

### Basic Windows Event Log Monitoring



#### Overview

ELM Event Log Monitor is a limited version Windows Event Log Monitoring tool. It has the focused functionality of an event log utility and is built on the same foundation as our enterprise class monitoring solution. ELM Event Log Monitor will reliably store the event logs from your servers and workstations, create informative security and management reports and launch alerts in real-time. With ELM Event Log Monitor, you can leverage the full benefits of the data in Windows event logs.

#### Precision Event Log Monitoring Controls

ELM Event Log Monitor reliably collects events from Windows systems, presents the information in a granular format, and launches alerts empowering System Administrators to replace forensic follow-up with proactive management.

#### Event Log Notifications and Alerts

ELM Event Log Monitor includes a rich, robust Notification Engine that enables you to customize pager and email notifications to suit your organizational needs. You can have separate notification methods for different events, or a single notification method for all similar events.

#### Views, Reporting and More

The Reporting container in the ELM Console contains the results of monitoring and management activities that have been configured. Here you can view numerous sample reports available “out of the box” and ready to be used or customized within ELM Editor.

#### Event Log Archiving

ELM Event Log Monitor includes a built-in database engine that provides database support for:

- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express Edition



#### Feature Summary

- This limited version allows you to preview the features found in our commercial product **ELM Enterprise Manager**.
- Collect all events or use custom filters to collect only those you need to see.
- Several pre-configured Event Views allow you to drill down by event type and category.
- Easily create custom Event Views to see exactly what you want.
- Customizable notifications alert you as conditions change, allowing you to manage by exception and be proactive with corrective actions.
- Included reports satisfy most compliance and management requirements.

#### Shareware

ELM Event Log Monitor 6.0 is offered as a limited version trial that can be used to monitor up to 5 servers and 2 workstations for one year.

#### Purchase Information

If you are looking for more monitoring features or to monitor more servers or workstations than the shareware version of ELM Event Log Monitor allows, then you have the option to purchase **ELM Enterprise Manager with Event Licenses**. The Event License provides the same functionality as ELM Event Log Monitor along with more highly valuable features included. In addition, the flexible licensing model in ELM Enterprise Manager also allows you to expand your monitoring even further to include syslogs/snmp, system health/status, performance and more. Visit our website at [www.tntsoftware.com](http://www.tntsoftware.com) for more details.



Silver Independent Software Vendor (ISV)

**Data Profile** Expiration date 08/09/2012

Event Age  
Lists oldest and newest events in the ELM Primary database.

Oldest event	2011-06-08 15:23:16
Newest event	2011-08-09 10:36:00

Event Type Count  
Count of all events by type in alphabetical order.

Count	Event Type
1	Critical
544	Error
38	Audit Failure
3,116	Informational
1,955	Audit Success
15	Verbose
44	Warning
5,715	TOTAL

Event Source and Event ID Count  
Count of top 10 events grouped by Event Source plus Event ID in descending order. NOTE: This query can take several minutes to complete.

EventSource	EventID	Count
Security-Auditing	5447	916
Service Control Manager	7036	786
amdmkdag	62464	234
Security-Auditing	4624	217
Security-Auditing	4672	213
Security-Auditing	4634	164

**Events**

Type	Generated	Computer	Source	EventID	Message
I	8/9/2011 6:40:07 AM	mktg-36	Service Control Manager	7036	The Application Experience...
W	8/9/2011 6:40:00 AM	mktg-22	TaskScheduler	332	Task Scheduler did not start...
E	8/9/2011 6:40:00 AM	mktg-10	TaskScheduler	101	Task Scheduler failed to start...
E	8/9/2011 6:40:00 AM	mktg-10	TaskScheduler	311	Task Scheduler failed to start...
I	8/9/2011 6:40:00 AM	mktg-36	TaskScheduler	107	Task Scheduler launched 'RS...
I	8/9/2011 6:37:38 AM	mktg-10	Service Control Manager	7036	The WMI Performance Adapt...
I	8/9/2011 6:36:00 AM	mktg-10	TaskScheduler	301	Task Scheduler is shutting do...
I	8/9/2011 6:36:00 AM	mktg-10	TaskScheduler	318	Task Scheduler shutdown Ta...
I	8/9/2011 6:36:00 AM	mktg-10	TaskScheduler	318	Task Scheduler shutdown Ta...
I	8/9/2011 6:32:32 AM	mktg-10	Service Control Manager	7036	The Disk Defragmenter servic...
I	8/9/2011 6:32:08 AM	mktg-22	TaskScheduler	318	Task Scheduler shutdown Ta...
I	8/9/2011 6:32:08 AM	mktg-22	TaskScheduler	318	Task Scheduler shutdown Ta...
I	8/9/2011 6:32:08 AM	mktg-22	TaskScheduler	301	Task Scheduler is shutting do...
I	8/9/2011 6:31:47 AM	mktg-36	ReadyBoost	1016	Boot plan calculation compl...
I	8/9/2011 5:27:39 AM	mktg-4	GroupPolicy	5320	Retrieving Domain Controller...
S	8/9/2011 6:31:38 AM	mktg-4	Security-Auditing	4624	An account was successfully l...
I	8/9/2011 6:31:38 AM	mktg-36	Service Control Manager	7036	The WMI Performance Adapt...
I	8/9/2011 6:31:38 AM	mktg-4	Security-Auditing	4672	Special privileges assigned to...
I	8/9/2011 6:31:00 AM	mktg-22	TaskScheduler	102	Task Scheduler successfully f...
I	8/9/2011 6:31:00 AM	mktg-22	TaskScheduler	129	Task Scheduler launch task "...
I	8/9/2011 6:31:00 AM	mktg-10	TaskScheduler	100	Task Scheduler started '1444...
I	8/9/2011 6:31:00 AM	mktg-10	TaskScheduler	314	Task Scheduler has not finish...

**Event Properties**

Event Detail | Event Views

Generated: 8/9/2011 10:59:35 AM  
Event ID: 4625  
Source: Security-Auditing  
Type: Failure Audit  
User: None  
Computer: mktg  
Category: Logon

Message: An account failed to log on.

Subject: Security ID: NT AUTHORITY\SYSTEM  
Account Name: MKTG-GREG  
Account Domain: DOMAIN  
Logon ID: 0x0E7

**Event View Settings**

General  
Magnify number of Events: 10000

View Style  
 Enable the Security View Style

Date Range  
From Date: 1 Weeks ago  
To Date: 2011

**Event Filters**

Name	Description	Type
All -- Events Filter	Matches all events and alerts	Event Filter
All Messages -- Audit Failures Filter	Matches all Security Audit Failure Events	Event Filter
All Messages -- Audit Success Filter	Matches all Security Audit Success Events	Event Filter
All Messages -- Criticals Filter	Matches all event, syslog, SNMP, and alert criticals	Event Filter
All Messages -- Errors Filter	Matches all event, syslog, SNMP, and alert errors	Event Filter
All Messages -- Informational Filter	Matches all event, syslog, SNMP, and alert informationals	Event Filter
All Messages -- Verbose Filter	Matches all event, syslog, SNMP, and alert verbose	Event Filter
All Messages -- Warnings Filter	Matches all event, syslog, SNMP, and alert warnings	Event Filter
ELM -- ELM Agent Events Filter	Events Generated by a TNT Agent	Event Filter
ELM -- ELM Server Events Filter	Events Generated by an ELM Server	Event Filter
ELM Monitor -- All Monitor Item Errors, Failures, and Cr...	Any error, failure, or critical events generated by ELM	Event Filter
ELM Monitor -- All Monitor Item Messages Filter	Events generated by any Monitor Item	Event Filter
Security -- Audit Logon Failure Filter	Logon Failure Events	Event Filter
Security -- Computer Account Changes Filter	Computer Account Management Events	Event Filter
Security -- Object Access Failures Filter	Access Failure Events	Event Filter
Security -- Terminal Services Successful Logoff Filter	Remote Desktop Logoff	Event Filter
Security -- Terminal Services Successful Logon Filter	Remote Desktop Logon	Event Filter
Security -- Terminal Services User Disconnected Filter	Remote Desktop Idle Session	Event Filter
Security -- Terminal Services User Reconnected Filter	Remote Desktop Reconnect to Session	Event Filter
Security -- User Account Locked, Unlocked Filter	Account Locked and Unlocked Audit Events	Event Filter
Security -- User Initiated Logoff Filter	Match 'Logon ID' field in events 501 and 528	Event Filter
Security W2K8 -- Audit Logon Failure Events Filter	Logon Failure Events for Windows 2008	Event Filter
Security W2K8 -- Computer Account Changes Filter	Computer Account Management Events for Windows 2008	Event Filter

**Events by Source**

Top 10 Event Sources  
Number of events from the ten highest sources.

Source	Events
DistributedCOM	1990
MSQSERVER	1990
DriverFrameworks-UserMode	1990
Diagnosis-PCW	1990
amdmkdag	1990
EEMSVR	1990
GroupPolicy	1990
Service Control Manager	1990
TaskScheduler	1990
Security-Auditing	1990

Events by source  
Number of each type of events for each source.

Source	Info	Warning	Error	Success	Failure	Total
amdmkdag	234	0	0	0	0	234
Application-Experience	28	0	0	0	0	28
Bits-Client	0	0	0	0	0	0
BranchCacheSMB	22	0	0	0	0	22
CertificateServicesClient-CertEnroll	8	0	0	0	0	8
Defrag	1	0	0	0	0	1
Desktop Window Manager	2	0	0	0	0	2
Dhcp-Client	4	0	0	0	0	4