Logmanager

Logmanager release notes version 3.10.2

Software Version:	3.10.2	Date:	May 29, 2023

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 for Logmanager software version 3.10.0 and above. If you need a detailed description of previous versions, see the Logmanager documentation in the release notes menu.

2.1 Supported models

2.1.1 Version 3.10.2

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)
- 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 functions and overview

3.1.1 Version 3.10.2

This release focuses to move index open/close to newly developed platform. This brings reliability and performance improvements in historical data searching.

- Replaced internal component for open/close historical data. Performance improvements and reliable searching in historical data.
    o Changed internal index database system, increased search speed by 5-15%.
    o Changed direction of histogram rendering, to search through the same direction as terms graphs.
- New tools in the Logmanager CLI interface:
    o LLDP - Link Layer Discovery Protocol
    o tcpdump
- Added information about current queue size in email alert.
- Added automatically admin email alert when DNS responses are too slow, which can cause slow event processing.
- Added new system status dashboard to bring detailed monitoring information about system resources, event processing, queue size etc. Including historical data.
- Added new column "Events count" in Database status overview.
- Dropped support for Oracle 11c.
- Added support for Oracle 21c.
- Added logging of admin search query content in event database. Every query that is sent to stored data is logged. Search request can be displayed in the newly added Logmanager internal log dashboard.
- DNS PTR results are now stored in lowercase.
- Added option to change SQL interval read time to 10-600 seconds.
- Increased syslog message size limit for input to 64kB.
- Added initial debug endpoint that will allow to show basic info about replication progress in cluster mode: "APIv1/system/cluster/listallnodesspace"
  Example: https://logmanager.example.com/APIv1/system/cluster/listallnodesspace
- Added more Beats filters examples.
- Completely dropped support for installing and managing Sysmon from Logmanager (was a public beta feature, which was deemed out of scope for Logmanager in the end). Support for Sysmon content is present (log ingestion via beats, Sysmon built-in dashboards), but the admins must install, configure and maintain Sysmon on their own.

3.1.2 Version 3.9.11

This release contains only fixes that may affect system stability. We recommend that you install it as soon as possible.

3.1.3 Version 3.9.9

- Reworked Logmanager cluster communication subsystem and communication between Logmanager and Logmanager Forwarders from IPSEC to WireGuard protocol. The systems will automatically migrate the connection from IPSEC to WireGuard on first startup after upgrade.

ATTENTION, it is necessary to update all nodes in the cluster! If a firewall is in the path between cluster members or between Logmanager Forwarder and Logmanager, it is necessary to enable throughput for UDP port 51820 (cluster) and UDP port 51821 (Forwarder).

- Up to 4 nodes can now be connected to the Logmanager Cluster.
- Disabled TLS1.0 and TLS1.1. Only TLS1.2 and TLS1.3 are now supported. If you are still using the older Agent for collecting logs from Windows - Logmanager WES, the already installed WES Agents will continue to work without problems, as they have downloaded a newer configuration from LM and use TLS1.2. Newly installed WES Agents will no longer connect to LM without manual intervention in their configuration. If you still need to install WES, contact technical support at the portal https://support.logmanager.com. However, we recommend that you stop using WES Agents and replace them with Logmanager Beats Agents.
- Stored values for built-in content (Regex substitution, Lookup tables, IP prefix lists) are now displayed.
- Option to automatically load balance the processing incoming messages across all nodes within the cluster.
- Reworked page for displaying the status of Forwarders. The status of the connection with the Forwarder is now displayed when the page is loaded and the version of the Forwarder is displayed. It is possible to perform updates and restarts of Logmanager Forwarders from the Logmanager environment (since Forwarder version 3.9.x).
- Added link to Logmanager support portal web on UI start page.
- Preparation for the deployment of Sysmon within the Beats Agent to improve the visibility of security events in the Microsoft environment. More details in the Logmanager online documentation under the "Sysmon" chapter.
- O365 endpoint can now be routed to any node in the cluster or through the Logmanager Forwarder (from Forwarder version 3.9.x).
- Improved internal communication of the cluster, the cluster now internally forwards requests to the control node. Newly, Beats Agents and WES Agents can query any node in the cluster for their configuration.

- **Beats Agent** version 1.0.42923:
    o Beats Agent now includes a complete certificate chain in its signature. An incomplete certificate chain caused problems with updating the Agent on systems without an Internet connection.
    o Beats Agent includes a redesigned installation system. Newly, only one version of the installer (logmanager-orchestrator-service-installer.msi) is available, which includes the option of choosing whether Logmanager Beats Agent should support its own automatic update or not.
    o This version does not yet include the option to install Sysmon. If you are interested in a version that allows centralized installation and management of Sysmon, please contact Logmanager technical support at the portal: https://support.logmanager.com.

- New dashboards:
    o Sysmon overview
    o Sysmon file events
    o Sysmon process events

- o Sysmon registry events
  - o Sysmon WMI events
  - o Sysmon threat hunting
  - o Vmware horizon
  - o Secure anybox
  - o Progress Kemp LoadMaster (for system logs and loadbalancer logs)
  - o Progress Kemp LoadMaster WAF (for web application firewall)
- Updated dashboards:
  - o Cisco config change
  - o Progress Flowmon ADS
  - o Vmware status change

3.1.4   Version 3.8.3 and 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.

3.1.5   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: *Beast 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.
    - 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.
    - New GUI for monitoring current and scheduled tasks is present in menu System > Task status.
    - Displays database export tasks and its actual state.
    - Added automated alerts when certain tasks cannot be completed or failed.
    - 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:
    - ISO Access Provisioning
    - Microsoft Exchange
    - DNS overview
    - Zyxel DHCP log
    - Zyxel Interface statistics log
    - Zyxel Performance log
    - Zyxel SSL VPN log
    - Zyxel System log
    - Zyxel Traffic log
    - Zyxel Webfilter log
    - Zyxel WLAN log
- Updated dashboards:
    - Dell servers iDRAC
    - Windows DHCP
    - Windows DNS

3.1.6 Version 3.7.0
- Added support for receiving logs from winlogbeat and filebeat
  - Encrypted data reception using TLS1.3 only.
  - 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 New Logmanager content:

4.1.1 Version 3.10.2
- New parsers
  - o Logmanager parser
  - o pfSense
- Updated parsers
  - o Palo Alto
  - o Cisco IOS
  - o Sophos
  - o Checkpoint
  - o SonicOS
  - o Oracle SQL
  - o Office 365
  - o ArubaOS CX
  - o Windows Beats
- New dashboards
  - o Logmanager internal log

4.1.2 Version 3.9.9
- New parsers
  - o Kemp LoadMaster
  - o Sysmon
- Updated parsers
  - o FortiWeb
  - o Beat-windows – added support for Windows Defender

4.1.3 Version 3.8.3 and 3.9.6
- New parsers
  - o VMware-horizon
  - o Jivex
- Updated parsers
  - o FortiWeb
    - ▪ Renamed the "log_id" field to "attack_id".
    - ▪ Added "msg_id" and "signature_id" fields.
  - o Fortigate
    - ▪ Fixed a parser that could create invalid fields under certain circumstances.
  - o Fortigate-lite
    - ▪ Fixed a parser that could create invalid fields under certain circumstances.
  - o Freeradius
    - ▪ Fixed a parser that could create invalid fields under certain circumstances.
  - o Apache tomcat
    - ▪ Added support for beat agent.
  - o 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.

4.1.4   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.

4.1.5   Version 3.7.0
- New parsers:
  - Beat-microsoft-iis
  - Beat-win-dhcp
  - Beat-win-dns
  - Beat-win-fileaccess
  - Beat-win-firewall

- o Beat-win-rdp
- o Beat-windows
- o Clearpass
- o Fortiadc
- o Fortisandbox
- o Fortiweb
- o Icewarp
- o Pulse secure
- o Qnap
- o Zimbra
- Updated parsers:
  - o Checkpoint – fixed possibility to create invalid fields name.
  - o Cisco-asa – added parsing of ACL logs.
  - o Cisco-ios – added parsing of ACL log.
  - o Cisco-ios-xe – added support for new Cisco log format.
  - o Firepower – added missing firewall tag.
  - o Flowmon – added support for IDS logs.
  - o Freeradius – renamed field auth_method to authenticationtype, for unification reasons.
  - o Huawei – added support for Huawei USG firewall.
  - o Nginx – renamed field status to status_code, for unification reasons.
  - o Pulse secure – renamed filed src_ip from VPN logs to remote_ip for unification reasons.
  - o Samba – added support for latest version, unification of field names for file audit.
  - o 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.
  - o Symantec-edr – added support for latest version.
  - o Vmware, microsoft – added tag virtualization.

5 Corrected errors

5.1.1 Version 3.10.2
- Fixed a bug that prevented searching in old indices.
- Fixed crashing task-manager.
- Fixed a bug of missing some information in task-status overview page.
- Fixed alert email generation, caused by invalid admin definition.
- Increased priority and added extra worker for exporting logs from GUI. When Logmanager was performing backup, GUI export was postponed forcing admin to wait.
- Fixed a bug which caused to force logout user from GUI when click on Sources – Beats global config.
- Increased RAM requirements for virtual Logmanager forwarder from 4GB to 6GB. In some cases Forwarder crashed with only 4GB RAM.
- Changed interface names from "eth" to predictable network interface names "ens…". Interface will migrate automatically to new format during reboot.

5.1.2 Version 3.9.11
- Fixed a bug that prevented saving some configuration in the GUI.
- Fixed a bug when Logmanager was sending ICMP packets to the DNS server.
- Fixed a bug that prevented saving the backup configuration when using special characters in the password for SMB share.
- Fixed a bug that caused the update component to loop, especially on demo boxes.
- Removed unsupported SSL key sizes for certificate management.
- Fixed a component for the Source Tracking functionality that would not send email notifications under certain scenarios.
- Added additional watchdog scripts that monitor the status of system services and disk space.

5.1.3 Version 3.9.9
- Fixed a possible failure of the internal task manager. If during communication with Logmanager technical support, while reporting a task manager failure error, you received an instruction that host name translation (DNS PTR) must be turned off until the release of a new version, after updating to version 3.9.9, this function can be turned on again.
- Logmanager Beats Agent version 1.0.36635 cannot be updated automatically. Unfortunately, due to an error during the compilation of Beats Agent, this version was not allowed to update itself. For the subsequent support of the automatic update of Beats Agents, it is necessary to perform a one-time update manually or via MS AD GP.
- Fixed a bug where the restored index might not have been properly locked and thus the restoration of the given daily index was interrupted.
- The proxy configuration change was not reflected immediately after setting, but only after a restart.
- Correction of SMTP configuration validation.
- Optimizing and speeding up the internal service for collecting data from Beats Agents.
- Changing the configuration of TLS certificates for Syslog over TLS did not take effect immediately, but only after a restart.

- Fixed bug where exported configuration backup could not be restored due to excessive backup size. Implemented internal configuration compression to minimize configuration backup size.
- Limiting the number of internal logs that are stored in the database. Internal service logs are now stored only in the debug log accessible in TSR.
- Correction of a possible leak of the SMB password for the backup index to the notification email for the system administrator when the task manager crashes in the middle of the backup. We recommend changing the password for the given username used to back up Logmanager's daily indexes to an external SMB server.

5.1.4   Version 3.8.3 and 3.9.6
- The CVE-2022-24903 vulnerability has been patched in the rsyslog component.
- In the MSI Beats Agent installation package, the version is now visible in the MSI file properties.
- Fixed DHCP template for Beats 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.

5.1.5   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.

5.1.6   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 Known bugs

6.1.1 Version 3.9.9

- Problem: Logmanager orchestrator agents do not update to newer versions.
- Details: A bug released by a bad version of the agent, where a version without self-updating support was released to production. This was caused by an improperly put together build process, where the release case reached a race-condition and released a version without an updater. This bug has been resolved by changing the build process, in such a way that only one version is released and it behaves differently depending on the parameters.
- Workaround: Since sysmon is planned to be released in the next LM release, there is no need to manually update the agents right away, since sysmon will require a re-installation using MSI. We will provide instructions on how to fix this bug in the next release.

- 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.

- 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.

7 Update process

Release 3.10.2 supports incremental cluster upgrades. You must update the cluster by installing new software on all boxes and restarting the Cluster Master first. After the Cluster Master has restarted, the Cluster Slave can be restarted.

For new version installation in WEB interface click on System > Software
Page with information about installed software will open

Software

Platform	LMDEMO1
HA status	standalone
Serial number	
Current firmware version	3.8.1
Next boot firmware version	3.8.1
Available firmware version	Update version 3.8.2 downloaded for main system.

Check connectivity to update server   Check for update

Backup configuration   Install update

Restart   Shutdown

Upgrade process:
- Click the button "Check for update".
- Available Version **3.10.2** will be displayed (based on hardware version).
- Click the button "Backup configuration" to backup the config prior upgrade.
- Click the button "Install update".
- Once the page is reloaded, in next boot firmware will be displayed 3.10.2**.**
- In the last step, just click Restart and system will restart to the new Version.
- After the restart, the system will consolidate database, automatically update necessary components and do all the health checks. This can take up to 1 hour. Please do not restart the box during this period again and wait patiently.

7.1.1 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 - when 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 long time depending on the size and number of stored events.

End of document.