log
  - FortiWeb system log
  - FortiWeb traffic log
  - MS Hyper-V overview
  - QNAP storage
  - SQL connector overview
  - HPE IMC
- Improved/fixed dashboards:
  - Squid proxy
  - Webservers access log
  - ISC DNS server



- CEF overview
- Fortigate IPsec

#### 4.1.4 Version 3.6.2

- Completely rewritten work with contexts
  - 2x faster processing of alerts using contexts.
  - The context is now locked during message processing. If a parallel access to the same context occurs, the second process waits for processing by the first process before processing the message (this can be turned on by significantly speeding up work with contexts). It is no longer necessary to predict values in contexts, as the exact numbers of the number of occurrences, etc. will always be stored in the context
  - Redesigned internal work with @int, @float objects, a new string representation of a numeric object is stored in the text representation of the object (previously this could have been confusing when counting in contexts where, for example, count = 2 and count @ int = 3. Newly, both numbers will be the same.)

#### 4.1.5 Version 3.6.1

- Caution: Log reading from CheckPoint using component / LEA protocol has been marked as EOL and will be obsoleted in the next version of LOGmanager software. CheckPoint logs can now be preferably sent using Syslog or Syslog via TLS, according to the instructions in the LM docs.
- Added test message window to classifiers. Note: In this version of the code, the window verifies the classification method only against the block in the given classification window / classification template.
- Added another set of so-called lite parsers, which parse only the most important information. Settings for how the data will be parsed can now be made in the Lite-parser-Settings lookup table. The use of the lite parser can speed up the system and significantly reduce the size of daily indexes, especially for windows logs. (Example for Windows logs - efficiency of using the "microsoft-windows-lite" parsing rule: 50% smaller size of daily indexes, 75% less memory consumption and 20% faster indexing.)
- Reduced the time of the system script, which takes care of data replication within the cluster. Originally opening and closing old indexes every hour, it now performs this operation every 15 minutes. This change will significantly speed up the synchronization of new clusters.
- Added ip2asn functionality, AS number (autonomous system) + AS name is newly added to all IP addresses, for greater efficiency of security analyzes and statistics.
- Added the function of automatic digital signing of exported database backups. Using 4096bit certificates generated in LM at system startup, each backup file is now automatically signed and signature can be evaluated externally or during the restore procedure. (Complete description in the documentation).
- Reduced the number of automatically open daily indexes from 8 to 6. This change brings performance improvements and the ability to search a larger amount of historical data on heavily used LM.
- Improved cluster indexing performance by 30 to 40% over a stand-alone unit. The individual nodes in the cluster now automatically distribute the indexing load.
- Significant optimization of the internal queue system, newly optimized queues need about 10 times less IO operations for their operation. This enhancement greatly improves device performance as it queues.

- Newly, all modified or newly created parsing rules will contain in the description information about the last update date and the tested software version of the source system for which the rule is written.
- Added a new RBAC privilege on system groups (search / read-only), which allows a user with a given system group to search only the data of currently open indexes. Suitable for operators who do not need or do not have to see the historical data of the system.
- Added complete support for new generation servers. LOGmanager SKU ends at G3.
- New and modified dashboards:
  - o Dell iDrac
  - o Synology NAS
  - o Veeam
  - o VMware status change
  - o VMware user session
  - o VMware overview
  - o CEF Flowmon
  - o FortiGate traffic log
  - o Windows update

#### 4.1.6 Version 3.5.0

- Caution: Significant change in the behavior of classifiers. The data source for the classification had been removed globally. The result of the modification is the unification of rules. Since LOGmanager version 3.5.0 on, it is possible to sort data from all sources by using one classification. Compatibility with previous user modification of the classifiers is maintained.
  - o This change will significantly simplify the classification and tagging of data.
  - o Renaming predefined classifiers to “vendor-\*” clearly distinguish classifiers created by the manufacturer from newly / user-created classifiers.
  - o Simplification of predefined classifiers and additional resources for optimal functionality.
  - o All new LOGmanagers with version 3.5.0 and above will contain just one default classifier named as vendor-default. It sends all the data to classifier template vendor-default-classification for processing of all sources.
- Caution: Dell PERC H470P controller contain error up to version 50.5.1-2633:
  - o The controller firmware contains an error that can cause data loss when replacing a damaged disk.
  - o LOGmanager will automatically perform a complete RAID check, upgrade the controller firmware, and then perform a second data integrity check. LOGmanager automatically notifies the administrator of the need to restart the server to apply the new firmware version to the controller = **please check the SMTP settings!**
  - o Both checks and automatic upgrades are run with low priority, expect a significant delay before LOGmanager send email notification with a restart request.
- VMware component:
  - o Update for proper functionality with VMware 7.x.
  - o Improved component logging.
- SQL component:
  - o Added support for reading exact time for Oracle databases.
  - o Improved error logging and timeout operations.

- NTP improvements. Overview / System status screen now shows the current status of the NTP process and time synchronization.
- New automated notification of a problem with automatic database backup had been added. If a problem with automatic database backup is detected, the LOGmanager administrator is now informed by email.
- New blockly text block "decamelize" – Sample: converts the text "SomeValueA" to "some\_value\_a".
- WES agent now uses TLS 1.2. After the first connection to the LM server, the Windows agent will automatically start using TLS 1.2 instead of the original TLS 1.0, which MS dotnet automatically prefers.
- New and improved dashboards:
  - o Windows updates
  - o O365 overview
  - o O365 Azure AD
  - o O365 Exchange
  - o O365 Exchange DLP/transport log
  - o O365 OneDrive
  - o O365 Power BI
  - o O365 SharePoint
  - o O365 Teams
  - o Webservers access log
  - o New account overview
  - o Sharepoint
  - o Linux Bash Activity

Note: Where is necessary to perform additional configuration on the source system to obtain data for LOGmanager use-cases, the dashboards now contain a minimized field with a step by step source config guide.

- New alerts and templates:
  - o New-account
  - o Linux-bash-activity
  - o O365-new-user-added
  - o O365-user-added-to-admin-role
  - o O365-user-login-from-unusual-region
  - o Webserver-excessive-number-of-404-error-codes
  - o Windows-update-failure

#### 4.1.7 Version 3.4.0

- Unique event ID in every message in field "meta.event@id".
- Correlation templates now contain tracing of "event@id" that took part in correlation.
- Alerts and classifiers - restrictions of blocks available for operations is now removed.
- New blockly block "in text replace" added.

- New option in blocks "raw\_real" is available. This variable contains full message without stripping by "raw\_offset". Use for processing messages that do not follow standard syslog header.
- Added possibility to reduce DNS PTR only to a given IP prefix list. System-wide DNS PTR can significantly reduce performance in certain deployments. Defining address space for DNS PTR brings balance between performance penalty and desired functionality. By default, the DNS PTR is enabled for all IPv4 and IPv6 addresses.
- Classifier and classifier templates overview enhanced and simplified.
- Correlations and Alerts with Thresholds - maximum context time increased from 15 to 30 minutes.
- Parsing processes (IP prefix list lookup and Regex cache) optimized for performance.
- New dashboard for Office365.

#### 4.1.8 Version 3.3.0

- Telemetry - Sending statistics on usage of LOGmanager functions to the manufacturer. What is being sent can be displayed and optionally disabled in LOGmanager menu Users> Authentication. The device will not send any data for the first week after system startup or upgrade. Please leave this feature enabled, if possible.
- Added support for Office365. Obtaining logs from Microsoft cloud environment.
- Added support for SMTP authentication and encryption of SMTP server connections.
- Added support for receiving logs from NXLOG Windows agent, LOGmanager treats these logs as if they were received from LOGmanager native Windows agent (adding tags, auto-expanding JSON in classifiers, etc.).
- Added missing blocks to Alerts - all sections of data processing now contain the same blocks.
- Added support for receiving logs using Syslog over TLS.
- Added alerts when building a cluster with warning information that all data on the "slave" system will be deleted.
- Added custom description field to tags.
- Syslog output now allows to set 4 different forwarded message formats. This option provides easier integration with third-party SIEM / UBA systems. (IBM QRadar, etc.).

## 5 New parsers:

### 5.1.1 Version 3.8.3 a 3.9.6

- New parsers
  - VMware-horizon
  - Jivex
- Updated parsers
  - FortiWeb
    - Renamed the "log\_id" field to "attack\_id".
    - Added "msg\_id" and "signature\_id" fields.
  - Fortigate
    - Fixed a parser that could create invalid fields under certain circumstances.
  - Fortigate-lite
    - Fixed a parser that could create invalid fields under certain circumstances.
  - Freeradius
    - Fixed a parser that could create invalid fields under certain circumstances.
  - Apache tomcat
    - Added support for beat agent.
  - Flowmon
    - Fix for parser that could create invalid values under certain circumstances, e.g. for "msg.vlan\_id".
  - OpenSSH
    - Fix for a parser that could produce invalid values under certain circumstances, e.g. for "msg.src\_ip".
  - Veeam
    - Added support for Beat agent.
  - Beat-windows
    - Fix for a parser that incorrectly parsed some logs under certain configurations, adding a space before the value for fields.
  - Qnap
    - Improved parser and added support for Qnap software version 4.5.x.
  - JSON
    - Added support for filebeat.
  - Logmanager
    - Fixed a parser that could create invalid fields under certain circumstances.

### 5.1.2 Version 3.8.2 and 3.9.5

- New parsers:
  - Beat-exchange
  - Siemens-scalance
  - Vectra-cognito
  - Zyxel
- Updated parsers:
  - Beat all parsers – unified field naming to match logic of Windows “legacy” parsers.
    - Added field systemtime

- Fixed logontype
  - Fixed restart reason
  - Added field filename in logs collected from text file logs
  - Fixed windows uptime
- Cisco-ios – Added support for Cisco IOS Wireless controller.
- Fortiauthenticator – Enhanced data extraction of status logs.
- Huawei – Added parsing of ACL logs.
- Classification changes:
  - The new “vendor-beats-template” classification template performs automatic classification for all our-of-the-box Beats parsers. Before configuring new Beats Log Files option, see this classification template for how to properly assign tags for DHCP, DNS, Exchange, and IIS log text files.

### 5.1.3 Version 3.7.0

- New parsers:
  - Beat-microsoft-iis
  - Beat-win-dhcp
  - Beat-win-dns
  - Beat-win-fileaccess
  - Beat-win-firewall
  - Beat-win-rdp
  - Beat-windows
  - Clearpass
  - Fortiadc
  - Fortisandbox
  - Fortiweb
  - Icewarp
  - Pulse secure
  - Qnap
  - Zimbra
- Updated parsers:
  - Checkpoint – fixed possibility to create invalid fields name.
  - Cisco-asa – added parsing of ACL logs.
  - Cisco-ios – added parsing of ACL log.
  - Cisco-ios-xe – added support for new Cisco log format.
  - Firepower – added missing firewall tag.
  - Flowmon – added support for IDS logs.
  - Freeradius – renamed field auth\_method to authenticationtype, for unification reasons.
  - Huawei – added support for Huawei USG firewall.
  - Nginx – renamed field status to status\_code, for unification reasons.
  - Pulse secure – renamed field src\_ip from VPN logs to remote\_ip for unification reasons.
  - Samba – added support for latest version, unification of field names for file audit.
  - Sophos – added tags loginfailed, loginsuccess, failed. Unification of the field names msg.rx > msg.rcvd\_byte, msg.tx > msg.sent\_byte. Support parsing of MTA logs.
  - Symantec-edr – added support for latest version.
  - Vmware, microsoft – added tag virtualization.

#### 5.1.4 Version 3.6.2

- Updated parsers:
  - Huawei
  - Windows DHCP
  - ArubaOS – added support for SDWAN
  - Microsoft IIS
  - Postfix
  - Openssh
  - Cron
  - HP Comware
  - Brocade
  - Dell iDrac
  - Cisco IOS
  - Linux iptables
  - Windows RDP
  - Cisco ASA
  - FortiGate-lite
  - Windows-lite
  - Postfix

#### 5.1.5 Version 3.6.1

- New parsers:
  - Windows lite
  - Cisco ASA lite
  - Veeam Backup & Replication
  - Hillstone NGFW
  - Microsoft Exchange tracking log
  - Pulse Secure
- Updated parsers:
  - Huawei – added new formats
  - Postfix – improved parsing
  - Checkpoint – added new formats
  - LOGmanager – improved internal message parsing
  - Windows DHCP – added lookup table
  - HP Aruba – improved parsing
  - Flowmon – now with severity # to text translation, additional msg.msg field content parsing
  - Firepower – improved parsing and optimization
  - Windows – improved parsing and optimization

#### 5.1.6 Version 3.5.0

- New parsers:
  - Oracle audit db
  - Windows DNS debug log

- AIP-safe
- Bash
- Updated parsers:
  - Fortimail – support for latest release of Fortimail OS
  - O365 – improved parsing
  - Windows – improved parsing
  - Tomcat – added support for Tomcat on Windows platform

#### 5.1.7 Version 3.4.0

- Updated parsers:
  - Windows – fixed wrong tags assignment for EventID: 4776 with status: 0x0
  - PaloAlto – Support for BSD message format
  - ArubaOS – Support for CEF message format introduced in Aruba 8.x
  - Optimized parsing in those parsers: Huawei, Sophos, Juniper, Exchange, epacs, Checkpoint, Greycortex, PaloAlto, Aruba

#### 5.1.8 Version 3.3.0

- New parsers:
  - Greycortex
  - Radware Defens Pro
  - F5 ASM
  - Cisco ISE
  - Cisco UCS
  - Office365
  - ePacs



## 6 Corrected errors

### 6.1.1 Version 3.8.3 a 3.9.6

- The CVE-2022-24903 vulnerability has been patched in the rsyslog component.
- In the MSI Beat agent installation package, the version is now visible in the MSI file properties.
- Fixed DHCP template for Beat agent.
- The classifier/parser/alert test window was incorrectly processing JSON messages.
- LOGmanager orchestrator agent did not correctly change DNS records when updating them.
- Fixed the Resource Monitoring feature, under specific conditions the LM system could be overloaded with resource monitoring.
- Fixed Syslog output/syslog forwarding - in specific scenario unexpected behavior could occur.
- Filebeat tag configuration is correctly escaped and sent as a list, originally it was incorrectly sent as a single string even in case of multiple tags.
- Filebeat fixed template for monitoring DHCP logs.

### 6.1.2 Version 3.8.2 and 3.9.5

- Searching web interface records in configuration forms sometimes did not work properly.
- Some automatically generated reports were not completed in a timely manner.
- The O365 connector did not work through the system proxy.
- The LOGmanager web interface did not display iLO / iDrac interface information.
- Decode CEF Blockly block did not support the latest version of the CEF standard. Therefore, some CEF fields that take advantage of the new features of the CEF format have not been processed correctly.

### 6.1.3 Version 3.7.0

- The O365 component did not respect the settings of the external proxy server and connected directly to the Internet.
- Fixed lite parser names in the lookup table to match the settings in the classifiers.
- Changed the architecture of internal queuing, speeding up the system when using queues.
- On systems with integrated LOGmanager Workload Accelerator, the oldest data may not have been deleted in specific situations. This could cause the administrator to be notified of a system error status (while new data was stored correctly).
- Fixed a bug where the parsing process could significantly spam the log with internal errors.
- Fixed shutdown button in bootmenu.
- Fixed permission for O365, as it was not possible to assign permission to any group.

### 6.1.4 Version 3.6.2

- Fixed mathematical operations within contexts

### 6.1.5 Version 3.6.1

- Updated kernel - fixes very slow communication with the disk controller on some HP servers.
- Fixed LEEF decode block, which can now decode according to the complete specification of LEEF format.
- Fixed backup export to external SMB server, under certain conditions incomplete backup could be copied on heavily loaded systems. Improved backup logic and efficiency.
- Improved display of NTP status page by other possible statuses of NTP service.

- Temporarily removed trunk (link aggregation) interface configuration from CLI LM.
- Events processed by the user parser, which did not have a return block in them, were not sent for further processing in alerts. It caused confusions. Newly, all traffic is sent for processing in alerts.
- Fixed memory leak bug in processes taking care of DB running, exports, closing / opening indexes, etc. The bug caused processes to consume more memory than designed. The result could be a slowdown of the whole system.

#### 6.1.6 Version 3.5.2

- Fixed a possible crash of the services of the entire LOGmanager system. We managed to replicate this state only on LMDemo boxes, but as a precaution, we issue a fix for all LOGmanager models.
- Fixed LEEFv2 decoder.
- SQL component fix - under certain circumstances, reading from tables using a timestamp in "datetime" format might be suspended. ("datetime2" format is no problem)

#### 6.1.7 Version 3.5.0

- Alert did not send an email notification in case of incorrectly defined formatting template. New information about the wrong configuration and the event causing this, is sent by email.
- The newly used NTP Chrony enables more stable synchronization with native (not exact) NTP implementations of Microsoft server operating systems.

#### 6.1.8 Version 3.4.0

- Syslog output could under certain combination of non-ASCII characters in message refuse to forward such message.
- WEB-API now provides detailed description of discovered error conditions.
- Fixed sorting of Windows agents by date/time of last connection.
- Removed blockly block "foreach" in conjunction with IP prefix lists. IP prefix list can be queried only by block "if in", as described in documentation.
- Fixed Juniper dashboard and several alert templates.

#### 6.1.9 Version 3.3.0

- Fixed "race condition" error where system boot might start under certain circumstances before disc subsystem is fully available.
- Fixed bug with not displaying IP addresses on LOGmanager console, which occurred with certain IP address settings.
- Fixed wrong escaping of Unicode regular expressions in Parsers. It is now possible to use any Unicode characters inside Regex.
- Fixed SQL connector - under certain conditions it did not respect configuration changes in the GUI and was still running with the previous configuration.
- Fixed SQL connector in some configuration it refused to connect to Oracle database. We modified internal behavior of component. **If you data from synonym instead of SQL table, you must now enter synonym name in UPPER CASE format as Oracle states in it's documentation.**
- The SQL connector may not have correctly read the logs from the MSSQL server due to poor transaction termination.
- Fixed dashboard documentation links.
- Improved Regex substitution for MAC address detection and normalization.

- Fixed SMTP configuration bug that may allow notifications to be sent through other than SMTP server defined in configuration.
- Fixed VMWare connector error when it could stop reading logs in certain circumstances.
- Report generation has been fixed. If a large number of reports were generated in a short period of time, some reports could be sent without populating data.

## 7 Known bugs

### 7.1.1 Version 3.8.3 a 3.9.6

- Problem: Wildcards cannot be used to create a source tracking rule compared to the documentation.
- Workaround: In the meantime, all important sources have to be specified manually. The correction will be made in the next version of the code.
- Problem: The new version of the LOGmanager Beats agent does not support central configuration and log forwarding via LOGmanager Forwarder.
- Workaround: Do not update branch offices to new Beats agent version yet. If it is necessary due to performance requirements, configure Beats agents to send logs to LOGmanager directly for the time being. This can be done via Beats agents manual/automated Windows registry modification – look into documentation for detailed explanation.

### 7.1.2 Versions 3.2.4 to 3.8.3 and 3.9.6

- Problem: Configuration screen containing Blockly sometimes does not load the blocks properly. Issue could appear mostly while using Chrome web browser.
- Workaround: Reload the page.
- Problem: Configuration screen containing Blockly sometimes does not show translated tag names (IDs of the tags are displayed instead of tag names).
- Workaround: Switch to XML view and back, tags will be translated correctly.
- Problem: While editing Blockly (in classifiers, parsers, alert) block “add tag” with creation of new tag name, sometimes it is not possible to save the edited work (with red error notification strip).
- Workaround: You cannot create new tag with the name already present in the system. Change the tag name to something else. Now, the save is not reporting the error.

