

## What's New in ELM Log Manager 3.0

ELM Log Manager 3.0 is the successor to Event Log Monitor - Small Business Edition 2.x. ELM Log Manager 3.0 includes many enhancements and improvements over Event Log Monitor. The table below lists the new and improved features of 3.0, as compared with version 2.x.

Feature	2.x	3.0	Improvement over 2.x
<b>Agents</b>			
Server/Workstation Agent	Server Agent	Service Agent or Remote Agent	Remote Agents now provide ability to monitor and collect data from Windows workstations and servers without installing an Agent on the monitored system.
TCP/IP Agent	TCP/IP Agent	IP Agent	Added TCP-based Syslog Receiver for TCP/IP-based systems and devices
Service Agent Configuration	Fixed TCP Port	Configurable TCP Port Settings	Service Agent no longer requires global registry change on all Agent when you want to use something other than default TCP port for Agent socket listen thread. 3.0 Service Agents can be configured to listen on any valid and available port, and Service Agents can use the same or different reports.
Agent activity	Service Stopped or Started	Added Enabled/Disabled	Agents can be disabled and enabled to control their activity during regularly scheduled maintenance. Also, if a dependency item for an Agent (e.g., a router between the ELM Server and the Agent) is down, you can disable an Agent (or some or all of its Monitor Items) to prevent unwanted alerts/events.
Agent installation	Via Console or via manual copy/command line process	Agent installable from ELM Console or by using Setup package	Agents can be installed via an ELM Console, and now can also be installed via the setup package.
<b>Monitoring</b>			
Event Log Monitoring and Collection	Filtering at Agent based on Event Type; filtering at Console based on most event criteria. Also, monitoring for presence of event required event collection	Granular filtering at Agent based on all event criteria. Monitoring presence of event does not require event collection.	You can now filter events for monitoring and collection based on all event criteria (including which log file) at the Agent level. Also, 3.0 includes an Event Alarm which allows you to look for the presence or absence of an event from the event log without having to collect events.
Log File Parsing	FileMon (separate component)	File Monitor	Version 2.0 used a separate executable called FileMon.exe, which ran in admin-created batch files to perform flat file (log file) parsing. 3.0 includes a completely integrated File Monitor that enables you to monitor multiple files at the same or different intervals for one or multiple matches.
<b>Notification and Action</b>			
Alerting	Remote Monitor	Alerts	Version 2.0 included a Remote Monitor application that could receive alert messages from a 2.0 Console. 3.0 replaces this functionality with a special container (Alerts) and separate database table (TNTAlerts) for storing alert messages.
Corrective Action	Batch File Notification Method	Command Script Notification Method	Version 2.0 included support for executing batch files and command line applications to take corrective action. 3.0 expands this ability to include

			scripts, in both cscript and wscript formats. This greatly increases the number of breadth of corrective actions that can be taken via the notification engine.
Electric Signs	N/A	Marquee Notification Method	3.0 includes a brand new notification option that can populate supported electronic marquees with events or alerts. 3.0 supports both serial and TCP/IP connections, which means the marquee does not need to be directly connected to the ELM Server in order to receive messages.
SNMP	SNMP Trap Notification Method	SNMP Trap and SNMP OID Notification Methods	Both 2.0 and 3.0 can re-package and transmit an event as an SNMP Trap for forwarding to a customer-owned SNMP management system. 3.0 also includes a brand new SNMP OID Notification Method that enables you to take any valid SNMP Object ID (OID) and put (write) it to the specified target host or SNMP management system.
Monitor Item Actions	N/A	Actions tab	In 2.0, the notification engine existed completely within the Console. This meant that data needed to travel from an Agent to the Console before notification was executed. In 3.0, there are four Actions that can be executed within the context of a Monitor Item: Alert, Event Log Entry, Network Pop-up Message and Command Scripts. This enables an Agent to execute notification and/or action without having to transmit any data from the Agent to the ELM Server. This makes it possible to execute notification and/or corrective action even quicker than before.

### Data Archiving and Reporting

Database Protection	N/A	Database Failover	In 2.0, if there were any problems communicating with the database, the data was likely lost. This made the database a single point of failure. In 3.0, a protection mechanism called Database Failover is automatically employed behind the scenes. If the database is inaccessible or otherwise unreachable, a temporary Access database is automatically created by the ELM Server. Once the original database is back online, the ELM Server merges the temporary database into the production database and resumes normal operations. This happens automatically without requiring administrator intervention. In addition, alert messages are generated to notify administrators of the loss and subsequent restoration of the database.
Reports	Runtime engine only	Full editor and schedule capabilities	Version 2.0 included a runtime version of a reporting engine that enabled administrators to view and print, but not edit, create or schedule reports without purchasing third-party software. Version 3.0 includes a fully-functional report engine that enables you to edit any report, create additional reports, and schedule reports for automatic output without having to purchase or install any additional software.

### General

User Interface	Proprietary	MMC Snap-In	Version 2.0's user interface was very flexible and configurable; however, it was proprietary and built into the primary Server process. In 3.0, the primary UI is an MMC snap-in called the ELM Console. The ELM Console is completely separate from the ELM Server. In addition, you can use the ELM Console as a standalone application, or you can add native operating system and third-party snap-ins. You can also set security (Windows ACLs) on items, as well as author custom ELM Consoles for distribution throughout your organization.
Encryption	N/A	Full Encryption	Version 3.0 includes a proprietary encryption mechanism that encrypts the data traveling between all of its components. All data sent between the following components is encrypted using this mechanism: Communication between a Service Agent and an ELM Server; Communication between an ELM Server and an ELM Console; and Communication between two ELM Servers (via the Forward Event Notification Method).
Security	Basic	Item-Level Security	In 2.0, access to objects, items and data was automatically granted to all Administrators. 3.0 integrates with the Windows security subsystem, enabling you to set security at the container level and at the item level.



## Sunbelt Software

<http://www.sunbelt-software.com>

<p><b>North America</b> 101 North Garden Avenue Clearwater, FL 33755</p> <p>888-NT UTILS (688-8457) 727-562-0101 Fax: 727-562-5199</p> <p><a href="mailto:sales@sunbelt-software.com">sales@sunbelt-software.com</a> <a href="mailto:support@sunbelt-software.com">support@sunbelt-software.com</a></p>	<p><b>France</b> 116-118 Avenue Paul Doumer 95500 Rueil Malmaison France Tel: +33 (0)1 47 77 05 00 Fax: +33 (0)1 47 77 02 99</p> <p><a href="mailto:sales@sunbelt.fr">sales@sunbelt.fr</a> <a href="mailto:support@sunbelt.fr">support@sunbelt.fr</a></p>	<p><b>United Kingdom</b> 3<sup>rd</sup> Floor, Victoria House 63-67 Foregate Street WR1 1DX Worcester United Kingdom Tel: +44 (0)1905 745711 Fax: +44 (0)1905 745722</p> <p><a href="mailto:info@sunbelt.demon.co.uk">info@sunbelt.demon.co.uk</a> <a href="mailto:support@sunbelt.fr">support@sunbelt.fr</a></p>
---	---	---