

The logo for ELM Event Log Monitor 6.0. 'ELM' is in large, bold, black letters with a small green square at the bottom of the 'M'. 'Event Log' is in a green, sans-serif font, and 'Monitor' is in a black, sans-serif font. '6.0' is in a smaller, black, sans-serif font. A trademark symbol (TM) is located at the top right of 'Log'.

**ELM** Event Log<sup>TM</sup>  
Monitor  
6.0

# User Guide

Copyright © 1996 - 2010 TNT Software, Inc.

# Table of Contents

<b>Part I User Guide</b>	<b>4</b>
1 Legal/Copyright Notice.....	4
2 Getting Started.....	5
Introduction .....	7
<b>System Requirements</b> .....	9
Best Practices.....	12
Sizing Guidelines.....	13
Network Guidelines.....	15
Security Introduction.....	15
<b>Installing the ELM Server</b> .....	17
3 <b>Monitoring</b> .....	18
<b>Agent Types and Monitoring Products</b> .....	19
Agent Installation.....	23
Agent Maintenance.....	28
<b>Monitor Item Container</b> .....	30
Event Collector.....	30
Event Filter .....	33
4 <b>Notification</b> .....	36
<b>Notification Wizard</b> .....	37
<b>Notification Rule</b> .....	39
<b>Event Filters</b> .....	40
<b>Notification Methods</b> .....	43
<b>Notification Thresholds</b> .....	44
<b>Environment Variables</b> .....	45
<b>Notification Methods</b> .....	46
Pager .....	46
Pager (Numeric) .....	47
Pager (Alpha-Numeric).....	48
Mail Notification.....	50
5 <b>Results</b> .....	51
<b>Alert View</b> .....	51
<b>Event Views</b> .....	53
Event Properties.....	55
Event View Settings.....	57
Event Filters.....	60
<b>Reporting</b> .....	63
ELM Editor.....	63
6 <b>Database Settings</b> .....	66
<b>Database Pruning</b> .....	71
7 <b>ELM Server</b> .....	75
<b>ELM At A Glance</b> .....	76
<b>Server Properties</b> .....	77
<b>Control Panel</b> .....	78
8 <b>Technical Resources</b> .....	80
<b>Glossary</b> .....	80

---

<b>Registry Entries .....</b>	<b>83</b>
ELM Console Registry Entries.....	83
ELM Server Registry Entries.....	85
ELM Service Agent Registry Entries.....	91
<b>Command Line Switches .....</b>	<b>95</b>
ELM Server Command Line Options.....	95
TNT Agent Command Line Options.....	96
 <b>Index .....</b>	 <b>98</b>

# 1 User Guide



Welcome to ELM Event Log Monitor 6.0. This is the on-line help for the next generation of TNT Software's award-winning monitoring, alerting, reporting, and archiving solution. Event Log Monitor is the TNT Software, Inc. Shareware product focused on Windows event log monitoring and collection.

Building on the success of its many predecessors, ELM 6.0 adds features for larger environments while maintaining its indispensability for administrators in small to medium size deployments. The [ELM Console](#) has been leveraged to provide a wide variety of monitoring, notifying, and result viewing options. Initial configuration can be accomplished quickly by using the new [Agent Deployment Wizard](#), and pre-configured Notification and Results containers. Generational Archive Databases provide manageable sets of historical data, and Reports give ELM administrators access to all data collected by ELM.

## 1.1 Legal/Copyright Notice

### [Copyright Notice](#)

This document is provided for informational purposes only. TNT Software, Inc. makes no warranties, either express or implied, in this or about this document. Information herein, including references, cites, URLs and other references, is subject to change without notice. The entire risk of the use or the results of the use of this document remains with the user. Complying with all applicable copyright laws is the responsibility of the user. This document and its contents are Copyright 1997-2010 TNT Software, Inc. All rights reserved.

Without limiting any rights, no part of this document or file may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of TNT Software, Inc.

TNT Software, Inc. may have patents, patent applications, trademarks, service marks, copyrights, or other intellectual property rights covering this document and/or its subject matter. Except as expressly provided in any written software license agreement (SLA) from TNT Software, Inc., the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

### [Legal Notice](#)

TNT Software, Inc. provides this document "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document are furnished under a license agreement or a non-disclosure agreement and may be used only in accordance with the terms of the agreement. This document may not be lent, sold, or given away without the written permission of TNT Software, Inc.. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of TNT Software, Inc..

U.S. Government Restricted Rights: Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of the DFARs 252.227-7013 and FAR 52.227-29(c) and any successor rules or regulations.

TNT Software, Inc.  
2001 Main Street  
Vancouver, WA 98660  
<http://www.tntsoftware.com>  
Phone: 360-546-0878  
FAX: 360-546-5017

## 1.2 Getting Started

Major new Features introduced in ELM 6.0 include the following:

- ▣ Only Available in ELM Enterprise Manager 6.0: [Flexible Licensing](#)

With the new flexible licensing model introduced in ELM 6.0, there are some noticeable changes to the ELM product lineup. To provide the most flexible and cost effective monitoring solution on the market today, we have combined the features of all four products in ELM 5.5 into a single product, ELM Enterprise Manager 6.0.

This is accomplished by being able to use four unique licenses within a single product, in a single environment, each with a different set of monitoring features. For example, in ELM 5.5 maybe the ideal scenario would have been to run ELM Enterprise Manager on 20 critical systems for comprehensive monitoring, while that functionality was not necessary for 30 others that just needed event log management.

The four ELM 5.5 products have become the licenses within ELM Enterprise Manager 6.0 These four licenses can be mixed and matched on the various systems in your environment for the most robust, yet cost effective monitoring solution

available.

- |   |  |
|---|--|
| <ul style="list-style-type: none"> <li>• ELM Enterprise Manger --» System License</li> <li>• ELM Log Manager --» Log License</li> <li>• ELM Performance Manager --» Performance License</li> <li>• ELM Event Log Monitor --» Event License (similar to Basic License in ELM Event Log Monitor 6.0)</li> </ul> | <p>Comprehensive system monitoring capabilities:</p> <ul style="list-style-type: none"> <li>• Log Management</li> <li>• Health &amp; Status Monitoring</li> <li>• Application &amp; Service Monitoring</li> <li>• Resiliency - Fault Tolerance Checking</li> </ul> |
|---|--|

⊕ **Only Available in ELM Enterprise Manager 6.0: SNMP and Syslog Receiver – now in console**

Now the Syslog and SNMP receivers are accessible and configurable right within the ELM Console. In addition, you can now assign both Include and Exclude filters for collection, not just in Views!

⊕ **UI Updates**

We've gone through the entire User Interface of ELM 6.0 and updated the icons with sharper, more identifiable shapes. What used to sometimes appear as little blobs of color are now crisp and clean images.

⊕ **Agent Deployment Wizard**

The Agent Deployment Wizard in ELM 6.0 has been streamlined to simplify deployment of single and multiple agents. Improvements include detailed status and progress reports, easier customization of installation, and new dialogues for assigning Licenses to the agents being deployed.

⊕ **Favorites Folder**

The ELM Console in version 6 includes a new 'Favorites' container. What can you do with it?

Just like a web browser bookmark or shortcuts on your desktop, with the Favorites container you'll be able to access your most used items in a single location, including:

- Event Views
- Monitor Items
- Notification Rules
- Notification Methods
- Agents and Agent Categories

### 1.2.1 Introduction

The ELM infrastructure must be planned prior to deploying ELM in your environment.

Consider the following questions:

#### What are my Windows Audit Policy settings?

Your Windows Audit Policy is going to determine which events are being written to your event logs. Some of these audit policies generate a lot of events, such as "Audit process tracking - Success". Determine what your business needs are and only turn on auditing for the events that you will need to collect.

#### Which events do you want to collect?

You decide which events are important to you. For example, in order to collect user logon events, you may decide to collect Audit Success and Audit Failure events on your domain controllers, but only Audit Failure events on your member server. You can determine which events are collected based on a number of event filter criteria. Filtering takes place at the Agent level, reducing the workload on the Agent, the ELM Server, and the network.

#### How frequently do you want to collect data?

Data can be collected in real-time (every second), or at periodic intervals. The frequency of data collection is directly related to resource consumption (overhead) and database size. The more frequently you collect data, the higher your resource utilization and the larger your database becomes (unless you use the built-in aggregation/pruning features).

#### How long do you want to keep data?

If you are planning to keep all event data for years, months, or weeks, the database will become very large and must eventually be archived. Developing a plan to prune unnecessary records and archive preferred data periodically will save time and resources.

For small installations, we recommend using the free Microsoft SQL Server 2008 R2 Express Edition since it has a maximum database size of 10 GB. If you anticipate your database growing beyond 10 GB, we recommend using Microsoft SQL Server Standard

or Enterprise Editions.

[Which notification methods work best for you?](#)

You might choose to send non-critical alerts by e-mail, and critical events by pager.

[What Type and Class of Agents do you want to use?](#)

**Agent** is the general term describing a monitored system. There are two classes of Agents that distinguish among operating systems. For example a Windows Server vs. a Windows Workstation. These two classes are:

- Class I = Windows Server Systems.
- Class II = Windows Workstation.

There are two types of Agents for monitoring Windows operating systems. So Type I and Type II licenses can be assigned to one of the following:

- Service Agents a program that runs as a service on the monitored system
- Virtual Agents provide agent-less monitoring, where the ELM Server performs monitoring and collection.

## Agent Types

- Service Agents run in the security context of the LocalSystem, or in a user security context (e.g., using a service account). Service Agents usually consume approximately 30-75MB of physical memory, and less than 3% of the overall CPU time on the monitored system. The resources actually consumed depend on the number of Monitor Items applied to the Agent, the frequency at which those Monitor Items are executed, and the amount of data generated by or being collected from the monitored system. Service Agents are used for monitoring only Windows 2000/2003/2008, Windows XP Pro, Vista Ultimate, and Windows 7 systems; if you do not wish to install software on the monitored system, use a Virtual Agent.

### Note

When setting the user security context (e.g., using a service account), the settings in the ELM Console override the user security context settings in the TNT Agent service in Windows services.

- Virtual Agents provide agent-less monitoring of Windows computers without installing a service on the monitored system. The ELM Server monitors and collects data from the Windows system remotely. Because Agent code is not used on the monitored system, Virtual Agents will add overhead to your network and to the ELM Server. In most situations, Service Agents are recommended, however Virtual Agents are useful when you do not want to install software on the monitored system. Virtual Agents require that the ELM Server service account has administrative privileges on the system to be monitored. Virtual Agents require RPC

and NetBIOS connectivity between the ELM Server and the monitored system. Because Virtual Agents remotely monitor Windows systems, they cannot monitor in real-time.

## 1.2.2 System Requirements

ELM Event Log Monitor 6.0

Copyright © 1997 – 2010 TNT Software, Inc.  
All rights reserved – Updated 9/13/2010

This section is a simplified presentation of ELM system requirements and should provide enough details for most ELM installations. Please check the web-based version of this document for recent updates and additional details:

<http://www.tntsoftware.com/elmsupport/supplementaldownloads.htm>

### System Requirements

All ELM product lines include the following software components:

- ELM Server Centralized data collection, notification, and reporting.
- ELM Console Main UI for configuring ELM and viewing collected data.
- ELM Service Agent Collects and sends data to the ELM Server.

#### Minimum Hardware Requirements

2 GB of RAM, Dual Core CPU, 300MB free disk space

- ELM Server 100MB free disk
- Service Agent 50MB free disk
- Virtual Agent 10MB memory for each, on ELM Server computer

Note: These disk requirements do not include space for databases, collected .evt(x) files, or ELM Service Agent cache files.

#### Operating System

Any of the ELM Log Monitor 6.0 components can be installed on any of the operating systems below.

- Windows 7 Enterprise / Ultimate
- Windows Server 2008 Standard / Enterprise
- Windows Server 2008 Standard R2 / Enterprise R2
- Windows Vista Business / Enterprise / Ultimate
- Windows Server 2003 Standard / Enterprise
- Windows XP Professional

Note: Windows 2000 is supported only for all agent installs.

Links to OS hardware requirements are maintained on the TNT Software Supplemental Download page: <http://www.tntsoftware.com/elmsupport/>

[supplementaldownloads.htm](#)

#### Database

The ELM Server requires 2 databases, primary and failover, and can authenticate using Windows Integrated (recommended) or SQL Authentication. The databases can be on the ELM Server or available via the local network, and can be a combination of any of the following:

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008 R2 Express Edition
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express Edition
- Microsoft SQL Server 2005
- Microsoft SQL Server 2005 Express Edition
- Microsoft SQL Server 2000

#### Required Software

A typical ELM installation includes one ELM Server, one or two ELM Consoles, and one ELM Agent for each monitored system. We recommend monitoring Windows systems with ELM Service Agents.

ELM Server and ELM Console - A common scenario is to install the ELM Server and ELM Console on a Windows Server in a datacenter or server room, and then use the ELM Console via remote desktop. A variation on this is to install the ELM Console on an administrator's workstation and connect it to the ELM Server in the datacenter. Whichever you prefer, computers hosting the ELM Server and/or the ELM Console should have the following:

- Microsoft cabinet.dll v5.0.2195.7000 or later
- MSXML 3.0 SP5 on Windows XP SP2, else KB284151
- .NET Framework 2.0
- Internet Explorer 6.0 or later
- MMC 3.0 or later

Links to these downloads are maintained on the TNT Software Supplemental Download page: <http://www.tntsoftware.com/elmsupport/supplementaldownloads.htm>

Service Agent - Service Agents run as a service on the monitored Windows computer and connect to the ELM Server when they need to transfer data. They can be installed by "pushing" them from the ELM Console, or by running the ELM setup package on the monitored computer. If an ELM Service Agent is installed using setup, the monitored computer will need the Microsoft cabinet.dll v5.0.2195.7000 or later. Some Monitor Items require the Remote Registry Service be started.

Virtual Agent - Virtual Agents run as part of the ELM Server service, so they have the same software requirements as the ELM Server. Allow 10MB of memory for every Virtual Agent. Virtual Agents require the Remote Registry Service be started on monitored systems.

#### Security

For proper functioning, the ELM installation requires solid name resolution and specific rights to gather data, notify administrators, and present results. Below are security

requirements for different ELM components.

ELM Server - The ELM Server service account requires Administrative rights on the ELM Server and on all systems monitored by a Virtual Agent.

ELM Console - During install, the Authenticated Users group will be given DCOM Allow Access permissions in My Computer on the computer running the ELM Console. COM+ server applications will also be created under the DCOM Config branch of Component Services.

Service Agent - If a service account is used by a Service Agent, then it requires local Administrative rights on the monitored system.

#### Notes

Miscellaneous notes for ELM components.

ELM Server - ELM Server 6.0 will recognize the /3GB switch if used with a Windows 32-bit operating system.

ELM Console - The ELM Console can be installed separately during setup.

Service Agent - If NetBIOS over TCP is disabled, a Service Agent installed by the .msi package can be registered to the ELM Server from the Agent by using the fully-qualified domain name or the TCP/IP address of the ELM Server computer in the Agent Register Server Wizard.

Virtual Agent - Virtual Agents run in the ELM Server process and use RPC to gather data from Windows systems. They are not visible as separate processes.

#### Windows 64-bit

ELM Log Monitor 6.0 has been tested on the 64-bit editions of Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and is supported.

#### Restrictions on Shareware Version

The shareware version is fully-functional in all aspects except for the following:

- The software will expire 365 days from day of install.
- Importing configuration data - ELM includes an export/import feature that enables you to export any object from ELM to an XML file that can be imported into any activated ELM Server. In shareware mode, you can export these objects, but the import function is disabled.

If you want to upgrade to ELM Enterprise Manager, please contact the TNT Software Sales Department [Sales@TNTSoftware.com](mailto:Sales@TNTSoftware.com).

#### Getting ELM Support

The shareware version comes with the Help File and documentation on <http://www.tntsoftware.com>.

There is no support via email or phone for the shareware version.

#### Contact Us

TNT Software, Inc.            Telephone: 360-546-0878  
2001 Main Street            FAX: 360-546-5017  
Vancouver, WA 98660

General:    [Info@TNTSoftware.com](mailto:Info@TNTSoftware.com)  
Sales :      [Sales@TNTSoftware.com](mailto:Sales@TNTSoftware.com)

### 1.2.2.1 Best Practices

#### SQL Best Practices

- Physical server, not virtual.
- Separate the Operating System from the database files and the log files.
- Separate the database files from the log files.
- For database files, performance increases with more spindles included in your RAID configuration.
- Use SATA with TCQ support or SCSI Drives, the faster the RPM the better.
- For better recoverability, use a SCSI interface instead of SATA and IDE.
- For large bandwidth demands on the I/O bus, use a different bus for the transaction log files.
- If there is a DBA on staff, defer to the DBA.

#### Database Best Practices

[Database Pruning and Archiving](#) - Event data can quickly fill a database. Plan to keep only the data you need, for as long as you need it. Microsoft SQL Server 2005/2008 Express has a 4GB limit and Microsoft SQL Server 2008 R2 has a 10GB limit.

Recommendation (based on monitoring 10 or more servers):

- Keep informational, audit success, and warning events for 7 days. Add a prune specification to the [Database Settings](#) in order to remove event data older than 7 days.
- Keep error events for two weeks, then prune them.
- Keep audit failure events for one month, then prune them.
- If physical disks is available, separating the Windows swapfile, SQL .ldf file, and .mdf file onto separate physical disks can help overall performance.

Recommendation (for compliance purposes):

- SQL Server Standard or Enterprise editions are preferred over SQL Express Edition.
- Keep events in the ELM primary database for two weeks, and then archive audit success events. Using a shorter time period will improve performance if the number of events is extremely high.
- Automate archiving the [Archive Database](#). You should expect to have several multi-gigabyte archive database files. These files may be moved to removable media as prescribed by your compliance plan.
- Configure Performance Data Collectors to aggregate data weekly, and prune annually. This will provide one week detail history, and 52 weeks of summary.

## Monitor Item Best Practices

- Only Service Agents can execute Monitor Items in real-time. For Virtual Agents, we recommend a Scheduled Interval of 10 seconds or greater.

## Notification Method Best Practices

- Set [Threshold](#) settings in order to reduce the impact of mass emailing.
- When using e-mail Notification Methods for events you review as part of a daily routine, but do not necessarily need to know about immediately, use an Exchange Public folder as the destination.

### 1.2.2.2 Sizing Guidelines

#### "How should I size my ELM Server?"

Because of the dynamic nature inherent in monitoring computers, it is difficult to provide specific recommendations for hardware specifications. Such recommendations depend on the number of Agents, the frequency of Monitor Items, the amount of data collected or received, etc.

Given those caveats, we offer the following guidelines, observations, and general recommendations for sizing an ELM Server.

The factors that would indicate a dedicated server is required would be:

- Is Monitoring Mission Critical?  
If the systems to be monitored are mission critical and the fastest possible notification of failures is required, you should consider a dedicated server.
- How many events per day are being collected?  
The number of Events Per Day can be estimated using the ELMSize.exe utility.

#### **Small Deployment of ELM**

*< 50000 Events Per Day*

SQL Server on the ELM Server.

Only ELM DB's are being used on the SQL server.

ELM\_Primary / ELM Archive DB's are local to the ELM server. ELM\_Failover DB is on a different SQL server than the Primary DB.

#### **Medium Deployment of ELM**

*50000-1000000 Events Per Day*

SQL Server on a separate server.

Multiple DB's to include ELM\_Primary and ELM Archive DB's on the same SQL server.

ELM\_Failover DB is local to the ELM server. (SQL 2005/2008 Express if needed)

#### **Large Deployment of ELM**

*>1000000 Events Per Day*

SQL Server on a separate server than ELM.

ELM Archive DB's and ELM\_Failover DB is on a different SQL server than the Primary DB.

**Ideal configuration:**

SQL Server on physical hardware on different physical I/O controllers and disk subsystems.

All 15k RPM disks, all hardware RAID:

5 Separate Partitions:

Operating System *Raid 1 (mirror)*

SQL Server exe *Raid 1 (mirror)*

Database Data *Raid 10 (mirror, stripe)*

Database Transaction Logs *Raid 1 (mirror)*

Temp database *Raid 10 (mirror, stripe)*

Choose one of the following approaches to estimate how large your primary database will be after you start monitoring Agents and collecting event data:

### Approach #1

Create a test environment with one ELM Server and one or more Agents that are typical of your enterprise.

Configure the ELM Server to collect the event data and/or performance data and reports per your requirements.

Use the ELGEN.exe utility distributed with ELM to generate the typical number of events each day.

Examine the database size every day in order to determine its size and calculate the growth over the previous day. This will give you a reasonable idea of how much data the database will be required to store per server and aid you in making decisions about how large the database server must be.

### Approach #2

Use the ELMSize.exe utility (call Support for the utility) to collect event data from production servers. In the tool, take a sample of your environment such as a Domain Controller, file server, application server, or web server, and then modify the results in the tool to fit your environment. Take the results from the tool and multiply it by the number of systems that you plan on monitoring.

### Sizing the ELM Server Database Hardware

Now that you know how large your database will be, the next step is to verify you have sufficient resources to run the database engine. Many hardware manufacturers include tools that can configure the appropriate hardware specifications for a server based on your answers to a few questions.

### 1.2.2.3 Network Guidelines

During the planning stage, some thought should be given to how ELM will fit into your network. Your network will have to meet certain minimum requirements:

#### Name Resolution

Healthy name resolution is essential to a trouble-free network. A thorough understanding of the name resolution methods used by Windows operating systems is essential to optimizing network resources. An unreliable name resolution system can create the appearance of slow, unreliable, or failed network applications. ELM uses TCP/IP to communicate and depends on the operating system and configured name resolution (e.g., WINS and/or DNS). If you have not implemented name resolution in your environment, you may use IP addresses for your ELM Server and Agents, and ELM will function normally.

#### Network Bandwidth

ELM makes very efficient use of network bandwidth.

#### ELM Server <--> Service Agent

When an event occurs on a Windows system running a Service Agent, the Service Agent reads the new event and forwards it to each ELM Server that is monitoring it. When multiple events occur in rapid succession, the Agent will group the events together and send them within the same session to the monitoring Server. This behavior optimizes network communication.

#### ELM Server <--> Virtual Agent

The amount of network traffic between an ELM Server and a Virtual Agent depends on what Monitor Items are used, the individual Monitor Item schedules (which determine the frequency of communication), and the amount of data to be collected.

#### Server <--> ELM Console

The ELM Console communicates with the Session Manager component of the ELM Server process. This communication is DCOM-based, encrypted and authenticated. DCOM and RPC connections are made between the ELM Server and the ELM Console to facilitate the transfer of the encrypted data. The amount of data transmitted depends on a variety of factors, including how much data is sent to the ELM Server by Service Agents, what containers are open in the ELM Console. etc.

### 1.2.2.4 Security Introduction

ELM is a client/server application that automates a variety of the administrative functions required for monitoring and managing Windows-based servers and TCP/IP systems and devices.

Since ELM is intended for system and network administrators, the default out-of-box security configuration is designed to allow only accounts with administrative rights to add, remove or change ELM settings. ELM has the following main components:

- ELM Server
- ELM Server Database
- Agents
- ELM Console

Each of the components can be secured at a granular level, enabling administrators to delegate permissions to individual users, groups, or class of user.

## ELM Server Security

There are multiple layers of security that surround an ELM Server:

**Setup / Installation** - To install an ELM Server, you must be logged into an account with administrative rights on the computer. Without these rights, setup will not be able to create the ELM Server service, write the appropriate registry entries, register DCOM classes, or grant log on as a service rights to the ELM Server service account.

**Management Console** - Communication between the ELM Server and the ELM Console is done with Distributed COM (DCOM). The ELM Server service requires DCOM Allow Access permissions to the ELM Console. In turn, users running the ELM Console require DCOM Allow Launch permissions to the ELM Server.

ELM uses integrated Windows Security (NTLM or Kerberos depending on the Server and Agent OS) for authenticating users. Some of the functions won't succeed (such as killing a task or managing services) unless you have administrative rights on the computer being monitored. ELM supports object and item-level security through the ELM Console. This means that you can apply Windows Access Control Lists (ACLs) to objects in your ELM hierarchy.

**Server Agents** - To install a Service Agent on a computer, you must be logged on an account with administrative rights on the Agent computer. Without those rights, you will not be allowed to copy the Agent binaries to the target system, create the TNT Agent service, or grant log on as a service rights to the Agent service account. When you install a Service Agent through the ELM Console, all files are copied from the ELM Console computer to the Agent computer. If your currently logged on account does not have administrative rights on the Agent computer, a Connect As dialog will appear, allowing you to specify alternate credentials (e.g., a local administrator username and password).

**Data Encryption** - ELM incorporates proprietary data encryption. All data sent between the Service Agent and ELM Server are encrypted using this mechanism:

Data sent between the Server and its database, the Server and the Management Console, the Server and Virtual Agents, and between the Server and IP Agents is not natively encrypted.

**Note**

If desired, you may configure additional encryption. Data between the Server and the Console can be encrypted by setting packet-level authentication via the Windows DCOM Configuration Utility (DCOMCNFG), also known as the Component Services snap-in. Refer to this utility's help file for instructions on configuring DCOM encryption. Because this additional encryption adds substantial overhead to the system, we recommend against using DCOM packet encryption.

**Integrated Security** - ELM integrates with Windows security to secure objects and containers in the ELM configuration. Windows Security access control lists are checked when users use the MMC Management Console, or the ELM COM interfaces. You may assign or explicitly deny the following types of access to users and groups:

- Read Only
- Read, Write, Delete
- Full Control

The default security settings for all objects and items are:

- Administrators - Full Control
- Everyone - Read Only

**Integrated Auditing** - ELM supports auditing of access and modification to ELM Server objects. This enables administrators to audit configuration changes to ELM Server objects.

### 1.2.3 Installing the ELM Server

Installing the ELM Server is an easy and straightforward process. When you've determined that your system meets the minimum system requirements and understand your ELM network architecture, begin the installation of the application.

#### Installing the ELM Server

To Install the ELM Server:

1. Double-click the EVM60\_###.msi file you downloaded to execute it (where ### is the build number). The Setup Wizard will launch.
2. Click Next to continue. The License Agreement screen will appear.
3. Select I accept the license agreement and click Next to continue.
4. Select the ELM features you wish to install, modify the install path if desired, and click Next to continue.
5. In the Username field, enter the account to use for the service account.

This account must have administrative rights on the ELM Server, rights to the SQL server if using Windows authentication, and on all Windows systems monitored by ELM Virtual Agents. For a domain account, use the pattern Domain\User. Enter the password for this account in the Password field. Click Next to continue. If the account specified in the preceding step does not already have Log on as a Service rights on the ELM Server, the Setup process will grant this right to the account. The Database Settings dialog will appear.

6. Complete the Primary Database settings dialog to configure the ELM Server primary database. If the database does not exist you will have the option to create it. For a named instance, use the pattern server\instance. Select Install maintenance Microsoft SQL job if you want ELM to automatically create a SQL maintenance job that will perform integrity checks on the database, backup the transaction log, rebuild indexes to optimize the database, and backup the database. Click Next to continue. The Failover Database Connection screen will appear.
7. Complete the Failover Database settings dialog to configure the ELM Server failover database. The failover database is used when the Primary database is offline. If the database does not exist you will have the option to create it after selecting Next. For a named instance, use the pattern server\instance. Click Next to continue.
8. Review the Configuration Settings that will be used by ELM during install. If any settings should be changed, use the Back button to return to the appropriate dialog and edit it. If the Configuration Settings are correct, then click Install to start the installation. The progress screen will appear.
9. Setup will copy the files to the destination folder, register its components, and install the ELM Server service.
10. If the Service Agent component was selected, then the Register Server Computer progress screen will appear. Follow the instructions to setup the service agent, using the Domain\User to authenticate to the ELM server.

**Note**

During install configuration changes are made. These changes are listed below.

**When installing the ELM Console:**

- DCOM permissions are set to allow users and the ELM Server service to communicate with the ELM Console snap-in and ELM Server process.

## 1.3 Monitoring

ELM can monitor systems and collect data in real-time or at scheduled intervals. Each

Monitor Item has its own schedule components:

- A scheduled interval, which determines how frequently the monitor item is executed.
- Scheduled hours, which specifies what days/hours the monitor item will run.

For real-time monitoring, a [Service Agent](#) must be used. [Virtual Agents](#) cannot monitor in real-time because all Virtual Agent monitoring is performed over the network by the ELM Server. We recommend a scheduled interval of 10 seconds or greater for Monitor Items assigned to Virtual Agents.

To monitor continuously, set the Scheduled Interval on the Monitor Item to Every 1 Second. The Scheduled Interval can be increased to the desired interval. For example, to collect event logs twice a day, an Event Collector's Scheduled Interval would be configured for every 12 hours.

## Getting Started

To begin monitoring, Right click on the Monitoring container. From the context menu choose New.

- Agent - Select New | Agent from the context menu to begin monitoring a computer.

### 1.3.1 Agent Types and Monitoring Products

#### Creating and managing Agent Objects

[Agent](#) is the general term describing a monitored system. There are two classes of Agents that distinguish among operating systems. For example a Windows Server vs. a Windows Workstation. These two classes are:

- Class I = Windows Server Systems.
- Class II = Windows Workstation.

There are two types for Agents monitoring Windows operating systems. So Class I and Class II licenses can be installed as one of the following:

- Service Agents a program that runs as a service on the monitored system
- Virtual Agents provide agent-less monitoring, where the ELM Server performs monitoring/collection.

#### Agent Types

- Service Agents run in the security context of the LocalSystem, or in a user security context (e.g., using a service account). Service Agents usually consume approximately 30-75MB of physical memory, and less than 3% of the overall CPU time on the monitored system. The resources actually consumed depend on the number of Monitor Items applied to the Agent, the frequency at which those Monitor Items are executed, and the amount of data generated by or being collected from the monitored system. Service Agents are used for monitoring only

Windows 2000/2003/2008, Windows XP Pro, Vista Ultimate, and Windows 7 systems; if you do not wish to install software on the monitored system, use a Virtual Agent.

**Note**

When setting the user security context (e.g., using a service account), the settings in the ELM Console override the user security context settings in the TNT Agent service in Windows services.

- Virtual Agents provide agent-less monitoring of Windows computers without installing a service on the monitored system. The ELM Server monitors and collects data from the Windows system remotely. Because Agent code is not used on the monitored system, Virtual Agents will add overhead to your network and to the ELM Server. In most situations, Service Agents are recommended, however Virtual Agents are useful when you do not want to install software on the monitored system. Virtual Agents require that the ELM Server service account has administrative privileges on the system to be monitored. Virtual Agents require RPC and NetBIOS connectivity between the ELM Server and the monitored system. Because Virtual Agents remotely monitor Windows systems, they cannot monitor in real-time.

### Monitoring Products Available in the ELM Enterprise Manager edition



### Monitoring Capability Feature Comparison

Log Management	System	Log	Performance	Event
Event Alarm	Sy	Lg	....	EV
Event Collector	Sy	Lg	....	EV
Event File Collector	Sy	Lg	....	....
File Monitor	Sy	Lg	....	....
SNMP Alarm	Sy	....	....	....
SNMP Collector	Sy	....	....	....
SNMP Receiver	Sy	Lg	....	....
Syslog Receiver	Sy	Lg	....	....
<b>Health &amp; Status Monitoring</b>				
Inventory Collector	Sy	....	....	....
Performance Alarm	Sy	....	Pf	....
Performance Collector	Sy	....	Pf	....
Ping Monitor	Sy	....	....	....
Process Monitor	Sy	....	Pf	....
Windows Configuration Monitor	Sy	....	....	....
WMI Monitoring	Sy	....	Pf	....
<b>Application &amp; Service Monitoring</b>				
Cluster Monitor	Sy	....	....	....
Exchange Monitor	Sy	....	....	....
FTP Monitor	Sy	....	....	....
IIS Monitor	Sy	....	....	....
Link Monitor	Sy	....	....	....
POP3 Monitor	Sy	....	....	....
Service Monitor	Sy	....	....	....
SMTP Monitor	Sy	....	....	....
SQL Monitor	Sy	....	....	....
TCP Port Monitor	Sy	....	....	....
Web Page Monitor	Sy	....	....	....
<b>Fault Tolerance Checking</b>				
Agent Monitor	Sy	Lg	Pf	EV
ELM Server Monitor	Sy	Lg	Pf	EV

## Agent Categories

Agent Categories group Agents for easy management and can be customized to your particular needs.

ELM has many pre-configured Categories, and will import Categories found during an upgrade.

The default All Agents category has special significance to ELM and should not be altered. However the other pre-configured Categories, can be renamed, deleted, or

otherwise altered. New Categories can be created as necessary.

Agents can exist within multiple categories. For example, an Agent monitoring SQL Server 2005 could be in the following categories:

- Windows 2003 Servers
- Service Agents
- Database Servers
- Corporate Servers

**Monitor Items** can be assigned to Agent Categories. Agents inherit the Monitors that are assigned to an Agent Category. Adding a Monitor to the Agent Category automatically assigns the monitor to each agent in the category.

### To create a new Agent Category

1. Right click on the Monitoring container and select New | Category. The New Category Wizard will appear. Click Next to continue.
2. The Item Name and Description dialog will appear. Enter the Name for the new Category, and an optional Description. Click Next to continue.
3. A list of Agents will appear. Select the Agent(s) you want in this category. Click Next to continue.

#### Note

You are not required to select any Agents. Categories can be created and assigned Monitor Items before Agent installation occurs.

4. A list of Monitor Items will appear. Select the Item(s) you want to assign to the Category.
5. Click Finish to create the category.

You can also create a new category from the Agent Categories tab inside the properties of an Agent, or from the Categories tab inside the properties of a Monitor Item. To do this, right-click anywhere in the tab dialog, select New Agent Category, and complete steps 2-5 above.

### Agents Tab

In the properties of a Category, the Agents tab will show all the configured Agents. Checkmarks appear next to Agents assigned to the Category.

### Monitor Items Within a Category

The Monitor Items container below an Agent Category lists all the Monitor Items assigned to the Category or at least 1 Agent in the Category. The columns Category Assignment and Agent Assignment indicate how the Monitor Items are assigned to the Category and Agents within with the Category. The table below lists the possible values for the Assignment columns and the resultant meaning:

Category Assignment	Agent Assignment	Meaning
Yes	All	The Monitor Item is assigned to the Category and to all Agents in the Category.
Yes	Some	The Monitor Item is assigned to the Category and to some Agents in the Category.
Yes	None	The Monitor Item is assigned to the Category, but not to any Agents in the Category.
No	All	The Monitor Item is not assigned to the Category, but is assigned to all Agents in the Category.
No	Some	The Monitor Item is not assigned to the Category, but is assigned to some Agents in the Category.
No	None	IMPOSSIBLE - Monitor Items must be assigned to the Category or at least 1 Agent to appear.

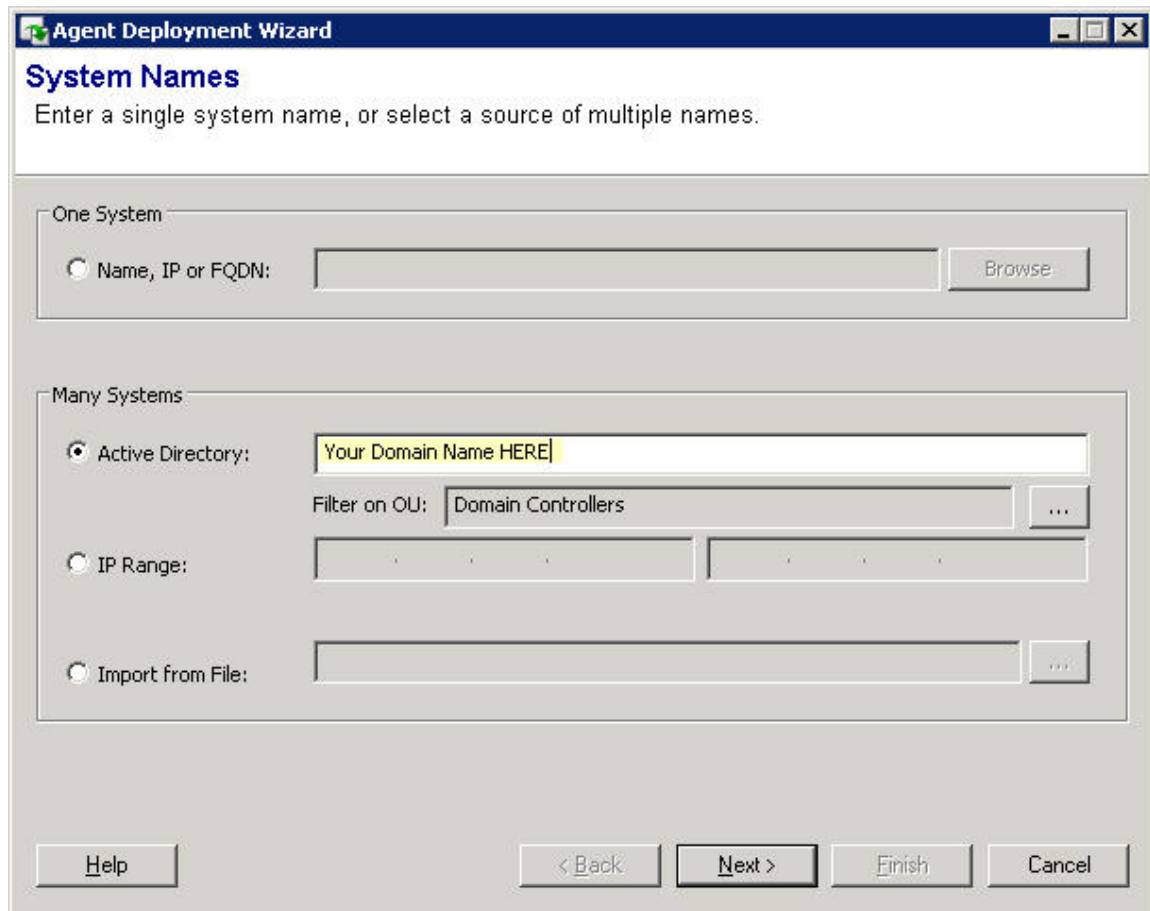
### 1.3.1.1 Agent Installation

#### Installing Agents

An ELM Server can monitor multiple Agents and a Service Agent can be monitored by multiple ELM Servers. Each Agent maintains separate configuration, collection set, and cache files for each ELM Server that monitors the Agent. You can install Agents remotely from the ELM Console, or you can install them manually on the target machine (see [Installing Service Agents Using Setup Package](#) below).

To Install Agent(s):

1. Right-click on the Monitoring container in the ELM Console and select New | Agent . The Agent Deployment Wizard will launch. When the Welcome dialog is displayed, click Next to continue.



2. From the System Names dialog box, there is the option of installing *One System* or *Many Systems*. This part of the guide will cover the *Many Systems* agent install.
3. In the *Many Systems* area, there are three options: Active Directory, IP Range, and Import from File.
  - Active Directory: Specify the Active Directory domain to search. Checking the box marked Filter allows you to further specify particular Organizational Units within the domain to search by using the drop down menu.
  - Scan IP Range: Specify a range of IP addresses to search for computers or devices.
  - Import From File: Use the ellipsis button to browse to a CSV (comma-separated value) file containing a list of machines or devices on which to install Agents.

The CSV file has the following syntax:

```
Agent1,Service Agent
Agent2,Virtual Agent
```

4. On the *Next* dialog, *Systems Found*, a *Succeeded* or *Failed* message will indicate if that system is online by using Ping. Click a system or multiple systems using CTRL or shift, right-click on the system(s) name to Add a System, Select All, or Selected Systems | Remove.

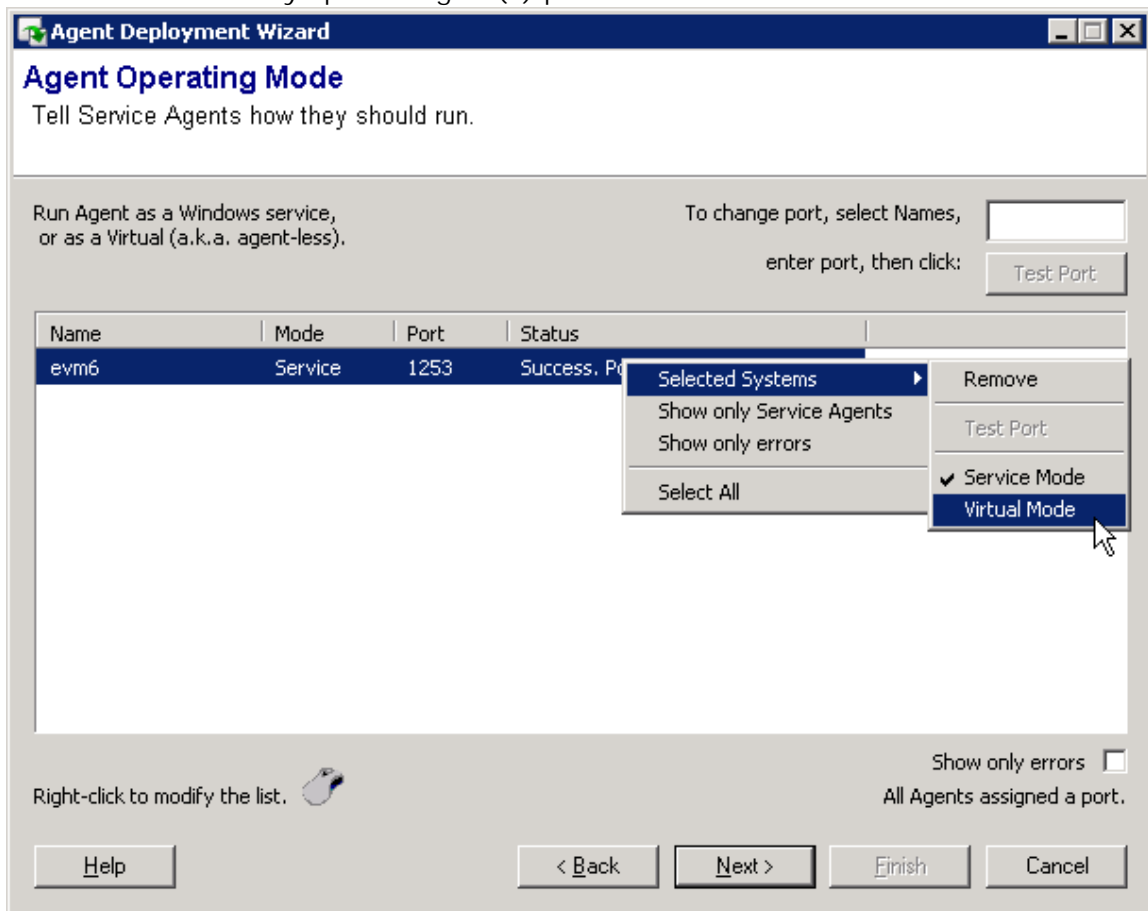
To change service agent defaults, select the Defaults button. Change the defaults to match the needs in your environment.

- Use the Install Credentials to specify the account used to connect and install the service agent. This account must have *local administrator* rights on the destination. For a DC, this would be a Domain Administrator account.
- Use the Share and path to specify the destination share and path for the service agent install.
- Using the Listening port to change the port that the agent will use.
- Use the Minimum disk free space in MB to limit how much disk space a cache file will take.
- Use the Maximum cache file size in MB to limit the size of the cache file.

**Note**

Once an Agent has been configured to listen on a specific port, you cannot change the port. If you want the Agent to listen on a different port, you must remove then re-add the Agent using the new port.

- The System Scan Summary dialog displays the scan results and gives the status to common agent installation issues. If there are any errors, Advanced is automatically checked. If there are no errors, but a few systems need to be customized, check Advanced before selecting next.
- The Agent Operating Mode dialog is used to change the agent to a different mode and/or modify specific agent(s) port.



- Select Show only Errors to filter the agents with errors.
  - Select a system that is not available and Remove by selecting and right clicking | Selected Systems | Remove.
- The Log On for Service Agents dialog is used to change the account used for the Service Agent(s). Select multiple agents by using CTRL and mouse click or shift and mouse click.

8. The Service Agent Install Location dialog is used to change the installation share and path. Select multiple agents by using CTRL and mouse click or shift and mouse click.
  - Use the Min. free disk (MB) to limit how much disk space a cache file will take.
  - Use the Max. cache file (MB) to limit the size of the cache file.
9. The Agent Categories dialog is used to assign agents to Agent Categories. Select multiple agents by using CTRL and mouse click or shift and mouse click.
10. The Monitoring Products dialog is used to assign agents to [Monitoring Products](#). Select multiple agents by using CTRL and mouse click or shift and mouse click. The Avail column show the number of licenses available for that product. The Used column shows the number of licenses used for that product.
11. The Install Agents dialog displays the status of all of your selections before selecting *Next* to install.
12. The Install Summary dialog displays the status of the installation. Click Finish to exit the Agent Deployment Wizard.

## Installing Service Agents Using the Setup Package

If the system you wish to monitor is on the other side of a firewall, in a DMZ environment, or located in an environment that restricts the use of NetBIOS and RPC endpoint ports, you can use the ELM Setup package to install a Service Agent on the remote system and then use the Agent UI or Registration Wizard to register the Agent with the ELM Server and select monitor items for the Agent.

### To install a Service Agent using Setup:

1. Double-click the ELM60\_###.msi file you downloaded (where ### is the build number). The Setup Wizard will launch.
2. Click Next to continue. The License Agreement screen will appear.
3. Review and then select I accept the license agreement and click Next to continue.
4. On the Select Features dialog:
  - Click on the Server component icon and select Entire feature will be unavailable.
  - Click on the Console component icon and select Entire feature will be unavailable.
  - Click on the Agent icon with the **X** and select Will be installed on local hard drive.
  - Click on Browse to change the default install path.
5. Click Next for the Install Application dialog. If any changes must be made, use the Back button to return to any dialogs requiring changes.

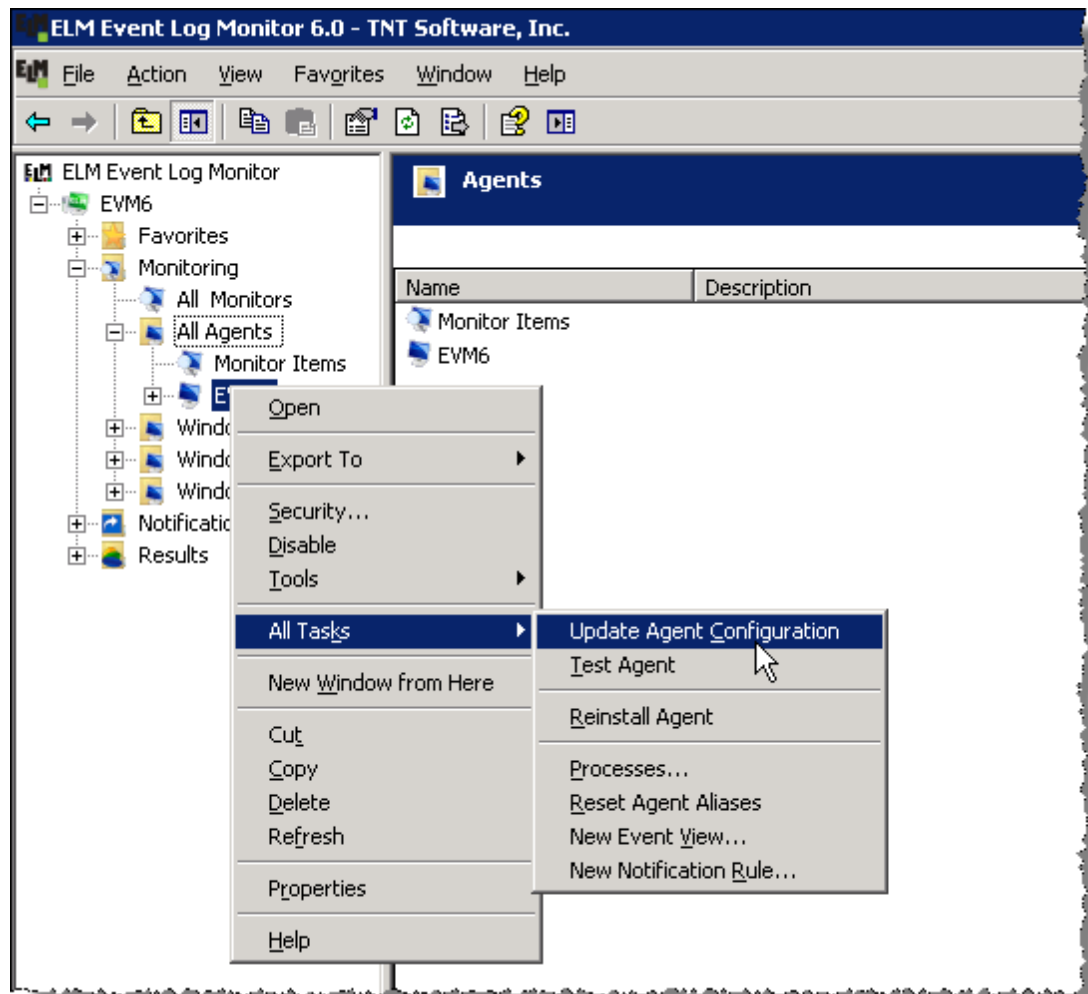
6. Click Install to start the Service Agent install process.
7. When the installation has completed, the Register Server Wizard will launch. In the Name field, enter the host name, IP address or fully-qualified domain name for the ELM Server you wish to register, or click the Browse button to browse the network for the ELM Server you wish to register. In the Port field, enter the TCP port on which the ELM Server is listening. By default, ELM Servers listen on port 1251. The port is configured at the ELM Server from the ELM Server control panel applet. Click Next to continue.
8. A logon prompt will appear. Provide an account that has administrative rights on the ELM Server computer. If a domain account is specified, use the pattern domain\user in the Username field. Click OK when an account and password have been entered.
9. The Monitoring Products dialog box will appear. Put a check in the box to the left of the type of [Monitoring Product](#) you want this agent to have. Click Next to continue.
10. The Agent Categories dialog box will appear. Put a check in the box to the left of each Category you want this Agent to join. You may view the properties of any Category by right-clicking the item and selecting Properties. Click Finish to save the Agent settings and ELM Server registration.
11. Click Finish to close the install wizard.

To uninstall a Service Agent that was installed using setup:

1. Open the Windows Control Panel and double-click 'Add/Remove Programs' or 'Programs and Features'.
2. Select the ELM Event Log Monitor 6.0 product and click the Change button.
3. If the Service Agent is the only ELM component installed on this system, or if there are other ELM components (e.g., ELM Server or ELM Console) and you wish to uninstall everything, select Remove and proceed through the Wizard. If there are other ELM components installed on this system and you do not wish to remove them, select Modify and continue through the Wizard. When the component dialog is shown, change the Service Agent from Will be installed on local hard drive to Entire feature will be unavailable. Then complete the Wizard to remove it.

### 1.3.1.2 Agent Maintenance

Agent maintenance tasks modify or restore Agents in various ways. The operations of Update Agent Configuration, Reinstall Agent, and Reset Agent Aliases are accessible through context menus for individual Agents, Agent Categories, or multiple Agents as illustrated below. Not all operations are relevant for Virtual Agents.



## Update Agent Configuration

There are 2 copies of a Service Agent's configuration, one in the ELM Server and one in the Agent. If the two do not match, the copy in the ELM Server is considered the authority. During normal operation, the ELM Server will automatically send configuration updates to Service Agents within about 3 minutes, depending on system activity, network latency, number of Agents needing updates, etc. The Update Agent Configuration operation allows an ELM administrator to manually refresh the configuration without waiting the default 3 minutes.

This operation applies only to Service Agents.

## Reinstall Agent

This operation will reinstall Agent binaries. It will attempt to use the Agent listening port to transfer files, but if unavailable, the operation will then try to use RPC to authenticate and connect to the *default: ADMIN\$* share like an initial Service Agent install. Reinstall Agent will create an update log, and will stop and start the Agent service.

This operation applies only to Service Agents.

## Reset Agent Aliases

This operation will refresh the SV\_Aliases property for an Agent using the name resolution mechanism of the OS hosting the ELM Server. The SV\_Aliases list is the primary source of Agent identity for the ELM Server and includes the IP address(es), and the fully qualified domain name (FQDN) for an Agent. A reset is occasionally needed when an IP address or FQDN is assigned to the wrong agent.

This operation applies to Service Agents and Virtual Agents.

## 1.3.2 Monitor Item Container

### All Monitors Container

The All Monitors container displays all of the configured monitor items. To disable all of the monitor items at the same time, right click the All Monitors container and select Disable. This disables all of the monitor items at the container level and doesn't change the specific monitor items settings.

### Data Collector and Real-Time Monitors

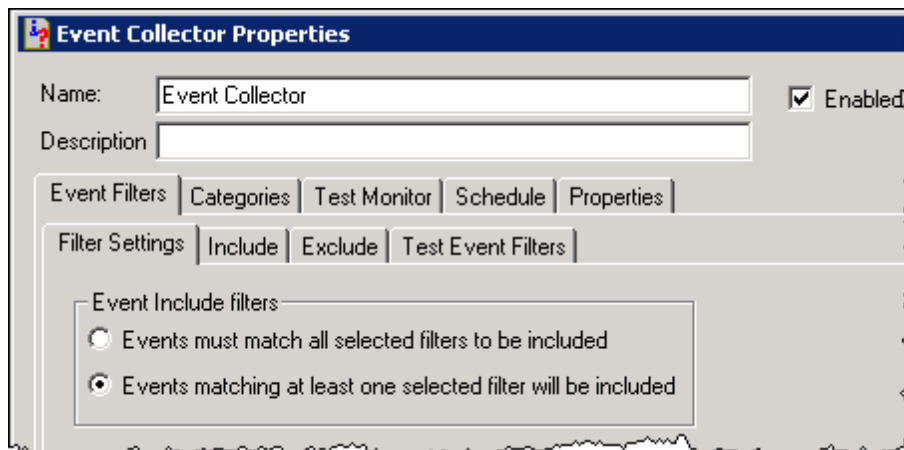
[Event Collector](#) - Event Collectors collect events from the event logs on Windows 2000, Windows XP, Windows Server 2003, Vista, Windows 7, and Windows Server 2008. You can specify the events to collect based on a variety of event criteria, including event type, source, event ID, and event details.

#### 1.3.2.1 Event Collector

Event Collector Monitor Items collect some or all events from the Agent(s) being monitored. Events can be collected based on a combination of include and exclude Filters. Each Filter has criteria for the following event fields:

- Computer Name
- Event Log
- Username
- Event Source
- Event ID
- Event Category
- Event Message

When a new event occurs, it is checked against the Filters assigned to the Event Collector Monitor Item. If it matches at least 1 Include Filter and no Exclude Filters, then it will be sent to the ELM Server. If the event does not match an Include Filter, or matches an Exclude Filter, the event will be skipped. This is true for both Service Agents and Virtual Agents.



When using Event Collectors, there are two important issues:

1. On very busy systems that generate many event log records, the Event Collector may not be able to keep up in real-time. There is a finite amount of data that can be collected and stored in a single monitor item interval. This means that there can be some lag time between when an event is logged to the event log and when it is received by the ELM Server. When collecting events, the Event Collector bookmarks the last record read so that it knows where to start reading at its next Scheduled Interval. On very busy systems, especially domain controllers with high levels of auditing enabled, it is possible for the Event Collector bookmark to roll off the event log before the records can be collected. If this happens, the bookmark is automatically reset at the most recent event. Any events that occurred between the old bookmark that rolled off the log and the new bookmark will not be collected. To prevent this from happening, we recommend setting the size of your event logs to a large enough value so that they hold at least 24 hours of event data. A large event log size should prevent the loss of a bookmark and allow the Event Collector to monitor all events.
2. When using multiple Event Collectors on the same Agent, any one of these Monitor Items can request that event logs be read. The request is initiated only if Scheduled Hours are "on" plus a Scheduled Interval has passed for the individual Monitor Item. Any request will cause the event logs to be read starting from the saved bookmarks, passing new events to all Event Collectors for the Agent, and then updating the bookmarks. Event Collectors check only their Event Criteria before deciding to process a new event, they do not check their Scheduled Hours.

## Reference Information

An Event Collector's job is to read events, expand the message, and deliver the record to the ELM Server. If it has trouble performing this task, then it or the ELM Server can create one or more of the following events:

Error 5566 - The bookmarked event record is no longer in the log, events are being skipped, and the bookmark reset to the beginning of the log (most recent event).

Error 5700 - The ELM Server had trouble receiving the event.

Error 5701 - The Event Collector had trouble creating or expanding the event into a record that could be delivered to the ELM Server.

Error 5702 - A Service Agent had trouble sending an event to the ELM Server.

Error 5703 - The ELM Server had trouble receiving an event from a Service Agent.

## See Also

[Event Filter Criteria](#)

## Categories

Displays the Agent Categories to which the Monitor is assigned. Click to select or deselect Agent Categories. Right click to create or edit Agent Categories.

## Test Monitor

Test any Monitor Item against any Agent capable of running the Item using the drop-down and Test button on this dialog box. Testing a Monitor Item prior to putting it into production validates that the monitor item is configured properly. To test a monitor item:

1. Select the Agent you wish to test against from the drop-down list.
2. Click the Start Test button.

If the test was successful, you will receive a pop-up indicating this and the option to see detailed results of the test. If the test failed, detailed results of the test will automatically open in Notepad.

## Schedule

Displays the Scheduled Interval and Scheduled Hours settings which control the frequency for the Monitor Item.

### Scheduled Interval tab

Specify the interval at which the monitoring, polling or action is to occur. Depending on the Monitor Item type, Items can be scheduled in interval increments of Seconds, Minutes, Hours and Days. The Scheduled Interval is relative to the top of the hour or top of the minute. For example, if a Scheduled Interval is configured for 10 minutes, the Monitor Item will execute at hh: 10:00, hh: 20:00, hh: 30:00, hh: 40:00, hh: 50:00, hh:00:00, etc. If a Scheduled Interval is configured for 15 seconds, the Monitor Item will execute at hh:00:15, hh:00:30, hh:00:45, hh:00:00, hh:01:15, etc.

### Scheduled Hours tab

Select the days and/or hours this item is active. By default, the schedule is set to ON for all hours and all days. Mouse clicks toggle squares between ON and OFF. Clicking

on an individual square will toggle the active schedule for that hour. Clicking on an hour at the top of the grid, or on a day of the week at the left of the grid will toggle the corresponding column or row. Keyboard equivalents are the arrow keys and the space bar.

## Properties Tab

This read-only tab displays the properties of the selected object and the values for those properties.

### 1.3.2.1.1 Event Filter

Filters are common objects within ELM and can be assigned to Notification Rules, Event Views, and to Event Collectors.

The primary contexts are the Include and Exclude tabs for [Notification Rules](#), [Event Views](#), and [Event Monitors](#). The Filter criteria entered by the user controls what events are gathered and displayed.

- Name - Enter a unique name.
- Description - Enter a description (optional).
- Default - This child item will be automatically assigned when a parent item is

created. In the case of Event Filters, any newly created Event Views, Notification Rules, or Event Collectors will have the default Event Filter (child item) automatically assigned.

## Event Filter Criteria

Event Filters provide a mechanism for isolating specific events, and multiple Event Filters can be combined to create a complex set of criteria. The same Filter can include or exclude events. They can also be created in the ELM Database Wizard to control database pruning, however these Filters will not be available in the Event Filter collections. Although filtered Alert views are not possible, Alert records can trigger Notification Methods if matching Filters and Notification Rules are configured.

The following fields are available for filtering purposes:

- Computer Name is
- Log Name is
- Username is
- Event Source is
- Event ID is
- Category is
- Message contains

This dialog box has a dynamic menu behavior. The ellipsis buttons next to the Computer Name is, Log Name is, and Event Source is fields browse and display the computer names, event log names and event sources. If the Computer Name is field is left empty, the list of event Logs and Sources is generated based on the event sources registered on the ELM Console computer (i.e., the local computer). If you enter a valid, resolvable name in the Computer Name is field and then click the ellipsis for the Log Name is or Event Source is fields, the list of event Logs and Sources from that system will be displayed. If the log or event source from which you want to collect data does not appear on the list, type it in the appropriate field. For example, if you are not running DNS on your ELM Server or Console, but want to collect events from the DNS log only, type *DNS* in the Log Name is field.

If a field is blank, it will match every value in the field. For example, if the Computer Name is field is blank, the Filter will apply to all computers. If all Event Types are unchecked when the Event Filter is saved, all of the Event Types will be checked. This is by design.

Leading and trailing wildcards ( \* ) and character position wildcards ( ? ) are supported, as are the Boolean operators Or ( | ), And ( & ), and Not ( ! ). However regular expressions are not supported. You may use these wildcards to specify the criteria to be applied. For example, to select messages from SQL Server you may specify \*SQL\* as the event source to select any Source name containing the letters SQL. To match SQL messages from servers ALPHA, BRAVO, or CHARLIE you would enter ALPHA|BRAVO|CHARLIE in the Computer Name is field.

**Important**

Leave no white space adjacent to the operators.

**Note**

If you enter the name of an untrusted system in the Computer Name is field and then use the ellipsis buttons for Log or Event Source, the menus will not be displayed. This is because authentication fails. To work around this problem, first make an IPC\$ connection to the target system using alternate credentials. For example, if the untrusted system's name is dArtagnan, you could use:

```
NET USE \\SERVERA\IPC$ /user:dArtagnan
\administrator *
```

You will be prompted for the password for the account you specify. The dynamic menu behavior will work after the IPC\$ connection has been established.

## Test Event Filter

Tests the filter to see which events pass the filter criteria.

You may specify the Computer name, Event Log, Event Source, and Event ID. You may also provide an Insertion string for the test. The insertion string is used for every parameter of the event description.

The Filter Status field displays whether or not an event matches the filter criteria after an Event ID is selected.

When testing event filters:

- You can test against all Event Filter Criteria fields *except* for the Category field. Event categories are determined at run-time by the application that generates them; consequently, you cannot use this field as a test criterion.
- The Computer Name field allows you to select any valid Windows workstation or server in order to select an event log, event source, and event from that computer. If you select an event log that does not also reside on the ELM Console computer, you will receive an error message stating that a file cannot be found. For example, if you are running the ELM Console on a Windows XP Professional machine and you select a Windows 2000 Active Directory domain controller, then select the Directory Service event log, you will receive an error message that ntdsmg.dll could not be found. This is because of an incorrectly parsed %systemroot% environment variable. This will occur only when the %systemroot% environment variable on the ELM Console is different from the variable on the server whose logs are being read.

## Notification Rules

Shows the Notification Rules associated with this Event Filter using an Include or Exclude relationship. Right click to create or edit a Notification Rule.

### Event Views

Shows the Event Views associated with this Event Filter using an Include or Exclude relationship. Right click to create or edit an Event View.

### Event Monitors

Shows the Event Collectors associated with this Event Filter using an Include or Exclude relationship. Right click to create or edit an Event Collector.

### Properties Tab

This read-only tab displays the properties of the selected object and the values for those properties.

## 1.4 Notification

The Notification container stores [Notification Rules](#), [Event Filters](#) and [Notification Methods](#).

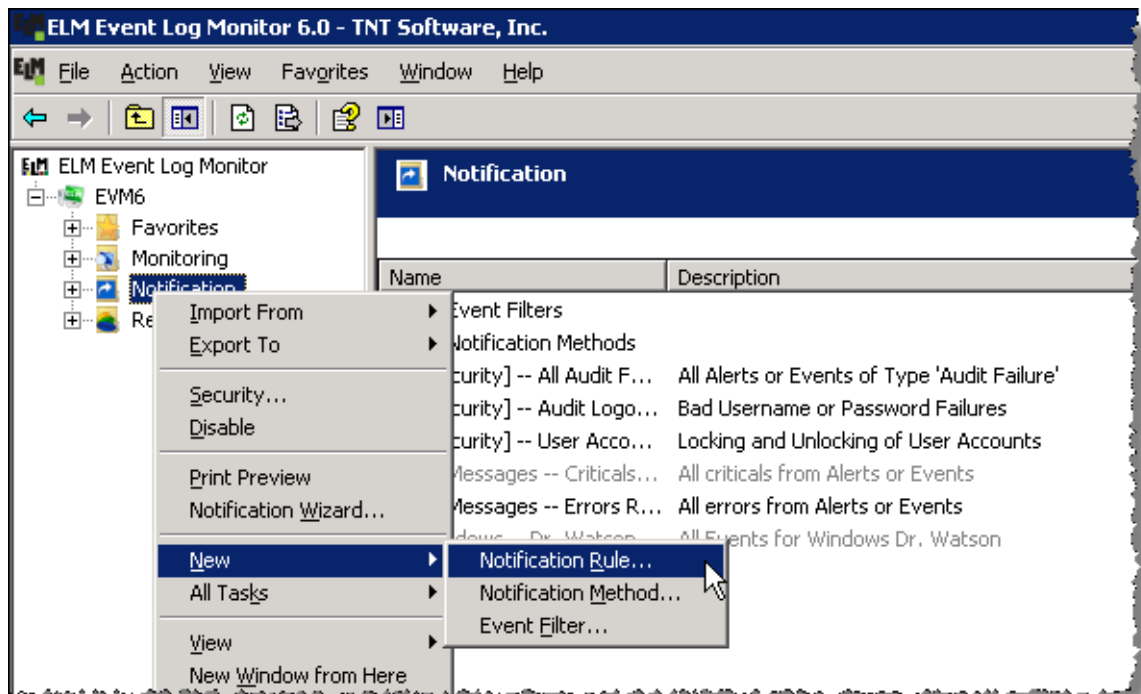
Notification Rules define which Events or Alerts will be sent via the Notification Methods.

### Notification Container

To disable all of the notification items at the same time, right click the Notification container and select Disable. This disables all of the notification items at the container level and doesn't change the specific notification items settings.

### Getting Started

To create a new Notification Rule, right-click on the Notification container and select New | Notification Rule from the menu.



To modify a Notification Rule, right-click on the Notification Rule in the Notification container and choose Properties from the menu.

#### Note

Notification Rules share Event Filters and Notification Methods. If you edit or change either Event Filters or Notification Methods they will be changed for all Notification Rules.

### 1.4.1 Notification Wizard

The Notification Wizard creates a new Notification Rule using Monitor Item Actions to populate Event Filter criteria.

To create a new Notification Rule using the Notification Wizard, right-click on the Notification container and choose Notification Wizard from the menu.

#### Select Monitor to Trigger Notification

Actions or Events from the selected Monitor Item will trigger the Notification Rule.

- Category - Filter the list of Monitor Items based on the category of the monitor item.
- Monitor Type - Filter the list of Monitor Items based on the type of monitor item.
- Keyword - Filter the list of Monitor Items based on a keyword or phrase in the Monitor Item description.

## Select Action to Trigger Notification

Displays a list of Actions defined by the Monitor Item selected in the previous dialog. Select the Actions about which you wish to be notified. If the Monitor Item has only one Action, then this dialog is skipped.

## Event Filter Definition

Here is where the Notification Wizard provides intelligence. Based on the Monitor Item and Action selected, the Event Filter Description dialog is populated with appropriate details for Event Source, Event ID, and Event Type to match. These details can then be adjusted for the desired criteria.

Each field will accept multiple entries. When an entry is selected from a list, it is added to the field and separated from earlier entries by the OR (|) operator. You may change this operator to AND (&) or NOT (!). Fields may be left blank to match all, or wildcards may be used. Asterisk (\*) matches multiple characters, and question mark (?) matches any one character.

- Computer Name is - enter the name of the computer(s) or click the ellipsis button to select the name(s) of the computer(s)
- Log Name is - click the ellipsis button to select the log(s) from which the Event is observed, or leave the field blank to include all logs.
- Username is - enter Username(s)
- Event Source is - click the ellipsis button to select specific Event source(s), or leave the field blank to include all.
- Event ID is - enter Event ID(s)
- Category is - enter Category(s)
- Message contains - enter a character string

Check the checkboxes to select the type(s) of Events to select.

## Select Notification Methods

Select the Notification Methods to be run when the Notification Rule created by this wizard is triggered.

## Name and Description

- Name - Enter a unique name.
- Description - Enter a description (optional).
- Enabled - The item can be enabled (checked) or disabled (unchecked). When disabled it is not active.

## Finished

- Monitor Item - Click the Monitor Item button to create another Notification Rule based on a Monitor Item.
- Action - Click the Action button to create another Notification Rule based on a Monitor Item Action
- Finished - Click the Finished button to create the Notification Rule.

## 1.4.2 Notification Rule

Notification Rules respond to events and generate Notifications.

Notification Rules are stored in the Notification container in the ELM Console. To create a new Notification Rule right click on the Notification container and select New | Notification Rule from the menu.

To disable all of the Notification Rules at the same time, right click the Notification container and select Disable. This disables all of the notification items at the container level and doesn't change the specific notification items settings.

Event Filters determine which events will trigger the Notification Rule. An event that passes the Event Filter test is passed to each Notification Method assigned to the Notification Rule.

- Name - Enter a unique name.
- Description - Enter a description (optional).
- Enabled - The item can be enabled (checked) or disabled (unchecked). When disabled it is not active.

### Notification Methods

Select the Notification method to run when this Notification Rule is triggered. Right click to create or edit a Notification method.

### Event Filters

#### Filter Settings

- Events must match all selected filters to be included - When this option is set, the Event must match all selected Event Filters and must not match any of the selected Exclude Filters.
- Events matching at least one selected filter will be included - When this option is set, the Event must match only one of the selected Event Filters and must not match any of the selected Exclude Filters.

#### Include

Select the Event Filters to trigger this Notification Rule. When a new Event or Alert is received, it will be compared to the selected Event Filters.

Right click to create a or edit Event Filter.

#### Exclude

Select the Event Filters for Events or Alerts that should not trigger this Notification Rule.

Right-click to create or edit an Event Filter.

#### Test Event Filters

Simulate events by selecting a Computer name, Event Log, Event Source, Event, and

optional Insertion String. The Filter Status field will indicate if the event will be included or excluded, and the Filter Name that decides.

## Properties Tab

This read-only tab displays the properties of the selected object and the values for those properties.

### 1.4.3 Event Filters

Filters are common objects within ELM and can be assigned to Notification Rules, Event Views, and to Event Collectors.

The primary contexts are the Include and Exclude tabs for [Notification Rules](#), [Event Views](#), and [Event Monitors](#). The Filter criteria entered by the user controls what events are gathered and displayed.

**Security -- Terminal Services Successful Logon Filter Properties**

Name: Security -- Terminal Services Successful Logon Filter

Description: Remote Desktop Logon

Default

Event Filter Criteria | Test Event Filter Criteria | Notification Rules | Event Views | Event Monitors | Prop

Use wild card operators (\* - match many characters), (? - match one character) and conditional operators [| - or], (& - and), and (! - not) to create advanced selection criteria.

Computer Name is:

Log Name is:

Username is:

Event Source is: Security

Event ID is: 528

Category is:

Message contains: \*Logon\*Type\*10\*

Event Type is:

Informational  Error  Failure  Critical

Warning  Success  Verbose

- Name - Enter a unique name.
- Description - Enter a description (optional).
- Default - This child item will be automatically assigned when a parent item is created. In the case of Event Filters, any newly created Event Views, Notification Rules, or Event Collectors will have the default Event Filter (child item) automatically assigned.

## Event Filter Criteria

Event Filters provide a mechanism for isolating specific events, and multiple Event Filters can be combined to create a complex set of criteria. The same Filter can include or exclude events. They can also be created in the ELM Database Wizard to control database pruning, however these Filters will not be available in the Event Filter collections. Although filtered Alert views are not possible, Alert records can trigger Notification Methods if matching Filters and Notification Rules are configured.

The following fields are available for filtering purposes:

- Computer Name is
- Log Name is
- Username is
- Event Source is
- Event ID is
- Category is
- Message contains

This dialog box has a dynamic menu behavior. The ellipsis buttons next to the Computer Name is, Log Name is, and Event Source is fields browse and display the computer names, event log names and event sources. If the Computer Name is field is left empty, the list of event Logs and Sources is generated based on the event sources registered on the ELM Console computer (i.e., the local computer). If you enter a valid, resolvable name in the Computer Name is field and then click the ellipsis for the Log Name is or Event Source is fields, the list of event Logs and Sources from that system will be displayed. If the log or event source from which you want to collect data does not appear on the list, type it in the appropriate field. For example, if you are not running DNS on your ELM Server or Console, but want to collect events from the DNS log only, type *DNS* in the Log Name is field.

If a field is blank, it will match every value in the field. For example, if the Computer Name is field is blank, the Filter will apply to all computers. If all Event Types are unchecked when the Event Filter is saved, all of the Event Types will be checked. This is by design.

Leading and trailing wildcards ( \* ) and character position wildcards ( ? ) are supported, as are the Boolean operators Or ( | ), And ( & ), and Not ( ! ). However regular expressions are not supported. You may use these wildcards to specify the criteria to be applied. For example, to select messages from SQL Server you may specify \*SQL\* as the event source to select any Source name containing the letters SQL. To match SQL messages from servers ALPHA, BRAVO, or CHARLIE you would enter ALPHA|BRAVO|CHARLIE in the Computer Name is field.

**Important**  
Leave no white space adjacent to the operators.

**Note**  
If you enter the name of an untrusted system in the Computer Name is field and then use the ellipsis buttons for Log or Event Source, the menus will not be displayed. This is because authentication fails. To work around this problem, first make an IPC\$ connection to the target system using alternate credentials. For example, if the untrusted system's name is dArtagnan, you could use:

```
NET USE \\SERVERA\IPC$ /user:dArtagnan
\administrator *
```

You will be prompted for the password for the account you specify. The dynamic menu behavior will work after the IPC\$ connection has been established.

## Test Event Filter

Tests the filter to see which events pass the filter criteria.

You may specify the Computer name, Event Log, Event Source, and Event ID. You may also provide an Insertion string for the test. The insertion string is used for every parameter of the event description.

The Filter Status field displays whether or not an event matches the filter criteria after an Event ID is selected.

When testing event filters:

- You can test against all Event Filter Criteria fields *except* for the Category field. Event categories are determined at run-time by the application that generates them; consequently, you cannot use this field as a test criterion.
- The Computer Name field allows you to select any valid Windows workstation or server in order to select an event log, event source, and event from that computer. If you select an event log that does not also reside on the ELM Console computer, you will receive an error message stating that a file cannot be found. For example, if you are running the ELM Console on a Windows XP Professional machine and you select a Windows 2000 Active Directory domain controller, then select the Directory Service event log, you will receive an error message that ntdsmg.dll could not be found. This is because of an incorrectly parsed %systemroot% environment variable. This will occur only when the %systemroot% environment variable on the ELM Console is different from the variable on the server whose logs are being read.

## Notification Rules

Shows the Notification Rules associated with this Event Filter using an Include or Exclude relationship. Right click to create or edit a Notification Rule.

### Event Views

Shows the Event Views associated with this Event Filter using an Include or Exclude relationship. Right click to create or edit an Event View.

### Event Monitors

Shows the Event Collectors associated with this Event Filter using an Include or Exclude relationship. Right click to create or edit an Event Collector.

### Properties Tab

This read-only tab displays the properties of the selected object and the values for those properties.

## 1.4.4 Notification Methods

Notification methods are how administrators learn of events or alerts. To create a new Notification method, right-click on the Notifications container in the ELM Console and select New | Notification Method.

Notification Methods are run using a Notification Rule. You may run separate Notification Methods for different events using Event Filters. For example, one method might describe how to notify a database administrator about important database related events, while another method might notify a security administrator about important security related events.

Notification methods pass the full event information to the notification engine, which in turn forwards that information depending on the methods selected. If desired, the information sent via the Notification Method can be customized. This is useful when there are restrictions on message length, as in the case of a mobile pager. Customizable messages are a convenient way of making notifications more meaningful.

To disable all of the Notification Methods at the same time, right click the All Notification Methods container and select Disable. This disables all of the notification methods at the container level and doesn't change the specific notification methods settings.

### Notification Methods

The list below describes the methods designed for use with a server or service available in EVM.

[Pager](#) - Send event information to pagers.

Mail Notification - Send event information to email addresses.

### 1.4.5 Notification Thresholds

Thresholds determine how many times identical events can occur before the Notification Method will be executed, or stopped from executing. There are three threshold settings available:

- Disable this notification when it is triggered. If the Notification Method is triggered the configured number of times within the specified time period, the notifications will stop. The Notification Method is then re-enabled after a specified time period .
- Activate this notification method after it is triggered. When this threshold is selected, the notifications will not be processed unless the rule is triggered the specified number of times within the time period selected.
- Consolidate notifications by waiting until either:
  - A specific number of similar events has occurred
  - A specific amount of time has elapsed

To disable this Notification Method for older data sent from a Service Agent, check the box that says Disable this notification method for all Cached (old) data. By default, 60 minutes is the window of time which differentiates old data from new data. If an event occurred within the last hour, even though it may be from a Service Agent cache file, ELM will not treat it as (old) cached data. This feature is designed to account for, and notify you of, events that occur during brief ELM Server outages (reboots, service restart, etc.). This window of time can be changed by setting the HKEY\_LOCAL\_MACHINE\SOFTWARE\TNT Software\ELM Event Log Monitor\6.0\Settings\CacheDataTrigger value in the Registry on the ELM Server.

#### Threshold Events Counter

The threshold count increments only for identical events; that is, events that have the same four fields:

- Computer Name
- Source
- User Name
- Event ID

For example, if you configure a Mail Notification Method with the Threshold set to Disable when triggered 2 times within 5 minutes, and re-enable after 30 minutes, and within a 5 minute period the following events are received triggering rules that use this Notification Method:

- Computer: SERVERA
- Source: Perflib
- Event ID: 1003
- User Name: None
- Category: None
- Type: Warning Time
- Generated: 4/10/2008 1:34:58 PM

- Log: Application
  - Message: Performance data cannot be collected.
- 
- Computer: SERVERA
  - Source: Perflib
  - Event ID: 1003
  - User Name: None
  - Category: None
  - Type: Warning
  - Time Generated: 4/10/2008 1:36:04 PM
  - Log: Application
  - Message: Performance data cannot be collected.

Then because the four fields match, the events increment the count. Because two identical events occurred within the defined 5 minute period, the Notification Method will be disabled for additional matching events for 30 minutes, and automatically re-enabled thereafter. While the Notification Method is disabled for one group of events, it will send notifications for other (non-matching) events unless they also reach the threshold. The threshold count would not be incremented if the second event looked like this:

- Computer: SERVERB
- Source: Perflib
- Event ID: 1003
- User Name: None
- Category: None
- Type: Warning
- Time Generated: 4/10/2005 1:34:58 PM
- Log: Application
- Message: Performance data cannot be collected.

Because the Computer name is different in the above event, it is not considered an identical event, and therefore does not increment the threshold count for the first event (and thus does not disable the Notification Method).

## 1.4.6 Environment Variables

The table below lists the Environment variables established by an event and available to notification methods. In addition any system or user defined environment variables may be used.

Environment Variable	Description
%COMPUTER%	Name of the computer the event was generated on.
%EVENT%	Event ID, equivalent to the Event Id field in Event Viewer.
%MESSAGE%	Message text of the event. This variable has white space, tabs, and new lines trimmed.

%DATE%	Date the event was created, from the TimeGenerated field.
%TIME%	Time the event was created, from the TimeGenerated field.
%TYPE%	Type of the event, I = Informational, W = Warning, E = Error, S = Audit Success, F = Audit Failure, C = Critical, and V = Verbose.
%LOGNAME%	Name of the event log the event originated from.
%SOURCE%	The source of the event, equivalent to the Source field in Event Viewer.
%CATEGORY%	The category of the event, equivalent to the Category field in Event Viewer.
%USER%	The Username of the account that generated the event.
%INDEX%	The unique index of the event. This index is a key to the TNTEvents table in the database.

Tip: To list the environment variables available to the ELM Server, issue the set command from the command prompt.

## 1.4.7 Notification Methods

### Notification Methods

The list below describes the methods designed for use with a server or service available in EVM.

[Pager](#) - Send event information to pagers.

Mail Notification - Send event information to email addresses.

#### 1.4.7.1 Pager

If a modem is attached to the ELM Server computer, ELM can send Pager Notifications using 2 main approaches:

[Pager \(Numeric\)](#)

[Pager \(Alpha-Numeric\)](#)

#### 1.4.7.1.1 Pager (Numeric)

The Numeric Pager Notification sends a numeric message to a pager.

### Message

- Numeric Message - Enter the numeric message or code to be sent to the pager.

Click the Test button to verify that your pager receives the intended message.

### Account Numbers

Use the list provided to add or remove recipients using the same pager service.

- Name - Enter the Name of the person to add to the list
- Pager Account Number - Enter the telephone number for this person's pager.
- Add account number to list - Click this button to add the person to the list
- Remove Account - Select a name from the list and click this button to remove the selected name.

### Connection Settings

- Number of Retries - Enter the number of times to retry if the pager service is busy.
- Pager Script - Select a script for your pager service.

Use the Edit, Copy, and New buttons to create or edit Pager Script Settings.

The Pager Notification includes many pre-defined Pager Scripts to be used as-is, or to be modified for your specific pager and pager service. To use a Pager Notification, a properly configured modem must be attached to the ELM Server computer and be available to the ELM Server application.

### Pager Script

The Pager Notification includes many pre-defined Pager Scripts to be used as-is, or to be modified for your specific pager and pager service. To use a Pager Notification, a properly configured modem must be attached to the ELM Server computer and be available to the ELM Server application.

Pager Notification uses a script to define the communication protocol. Scripts are provided for Numeric, Alpha-Numeric, and SMS messaging. If the telecom service provider requires a variation of one of these protocols, the script allows you to customize communication in order to adapt to the protocol of your service provider.

#### Note

For SMS messaging, the ELM Server will need a GSM/GPRS enabled modem connected to the computer hosting the ELM Server.

To customize the pager script settings, open the Pager Notification properties, go to the Connection Settings dialog, select the Pager Script you wish to modify, then click

the Edit button.

**Note**

It is best to make a backup copy of the current script before changing it. This will enable you to revert back to the original script if necessary.

- Name - Enter a unique name.
- Description - Enter a description (optional).
- Enabled - The item can be enabled (checked) or disabled (unchecked). When disabled it is not active.
- Default - This child item will be automatically assigned when a parent item is created. In the case of Notification Methods, any newly created Notification Rules will have default Notification Methods automatically assigned.

### Notification Rules

The Notification Rules that will trigger this Notification when the Notification Rule is satisfied. Right click to create or edit a Notification Rule.

### Threshold

The [Threshold](#) settings for this Notification. The Threshold allows you to control how often the Notification is run.

### Scheduled Hours

The Schedule setting for this Notification. The Schedule allows you to control when the Notification is run.

Select the times that this Notification is active. By default, the schedule is set to ON for all hours and all days. Mouse clicks toggle each time period ON and OFF. Clicking on an individual square will toggle the active schedule for that hour. Clicking on an hour at the top of the grid, or on a day of the week at the left of the grid will toggle the entire column or row. Keyboard equivalents are the arrow keys and the space bar.

### Properties Tab

This read-only tab displays the properties of the selected object and the values for those properties.

#### 1.4.7.1.2 Pager (Alpha-Numeric)

The Alphanumeric Pager Notification sends event information to an alpha numeric pager.

### Access Number

- Pager Server Access Number - Enter the telephone number for your pager service. Enter a comma to cause a 3 second delay. If you must dial a number for an outside line, or for a long distance number, add the appropriate leading

characters to this string. For example, if you must dial 9 for an outside line and your pager service is a 1-800 number, you should enter 9,1800/n/n/n/n/n/n/n/n.

- Message - Enter the message to be transmitted to your pager. Use the Insert Variable button to insert [Environment Variables](#) into the message text.

Use the Test button to test the notification method.

## Account Numbers

Add or remove recipients using the same pager service.

- Name - Name of the person to be added to the list
- Pager Account Number - PIN (pager account number) for this person's pager.
- Add - Add the person to the list
- Remove - Select a name from the list and click the Remove Account button to remove it.

## Connection Settings

- Number of Retries - Enter the number of times to retry if the pager service is busy.
- Pager Script - Select a script for your pager service.

Use the Edit, Copy, and New buttons to create or edit Pager Script Settings.

## Pager Script

The Pager Notification includes many pre-defined Pager Scripts to be used as-is, or to be modified for your specific pager and pager service. To use a Pager Notification, a properly configured modem must be attached to the ELM Server computer and be available to the ELM Server application.

Pager Notification uses a script to define the communication protocol. Scripts are provided for Numeric, Alpha-Numeric, and SMS messaging. If the telecom service provider requires a variation of one of these protocols, the script allows you to customize communication in order to adapt to the protocol of your service provider.

### Note

For SMS messaging, the ELM Server will need a GSM/GPRS enabled modem connected to the computer hosting the ELM Server.

To customize the pager script settings, open the Pager Notification properties, go to the Connection Settings dialog, select the Pager Script you wish to modify, then click the Edit button.

### Note

It is best to make a backup copy of the current script before changing it. This will enable you to revert back to the original script if necessary.

### 1.4.7.2 Mail Notification

The Mail Notification sends event information in a mail message using the SMTP protocol.

#### Mail Message

- To - Enter the email address for the recipient(s). Multiple addresses must be separated by semi-colons (;).
- Subject - Enter the subject of the email message. You may use the Insert Variable button to insert [Environment Variables](#) to be substituted when the notification is sent.
- Message - Enter the message to send. You can use the Insert Variable button to insert Environment Variables to be substituted when the notification is sent.

Click the Test button to test the email settings and notification.

#### SMTP Host Tab

- SMTP Server - Enter the name or TCP/IP address of your SMTP Server.
- From - When using SMTP servers that have been configured to disallow relaying, you must use the From field. Using ELM@yourdomain.com, where yourdomain.com is a domain that is served by the SMTP server should be sufficient.

#### Mail Message Options Tab

- Max Message - Specify a maximum message size. By default, the message size is limited to 1,024 characters. Setting a lower value may be necessary for those email clients/devices (e.g., cell phone, etc.) that have limited viewing size. The message is truncated at the maximum size limit.
- Compress White Space - When this box is checked, all white space (CR/LF) is removed from the message before transmission. This removes line breaks in the message and reduces message size.
- Name - Enter a unique name.
- Description - Enter a description (optional).
- Enabled - The item can be enabled (checked) or disabled (unchecked). When disabled it is not active.
- Default - This child item will be automatically assigned when a parent item is created. In the case of Notification Methods, any newly created Notification Rules will have default Notification Methods automatically assigned.

#### Notification Rules

The Notification Rules that will trigger this Notification when the Notification Rule is satisfied. Right click to create or edit a Notification Rule.

#### Threshold

The [Threshold](#) settings for this Notification. The Threshold allows you to control how often the Notification is run.

#### Scheduled Hours

The Schedule setting for this Notification. The Schedule allows you to control when the Notification is run.

Select the times that this Notification is active. By default, the schedule is set to ON for all hours and all days. Mouse clicks toggle each time period ON and OFF. Clicking on an individual square will toggle the active schedule for that hour. Clicking on an hour at the top of the grid, or on a day of the week at the left of the grid will toggle the entire column or row. Keyboard equivalents are the arrow keys and the space bar.

## Properties Tab

This read-only tab displays the properties of the selected object and the values for those properties.

## 1.5 Results

The Results container in the ELM Console contains results of monitoring and management activities.

### Alert View

Displays all alerts generated by monitoring activity. The Alert View can be used as a status view for the ELM Server and ELM Agent. Alerts can be closed by right clicking the Alert so that the view is showing Alerts that haven't been remedied. Below each Agent computer is a Agent specific Alerts folder, showing Alerts for that Agent only. The Alerts folder under the Results folder displays all Alerts. Alerts are generated from the ELM Server process and from the Agents.

### Event Views

Event Views provide a mechanism for grouping events into a view that match one or more filters. Filters can be created and edited to fine-tune which events are displayed.

### Reporting

Access to [ELM Editor Reports](#).


### 1.5.1 Alert View

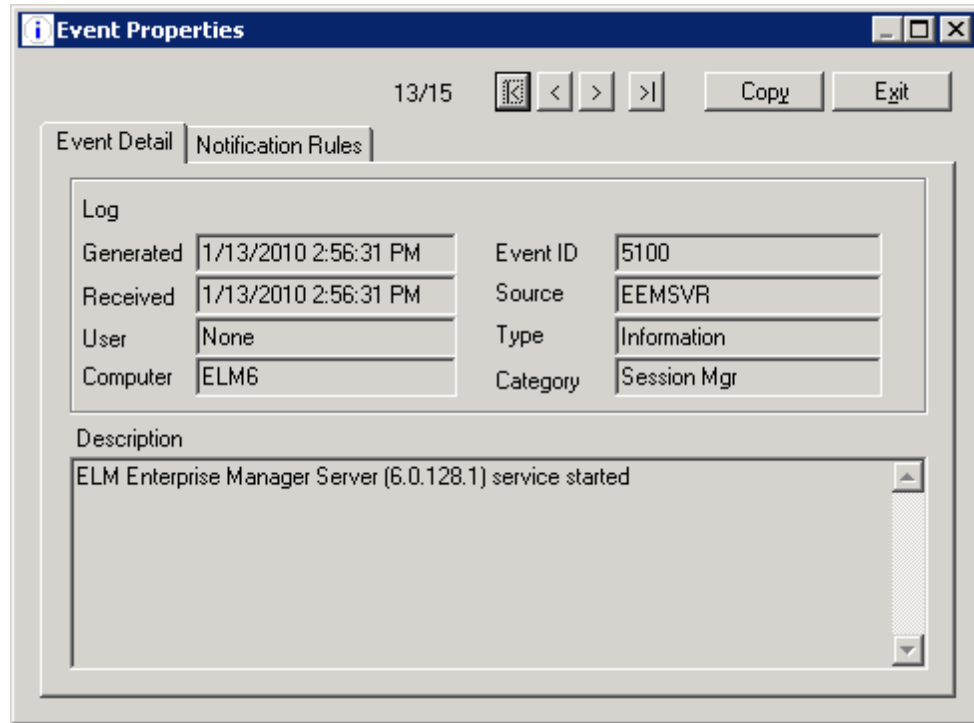
Provides details about an Alert. Right click the Alert to close it from the Alert View.

To view Alert Properties, expand the Results container, click on the Alerts container, then double-click on an Alert or select the Alert and choose Properties from the Action menu.

Alerts are stored in the TNTAlerts table in the ELM Server's database. Use the

[Database Connection Wizard](#) to configure pruning and archiving of Alert records.

The Alert Properties dialog includes navigation controls (  ) to browse Alerts.



Copy - Click the Copy button to place the Event Detail information on the Windows clipboard.

## Alert Details

In the properties of an Alert, the tab is named Event Details, and displays the following fields:

- Log - Does not apply to Alerts, only to Windows Events.
- Generated - Displays the time the event was created by the Monitor Item.
- Received - Displays the time the event was received by the ELM Server.
- User - Always displays None for Alerts.
- Computer - Identifies the computer being watched by the Monitor Item or ELM service that generated the Alert.
- Event ID - Determined by the application or process that created the alert.
- Source - Will be ELM Event Log Monitor 6, or TNTAGENT if a Service Agent generated the Alert.
- Type - Can be Error, Warning, or Informational.
- Category - Determined by the application or process that created the alert.
- Description - Determined by the application or process that created the alert.

## Notification Rules

Displays a list of the [Notification Rules](#) triggered by this Alert. Event Filters determine which Alerts trigger the Notification Rule. Editing Event Filters after the Alert has been received and processed by the ELM server may change the results displayed in this list.

To view properties of a Notification Rule, right click on the Notification Rule and select Properties from the menu.

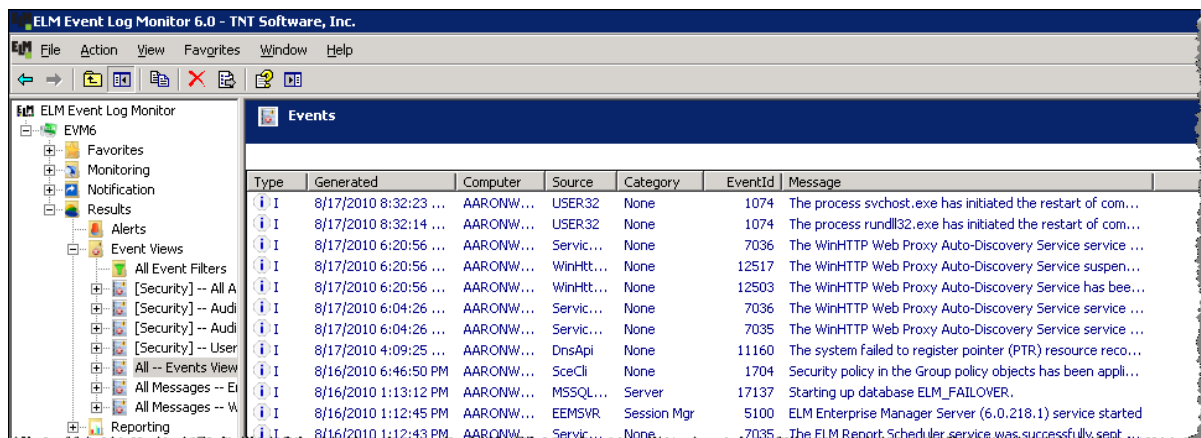
## 1.5.2 Event Views

Event Views allow you to group events into a View that matches one or more Filters. To conserve MMC resources, dynamic updating can be disabled via the [ELM Server applet](#) in Windows Control Panel.

Administrators can quickly diagnose problems by using Views to organize large amounts of event log information.

### Note

If no Event Filters are assigned to the Event View, then all events will be displayed by the View. If an Event is collected by an Event Collector but isn't associated with an Event View using an Include Filter, that event will be excluded from the database. We recommended you assign at least one Event Filter to each Event View.




ELM comes pre configured with a variety of Event Views. These Views are sorted into logical groupings. Views beginning with [Security] are configured to present security related information and are sorted to the top of the list. Views beginning with All represent general events grouped by type or protocol. Also see one of the Alerts containers for records created by ELM. Names can be modified for the requirements of a specific environment.

Open an Event View to see new events as they occur plus events that may be present from past database queries (view refreshes). The first time an Event View is

opened, a database query will be run if the Event View is empty. Otherwise, database queries are run only when a view is manually refreshed or when the properties of the view are modified. When an Event View is refreshed or an Event View's properties are modified, a database query is run and events from the database, as well as those streaming in, will be displayed.

- The combination of Event Filters applied to all Event Views determines which events are stored in the Events table in the ELM Server's database.
- **Events that are excluded from all Event Views will be excluded from the ELM Server database.**
- To collect events for notification or corrective action purposes only, and not for storage in the ELM Server's database, create one or more Event Filters with criteria isolating the events. Then checkmark these Event Filters on the Exclude Event Filters tab of all Event View property dialogs.

 Note

When viewing the Event Views container, the right pane (results pane) displays a list of Event Views with properties columns for each view. The Size column displays the number of items in the Event View (or in the Alerts container). The value for this column will be empty for each view until the Event View (or Alerts container) is opened, or until new events stream in. When the view is opened, a database query is run to update the Size column value. New events stream in even when the view has not been populated from the database.

An Event View has two display modes

- Detail Event View (default) which shows each event on a single line in the Event View.
- Summary Event View which displays a summary roll-up (i.e., count of events).

The Summary display mode groups records based on the following fields:

- Type
- Computer
- Source
- Category
- EventId
- UserName
- Log

In the properties of an Event View, you may enable the Security View Style on the Event View Settings tab. This view parses values from the Event Description field (e.g. Logon Type, Logon ID, etc.) as individual columns for easy sorting. It also allows you to customize views to display specific information that is normally buried within the security event log record.

When working with Event Views and event view columns, please be aware of the following:

- The MMC can maintain only one customized set of columns for all standard Event Views and one customized set of columns for all Event Views that use the Security View style. This means that changes made in one Event View will be reflected in the other Event Views that use the same style. Opening an Event View with a different security style setting will reset the customized display to show all available columns in both types of Event Views. If this happens, you can restore a previously customized Event View by closing and re-opening the ELM Console. Make sure to select No when prompted to Save the current console settings. If you select Yes, the previous customizations will be lost.

See Also


[Event View Settings](#)

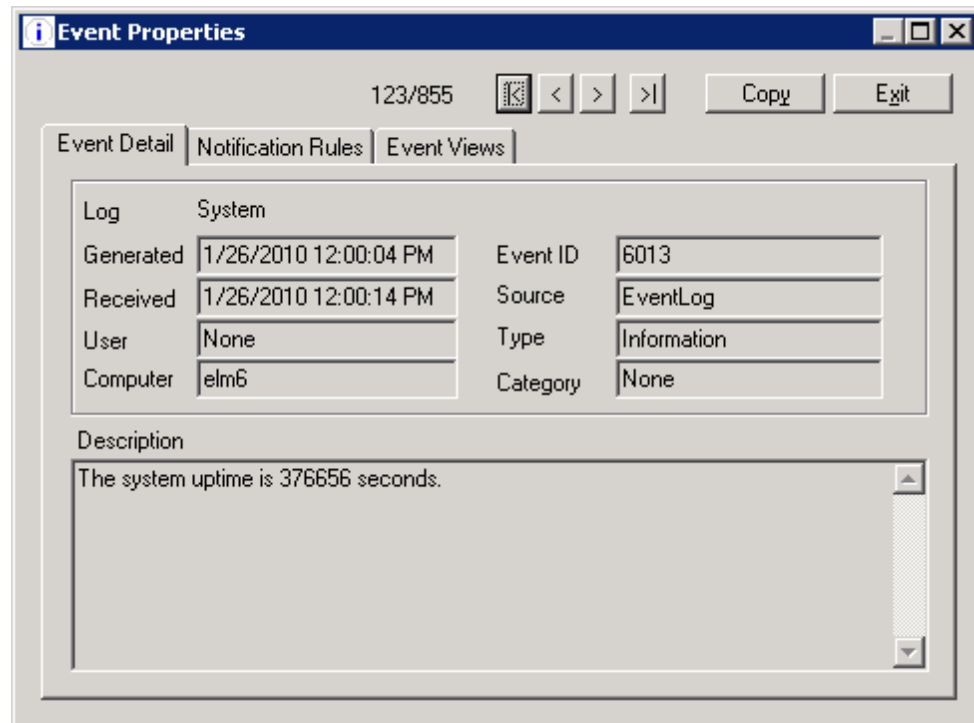
### 1.5.2.1 Event Properties

Provides details about an event.

To view Event Properties, expand the Results container, click on the Event Views container, and click on an Event View. On the right-hand side, double-click on an Event or select Event and choose Properties from the Action menu.

Events are stored in the TNTEvents table in the ELM Server's database. Use the [Database Connection Wizard](#) to configure pruning and archiving of Event records.

The Event Properties dialog includes navigation controls () to browse events in a collection of Events.



Copy - Click the Copy button to place the Event detail information on the Windows clipboard.

## Event Details

In the properties of an Event, the tab is named Event Details, and displays the following fields:

- Log - Displays the Windows log where the event originated.
- Generated - Displays the time the event was created in the event log.
- Received - Displays the time the event was received by the ELM Server.
- User - If available, displays the user from the event record.
- Computer - Identifies the computer where the event was collected.
- Event ID - Determined by the application or process that created the event.
- Source - Depends on the process that generated the event.
- Type - Can be Error, Warning, Informational, Failure Audit, Success Audit, Critical, or Verbose.
- Category - Determined by the application or process that created the alert.
- Description - Determined by the application or process that created the alert.

## Notification Rules

Displays a list of the [Notification Rules](#) triggered by this event. Event Filters determine which events trigger the Notification Rule. Editing Event Filters after the event has been received and processed by the ELM server may change the results displayed in this list.

To view properties of a Notification Rule, right click on the Notification Rule and select Properties from the menu.

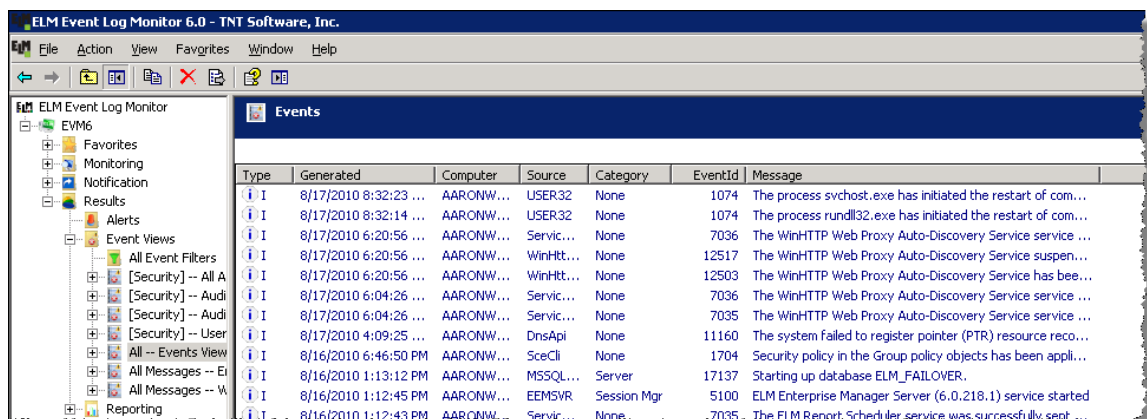
## Event Views

Displays a list of Event Views that will display this event. Event Filters determine which Event Views will display the event. Editing Event Filters after the event has been received and processed by the ELM server may change the results displayed in this list.

To view properties of an Event View, right click on the Event View and select Properties from the menu.

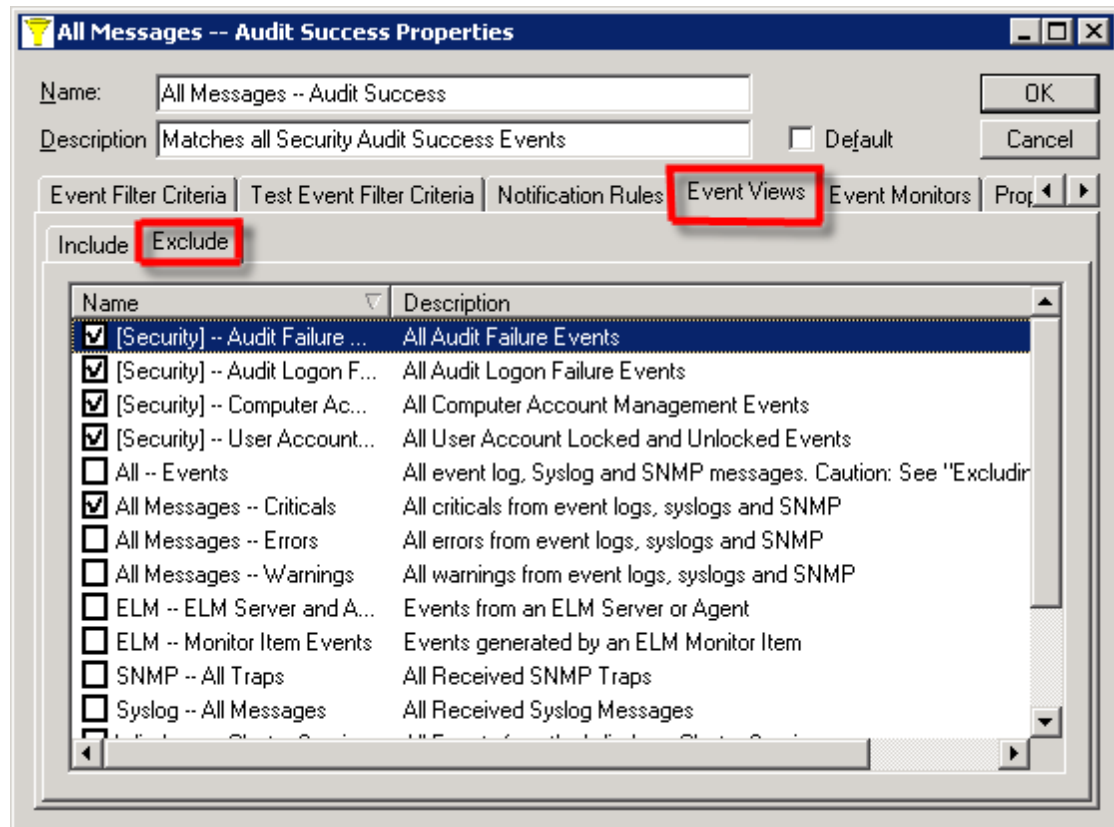
### 1.5.2.2 Event View Settings

After the initial database query, Event Views display events received by the ELM server. To conserve MMC resources, dynamic updating can be disabled via the [ELM Server applet](#) in Windows Control Panel.



Events are stored in the TNTEvents table in the ELM Server's database. Use the [Database Connection Wizard](#) to configure pruning and archiving of Event records.

Events that are excluded from all Event Views will not be stored in the ELM Server database. To collect events for notification purposes only, create one or more Event Filters with criteria to match the events. Then apply these Filters as Exclude Filters to all Event Views. This can be done through the Event Filter property dialog. Matching events will not to be stored in the ELM Server database.



**New** - To create a new Event View right-click the Event Views container and select New | Event View from the menu.

**Edit** - To edit properties of an Event View right-click the Event View and select Properties from the menu.

**Delete** - To delete an Event View right-click the Event View and select Delete from the menu.

## Event View Settings

The Event View Settings determine how Events are selected and displayed.

**View Style** - Check the Enable the Security View Style check box to specify that only security-related events (audit success and audit failure events) are displayed in the view, and that the view should use a security-centric layout to display critical security information from the events. This view displays values from the Event Description field (e.g., Logon Type, Logon ID, etc.) as individual columns for easy sorting. This allows you to customize Views with specific information that is normally buried within the security event log record.

Most security events will originate in the Security event log; however, some applications (such as Microsoft Exchange) can log security events to the Application event log. When the Security View Style is selected, it does not matter where the event originates. Any type of Audit Success or Audit Failure will be included in this view when this setting is enabled.

## Event Filters

- Select the Events must match all selected filters to be included radio button to include only events that match all of the assigned filters.

#### Notes

Exclude Filters are evaluated before the Include Filters. An Event that matches any of the Exclude Filters will not be displayed. This is a way to use multiple filters to display a focused subset of the events you want to isolate.

If no Event Filters are assigned to the Event View, then all events will be displayed by the View. We recommended you assign at least one Event Filter to each Event View.

- Select the Events matching one or more selected filters will be included radio button to include events that match at least one assigned Event Filter. Exclude Filters are evaluated before the Include Filters. An Event that matches any of the Exclude Filters will not be displayed.

#### Detail Event View Settings

- Max Events displayed specifies the maximum number of rows displayed in the Event View. You may select any value from 1 through 50000. The larger the number, the more memory the mmc.exe process will consume.

#### Date Range

- The From Date and To Date fields specify a date range. By default the To Date range is Now . New events that meet the filter criteria can be added dynamically to this view as they are received. You may select one of the pre-selected choices from the drop-down, or enter your own date range.

Caution: If the To Date is not set to Now, then new events might not be displayed in a View and will not be written to the database. We recommend you leave the All -- Events View set to Now and create a new Event View when you want to see older events.

#### Include Event Filters

Select the [Event Filters](#) that identify events to be displayed in this Event View.

- New Event Filter - Right-click an event filter and select New Event Filter to create a new Event Filter.
- Properties - Right-click an event filter and select Properties to edit or view the properties of an Event Filter.

#### Exclude Event Filters

Select the Event Filters that identify events to be displayed in this Event View.

- New Event Filter - Right-click an event filter and select New Event Filter to create a new Event Filter.
- Properties - Right-click and event filter and select Properties to edit or view the properties of an Event Filter.

## Properties Tab

This read-only tab displays the properties of the selected object and the values for those properties.

### 1.5.2.3 Event Filters

Filters are common objects within ELM and can be assigned to Notification Rules, Event Views, and to Event Collectors.

The primary contexts are the Include and Exclude tabs for [Notification Rules](#), [Event Views](#), and [Event Monitors](#). The Filter criteria entered by the user controls what events are gathered and displayed.

- Name - Enter a unique name.
- Description - Enter a description (optional).
- Default - This child item will be automatically assigned when a parent item is created. In the case of Event Filters, any newly created Event Views, Notification Rules, or Event Collectors will have the default Event Filter (child item)

automatically assigned.

## Event Filter Criteria

Event Filters provide a mechanism for isolating specific events, and multiple Event Filters can be combined to create a complex set of criteria. The same Filter can include or exclude events. They can also be created in the ELM Database Wizard to control database pruning, however these Filters will not be available in the Event Filter collections. Although filtered Alert views are not possible, Alert records can trigger Notification Methods if matching Filters and Notification Rules are configured.

The following fields are available for filtering purposes:

- Computer Name is
- Log Name is
- Username is
- Event Source is
- Event ID is
- Category is
- Message contains

This dialog box has a dynamic menu behavior. The ellipsis buttons next to the Computer Name is, Log Name is, and Event Source is fields browse and display the computer names, event log names and event sources. If the Computer Name is field is left empty, the list of event Logs and Sources is generated based on the event sources registered on the ELM Console computer (i.e., the local computer). If you enter a valid, resolvable name in the Computer Name is field and then click the ellipsis for the Log Name is or Event Source is fields, the list of event Logs and Sources from that system will be displayed. If the log or event source from which you want to collect data does not appear on the list, type it in the appropriate field. For example, if you are not running DNS on your ELM Server or Console, but want to collect events from the DNS log only, type *DNS* in the Log Name is field.

If a field is blank, it will match every value in the field. For example, if the Computer Name is field is blank, the Filter will apply to all computers. If all Event Types are unchecked when the Event Filter is saved, all of the Event Types will be checked. This is by design.

Leading and trailing wildcards ( \* ) and character position wildcards ( ? ) are supported, as are the Boolean operators Or ( | ), And ( & ), and Not ( ! ). However regular expressions are not supported. You may use these wildcards to specify the criteria to be applied. For example, to select messages from SQL Server you may specify \*SQL\* as the event source to select any Source name containing the letters SQL. To match SQL messages from servers ALPHA, BRAVO, or CHARLIE you would enter ALPHA|BRAVO|CHARLIE in the Computer Name is field.

**Important**  
Leave no white space adjacent to the operators.

**Note**  
If you enter the name of an untrusted system in the Computer Name is field and then use the ellipsis buttons for Log or Event Source, the menus will not be displayed. This is because authentication fails. To work around this problem, first make an IPC\$ connection to the target system using alternate credentials. For example, if the untrusted system's name is dArtagnan, you could use:

```
NET USE \\SERVERA\IPC$ /user:dArtagnan
\administrator *
```

You will be prompted for the password for the account you specify. The dynamic menu behavior will work after the IPC\$ connection has been established.

## Test Event Filter

Tests the filter to see which events pass the filter criteria.

You may specify the Computer name, Event Log, Event Source, and Event ID. You may also provide an Insertion string for the test. The insertion string is used for every parameter of the event description.

The Filter Status field displays whether or not an event matches the filter criteria after an Event ID is selected.

When testing event filters:

- You can test against all Event Filter Criteria fields *except* for the Category field. Event categories are determined at run-time by the application that generates them; consequently, you cannot use this field as a test criterion.
- The Computer Name field allows you to select any valid Windows workstation or server in order to select an event log, event source, and event from that computer. If you select an event log that does not also reside on the ELM Console computer, you will receive an error message stating that a file cannot be found. For example, if you are running the ELM Console on a Windows XP Professional machine and you select a Windows 2000 Active Directory domain controller, then select the Directory Service event log, you will receive an error message that ntdsmg.dll could not be found. This is because of an incorrectly parsed %systemroot% environment variable. This will occur only when the %systemroot% environment variable on the ELM Console is different from the variable on the server whose logs are being read.

## Notification Rules

Shows the Notification Rules associated with this Event Filter using an Include or Exclude relationship. Right click to create or edit a Notification Rule.

### Event Views

Shows the Event Views associated with this Event Filter using an Include or Exclude relationship. Right click to create or edit an Event View.

### Event Monitors

Shows the Event Collectors associated with this Event Filter using an Include or Exclude relationship. Right click to create or edit an Event Collector.

### Properties Tab

This read-only tab displays the properties of the selected object and the values for those properties.

## 1.5.3 Reporting

The ELM Editor reporting engine is located below the Reporting container in the ELM Console. From here, administrators can select from a variety of pre-configured Reports or create, manage, and run customizable reports.

### Getting Started

To create and run a custom report, right-click on ELM Editor and choose New Custom Report from the context menu. For more details, see the [ELM Editor Help](#) page.

#### 1.5.3.1 ELM Editor

Custom reports can be generated from the ELM Console by clicking on the ELM Editor container in the Results-->Reporting section of the ELM Console tree. Custom reports can be viewed through the ELM Console.

### Report Definitions

Report definitions can be modified by editing the appropriate custom report section. The custom reports generator is a graphical environment that allows the creation of SQL queries and displays the results in a chart, datagrid, or graph.

**Note**

For the purposes of this example, we will create a custom report for events. It requires a [Event Collector Monitor Item](#) and some data collected by this Monitor Item.

1. Right-click on the ELM Editor container and choose New Custom Report. The Report Section Properties dialog will open.
2. Accept the defaults for Section Style, Section Title, Section Description, and Row Grid Options. Click Next.
3. The Query Builder dialog opens. Select the tabs to see details on the SQL query as presented by the Query Builder, SQL Text, Performance of the query, and any Error Messages about the query. Select Finish to save the report.
4. The report will be named New Report by default. Right-click the report and select Rename to change the report name.

Additional report sections may be added by right-clicking on the report and selecting Edit --> Add Section from the context menu. Existing report sections may be modified by right-clicking on the section and selecting Edit-->Properties from the context menu.

Another method for creating custom reports is to base them on Event Views. To generate a custom report based on an existing Event View:

- Expand the Results container | Event Views container and choose an Event View on which to base a custom report. Right-click the Event View and choose New-->New Custom Report.

These Custom Reports may be edited or modified like any other custom report.

**Note**

When editing SQL queries, if column aliases are used, avoid exotic characters. Instead, select from the following characters: % \* ( ) - \_ /

For example:

```
select TNTTimeGenerated as [Date - Time],
       PDLogicalDisk as [% Free],
       PDTemperature as [Temp (F)] from TNTTables
```

## Viewing Reports

Reports can be viewed through the ELM Console.

To view a report

1. Click on the ELM Editor container to view available custom reports.
2. Expand the ELM Editor container.

3. Click on the report name to view the report sections in the right-hand pane.

## Using the report viewer

Sections of a Custom Report may be expanded or collapsed by clicking the arrow icon near the right edge of the report section title bar.

Reports may be saved by right-clicking on the Report and selecting Save As... from the context menu.

## Managing Scheduled Reports

Scheduling reports allows you to run the report at regular intervals.

To Open the custom report scheduler:

1. Right-click on the custom report you wish to schedule.
2. Choose Schedule Report, and the Custom Report Schedule Wizard dialog will appear.
3. Select the frequency you desire the report to run (Schedule Type).
4. Select the time of day you wish the report to run (Run at).
5. Select the starting day for the schedule (On).
6. Select the days you want the report to run (Days). Click Next.
7. Select the delivery Method for the report (Type). Options are e-mail, File, and Database. Further options depend on the Type selected.
  - If e-mail is selected, enter the recipient's e-mail address and the Mail Server name or IP address.  
Multiple recipients must be comma delimited.
  - If File is selected, enter the path to the file storage location.
  - If Database is selected, no additional options are available. The report will be stored in the ELM Primary database.
9. Click Finish.

### Note

Variables can be used in the Directory and Name fields. Using variables, you may replace or create new files as needed. To replace files, ensure the name will be identical each time the report is run. To create new files, ensure it is different by using the appropriate variables. Possible variables: %ELMInstallPath%, %ReportName%, %Time%, %Month%, %Year%, %Day%. A network directory can be used as well.

## To Change a Report Schedule

1. Under Report Schedules, right-click on the Custom Report and select Properties.
2. Enter values for the Scheduler Wizard dialogs as in the above steps 4-9.

## To Delete a Report Schedule

1. Select the Report Schedules node.
2. Right-click on the undesired schedule.

3. Select Delete from the context menu.

## Viewing Completed Reports

Schedule status and completed reports can be viewed in the Report Schedules node.

To view a report through the Report Schedules node:

1. Expand Results-->ELM Editor and select Report Schedules in the navigation tree.
2. On the right-hand side, click on View Results for any completed reports.

## 1.6 Database Settings

Configuring the ELM Server Databases

During installation, ELM requires two databases, a primary and a failover database. These databases can be in any combination of:

- Microsoft SQL 2000, Microsoft SQL 2005, Microsoft SQL 2005 Express, Microsoft SQL 2008, Microsoft SQL 2008 Express, Microsoft SQL 2008 Express R2, Microsoft SQL 2008 R2.
- the same instance or separate instances
- local to the ELM Server computer or on a computer available on the network
- default instances or named instances

ELM will need write permissions so that it can create the databases. Given an instance and permissions, ELM will create the database, tables, indices, and constraints required.

**Important**  
ELM requires a case-insensitive sort order for SQL Server. This means you cannot use case-sensitive or binary sort orders on the SQL Server used for your ELM Server databases.

### Database Settings Wizard

The Database Settings Wizard is used to configure database connections, archiving, and [pruning](#). To open the Database Settings Wizard right click on the ELM Server computer name and select All Tasks | Database Settings from the menu.

When entering the SQL Server name for the ELM databases, the name can use one of 4 possible formats as described below.

For a default instance of SQL

For a default instance listening on a

listening on default port 1433, use just the servername. For example:

The screenshot shows a 'Wizard' window titled 'Primary Database'. Below the title bar, it says 'Complete this form to configure the primary SQL'. There are two main sections: 'Name' and 'Database'. Under 'Name', the 'Server:' field contains 'SQL-SERVER' and has a 'Browse...' button to its right. Under 'Database', there is a dropdown menu with 'ELM\_PRIMARY' selected and a 'Create' button to its right.

custom port, use servername,portnumber. For example:

The screenshot shows a 'Wizard' window titled 'Primary Database'. Below the title bar, it says 'Complete this form to configure the primary SQL'. There are two main sections: 'Name' and 'Database'. Under 'Name', the 'Server:' field contains 'SQL-SERVER,14330' and has a 'Browse...' button to its right. Under 'Database', there is a dropdown menu with 'ELM\_PRIMARY' selected and a 'Create' button to its right.

For a named instance listening on default port 1433, use servername\instancename. For example:

The screenshot shows a 'Wizard' window titled 'Primary Database'. Below the title bar, it says 'Complete this form to configure the primary SQL'. There are two main sections: 'Name' and 'Database'. Under 'Name', the 'Server:' field contains 'SQL-SERVER\INSTANCE' and has a 'Browse...' button to its right. Under 'Database', there is a dropdown menu with 'ELM\_PRIMARY' selected and a 'Create' button to its right.

For a named instance listening on a custom port, use servername\instancename, portnumber. For example:

The screenshot shows a 'Wizard' window titled 'Primary Database'. Below the title bar, it says 'Complete this form to configure the primary SQL'. There are two main sections: 'Name' and 'Database'. Under 'Name', the 'Server:' field contains 'SQL-SERVER\INSTANCENAME,14330' and has a 'Browse...' button to its right. Under 'Database', there is a dropdown menu with 'ELM\_PRIMARY' selected and a 'Create' button to its right.

**Note**

This syntax for SQL Server name can be used for all 3 ELM databases: Primary, Failover, and the optional Archive database.

### Primary Database

The primary database is the database used by ELM for storing data gathered from monitored systems. Types of data collected include:

- Windows event log entries
- ELM Alerts
- Alerts generated by the ELM Server

Event-type data is stored in a group of tables beginning with TNT in the name.

### ELM Database Authentication

ELM can authenticate to the database using either Windows Authentication (recommended) or SQL Authentication. With either type of authentication, the ELM Server service will need DDL permissions like create databases, tables, and views, and DML permissions like select, insert and delete records. These permissions are inherited when the db\_owner role is assigned to a user account in SQL Management Studio.

### ELM Database Service Dependency

If the ELM Server is installed on the same computer as the database, an optional service dependency of ELM depending on SQL can be created. With this in place, the ELM Server will wait for SQL Server to startup before trying to start (and connect to the database). This will help avoid database failovers if the ELM Server starts faster than SQL Server.

### Install Maintenance Microsoft SQL job

An optional database maintenance plan can be created for the ELM primary database. The plan will perform integrity checks on the database, backup the transaction log, rebuild indexes to optimize the database, and backup the database. More details about the SQL job can be found in the TNTDatabaseMaintenancePlan.sql script in the ELM install folder.

#### Note

The database maintenance job requires the SQL Server Agent service be started.

### Failover Database

The ELM Server has built-in database failover protection to minimize data loss in the event the ELM Server's primary database is unavailable. During normal operation, there will be no tables created in this database by ELM. When ELM is using the failover database, tables will be created as necessary .

When the ELM Server detects a connectivity problem with its primary database, ELM will log the following event:

Event Type: Warning  
Event Source: EEMSVR  
Event Category: None  
Event ID: 5214  
Date: 4/26/2008  
Time: 1:15:02 PM  
User: N/A  
Computer: ELMSERVERCOMPUTER  
Description: A critical database failure occurred and the temporary database ELM\_FAILOVER on SQLSERVER\INSTANCENAME has been enabled. Data in this temporary database will be merged with the configured database when it becomes

available. Error: 0x80004005, Microsoft OLE DB Provider for SQL Server, [DBNETLIB][ConnectionOpen (Connect()).]SQL Server does not exist or access denied. SQL Error: 0x00000011, 08001

When this happens, ELM begins using the configured failover database and stores data in matching table names. When connectivity to the primary database is restored, the following event will be logged:

Event Type: Information  
Event Source: EEMSVR  
Event Category: None  
Event ID: 5216  
Date: 4/26/2008  
Time: 1:22:22 PM  
User: N/A  
Computer: ELMSERVERCOMPUTER  
Description: The configured database has returned on-line. Temporary data written to ELM\_FAILOVER on SQLSERVER\INSTANCENAME is now being merged with the database.

When ELM has completed merging data back into the primary database, the tables in the failover database will be deleted and the following event will be logged:

Event Type: Information  
Event Source: EEMSVR  
Event Category: None  
Event ID: 5217  
Date: 4/26/2008  
Time: 1:22:26 PM  
User: N/A  
Computer: ELMSERVERCOMPUTER  
Description: Success, recovery attempt completed for the database.  
Table: TNTAlerts  
Status: Success  
Rows processed: 1 [Succeeded: 1 Duplicate: 0 Failed: 0]  
Processing Time: 0h:0m:1s  
Table: TNTEvents  
Status: Success  
Rows processed: 112 [Succeeded: 112 Duplicate: 0 Failed: 0]  
Processing Time: 0h:0m:1s  
Table: TNTSecurity  
Status: Success  
Rows processed: 38 [Succeeded: 38 Duplicate: 0 Failed: 0]  
Processing Time: 0h:0m:1s  
Total Processing Time: 0h:0m:3s

All data written to the failover database will be automatically merged into the primary database.

**Note**

The ELM Server will try once to failback the temporary database and merge with its original database. If this process fails, tables in the failover database will be renamed ERR%y% m%d-%H%M%S, where %y%m%d-%H%M%S represents the Year, Month, Day, Hour, Minute, Second at which the renaming took place.

During database failover, it is possible for Events or Alerts to appear in the ELM Console that are stored only in the ELM Server's primary database, and not in the temporary database. An attempt to open one of these items will fail because the record will not be in the database currently in use. When the database has failed back to the primary database, all Alerts and Events will be accessible.

#### ELM Database Authentication

ELM can authenticate to the database using either Windows Authentication (recommended) or SQL Authentication. With either type of authentication, the ELM Server service will need DDL permissions like create databases, tables, and views, and DML permissions like select, insert and delete records. These permissions are inherited when the db\_owner role is assigned to a user account in SQL Management Studio.

#### ELM Database Service Dependency

If the ELM Server is installed on the same computer as the database, an optional service dependency of ELM depending on SQL can be created. With this in place, the ELM Server will wait for SQL Server to startup before trying to start (and connect to the database). This will help avoid database failovers if the ELM Server starts faster than SQL Server.

### Archive Database

The Archive database is an optional database that can be used to minimize the size of the ELM primary database, improving the responsiveness of the ELM Console. There is also a rollover option to provide generational archives. Once the archives are created, the ELM Console can be connected to these historical databases for ad hoc reports or forensic investigation. The Server can be a local or remote Microsoft SQL instance. If a named instance of SQL is used, enter the server name using the pattern: servername\instancename. It is not required that the Database be created ahead of time; ELM can create the database and tables if it has adequate permissions to SQL. The Browse button will scan the local network for instances of SQL and provide a list. The Create button will provide options for setting data and transaction log initial sizes and growth characteristics.

#### ELM Database Authentication

ELM can authenticate to the database using either Windows Authentication (recommended) or SQL Authentication. With either type of authentication, the ELM Server service will need DDL permissions like create databases, tables, and views, and DML permissions like select, insert and delete records. These permissions are inherited

when the db\_owner role is assigned to a user account in SQL Management Studio.

### ELM Database Service Dependency

If the ELM Server is installed on the same computer as the database, an optional service dependency of ELM depending on SQL can be created. With this in place, the ELM Server will wait for SQL Server to startup before trying to start (and connect to the database). This will help avoid database failovers if the ELM Server starts faster than SQL Server.

## 1.6.1 Database Pruning

### Database Pruning and Archiving

Space limitations may require that database records be periodically archived or erased. Use the Database Settings Wizard to configure database connections, archiving, and pruning.

#### Alerts and Events Data

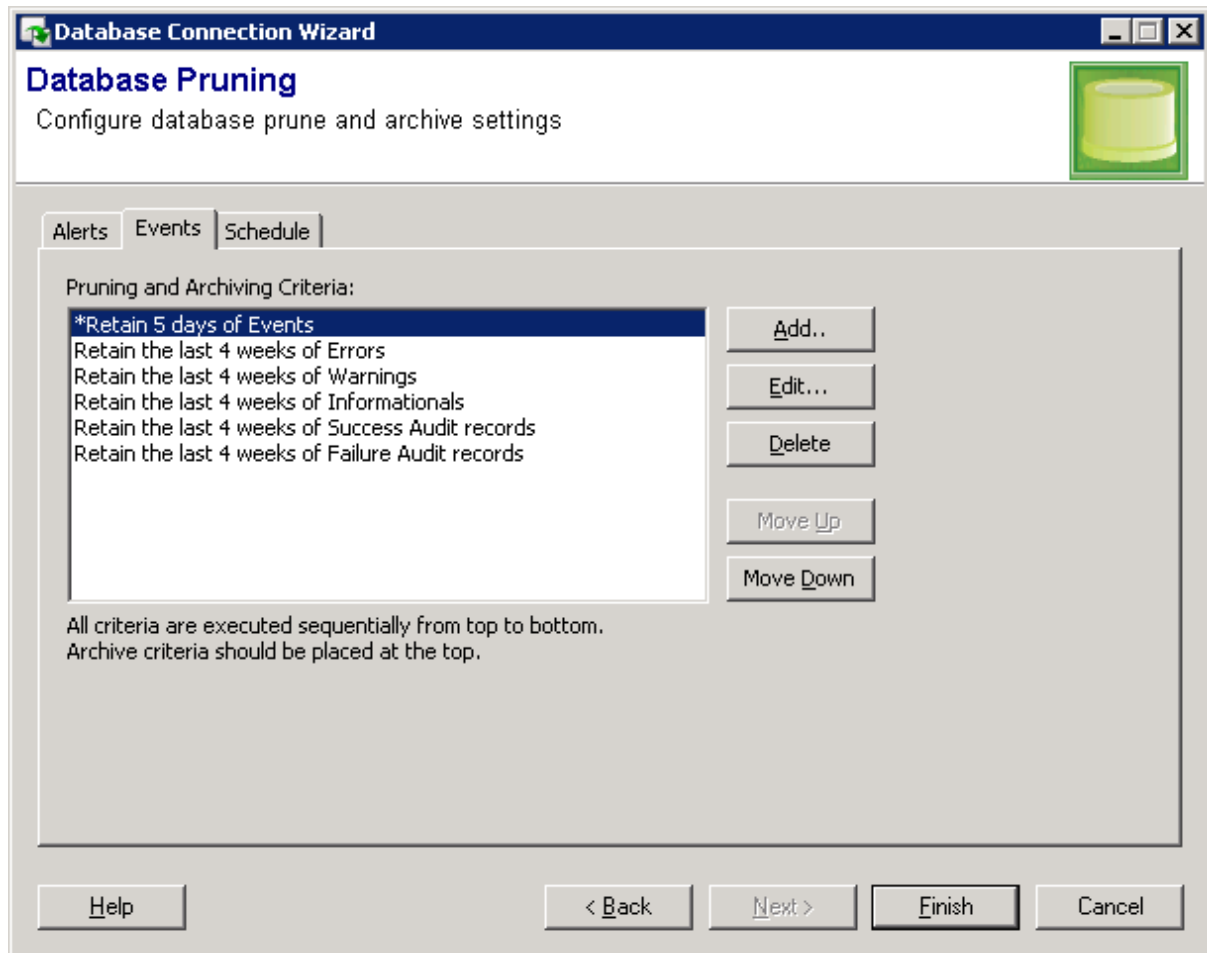
Event log records and Alerts produce a high volume of data. It is recommended that you add Pruning and Archiving Criteria to periodically archive and/or prune (erase) out-dated or unneeded records. Informational, Warning, and Error events might be pruned after one week. Audit Success and Audit Failure events may require longer retention.

#### Database Pruning

There are up to three databases configured for the ELM Server: primary, failover, and archive (optional). Alerts and Events can be copied to the archive database and then pruned from the primary database, or they can be pruned without archiving.

The Pruning and Archiving Criteria filters determine which records are pruned, at what age, and if they are to be archived before pruning. The filters are processed sequentially from top to bottom. This provides the ability to archive and prune selected records, followed by pruning all remaining records. For example, the first (top) Filter could archive and then prune all ELM error alerts. Then a second Filter could prune all remaining alerts without archiving. To enable archiving of all pruned records, place a checkmark in the Archive checkbox on the Retention tab.

Many customers are surprised by the large volume of data generated by Windows events. To help customers avoid bloated databases, a default installation of ELM is configured for aggressive pruning. As the image below, all events will be pruned after 5 days. To allow longer data retentions, the top filter (marked by an asterisk) can easily be selected and deleted.



The last 5 event pruning Filters in the image above are somewhat redundant, but are purposely setup this way to demonstrate the granularity possible with pruning and to simplify rollover Archive databases. All the Filters are setup to archive data if an Archive database is available. If events do not need to be archived, for example informational events, then the "Informationals" Filter can be easily modified without effecting the archiving of Errors, Warnings, and Audit events. With all 5 event types set to prune at 4 weeks, this simplifies forensic investigation into rollover Archive databases. In contrast, if the main purpose of events is for more immediate use from the ELM primary database, then you may prefer to prune Informational events sooner, and extend the retention of Audit records.

- Add - Add a new pruning criteria.
- Edit - Edit the selected pruning criteria.
- Delete - Delete the selected pruning criteria.
- Move Up - Move the selected pruning criteria up in the list.
- Move Down - Move the selected pruning criteria down in the list.

The Retention period for Alerts and Events controls the age of records in the ELM primary database. The Retain options can be described as follows:

- Retain 1 day = keep the records for 24 hours (to the second) each time the scheduler runs
- Retain 1 week = keep the records for 7 days (to the second)

- Retain 1 month = keep the records for 1 month (same day of last month at the same time)
- Retain 1 quarter = keep the records for 3 months
- Retain 1 year = keep the records for 12 months

For example, if the scheduler runs at 28 July 2007 at 10:21:13 AM:

- Retain 1 day will prune any data with a timestamp before 27 July 2007 at 10:21:13 AM
- Retain 1 week will prune before 21 July 2007 at 10:21:13 AM
- Retain 1 month will prune before 28 June 2007 at 10:21:13 AM
- Retain 1 quarter will prune before 28 April 2007 at 10:21:13 AM
- Retain 1 year will prune before 28 July 2006 at 10:21:13 AM

### Event Filter Criteria

The following fields are available for filtering purposes:

- Computer Name is
- Log Name is
- Username is
- Event Source is
- Event ID is
- Category is
- Message contains

This dialog box has a dynamic menu behavior. The ellipsis buttons next to the Computer Name is, Log Name is, and Event Source is fields browse and display the computer names, event log names and event sources. If the Computer Name is field is left empty, the list of event Logs and Sources is generated based on the event sources registered on the ELM Console computer (e.g., the local computer). If you enter a valid, resolvable name in the Computer Name is field and then click the ellipsis for the Log Name is or Event Source is fields, the list of event Logs and Sources from that system will be displayed. If the log or event source from which you want to collect data does not appear on the list, type it in the appropriate field. For example, if you are not running DNS on your ELM Server or Console, but want to collect events from the DNS log only, type DNS in the Log Name is field.

If a field is blank, it will match every value in the field. For example, if the Computer Name is field is blank, the Filter will apply to all monitored computers. If all Event Types are unchecked when the Event Filter is saved, all of the Event Types will be checked. This is by design.

Leading and trailing wildcards ( \* ) and character position wildcards ( ? ) are supported, as are the Boolean operators Or ( | ), And ( & ), and Not ( ! ). However regular expressions are not supported. You may use these wildcards to specify the criteria to be applied. For example, to select messages from SQL Server you may specify \*SQL\* as the event source to select any Source name containing the letters SQL . To match SQL messages from servers ALPHA, BRAVO, or CHARLIE you would enter ALPHA|BRAVO|CHARLIE in the Computer Name is field.

**Important**  
Leave no white space adjacent to the operators.

**Note**  
If you enter the name of an untrusted system in the Computer Name is field and then use the ellipsis buttons for Log or Event Source, the menus will not be displayed. This is because authentication fails. To work around this problem, first make an IPC\$ connection to the target system using alternate credentials. For example, if the untrusted system's name is SERVERA , you could use:

```
NET USE \\SERVERA\IPC$ /user:SERVERA\administrator *
```

You will be prompted for the password for the account you specify. The dynamic menu behavior will work when the IPC\$ connection has been established.

## Retention

The Retention tab controls the amount of time that events or alerts are kept in the primary ELM database. Records older than the age specified in this window are deleted at the Scheduled Interval and Scheduled Hours selected in the Schedule dialogs.

**Retain** - Enter the amount of time to keep data in the ELM primary database.

**Archive** - If Archive is enabled (checked), pruned records will be copied to the [Archive Database](#) before deletion from the Primary database. The Archive checkbox is disabled (grayed out) if the archive database has not been configured.

## Schedule

These tabs control how frequently ELM will try to prune old data, and what hours during the week it is allowed to prune.

**Scheduled Interval** - This setting controls how often ELM will try to prune old data. In general, if the Scheduled Interval has elapsed, and if the Scheduled Hours are *on* (allow pruning), then ELM will prune old data.

**Scheduled Hours** - This setting controls which hours during the week ELM is allowed to prune data. If the Scheduled Interval has passed, but Scheduled Hours are *off*, then ELM will check approximately every 15 seconds until Scheduled Hours are *on*, and then it will begin pruning data.

So if the Scheduled Interval is set to 1 day, and if the Scheduled Hours are *on* 24/7, then ELM will prune at midnight each day. If the Interval is 1 day, and the Scheduled Hours are *on* only from 4:00 a.m. to 5:00 a.m., then ELM will prune just

after 4:00 a.m.

## Additional Information

If [Logging Level](#) is set to high, the ELM Server writes events at the beginning and end of pruning steps. Events will be written to the Application log, and will be similar to the examples below.

```
Event Type: Information
Event Source: EEMSVR
Event Category: None
Event ID: 5224
Date: 12/3/2008
Time: 1:41:45 PM
User: N/A
Computer: SERVER1
Description: Database pruning on tablename has begun.
```

```
Event Type: Information
Event Source: EEMSVR
Event Category: None
Event ID: 5218
Date: 12/3/2008
Time: 1:41:45 PM
User: N/A
Computer: SERVER1
Description: ELM prune tablename records completed.
```

Where *tablename* is one of the following:

- TNTAlerts
- TNTEvents

## 1.7 ELM Server

[Contents](#)

[ELM Server Properties](#)

Describes the ELM Server Properties dialog.

[ELM Server Control Panel Applet](#)

Describes the ELM Server Control panel applet.

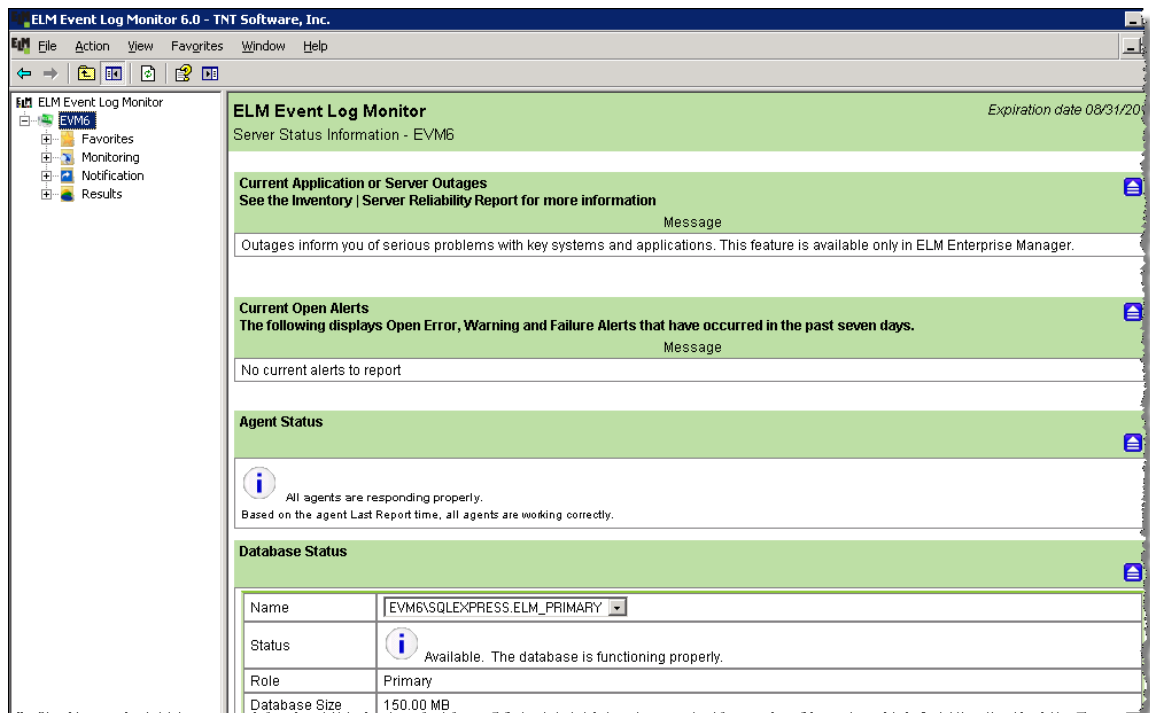
## 1.7.1 ELM At A Glance

### New Default ELM Install Folder

When ELM 6.0 is installed for the first time on a computer, the default install folder for a 32 bit system is: c: \ Program Files \ ELM Event Log Monitor and for a 64 bit system: c: \ Program Files (x86) \ ELM Event Log Monitor.

### At a Glance

A global view of ELM monitoring can be displayed by selecting the ELM Server root node in the console tree. It shows a summary of application or system outages (available only in ELM Enterprise Manager), Alerts from all monitored systems, and the status of Agents, ELM Database, and ELM Server.



- **Current Alert Entries** - Displays a summary of the current Open alerts. Alerts are created by the ELM Server as problems arise. Alerts are managed (Closed) using the Status menu option in the Alerts container. Click on the Show Details option to see all the entries.
- **Agent Status** - Displays if an Agent is not responding or it is sending information to the ELM Server that it is not working properly.
- **ELM Database Status** - Displays the current status of the database. If a database is nearing capacity or it is offline, an alert appears here indicating the issue. Click on Show Details to see the database settings and how much space is being used by each database.
- **ELM Server Status** - Displays the current system resources in use by the ELM Server.

## 1.7.2 Server Properties

The ELM Server properties dialog displays diagnostic and licensing information about the ELM Server.

### Modules

This tab displays module (DLL), process, thread, and other diagnostic information about the [ELM Server](#) and [ELM Console](#).

To view the Modules tab:

1. Open the ELM Console.
2. Right-click on an ELM Server and select Properties.
3. Click on the Modules tab.

To copy the Module information:

1. Right-click anywhere in the module details.
2. Click Select All to highlight all the module details.
3. Right-click the highlighted area and click Copy.
4. Open a text editor and paste the module details to a text file.

You can gather additional diagnostic information through the Server Properties Diagnostic tab.

### Diagnostics

The Start Diagnostics button launches the ELM Diagnostics Tool (TNTDiag.exe).

The ELM Diagnostic Tool (TNTDiag) is a troubleshooting tool used to trace some or all activity of an ELM Server, an ELM Console, and/or a Service Agent. The diagnostic output produced by this tool is intended for TNT Software's Product Support Group. This tool adds overhead to the system and should be used only under the direction of TNT Software support personnel.

TNTDiag installs itself as a service when performing its operations. It can be used by administrators only. TNTDiag requires version 3 of Microsoft's XML parser (MSXML3.DLL) in order to save trace files. This file is present by default in Windows XP Professional, Windows Server 2008, and Windows Server 2008. On Windows 2000 systems, it can be installed by installing MDAC 2.7 SP1 or later, or Internet Explorer 6.0 or later.

TNTDiag can also be started from a command prompt. This enables starting a diagnostic trace from a Windows scheduled task. Syntax is:

```
/Quiet - Starts a TNTDiag trace using the options in TNDiagConfig.xml  
/Save - Saves a currently running TNTDiag trace started using the Quiet  
command line
```


/Stop - Stops and saves a currently running TNTDiag trace started using the Quiet command line

/? or H[elp] - Display this text and exit

To view the Licensing tab:

1. Open the ELM Console.
2. Right-click on an ELM Server and select Properties.
3. Click on the Licensing tab.

The number of Agents in-use and total number of Agents for the license, by class, are displayed in the Licensing dialog. The Quantity shows how many licenses are available for each class and it also shows that no licenses are in use.

License	Quantity	In Use
 Class I Basic (Bcl)	20	0
 Class II Basic (Bcll)	5	0

If you have any licensing or registration questions, please contact TNT Software's Sales Department: [Sales@TNTSoftware.com](mailto:Sales@TNTSoftware.com).

## About

Displays a splash screen with current release information.

## Properties Tab

This read-only tab displays the properties of the selected object and the values for those properties.

### 1.7.3 Control Panel

The ELM Server includes the ELM Control Panel applet, which appears in the Windows Control Panel. To access it, open Control Panel and choose the ELM Event Log Monitor 6.0 applet.

**Note**  
For Windows 2003 64bit systems, in the control panel, the ELM applet is located under the "View x86 Control Panel Icons".

It has the following tabs:

## Options

ELM Server Listen Port - Enter the port number on which the ELM Server listens. By default, an ELM Server will listen on port 1251.

Real-Time Console - Toggle the streaming of new events from the ELM Server to the ELM Console on and off. When this checkbox is checked, Event Views in the ELM Console are database driven and must be manually refreshed in order to display data. When this checkbox is empty, events stream into and are displayed in the ELM Console as they are received by the ELM Server.

## Logging

The options on this tab allow you to specify the level and type of logging you want the ELM Server to perform. There are several logging options available:

### Logging Level

Set the level of logging activity to one of four pre-defined settings. In general the four levels control logging by event type as indicated below.

- None - No logging.
- Low - Log errors only.
- Medium - Log errors and warnings.
- High - Log errors, warnings and informational events.

### Specify where to log the activity and error information.

Use the checkboxes to select the location for the log information. You may specify multiple locations. Your choices are:

- Log to server's Application Event Log
- Log internal errors as Alerts
- Log to File (in server's Application directory)
- Enter a file name. If you log activity to a file, click the View button to open and view the log file. This button is only available when logging to a file.

## Diagnostics

The Start Diagnostics button launches the ELM Diagnostics Tool (TNTDiag.exe).

The ELM Diagnostic Tool (TNTDiag) is a troubleshooting tool used to trace some or all activity of an ELM Server, an ELM Console, and/or a Service Agent. The diagnostic output produced by this tool is intended for TNT Software's Product Support Group. This tool adds overhead to the system and should be used only under the direction of TNT Software support personnel.

TNTDiag installs itself as a service when performing its operations. It can be used by administrators only. TNTDiag requires version 3 of Microsoft's XML parser (MSXML3.DLL) in order to save trace files. This file is present by default in Windows XP Professional, Windows Server 2008, and Windows Server 2008. On Windows 2000 systems, it can be installed by installing MDAC 2.7 SP1 or later, or Internet Explorer 6.0 or later.

TNTDiag can also be started from a command prompt. This enables starting a diagnostic trace from a Windows scheduled task. Syntax is:

```
/Quiet - Starts a TNTDiag trace using the options in TNDiagConfig.xml
/Save - Saves a currently running TNTDiag trace started using the Quiet
command line
/Stop - Stops and saves a currently running TNTDiag trace started using the
Quiet command line
/? or H[elp] - Display this text and exit
```

## Database

This tab displays current database configuration information. You may click the Database Wizard button to launch the Database Wizard.

## 1.8 Technical Resources

### Online Reference

TNT Software Support  
(<http://www.tntsoftware.com/support>)

Support Knowledge Base  
(<http://www.tntsoftware.com/support/kba>)

Software Prerequisites and Downloads  
(<http://www.tntsoftware.com/elmsupport/supplementaldownloads.htm>)

### Command Line Reference

[ELM Server Command Line Options](#)

### Registry Settings

[ELM Server Registry Entries](#)

[ELM Console Registry Entries](#)

[ELM Service Agent Registry Entries](#)

### 1.8.1 Glossary

Actions	Actions are a form of response executed by a Monitor Item and
---------	---

	occur as a result of changing conditions observed by the Monitor Item. There are four Actions that can be executed: generate Alert, generate application event log message, send a Network Pop-up Message, or execute a script.
Agent Categories	Categories are user configurable containers for organizing ELM Agents. Monitor Items are assigned to Categories which then assign them to any Agents in the Category.
Agent Deployment Wizard	Agent Deployment Wizard allows installation of multiple Agents using lists generated from Active Directory, an IP Address range, or a text file of computer names.
Agents	Agents are the fundamental component for identifying the devices to be monitored. ELM pricing is based on the License and Class of the Agent. There are 4 licenses: System, Log, Performance, and Event. There are 2 classes: Class I = Windows Server and Windows Cluster Server Systems and Class II = Windows Workstation and non-Windows Systems.
Alerts	Alert is a special type of event that can be generated from a Monitor Item or by the Alert Notification Method. Alerts are stored in the TNTAlerts database table and displayed in the Alerts containers within the ELM Console. Alerts can be given a status of 'open' or 'closed.'
At-a-Glance	At-a-Glance views are a summarization of overall status information for the ELM Server, Agents, Application Outages, Inventory, and System Information.
Containers	Container is a general term and is found on the left-hand side of the ELM Console. They are typically, but not always, shown as a folder icon with an overlaid design. Agent Categories are a special class of container.
DDL	Data Definition Language (DDL) is used to define and manage objects in SQL. See SQL Books On Line (BOL) for more details.
DML	Data Manipulation Language (DML) is used to retrieve and manipulate data. See SQL Books On Line (BOL) for more details.
ELM Console	ELM Console refers to the snap-in that resides in a Microsoft Management Console and is the primary user interface for the product. Each snap-in can connect to multiple ELM Servers, and the ELM Console stand alone snap-in can be co-mingled with other MMC snap-ins to provide single-seat administration.
ELM Editor	ELM Editor refers to a report creation tool that can build custom reports. Reports can be generated both on an ad hoc basis and at periodic intervals, and then output as a web archive file (.mht), e-mailed, or stored in the ELM database.
ELM Server	ELM Server is comprised of several engines that handle tasks such as creating and maintaining a database for data storage, archiving and reporting, managing Agents and Agent licensing, processing Event Filters and Rules, and executing Notification Methods.
ELM Server Database	ELM Server Database contains data collected from Agents, Alerts generated by Actions and the Alert Notification Method, System Configuration, Inventory, Outage information, and when configured, ELM Server diagnostic events.

Event Filter	Filters look for matches in messages received by the ELM Server. Messages include Windows event log records or Alerts.
Event Monitor	Event Monitor is a general term which refers to Event Collector and Event Alarm Monitor Items.
Event View	Event Views use one or more Event Filters to display some or all events. You can associate one or more Event Filters to filter what events are displayed.
Events	An event is a single record from a Windows event log or an Alert from an ELM Agent.
Monitor Items	Monitor Items determine the type of information or activity to monitor. Examples include Event Collector (which collects events), Service Monitor (which watches the state of Windows services), and Performance Collector (which gathers performance counter values).
Notification Methods	Notification Methods control the message and how it is delivered to you. They're triggered by events or alerts and have thresholds which can protect you from being flooded by notifications.
Notification Rules	Notification Rules associate Filters with Notification Methods. They provide a level abstraction which allows you to reuse Filters and Notification Rules in new combinations.
Notification Wizard	This Notification Wizard assists creating Notification Rules for Monitor Item actions.
Report Section	Report section refers to different areas of an ELM Editor report. Each area displays the results of a single SQL query. Results can be displayed in graphical or textural style.
Service Agents	Service Agents execute Monitor Items, collect data, transmit collected data to the ELM Server, and execute the configured Actions for assigned Monitor Items. Service Agents are required in order to monitor event logs, health and performance and other subsystems in real-time.
Software License Agreement	You should receive a Software License Agreement (SLA) with your install. The SLA provides details on your license agreement, and includes your registration information. If you did not receive an SLA with your purchase, or if you cannot locate your SLA, please contact <a href="mailto:Sales@TNTSoftware.com">Sales@TNTSoftware.com</a>
TNT Agent	Agents are the fundamental component for identifying the devices to be monitored.
Virtual Agents	Virtual Agents are used for agentless monitoring. Nothing is installed on the system being monitored when it is configured as a Virtual Agent. The actual monitoring functions for a Virtual Agent execute within the ELM Server Process so Virtual Agents cannot monitor in real-time.
Wizard	Wizards take the administrator or end-user step-by-step through the creation of a new object in ELM. Wizards are launched whenever new object creation is invoked from within the ELM Console.

## 1.8.2 Registry Entries

The tables in this section list command line options for the ELM Event Log Monitor 6.0 Server, and registry settings for the ELM Service Agent, Console, and Server.

[ELM Console Registry Entries](#)

[ELM Server Registry Entries](#)

[ELM Service Agent Registry Entries](#)

### 1.8.2.1 ELM Console Registry Entries

The table below lists registry entries from the Windows Registry recognized by ELM .

- Not all registry entries are created by default; some must be manually created.
- If a Name entry is not in the registry, ELM will use the default value listed.
- *Not* all values should be edited through the registry; when this is true, the appropriate interface is given in the Description.
- This table does not include the COM classes and libraries that are registered and written to the Registry (under HKEY\_CLASSES\_ROOT) during Setup.
- This table does not include the ELM Server service registry entries (under HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services).

### ELM Console Registry Keys

HKEY\_CURRENT\_USER \ SOFTWARE \ TNT Software \ ELM Event Log Monitor 6.0 \ Snapin \ Settings

Name Type Default Value Restart Required Description	DefaultEventViewIsDetail REG_DWORD 0 No If set to 0, then Views will summarize events, and if set to 1, then Views will display one event per line. Views listed in the DetailEventViews and SummaryEventViews registry entries will override this registry entry. This is a global setting that affects all Event and Alert Views.
Name Type Default Value Restart Required Description	DetailEventViews REG_SZ <NULL> No This entry lists GUID's for Views that were set to detail display the last time the ELM Console was closed and

	the console settings saved.
Name Type Default Value Restart Required Description	MaxNumAdvises REG_SZ 5000 No When the number of advises held in memory reaches this maximum value, they are deleted from memory. No message is generated. If advises are dropped from memory, the alerts or events can be displayed by refreshing the view. Increasing this value increases the memory required by the ELM Console (mmc.exe) process. The ELM Console must be closed and re-opened to activate changes. See also SnapinAdviseTimerInMilliseconds.
Name Type Default Value Restart Required Description	SnapinAdviseTimerInMilliseconds REG_SZ 50 No This entry controls how frequently the ELM Console looks in its own queue for new advises (messages) from the ELM Server. Checking the queue and processing waiting advises delays processing of user input like mouse clicks or keystrokes. So setting this value to a high number will make the ELM Console more responsive, but display updates from advises will be slower. Advise updates are independent of user initiated refreshes. The ELM Console must be closed and re-opened to activate changes. See also MaxNumAdvises.
Name Type Default Value Restart Required Description	SplashScreen REG_DWORD 1 ELM Console restart required Display (1) or do not display (0) TNT Software splash screen when opening the ELM Console.
Name Type Default Value Restart Required Description	SummaryEventViews REG_SZ <NULL> No This entry lists GUID's for Views that were set to summary display the last time the ELM Console was closed and the console settings saved.

### 1.8.2.2 ELM Server Registry Entries

The table below lists registry entries from the Windows Registry recognized by ELM .

- Not all registry entries are created by default; some must be manually created.
- If a Name entry is not in the registry, ELM will use the default value listed.
- *Not* all values should be edited through the registry; when this is true, the appropriate interface is given in the Description.
- This table does not include the COM classes and libraries that are registered and written to the Registry (under HKEY\_CLASSES\_ROOT) during Setup.
- This table does not include the ELM Server service registry entries (under HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services).

### ELM Server Registry Keys

HKEY\_LOCAL\_MACHINE \ SOFTWARE \ TNT Software \ ELM Event Log Monitor 6.0 \ Settings

Name Type Default Value Restart Required Description	AgentHeartbeatInSeconds REG_DWORD 60 (seconds) ELM Server restart required This sets the interval used by TNT Agent for checking in with the ELM Server. The ELM Server uses this heartbeat check to provide At-a-Glance Agent status information.
Name Type Default Value Restart Required Description	BatchMoveTableChunkSize REG_DWORD 5000 ELM Server restart required This setting controls how many rows of data are copied from the primary to the archive database in each batch. It also controls how many rows of events are deleted before the next copy operation. For non-event data, all valid rows are deleted after copy operations are complete. Valid values are positive integers greater than 5000. Setting it to a number less than 5000 will be ignored by ELM.
Name Type Default Value Restart Required Description	CacheDataTrigger REG_DWORD 60 (minutes) ELM Server restart required Interval for cached data window in minutes. Applies to EEM, ELM, and EVM only.

Name Type Default Value Restart Required Description	ContinuePruneOnArchiveError REG_DWORD 0 ELM Server restart required This setting controls continued processing if an error occurs when moving events from the primary to the archive database. Setting it to 0 will stop the archiving process, and is intended to prevent any data loss. Setting it to 1 will continue the archiving process, but may result in data loss. With either setting, if an error occurs, ELM will write error event 5219 to the Windows application log on the ELM Server computer.
Name Type Default Value Restart Required Description	CustomReportsImported REG_DWORD 0 No When set to 1, the ELM Server will not import ELM Editor custom reports. If the key is missing or set to 0, and there are no reports or folders in the ELM Editor container, then selecting or refreshing the ELM Editor container will import the reports in EEMReports.xml.
Name Type Default Value Restart Required Description	DisableMonitorJobQueue REG_DWORD 0 No This value is set through the ELM Console. This value changes from 0 (default - queue enabled) to 1 (queue disabled) when the Monitor Items container is disabled.
Name Type Default Value Restart Required Description	DisableNotificationJobQueue REG_DWORD 0 No This value is set through the ELM Console. This value changes from 0 (default - queue enabled) to 1 (queue disabled) when the Notification Methods container is disabled.
Name Type Default Value Restart Required Description	DisableReportsQueue REG_DWORD 0 No This value is set through the ELM Console. This value changes from 0 (default - queue enabled) to 1 (queue disabled) when the Reports container is disabled.

Name Type Default Value Restart Required Description	ELGen AutoGenInterval REG_DWORD 1 No This value is set through the <i>Event Generator</i> tool. This value is configured using the ELGEN (Event Log Generator) tool that ships with ELM. This is the frequency at which ELGEN auto-generates events.
Name Type Default Value Restart Required Description	ELGen ComputerName REG_SZ <localhost > No This value is set through the <i>Event Generator</i> tool. This is the name of the computer to which ELGEN was last connected. When re-launched, ELGEN will set its initial focus to this computer.
Name Type Default Value Restart Required Description	ELGen EventSource REG_SZ <NULL > No This value is set through the <i>Event Generator</i> tool. This is the last used Event Source in ELGEN.
Name Type Default Value Restart Required Description	ELGen GenCount REG_DWORD 1 No This value is set through the <i>Event Generator</i> tool. This is the last number of events generated at each click of the Generate Events button or at each Auto Generate interval.
Name Type Default Value Restart Required Description	ELGen InsertionString REG_SZ TEST No This value is set through the <i>Event Generator</i> tool. This is the last string entered into the Insertion String field of ELGEN.
Name Type Default Value Restart Required Description	ELGen LogName REG_SZ Application No This value is set through the <i>Event Generator</i> tool. This is the log last accessed by ELGEN.

<p>Name Type Default Value Restart Required Description</p>	<p>ELGen WindowPos REG_BINARY &lt;Binary Value&gt; No This value is set through the <i>Event Generator</i> tool. This indicates ELGEN's last window position (i.e., where the UI was on the screen).</p>
<p>Name Type Default Value Restart Required Description</p>	<p>MaxNotificationQueueEntriesPerItem REG_DWORD 50000 ELM Server restart required Number of pending notifications that can be in the Notification queue for an individual Notification Method. If a Method creates more than the default or registry configured number of Notifications, then the ELM Server will generate error 5104 and discard all pending notifications for the one Notification Method. Pending notifications queued for other Notification Methods, even if they are the same type, will not be deleted. Increasing this value will increase memory requirements of the ELM Server process. Maximum value is 2147483647 (MAX_INT).</p>
<p>Name Type Default Value Restart Required Description</p>	<p>MaxNumMonitorJobWorkerThreads REG_DWORD 100 ELM Server restart required Controls the number of Monitor Item worker threads spawned by the ELM Server process for Virtual Agents and by the TNT Agent process for Service Agents.  With Virtual Agents, this entry must be entered in the ELM Server computer registry. With Service Agents this entry must be entered in the Agent computer registry.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>MaxNumRecordsReadBeforeForceSend REG_DWORD 1000 No This value is used for Event Alarms and Event Collectors. This is the maximum number of event log records that will be read in a single monitor item interval.  With Virtual Agents, this entry must be entered in the ELM Server computer registry. With Service Agents this entry must be entered in the Agent computer registry.</p>

Name Type Default Value Restart Required Description	MaxPagerMsgLength REG_DWORD 240 No The maximum message size for TAP (Telocator Alphanumeric Protocol) is 250 bytes, and for SMS (Short Message Service) it's 160 bytes. Service providers are free to implement their own interpretation of these protocols, and 240 bytes has proven to be successful in practice.
Name Type Default Value Restart Required Description	MonitorNumLoggingChars REG_DWORD 512 ELM Server restart required This key controls the number of bytes that TNTDiag will capture for Monitor Item activity. Use the Server registry key when the Monitor Items are assigned to Virtual Agents.
Name Type Default Value Restart Required Description	NormalShutdown REG_DWORD 1 No Users should not change this registry entry. This value is set internally by the ELM Server. A value of 1 indicates a normal shutdown. When the ELM Server service is restarted, this flag is removed from the registry. Before a Service Agent or the ELM Advisor will attempt to restart a stopped ELM Server, it will read the registry to see if this flag is present. If the flag exists, the Service Agent or ELM Advisor will not attempt to restart the ELM Server. If the flag does not exist, the Service Agent or ELM Advisor will attempt to restart the ELM Server (if configured to do so).
Name Type Default Value Restart Required Description	RealTimeEventViewUpdates REG_DWORD 1 No This value is set through the <i>Options</i> tab of the ELM Control Panel applet. Specifies whether real-time streaming of new events is enabled (1) or disabled (0).
Name Type Default Value Restart Required Description	SaveInterval REG_DWORD 15 ELM Server restart required Users should not change this registry entry. Interval

	<p>number of seconds ELM Server waits before checking for configuration changes. If changes are found, then they will be written to the ELM Server .dat file.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>ServerName REG_SZ &lt; NetBIOS Name of the ELM Server computer &gt; ELM Server restart required When the ELM Server service starts, this name is loaded into memory. Once loaded, this name will be passed to Service Agents as the name they should use for the ELM Server. The name is passed when an Agent configuration is updated, or when a new Agent is installed.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>SMTPEmailNotificationTimeOut REG_DWORD 60 ELM Server restart required Specifies the number of seconds the ELM Server will wait for an SMTP Server to respond when using the SMTP e-mail Notification Method. Valid values are 5-SMTPMaxTimeoutInSeconds. If the key SMTPMaxTimeoutInSeconds is absent, then valid values are 5-300 (the SMTPMaxTimeoutInSeconds default value).</p>
<p>Name Type Default Value Restart Required Description</p>	<p>SMTPMaxTimeoutInSeconds REG_DWORD 300 ELM Server restart required Specifies the maximum number of seconds ELM will wait for an SMTP Server to respond. This entry sets an upper bound which limits both the ELM SMTP Monitor and the ELM SMTP Notification Method. The lower bound is hard-coded to 5 seconds. Valid values for this key are 5-4,294,967,295.</p> <p>An ELM SMTP Notification Method wait-time will use the SMTPEmailNotificationTimeOut registry key (or default value) if it is within the upper and lower bounds. Otherwise the nearest boundary value is used. This would be made in the ELM Server.</p> <p>An ELM SMTP Monitor wait-time will use two times the Quality of Service (QoS) value if it is within the upper and lower bounds. Otherwise the nearest boundary value is used. With Virtual Agents, this entry must be entered in the ELM Server computer registry. With Service Agents this entry must be entered in the Agent</p>

	computer registry.
Name Type Default Value Restart Required Description	SMTPWaitForPreEHLOGreetingInSeconds REG_DWORD 0 ELM Server restart required When the ELM Server connects to an SMTP server, this entry adds a delay, in seconds, after connecting and before sending EHLO. This setting affects all SMTP E-mail Notification Methods, and all SMTP Monitor Items.
Name Type Default Value Restart Required Description	TCPAgentPort REG_DWORD 1253 ELM Server restart required Default listening port to assign to each new Service Agent.
Name Type Default Value Restart Required Description	TCPServerPort REG_DWORD 1251 ELM Server restart required This value is set through the <i>Options</i> tab of the ELM Control Panel applet. Default listening port used by the ELM Server at startup.
Name Type Default Value Restart Required Description	TrustedServers REG_SZ <IP Address> No This value is set through the <i>Forwarded Events</i> tab of the ELM Control Panel applet. The Event Forward Notification Method Wizard will attempt to create this value on the receiving ELM Server. If this fails, use the ELM Control Panel applet. IP addresses of sending ELM Servers that are not in this list will be ignored by the receiving ELM Server.

### 1.8.2.3 ELM Service Agent Registry Entries

The table below lists registry entries from the Windows Registry recognized by ELM .

- Not all registry entries are created by default; some must be manually created.
- If a Name entry is not in the registry, ELM will use the default value listed.
- *Not* all values should be edited through the registry; when this is true, the appropriate interface is given in the Description.
- This table does not include the COM classes and libraries that are registered and

- written to the Registry (under HKEY\_CLASSES\_ROOT) during Setup.
- This table does not include the ELM Server service registry entries (under HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services).

## Service Agent Registry Keys

HKEY\_LOCAL\_MACHINE \ SOFTWARE \ TNT Software \ ELM Manager Agent \ 6.0 \ Settings

Name Type Default Value Restart Required Description	CacheDataMaxSize REG_DWORD 104,857,600 (100MB) Service Agent restart required This value is set through the Agent properties. Controls the maximum size of the TNT Agent cache file size.
Name Type Default Value Restart Required Description	CachePath REG_SZ %systemroot%\TNTAgent Service Agent restart required This value is set through the Agent properties. Controls the destination of the TNT Agent cache file on the local computer. Also see MinDiskFreeSpaceInMBToContinueCaching.
Name Type Default Value Restart Required Description	InternetConnectTimeout REG_DWORD 5000 (5 seconds) Service Agent restart required This is the time-out value, in milliseconds, for Internet connection requests in the Link Monitor Item. If a connection request takes longer than this time-out value, the request is canceled.  Applies to EEM only.
Name Type Default Value Restart Required Description	MaxNumMonitorJobWorkerThreads REG_DWORD 100 Service Agent restart required Controls the number of Monitor Item worker threads spawned by the ELM Server process for Virtual Agents and by TNT Agent process for Service Agents.  With Virtual Agents, this entry must be entered in the ELM Server computer registry. With Service Agents this entry must be entered in the Agent computer registry.

<p>Name Type Default Value Restart Required Description</p>	<p>MaxNumRecordsReadBeforeForceSend REG_DWORD 1000 No This value is used for Event Alarms and Event Collectors. This is the maximum number of event log records that will be read in a single monitor item interval.</p> <p>To use this with Service Agents this entry must be manually entered in the registry of the Agent computer. To use this with Virtual Agents this entry must be manually entered in the registry of the ELM Server computer.</p> <p>Applies to EEM, ELM, and EVM only.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>MinDiskFreeSpaceInMBToContinueCaching REG_DWORD 20 MB Service Agent restart required Controls the minimum free space in MB before a TNT Agent will write to a cache file. If disk free space drops below this value, then the Agent will stop saving data to the cache file. Logical drive checked is determined by CachePath.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>MonitorNumLoggingChars REG_DWORD 512 Service Agent restart required This key controls the number of bytes that TNTDiag will capture for Monitor Item activity. Use the Agent registry key when the Monitor Items are assigned to Service Agents.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>ProcessRefreshRate REG_DWORD 3 Service Agent restart required The number of seconds between refreshing ELM Processes Tool, Performance tab.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>RemoteAgentInstall REG_DWORD 1 No Users should not change this registry entry. This value is set internally by ELM. This value indicates if</p>

	<p>the Service Agent was installed through the ELM Console (1) or using Windows Installer (0).</p>
<p>Name Type Default Value Restart Required Description</p>	<p>RestartHandleCountMax REG_DWORD 4000 Service Agent restart required When the handle count of the TNTAgent.exe process exceeds this value the service will restart itself. The minimum value you can set is 2000. When this is triggered, the Service Agent will log event 5066 in the application event log and restart the Service Agent.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>RestartThreadCountMax REG_DWORD 400 Service Agent restart required When the thread count of the TNTAgent.exe process exceeds this value the service will restart itself. The minimum value you can set is 200. When this is triggered, the Service Agent will log event 5066 in the application event log and restart the Service Agent.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>RestartVirtualMemoryMaxMb REG_DWORD 400 Service Agent restart required When the virtual memory allocation for the TNTAgent.exe process exceeds this value the service will restart itself. The minimum value (in MB) you can set is 200. When this is triggered, the Service Agent will log event 5066 in the application event log and restart the Service Agent.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>SMTPMaxTimeoutInSeconds REG_DWORD 300 Service Agent restart required Specifies the maximum number of seconds ELM will wait for an SMTP Server to respond. This entry sets an upper bound which limits both the ELM SMTP Monitor and the ELM SMTP Notification Method. The lower bound is hard-coded to 5 seconds. Valid values for this key are 5-4,294,967,295.</p> <p>An ELM SMTP Notification Method wait-time will use the SMTPEmailNotificationTimeOut registry key (or default value) if it is within the upper and lower bounds. Otherwise the nearest boundary value is</p>

	<p>used. This would be made in the ELM Server.</p> <p>An ELM SMTP Monitor wait-time will use two times the Quality of Service (QoS) value if it is within the upper and lower bounds. Otherwise the nearest boundary value is used. With Virtual Agents, this entry must be entered in the ELM Server computer registry. With Service Agents this entry must be entered in the Agent computer registry.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>TCPAgentPort REG_DWORD 1253 Service Agent restart required The listening port used by the TNT Agent service when started.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>TCPServerPort REG_DWORD 1251 Service Agent restart required The port used by TNT Agent when it contacts the ELM Server.</p>
<p>Name Type Default Value Restart Required Description</p>	<p>TrustedServers REG_SZ &lt;IP Address&gt; No This value is set through the Agent Install Wizard or the Server Registration Wizard. A list of IP addresses of accepted ELM Servers. ELM Server IP addresses not in this list will be ignored by TNT Agent.</p>

### 1.8.3 Command Line Switches

The tables in this section list command line options for the ELM Event Log Monitor 6.0 Server and TNT Service Agent.

[ELM Server Command Line Options](#)

#### 1.8.3.1 ELM Server Command Line Options

The table below lists command line switches that are recognized by the ELM Server.

Some switches have equivalents, but only 1 switch needs to be used.

## ELM Server Command Line Switches

Switch	Usage Examples	Description
/?	svr.exe /help	Show the ELM Server command line help.
/help		
/RegServer	svr.exe /regserver	Register the ELM Server as a COM server and as a Windows service.
/regservice		
/service		
/Restart	svr.exe /restart	Restart the ELM Server service.
/SaveXML [=file]	svr.exe /savexml	Saves all ELM Server configuration data to an XML file. If <i>file</i> is not specified, the ELM server will use a filename based on the Server executable.
/Start	svr.exe /start	Start the ELM Server service.
/Stop	svr.exe /stop	Stop the ELM Server service.
/UnRegServer	svr.exe / unregserver	Remove the ELM Server service and unregister the ELM Server as a COM server.
/UnRegService		

### 1.8.3.2 TNT Agent Command Line Options

The table below lists command line switches that are recognized by TNT Agents.

Some switches have equivalents, but only 1 switch needs to be used.

## ELM Server Command Line Switches

Switch	Usage Examples	Description
/?	tntagent.exe /help	Show the TNT Agent command line help.
/help		

/Install	<code>tntagent.exe /install</code>	Creates the TNT Agent service.
/Register	<code>tntagent.exe /register</code>	Displays the wizard dialog to connect the agent to an ELM Server.
/Remove	<code>tntagent.exe /remove</code>	Deletes the TNT Agent service.  Note: You should deregister servers before using this option. Double-click TNTAgent.exe to open the UI, and then Deregister is under the File menu.
/Restart	<code>tntagent.exe /restart</code>	Stops and restarts the TNT Agent service
/Start	<code>tntagent.exe /start</code>	Starts the TNT Agent service
/Stop	<code>tntagent.exe /stop</code>	Stops the TNT Agent service.
/Trust="nnn.nnn.nnn"]	<code>tntagent.exe /trust="192.168.1.10"</code>	Adds the specified TCP/IP address to the list of trusted servers. After the server is trusted, it can register with the Agent.
/Untrust="nnn.nnn.nnn"]	<code>tntagent.exe /untrust="192.168.1.10"</code>	Removes the specified TCP/IP address from the list of trusted servers.

# Index

## - A -

Actions 80  
Agent Categories 80  
Agents 23, 80  
Alarms 30  
alerting 4  
Archive Databases 4  
Archiving 4

## - C -

Collectors 30  
Copyright Notice 4

## - D -

Data Collector and Real-Time Monitors 30  
Database 80

## - E -

ELM Console 4, 80  
ELM Event Log Monitor 4  
ELM Server 80  
Event Collectors 30, 33  
Event Monitors 33  
Event Views 33  
Exclude 33  
Exclude Filters 30

## - F -

Filters 33

## - I -

Include 33  
Include Filters 30  
Install 23

## - L -

Legal Notice 4

## - M -

Monitor Items 30  
Monitoring 18

## - N -

New Features 5  
Notification 80  
Notification Methods 5  
Notification Rules 33

## - P -

Primary Database 67

## - R -

Report 80  
Reporting 63

## - S -

Scheduled hours 18  
Scheduled Interval 18  
Server 23  
Service Agent 18  
Service Agents 23

## - U -

Uninstall 23

## - V -

Virtual Agents 18, 23





[www.tntsoftware.com](http://www.tntsoftware.com)

TNT Software, Inc.  
2001 Main Street  
Vancouver, Washington 98660  
U.S.A.

Voice: (360) 546-0878  
Toll Free: (877) 546-0878  
Fax: (360) 546-5017

[sales@tntsoftware.com](mailto:sales@tntsoftware.com)  
[support@tntsoftware.com](mailto:support@tntsoftware.com)