ELM Enterprise Manager

USER MANUAL

Fire Mountain Software

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

1. Legal/Copyright Notice 7

2. Quick Start Guide 11

3. ELM Management Console 15

3.1 Database ... 16

3.1.1 Advanced Database Settings ... 19

3.2 Explorer ... 21

3.3 Ribbon Toolbar ... 23

3.4 Document Types ... 24

3.4.1 ELM Server Document ... 24

3.4.1.1 Edit Panel-ELM Server Configuration ... 27

3.5 Reporting ... 30

3.6 Tools ... 32

3.6.1 ELM Size ... 33

3.6.2 ELM Event Generator ... 35

3.6.3 Event File Verifer ... 36

4. ELM Console (MMC) 37

4.1 Monitoring and Management ... 38

4.1.1 Agents and Monitors Library ... 39

4.1.1.1 All Monitors ... 40

4.1.1.1.1 Agent Monitor ... 41

4.1.1.1.2 Event Monitor ... 42

4.1.1.1.3 Event Collector ... 45

4.1.1.1.4 Event File Collector ... 47

4.1.1.1.5 Event Writer ... 50

4.1.1.1.6 File Monitor ... 51

4.1.1.1.7 FTP Monitor ... 53

4.1.1.1.8 Inventory Collector ... 55

4.1.1.1.9 Performance Monitor ... 57

4.1.1.1.10 Performance Collector ... 58

4.1.1.1.11 Ping Monitor ... 59

4.1.1.1.12 Process Monitor ... 61

4.1.1.1.13 Service Monitor ... 63

4.1.1.1.14 SMTP Monitor ... 65

4.1.1.1.15 SNMP Monitor ... 66

4.1.1.1.16 SNMP Collector ... 69

4.1.1.1.17 SNMP Receiver ... 71

4.1.1.1.18 SQL Monitor ... 71

4.1.1.1.19 Script Monitor ... 73

4.1.1.1.20 Syslog Receiver ... 75

4.1.1.1.21 TCP Port Monitor ... 78
4.1.1.1.22 Web Page Monitor ... 79
4.1.1.1.23 WMI Monitor ... 81
4.1.1.2 All Agents ... 83
4.1.1.2.1 Agent Installation ... 83
4.1.1.2.1.1 Agent Properties ... 89
4.1.1.2.1.2 Service Agents ... 94
4.1.1.2.2 Agent Tasks ... 94
4.1.2 Monitoring Categories ... 96
4.1.3 Maintenance Categories ... 97
4.2 Viewing and Notifying ... 98
4.2.1 Filters and Methods Library ... 99
4.2.1.1 All Exclude Filters ... 99
4.2.1.2 All Include Filters ... 103
4.2.1.3 All Correlation Filters ... 106
4.2.1.4 All Notification Methods ... 111
4.2.1.4.1 Command Script ... 112
4.2.1.4.2 Dashboard Notification ... 113
4.2.1.4.3 Forward Event ... 113
4.2.1.4.4 SNMP ... 114
4.2.1.4.5 Syslog Message ... 115
4.2.1.4.6 Mail Notification (SMTP) ... 117
4.2.1.4.7 ELM Advisor Notification ... 117
4.2.2 Event Views ... 118
4.2.2.1 Event View Properties ... 121
4.2.2.2 Event Properties ... 123
4.2.3 Security Views ... 125
4.2.3.1 Event View Properties ... 125
4.2.3.2 Event Properties ... 128
4.2.3.3 Event Filters ... 130
4.2.4 Correlation Views ... 130
4.2.4.1 Correlation View Properties ... 131
5. Server Properties 137
6. Technical Resources 141
6.1 Security Guide ... 142
6.1.1 Security Introduction ... 142
6.1.2 Security Guidelines ... 144
6.1.3 Configuring ELM Server Security ... 146
6.2 Server and Agent Events ... 147
6.2.1 Event IDs 5050 - 5099 ... 147
6.2.2 Event IDs 5100 - 5199 ... 149
6.2.3 Event IDs 5200 - 5299 ... 149

6.2.4 Event IDs 5300 - 5399 150
6.2.5 Event IDs 5400 - 5499 151
6.2.6 Event IDs 5500 - 5599 152
6.2.7 Event IDs 5600 - 5699 156
6.2.8 Event IDs 5700 - 5799 156
6.2.9 Event IDs 5800 - 5899 156
6.2.10 Event IDs 5900 - 5999 157
6.3 Registry Entries 157
6.3.1 ELM Wizard Registry Entries 158
6.3.2 ELM Console Registry Entries 158
6.3.3 ELM Server Registry Entries 160
6.3.4 ELM Service Agent Registry Entries 167
6.4 Command Line Switches 170
6.4.1 Silent Install 170
6.4.2 ELM Server Command Line Options 175
6.4.3 TNT Agent Command Line Options 177
6.5 Home and Standby 177

Index 183

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

Legal/Copyright Notice

1 Legal/Copyright Notice

Copyright Notice

Legal Notice

Fire Mountain Software
PO Box 1630
Castle Rock, WA 98611
https://www.firemtsoftware.com
Phone: 360-546-0878

Quick Start Guide

2 Quick Start Guide

System Requirements

- Windows Server or Desktop OS (7,2008R2 or later)
- Min. 4GB of Memory (8GB+ recommended)
- Optional: MS SQL Server 2008R2 or later
  - The default Install will use an embedded version of Microsoft SQL Express LocalDB 2014

Backup

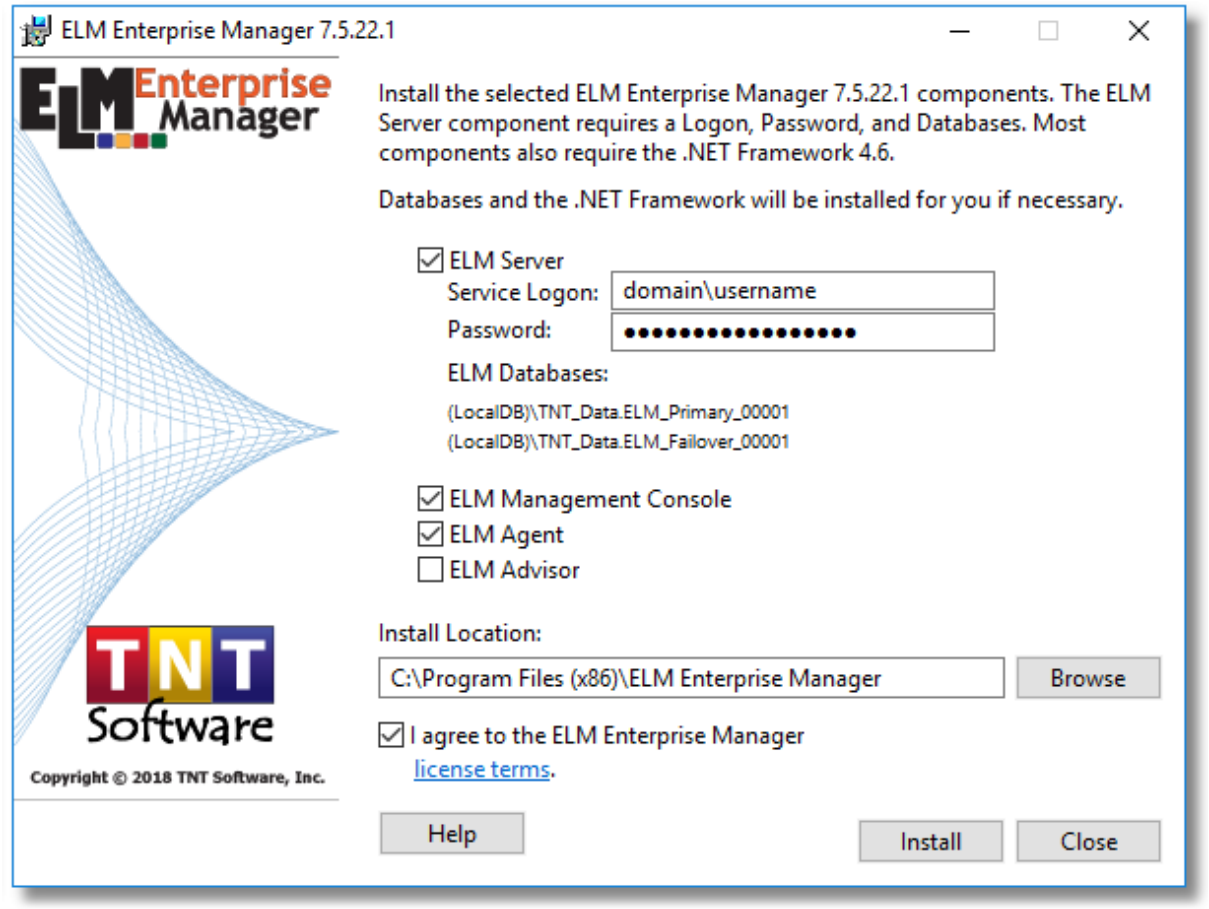
- Best practice is to Backup the ELM program directory and primary database.
- Right click and Export all custom reports

Special Notes and considerations

ELM 7.5 has a redesigned reporting engine only accessible in the new ELM Management console. Legacy reports and report schedules will need to be manually recreated as user reports and publications after upgrade. If you are unable to use default reports or unable to recreate reports based on event views then you will need to contact Support for any customizations. See Reporting 30 on how to create reports and publications.

Installation

- Right click and Run As Administrator the ELM 7.5.exe
- Provide User name and password for the ELM services, select products to install, and agree to license terms.
  - User account should have local Administrator rights. If using a non-embedded Microsoft SQL server then the account used will need at minimum DBCreator rights.
- Agent are deployed using the ELM Console (mmc). Under Monitoring and Management > Agents and Monitors Library Right click on the All Agents container and select New > Agent to launch the wizard.



ELM Installation Wizard

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

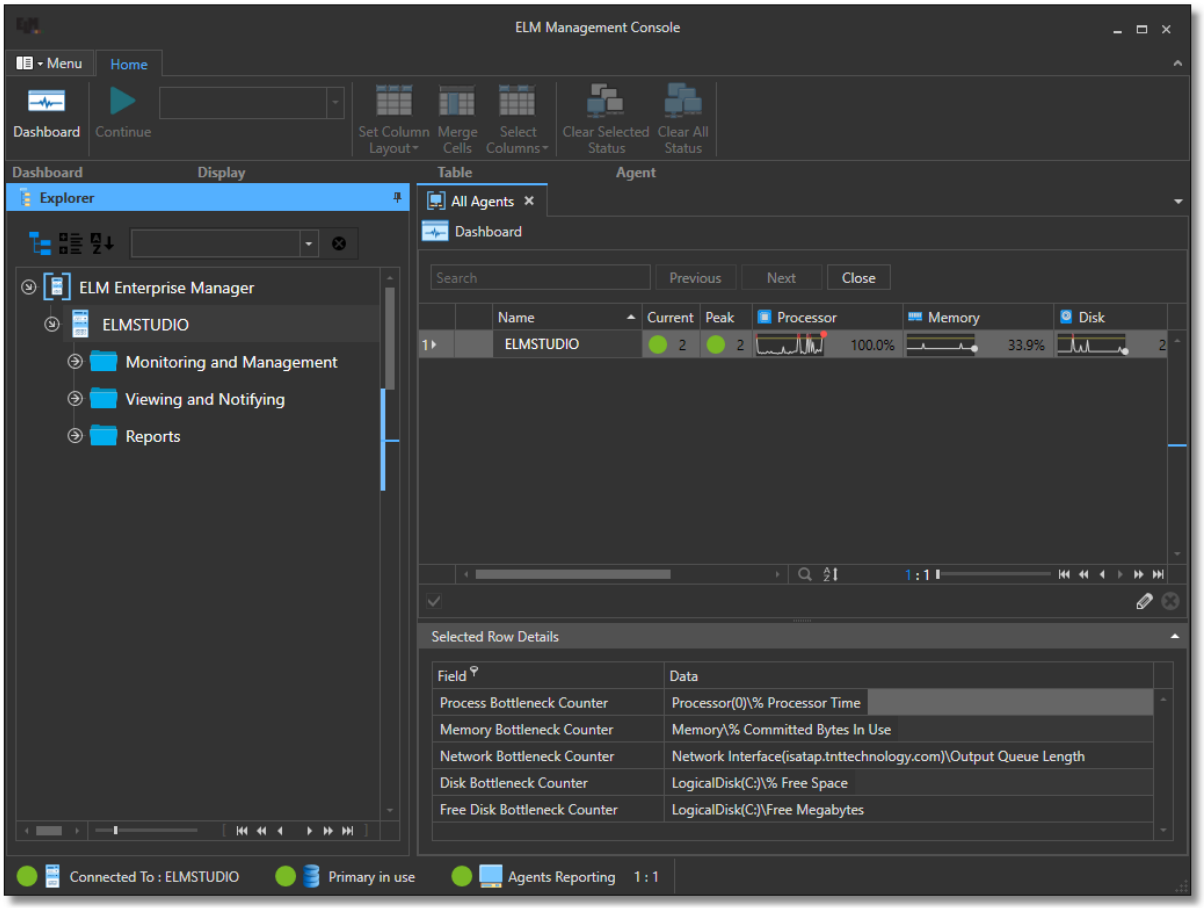
ELM Management Console

3 ELM Management Console

Description

The ELM Management Console provides a rich user interface experience. The Management console is used for viewing the results of data collection, database configuration, report generation, snmp configuration, IP Trusts and general program settings such as ports.

For other program options such as creating/modifing Events views, deploying agents or configuring monitor items please refer to the *ELM Console (MMC)* 38.



3.1 Database

Description

The database wizard is a central location for setting up the ELM Primary, Failover and Archive databases. The wizard will allow you change databases and attach archive databases for reporting.

Note: For changing the data retention policy and archive settings, see the ELM Server Configuration 24 document.

Accessing the Database Wizard

To access the database wizard launch the ELM Management Console. From the Menu in the top left corner select New > Server > Database. This will launch a Database wizard document.

Configure a Database

Your first option in the database wizard wants you to select either Create or Connect.

Create New Database

1. Define the database role:
   Primary-This database is the active primary database were all data is stored.
   Failover-This database is used if the primary is not available or during nightly maintenance.
   Archive-Data from the primary is moved to this database for long term storage.
2. Enter the Server Name:
   This is the name and if needed the instance of the SQL server where ELM will create the database
   Example: MySQLServer\Instancename or MySQLServer
3. Enter the Name of the database:
   This is the database name the ELM will create on the specified server.
4. Authentication:
   How ELM with authenticate to the Microsoft SQL server to create the database. This account needs to have DBCreator rights.
   If using SQL Server Authentication enter the user name and password in the space provided.
   Note: Windows Authentication is the preferred method
5. Click Finish and a confirmation document will appear showing the status of the creation.

Connect to an Existing ELM Database

1. Define the database role:
   Primary-When using the connect to existing this will change your current primary to an existing database.
   Failover-When using the connect to existing this will change your current failover to an existing database.
   Archive-Data from the primary is moved to this database for long term storage.

Other- This is used to connect an ELM archive database or other ELM database for reporting only.

Note: ELM will run its typical validation scripts against a connecting database and create any missing database structure needed for it to function as the defined role.

2. Enter the Server Name:

This is the name and if needed the instance of the SQL server where ELM will create the database

Example: MySQLServer\Instancename or MySQLServer

3. Enter the Name of the database:

This is the database name the ELM will create on the specified server.

4. Authentication:

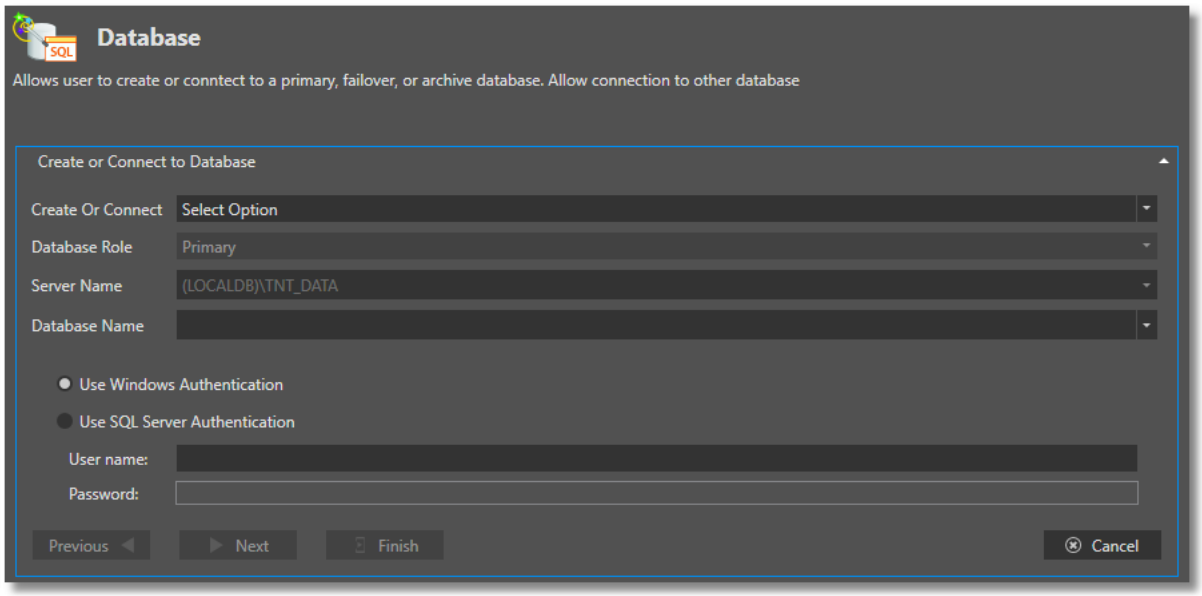
How ELM with authenticate to the Microsoft SQL server to create the database. This account needs to have DBCreator rights.

If using SQL Server Authentication enter the user name and password in the space provided.

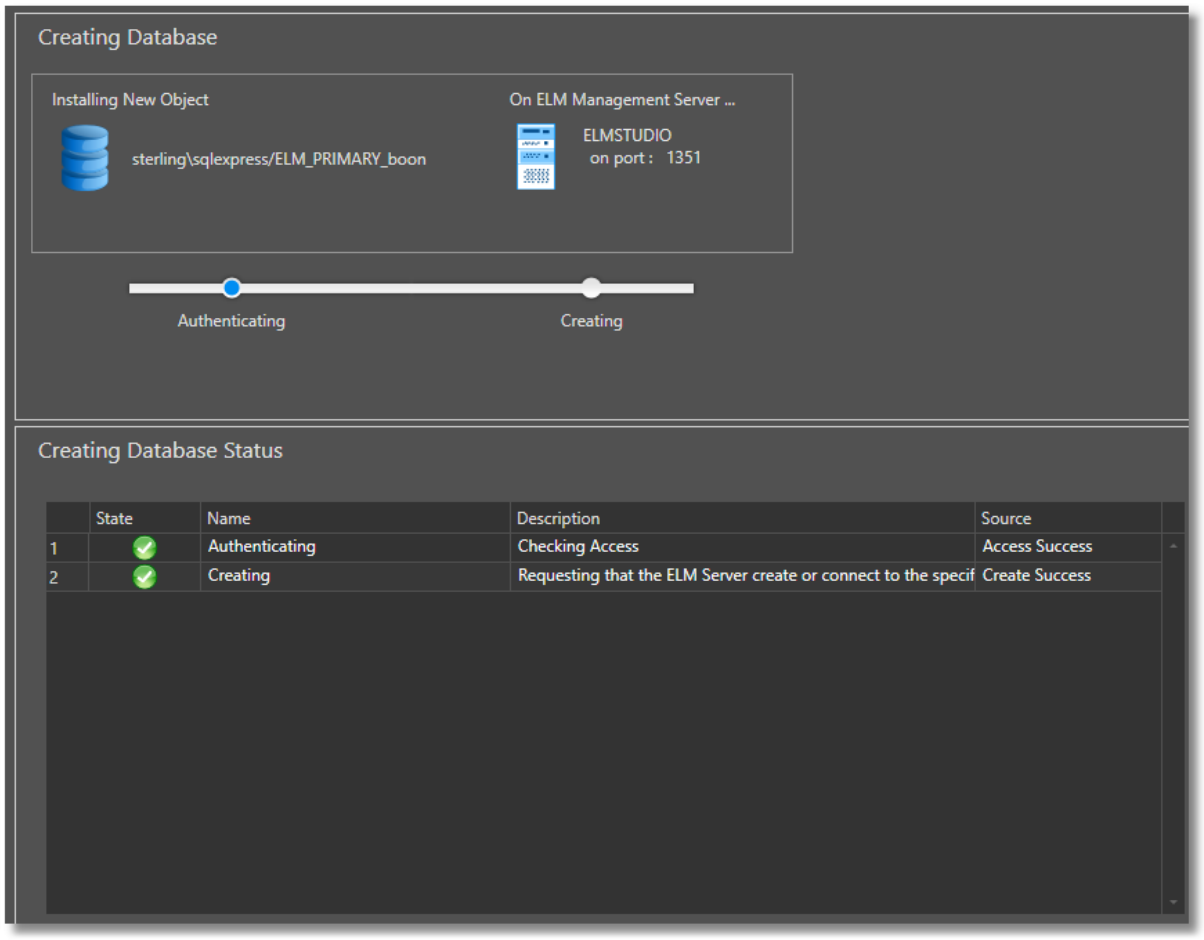
Note: Windows Authentication is the preferred method

Samples:

Database Wizard



Database Wizard

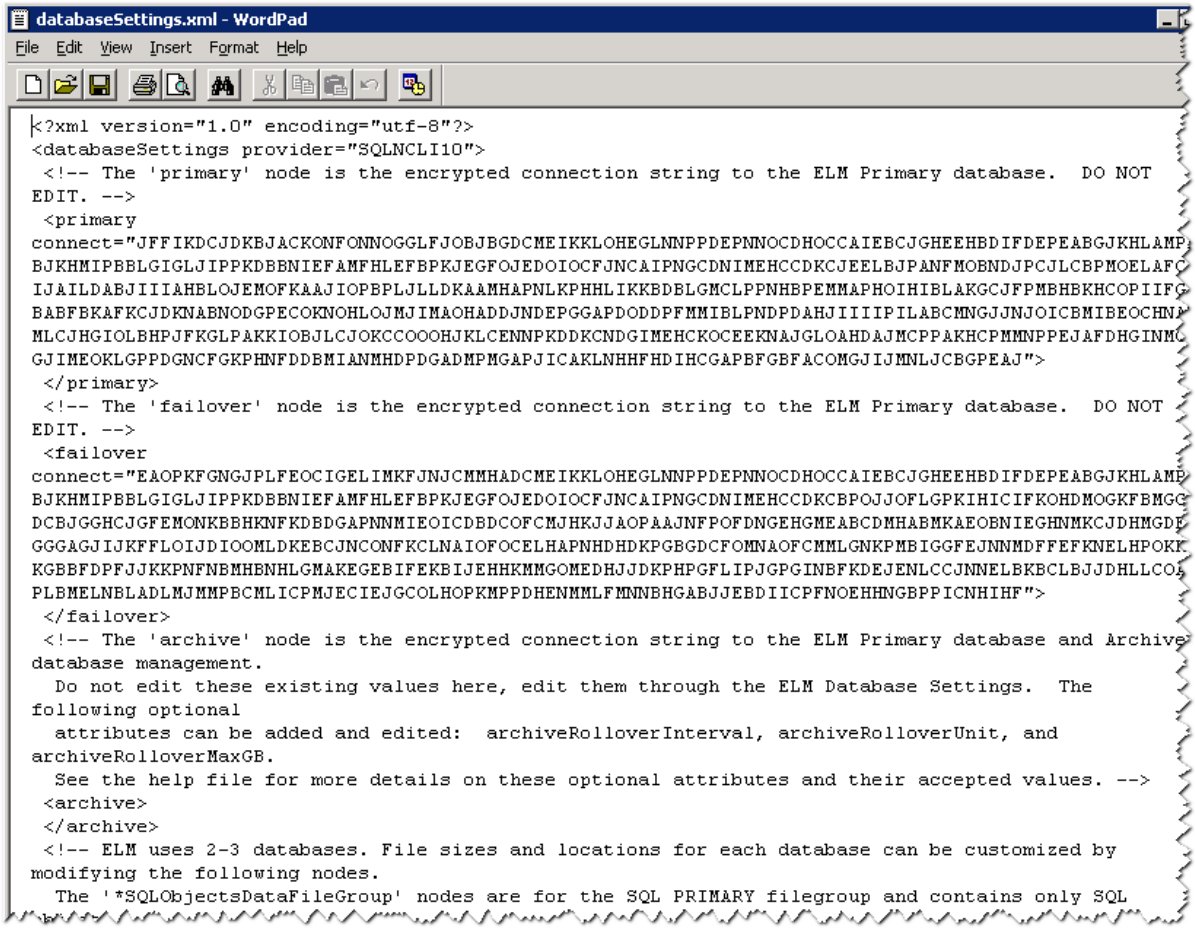


Database wizard confirmation document

To make advanced changes to database configuration please see Advanced Database Settings 19 topic.

3.1.1 Advanced Database Settings

Database settings are stored in the **databaseSettings.xml** file located in the default install folder for a 32 bit system: **c: \ Program Files ** and for a 64 bit system: **c: \ Program Files (x86) \. Contained within the file is the documentation on how to manual edit settings.**



1. In the Database Settings dialog, create an Archive DB and set it to rollover.
2. Stop the ELM Server service.
3. Edit the databaseSettings.xml file.

    a. If you're setting it to rollover with time-based criteria, add the following attributes to the "archive" node:

    Name: ***archiveRolloverInterval***

    Values: integer from

    Description: Sets what number of time units, as defined in the archiveRolloverUnit attribute, pass before a new Archive DB is created. So, if set to 3, and the archiveRolloverUnit is set to 86400, every 3 days a new Archive DB will be created.

    Name: ***archiveRolloverUnit***
    Values: 86400, 604800, or 2592000

    Description: Sets the time unit that archiveRolloverInterval will use. If set to 86400, the time unit is set to days, 604800 is weeks, and 2592000 is months.

b. If you're setting it to rollover with size-based criteria, add the following attributes to the "archive" node:

Name: ***archiveRolloverMaxGB***
Values: integer from
Description: Set the size an individual Archive DB is allowed to grow before a new one is created during the next archive event. If set to 10, then after the active Archive DB reaches a size of 10 GB or greater, the next time the archive event happens, a new database is created.

c. By default, the next time a rollover is executed is 1 month in the future, and changing the above settings will not affect this. To set it to rollover immediately (after which using the changed settings), in the "archive" node, set "**dateNextRollover**" to a non-zero low number, such as "10".

4. Start the ELM Server and verify that your changes are reflected correctly in the Database Settings dialog.

When customizing rollover size criteria you must specify both archiveRolloverMaxGB and archiveRolloverSizeCriterion in the databasesettings.xml file.
Example 1:
archiveRolloverSizeCriterion=1
archiveRolloverMaxGB=50
Results in the database rolling over once it reaches the 50GB threshold.

Example 2:
archiveRolloverSizeCriterion=0
archiveRolloverMaxGB=50
Results in the database rolling over based on the time attribute ignoring the 50GB threshold.

3.2 Explorer

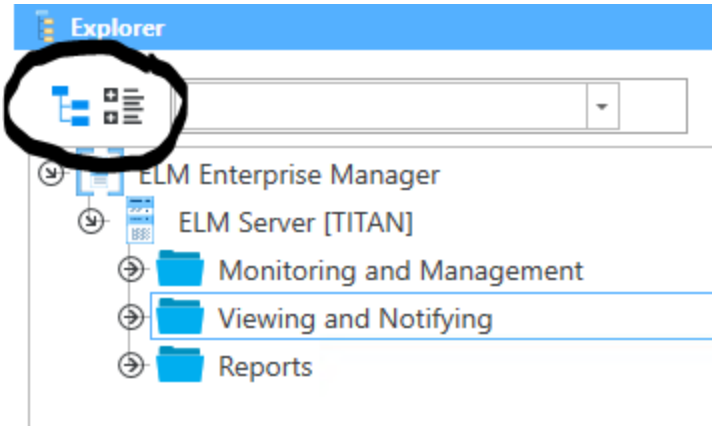
Description

The ELM Explorer panel provides the construct for navigating and launching various Documents 24 and settings within the Management Console.

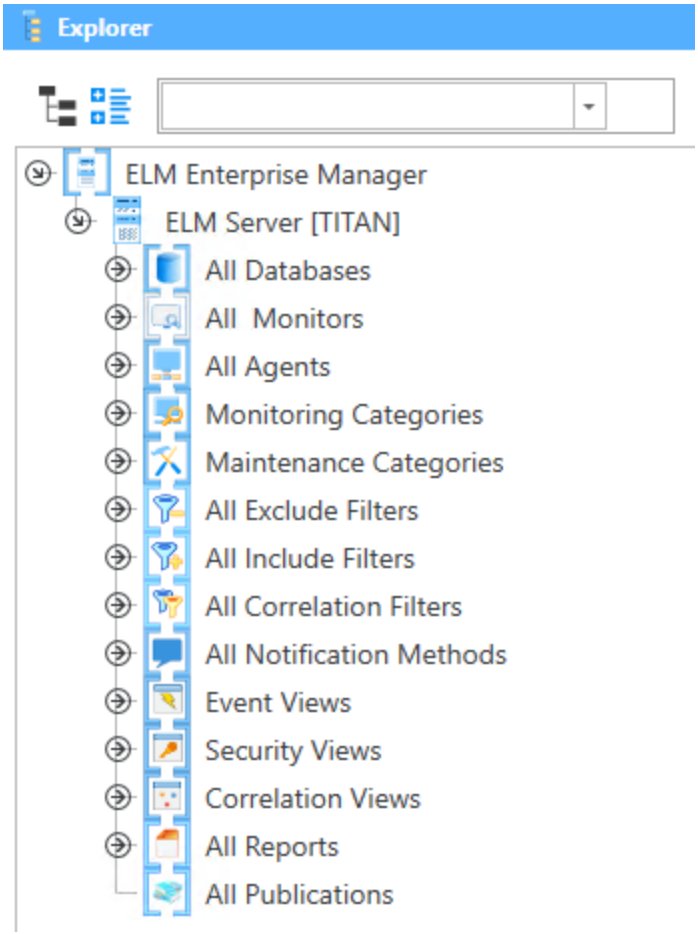
The panel itself contains the following attributes:
Display Mode
Search box

Attributes

Display Mode : Two icons located in the top left of the Explorer panel are used to switch between a tree structure or categorized listing of the nodes.



Tree View



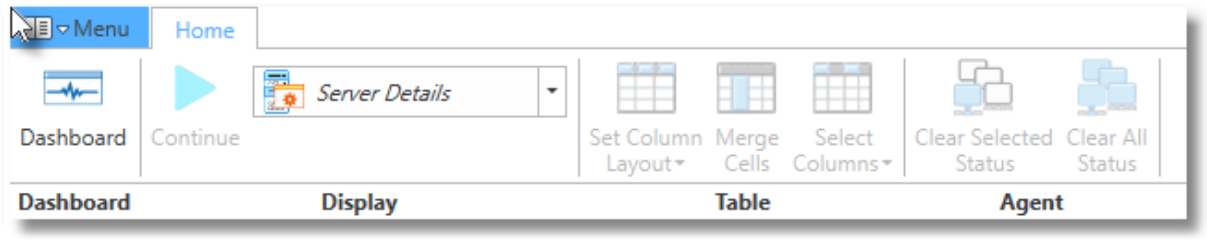
Category View

Search box: If you know that name of the item, you may use the search panel to find it. As you type the search results will be highlighted in the panel. At this point you can click on the result you want or use the Navigation controls to iterate through found results. The X may be press to clear your search results.

3.3 Ribbon Toolbar

Description

The Ribbon Toolbar provides display options based on the document type you have open. Home is the primary tab for the ribbon, on this tab you will find 4 sections. Dashboard, Display, Table and Agent. Options are either disabled or enabled based on the active document and its type.



Home Ribbon Toolbar

Dashboard

The Dashboard section offers a button to quickly access the All Agent category Dashboard display.

Display

A "Continue" button and a Display drop down menu are offered in this section. The Continue button is used to resume real-time updates when an Event View document is active, has focus and paused. In all other cases the button is in a disabled state if not applicable to the active document. The contents of the display drop down will change based on the Document type 24 that has focus.

Table

Column layouts and column selections can be made using the Table section. When this section is enabled it provides pre-defined column layouts along with the ability to select specific columns when an Agent Document or Event View Document are active. The Merge Cells button will combine column data grouping common attributes such as event type, computer name, and event id's.

Agent

The Agent section is only enabled and used when viewing Dashboard document. The two options allow you to clear the current and peak dashboard status notifications from the display for either individual servers or for all the servers listed.

3.4 Document Types

Description

Documents provide tab like visual display of data relating to the ELM server. Documents are generally launched by double click or by Right click menu option "Document".

ELM Server Document 24

Agent Document

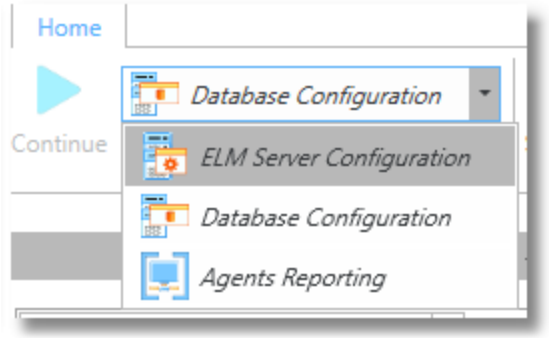
Category Document

Wizard Document - Wizard documents are launched from the main Menu and vary based on which Wizard is launched. Wizards have two categories (Report and Server) for performing functions such as database connections, ELM server connections, Import/Export, Publications and Reporting.

Event View Document - Displays event data.

3.4.1 ELM Server Document

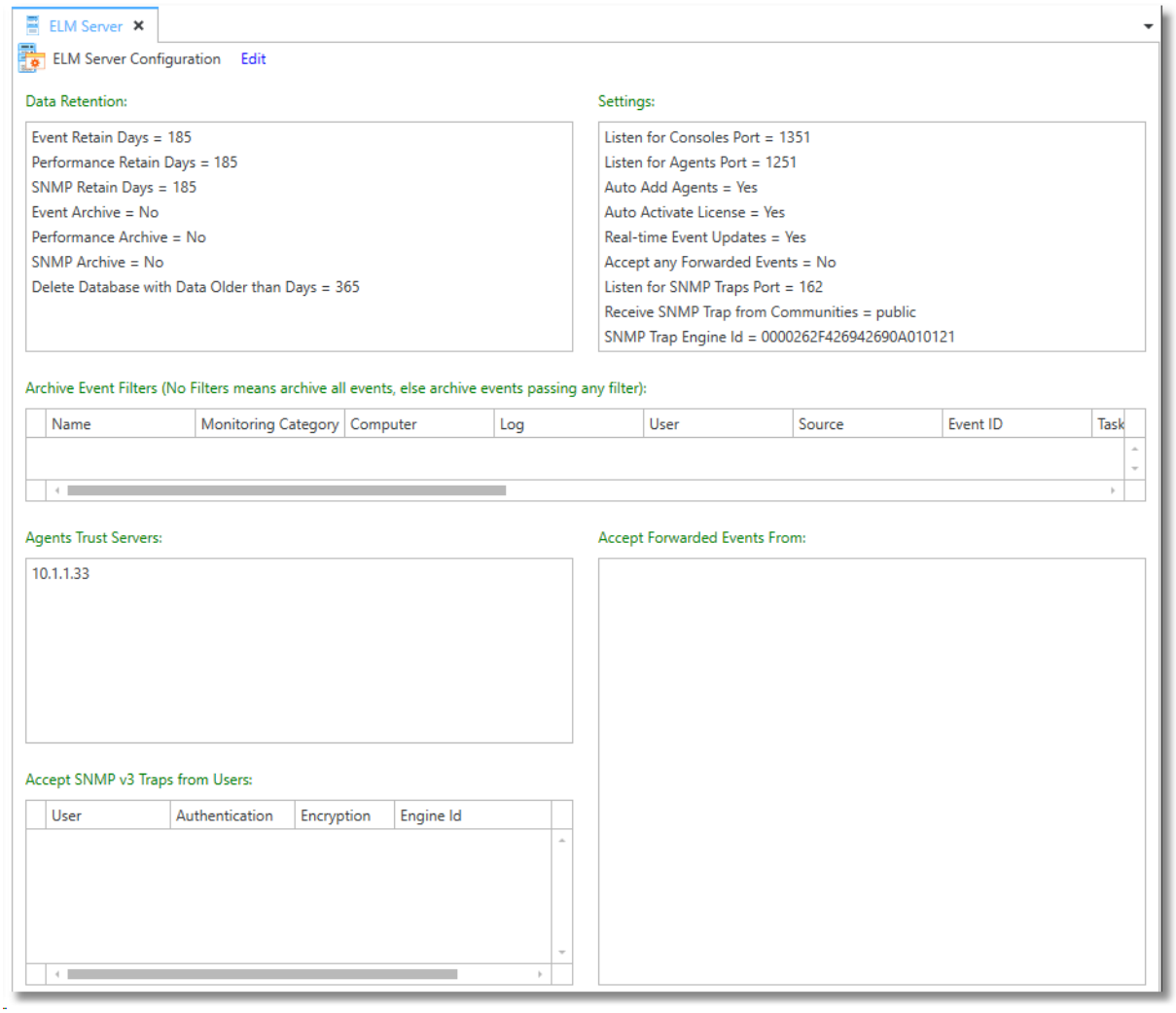
The ELM Server document has three displays options selectable from the Ribbon toolbar: ELM Server Configuration, Database Configuration and Agents Reporting. The document can be accessed by Right clicking on the ELM server name in the Explorer panel then select Document or double click of the ELM Server name in the Explorer panel. Once the ELM Server Document has opened select ELM Server Configuration from the the Display option on the toolbar.



Ribbon Display options for ELM Server Document

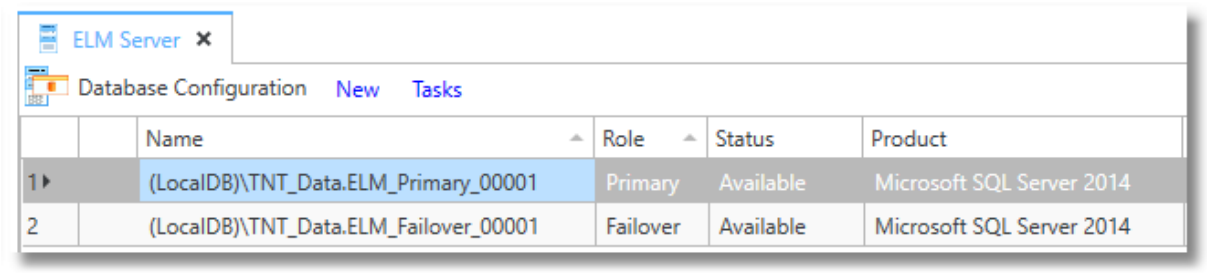
ELM Server Configuration Display

All configuration options shown in the display may be modified by using the Edit link which will launch an Edit panel 27.

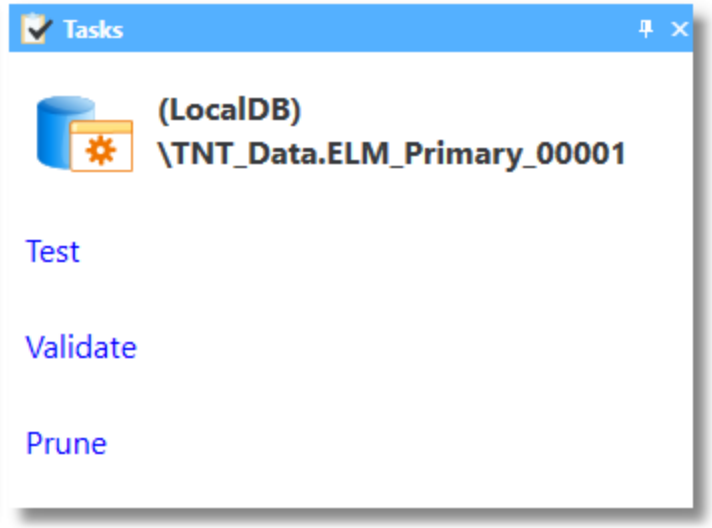


Database Configuration Display

This display shows information about the status and role of each ELM managed database. The link for New will launch the Database wizard document found under Menu > New > Server > Database. The Task link will launch a task panel that allows you to Test, Validate (Runs validation scripts) and Prune operations on the currently selected database. Task panel options will change depending on which database is selected when the Task link is clicked.



Database configuration display on the ELM Server Document



Database Task Panel

3.4.1.1 Edit Panel-ELM Server Configuration

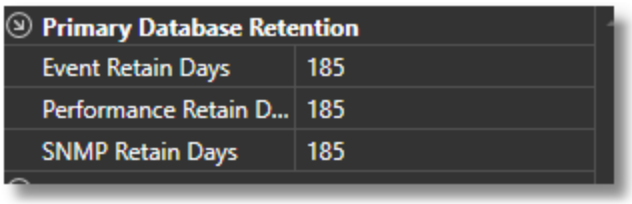
Description

The ELM Server edit panel allows you to configure Primary and Archive database retention, Archive filters, Server Settings, IP Trusts and SNMP settings.

After launching the ELM Management Console Right click on the ELM server name in the Explorer then select Edit from the menu. To view these settings without editing them, you can double click the ELM server name or Right click then select Document on the ELM server name from the Explorer panel. When the ELM server Document launches select ELM server Configuration from the Display section of the ribbon toolbar.

Primary Database Retention

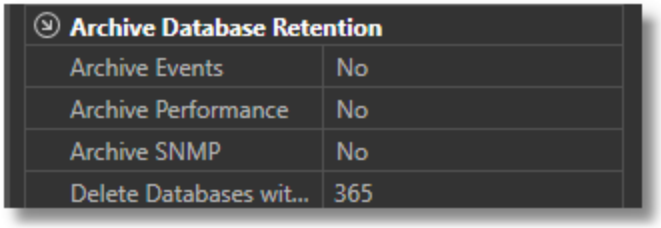
These settings define how much data is keep in the ELM Primary database. Data older than these settings will be either deleted or moved to an archive if enabled.



Archive Database Retention

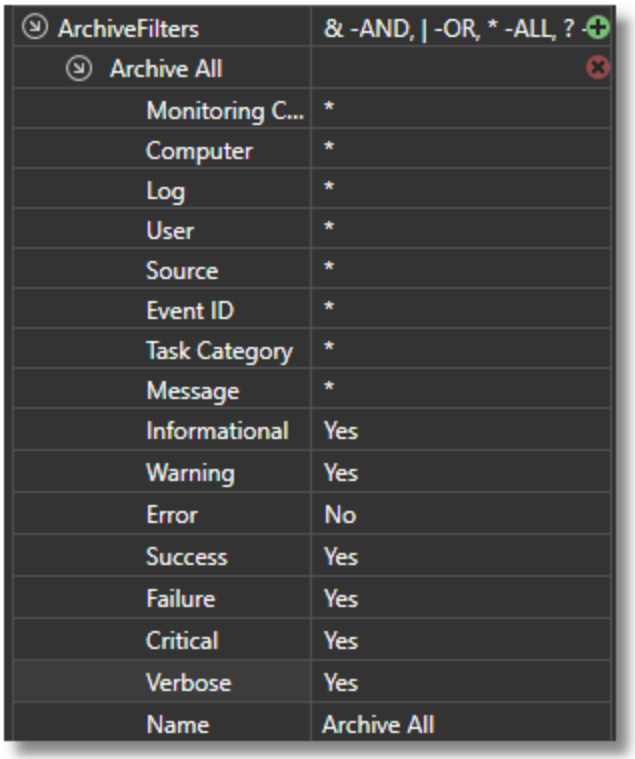
If you want to archive collected data for a period of time this is where you enable archiving. Before you can enable archiving you must first create an archive database. This is accomplished from the Database Wizard 16 located in the Management console Menu.

After you have created the Archive database you can then enable archiving. Once enabled, data from the Primary database will be moved to the Archive database at which point you configure how long you would like to keep the archived data.



Archive Event Filters

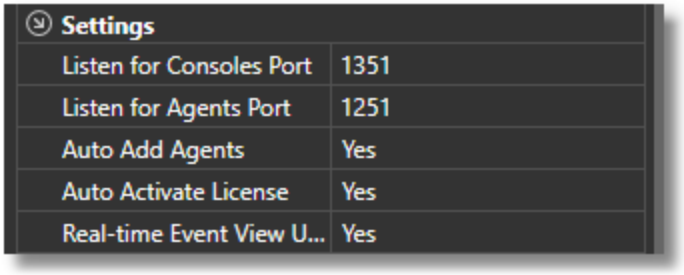
You can create archive filters to define which data in the Primary database you would like to keep in your Archive. For example if you only want to archive security data you can create a filter here to only save those logs; all other data would be deleted once the retention threshold is reached in the primary. Wild card characters (&, |, ?, !,*) may be used in the filter fields. If no archive filter is defined the default will archive all events.



Settings

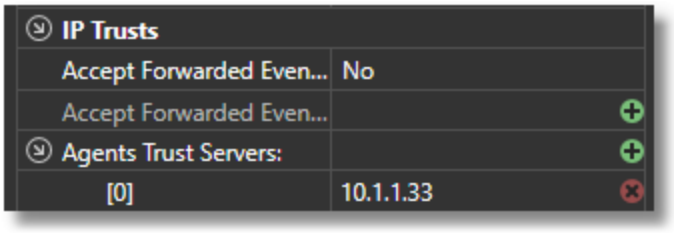
Listen for Console port: This TCP port is used by ELM Management Console to connect to an ELM server.

Listen for Agents Port: This is used by the ELM server services to listen for incoming Agent communications. *If the ELM server is unable to start because the port is in use you will need to to use the Port Wizard located under Menu > New > Server >Port as this Edit dialog is only available when the ELM server is running.*
Auto Add Agents: This setting turns off/on the automatic adding of agents to the ELM Console. Typically used with IP agents when sending syslog message it allows the ELM server to automatically add the agent and collect data without going through the agent deployment wizard.
Auto Active License: This automatically updates your license information from Fire Mountain Software. for support expiration and license changes or addons.
Real-time Event View Updates: When active, event data is sent to the display as received without having to click a "refresh" button. This provides real-time updates to the display but does use more memory and cpu for processing.



IP Trusts

Accept Forwarded Events: When using the Forwarding notification method then allows the receiving ELM server to either accept/reject data forwarded from other ELM servers.

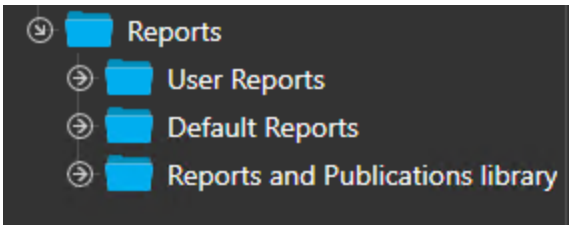


SNMP

Listen for SNMP Traps: Define the port the ELM Server listens for incoming SNMP trap messages.
Receive SNMP Trap from: This is the community string ELM will get messages.
Accept SNMPv3: Allows receiving of secure SNMPv3 messages.

3.5 Reporting

ELM 7.5 contains a completely redesigned reporting engine. The new reporting engine has been simplified however it now allows for easy custom logos and output types.



User Reports - Reports created from existing Event views and/or imported custom reports.

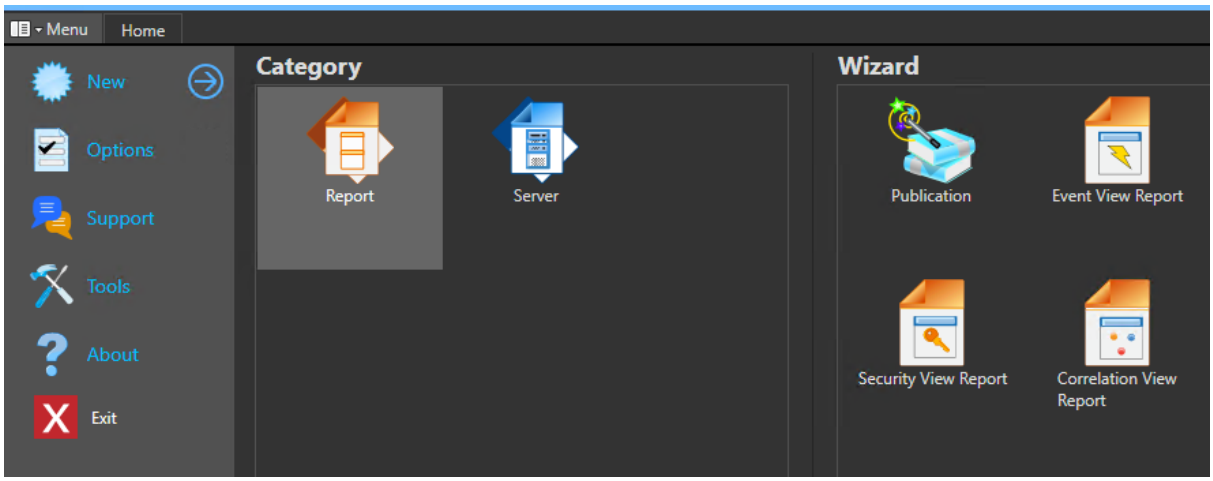
Default Reports - Pre-defined reports to meet the most common needs. These reports include SQL information, Event summaries, Inventory, Performance data and Security reports.

Reports and Publication Library - This section contains a full listing of All reports available in addition to any scheduled Publication reports.

Create a new Report

NOTE: If creating a new report based on an Event view it must be created using the MMC prior to running any report Wizard.

- Open the Windows start menu launch the ELM Management Console using the "Run as Administrator" option.
- In the top left corner select the ELM main "Menu" option.
- After the menu opens Select the Report Category and then select the Wizard type for the report you would like to create which will launch that respective Wizard.

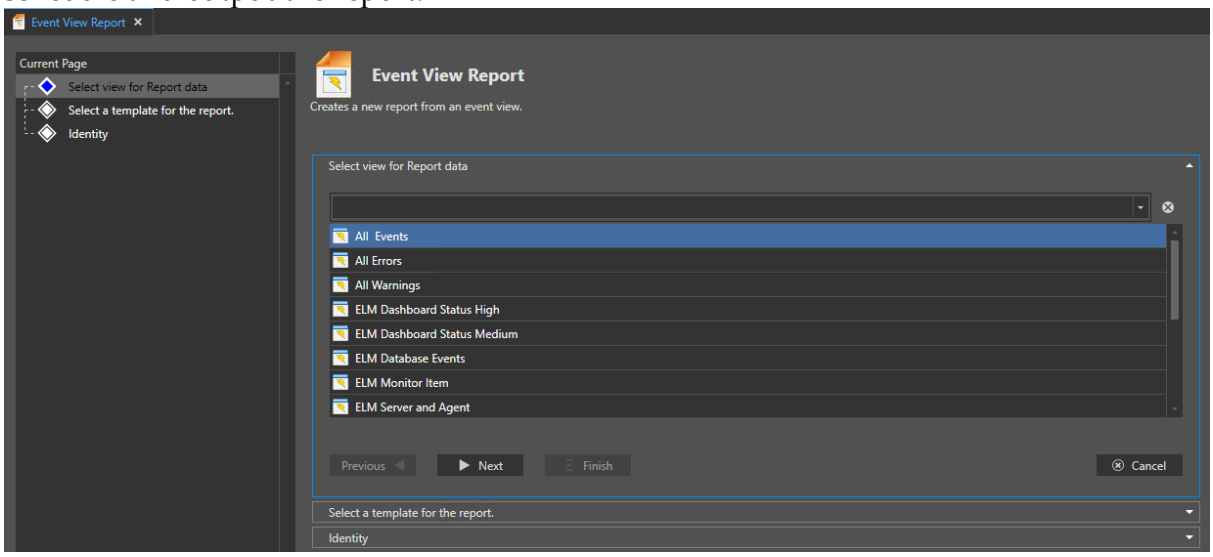


Report Wizard Document pages:

- Select view: Click the name of the view that the report should be based.
- Select template: Templates define how the data is displayed.
- Identity: Define the report name and description.

When finish is clicked the ELM server will install the report and it will become available for preview under the User Reports section in the Explorer panel and also become available in the Publication Wizard.

After you have created the custom Report, you can then use the Publication wizard to schedule and output the report.



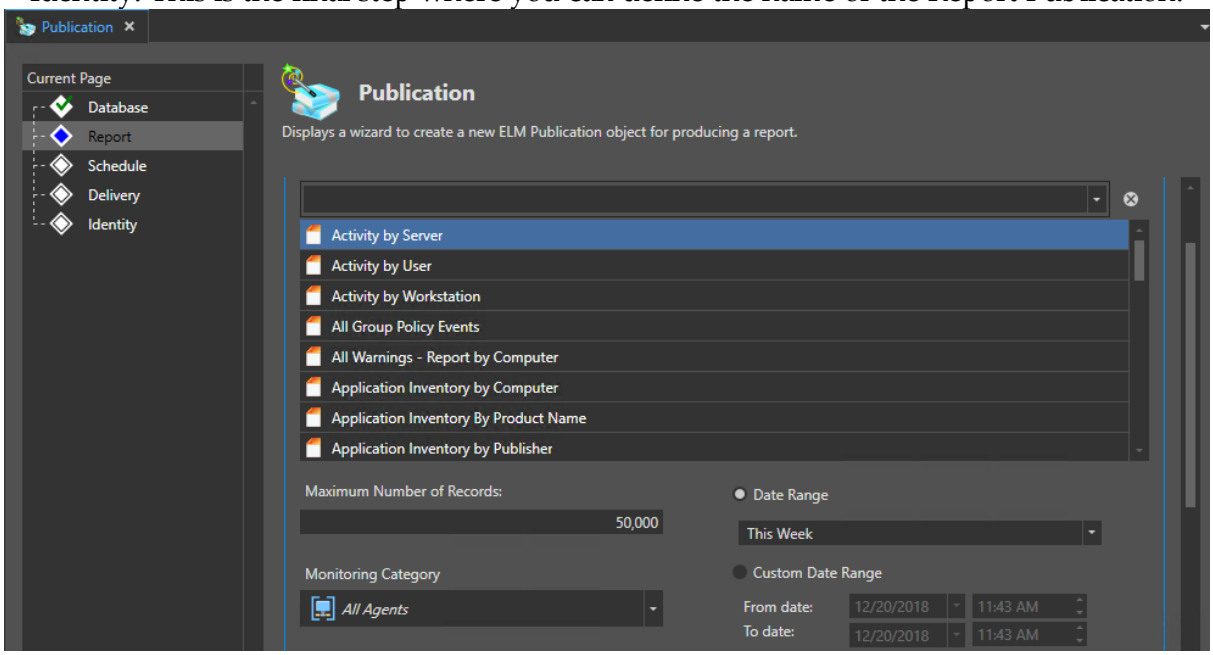
Publish a Report

You can use the Publication wizard to schedule reports, define output types and custom logos for reports.

- Open the Windows start menu launch the ELM Management Console using the "Run as Administrator" option.
- In the top left corner select the ELM main "Menu" option.
- After the menu opens Select the Report Category and then select Publication from the Wizard. This will launch the Publication Wizard document.

Publication Wizard Document pages:

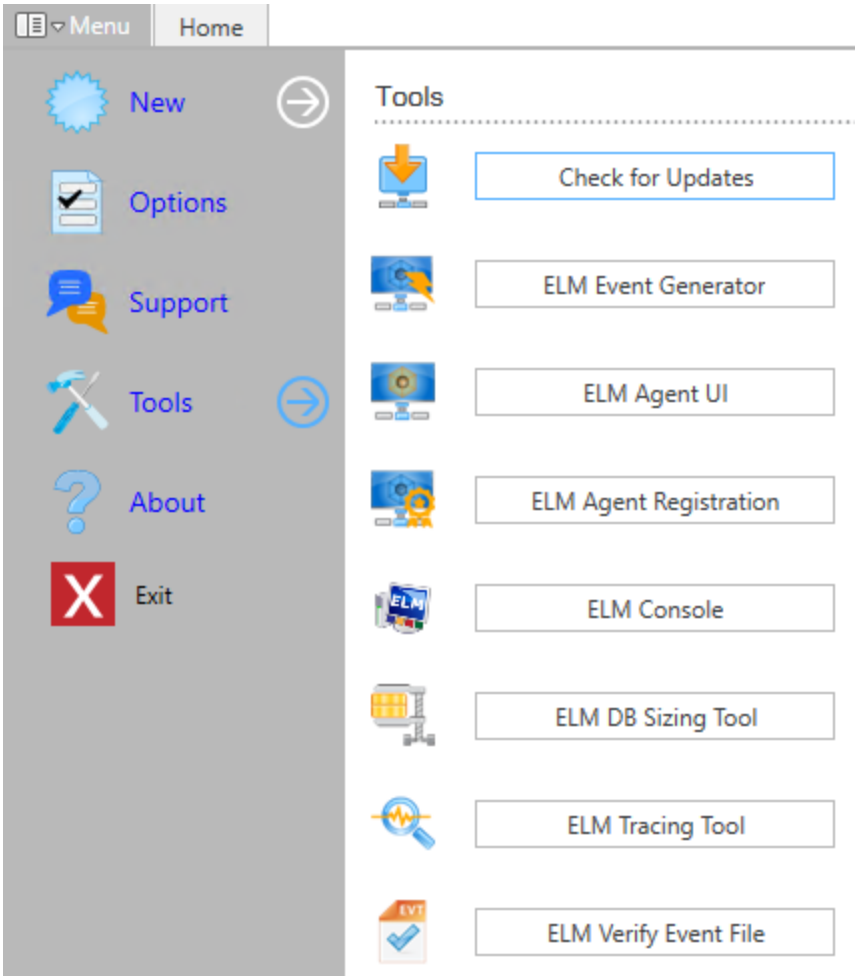
- Database: Select a currently attached database for the source of the report.
- Report: Select and existing report to publish. Use the scroll bar or search box to find the report. This section also has multiple options for the max number of records, date range, Category selection, Header/Footer images and page footer text such as copyright.
- Schedule: Select the time and how often you would like to run the report.
- Delivery: Here you specify how the report will be delivered (Email or file system) and in which format.
- Identity: This is the final step where you can define the name of the Report Publication.



3.6 Tools

Check for Updates: Checks for the latest available version of ELM Enterprise Manager.
ELM Event Generator: May be used to generate test events on local or report servers.
ELM Agent UI: Opens the local ELM Agent for diagnostics
ELM Agent Registration: Opens the local ELM Agent registration wizard.
ELM Console: ELM Legacy user interface. Used for deploying agents, monitor items, notifications and event views.
ELM DB Sizing Tool: Can be used to estimate database size requirements.

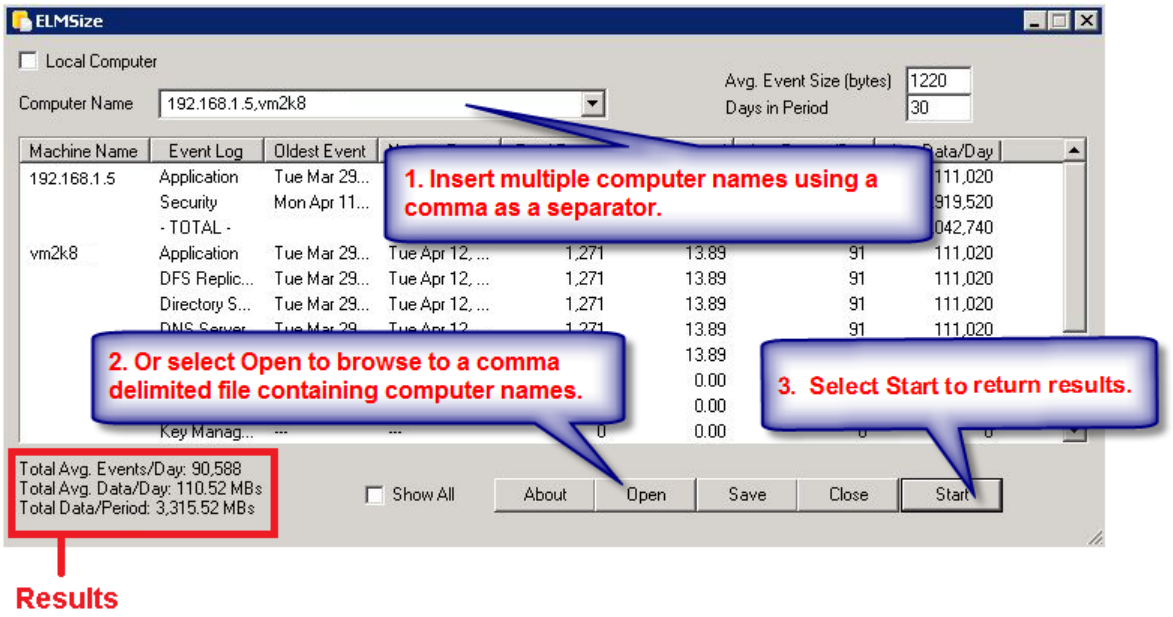
ELM Tracing Tool: Diagnostic tool for troubleshooting.
ELM Verify Event File: Used to Verify previously collected raw .evt/evtx files against a generated hash file. Can also be used to decompress .gz files.



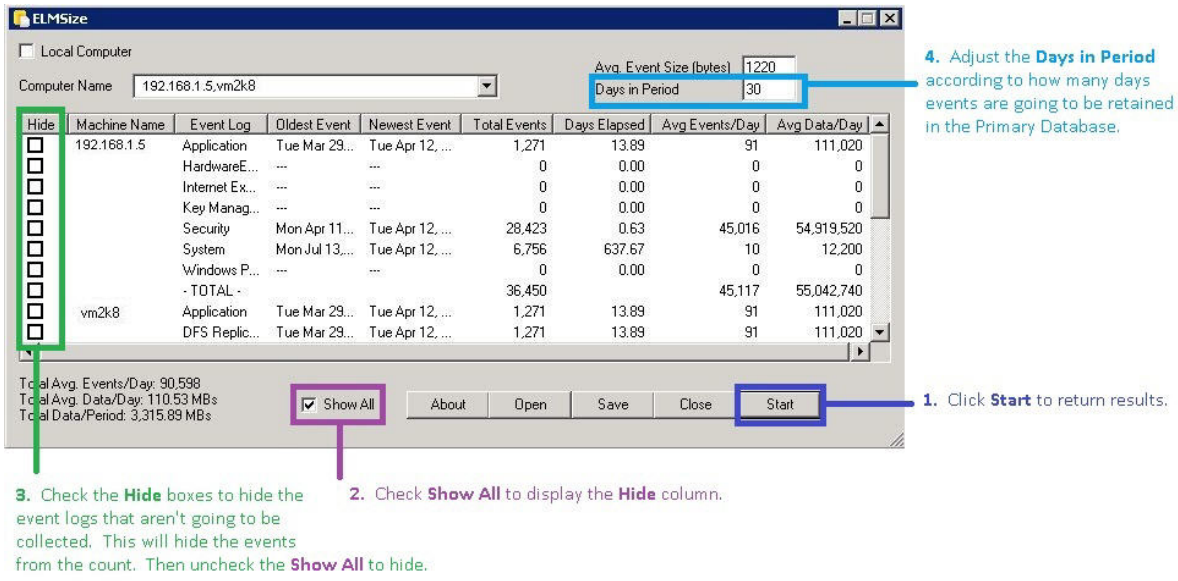
3.6.1 ELM Size

Use this tool to count event data from production servers to get an example of the size requirements to expect for your database. 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.

To Return Event Data:



To Hide Event Data:



Use the **Save** button to save the results to a text file for a report.

Note

*The **Avg. Event Size** has been set by Fire Mountain Software according to the average event size in our database schema.*

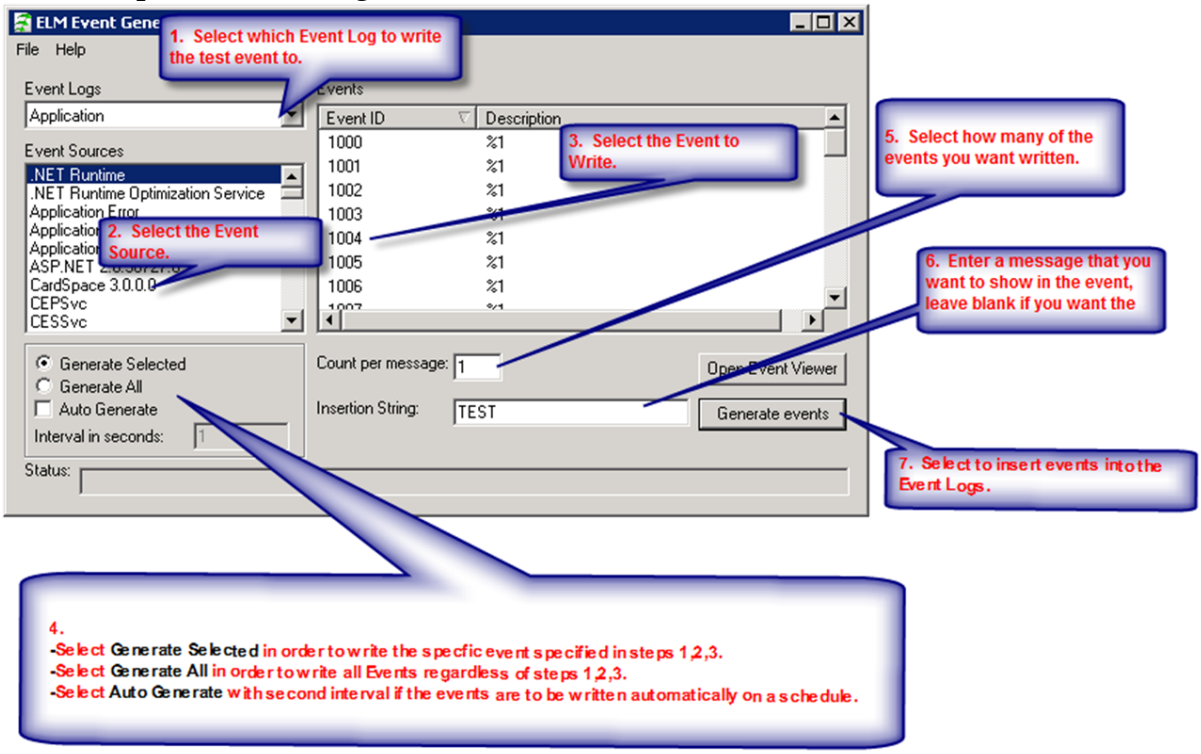
3.6.2 ELM Event Generator

This tool writes Windows events to all available Event Logs for a system **except** for the Security Event Log, Vista and above events, and application specific events. This tool is normally used for testing purposes to ensure that events are being collected or excluded from an agent.

It's located in the Windows Start Menu -> ELM Enterprise Manager -> ELM Event Generator. It can also be found by right clicking on an agent -> Tools -> ELM Event Generator.

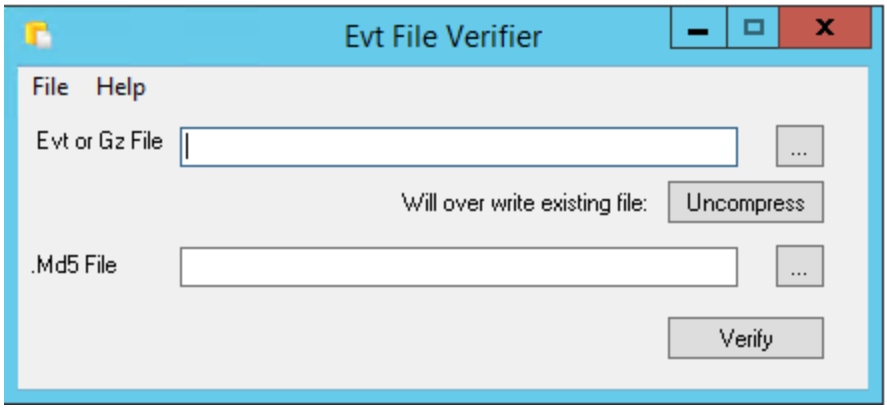
When opened from an agent, the ELM Event Generator is automatically opened in the context of that agent and will display the Event Log sources from that system. To write an event to a different system, in the ELM Event Generator -> File -> Connect to another computer.

Seven Steps to Generating Events.



3.6.3 Event File Verifer

When using the Event File Collector, you have an option to save a md5 hash value. This value is created when the event log is collected and is based on the raw event log or the compressed depending on selected option. The Event File Verifier tool can then be used to verify the integrity of the collected event log file. In addition, if the file is compressed after collection, the tool may also be used to uncompress the file for the hash comparison.



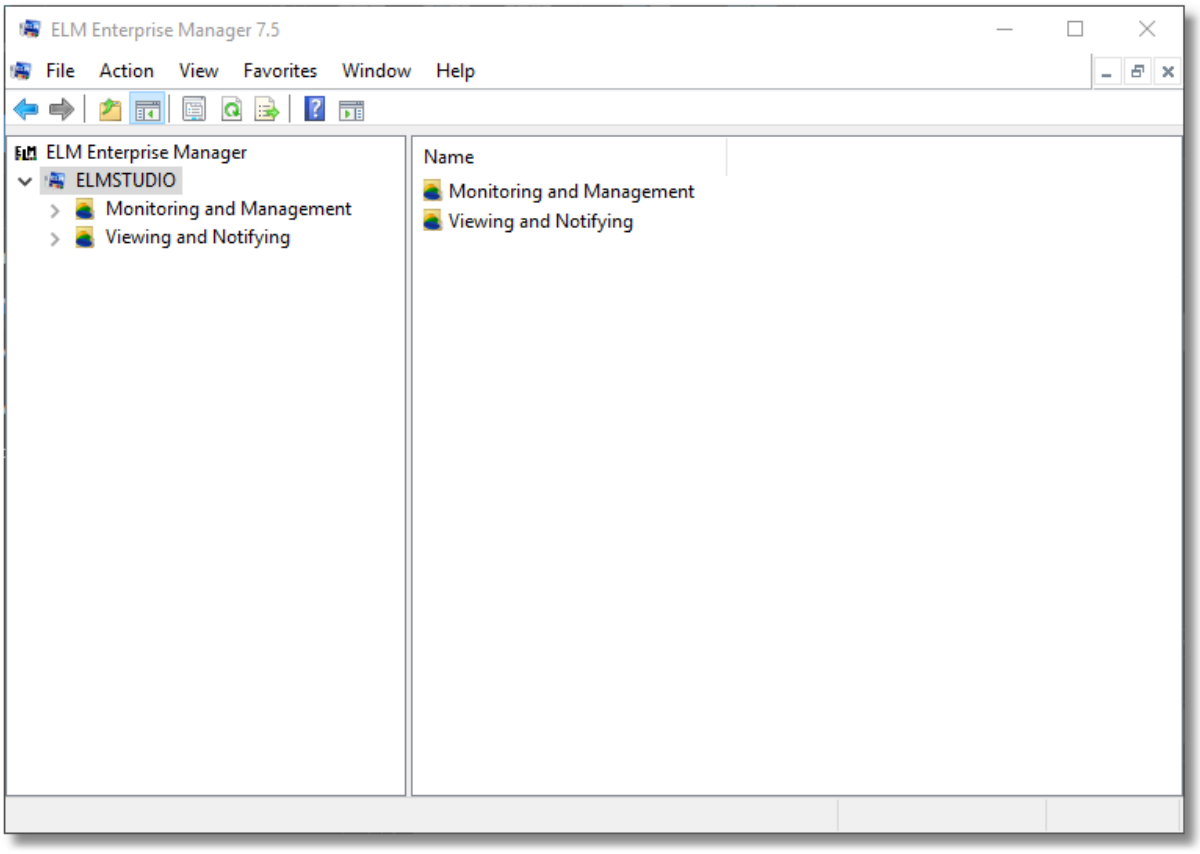
ELM Console (MMC)

4 ELM Console (MMC)

Description

The ELM Console (MMC) provides the classic interface for managing ELM objects. The MMC console is used for configuring ELM Event Views 118, Include/Exclude/Correlation Filters, Monitor Items 40, Notifications, Agent deployment and License Management 138. In ELM 7.5 real-time updates to the display and reporting are no longer available in the classic MMC and are now exclusive to the ELM Management Console.

For advanced viewing of data collection and ELM server setting configuration please refer to the ELM Management Console 16.



4.1 Monitoring and Management

The Monitoring and Management container in the ELM Console is where Agents, Monitor Items, Monitoring Categories and Maintenance Categories reside.
This section includes:
Agent and Monitoring Library 39 - Describes the different agent types, agent licensing options and classes, Monitoring Categories, agent folders, and the agent(s) installation process.
Monitoring Categories 96 - Allows you to group Agents for easy management.

Maintenance Categories 97 - Allows for grouping of Agents for easy management during scheduled maintenance periods.

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 94 must be used. Virtual Agents 83 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.

4.1.1 Agents and Monitors Library

This container includes All Monitors in ELM that are configured to monitor your systems and All Agents lists all systems being monitored by ELM. All Agents is a category within ELM, similar to other Monitoring Categories, but it cannot be modified. It will always show a list of all agents.

Monitoring Capability Feature Comparison

Log Management	Licenses in ELM Enterprise Manager					
Event Monitor	Ev	Cr	····	Sy	Lg	····
Event Collector	Ev	Cr	····	Sy	Lg	····
File Monitor	····	Cr	····	Sy	Lg	····
Event File Collector	····	····	····	Sy	Lg	····
Syslog Receiver	····	····	Nt	Sy	Lg	····
SNMP Receiver	····	····	Nt	Sy	Lg	····
SNMP Monitor	····	····	Nt	Sy	····	····
SNMP Collector	····	····	Nt	Sy	····	····
Health & Status Monitoring						
PING Monitor	Ev	Cr	Nt	Sy	Lg	Pf
Performance Monitor	····	Cr	····	Sy	····	Pf
Performance Collector	····	Cr	····	Sy	····	Pf
Process Monitor	····	Cr	····	Sy	····	Pf
Service Monitor	····	Cr	····	Sy	····	····
WMI Monitor	····	····	····	Sy	····	Pf
Windows Configuration Monitor	····	····	····	Sy	····	····
Inventory Collector	····	····	····	Sy	····	····
Application & Internet Service Monitoring						
TCP Port Monitor	····	····	Nt	Sy	····	····
Cluster Monitor	····	····	····	Sy	····	····
FTP Monitor	····	····	····	Sy	····	····
SMTP Monitor	····	····	····	Sy	····	····
SQL Monitor	····	····	····	Sy	····	····
Web Page Monitor	····	····	····	Sy	····	····
Fault Tolerance Checking						
Agent Monitor	Ev	Cr	····	Sy	Lg	Pf
Event Writer	Ev	Cr	····	Sy	Lg	····

4.1.1.1 All Monitors

Monitor Items control the different types of information collected by ELM. For example, to collect events from a Windows computer, you would use an Event Collector; to monitor services, you would use a Service Monitor; and to watch a performance counter threshold, you would use a Performance Monitor. Below are the Monitor Items included in .

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.

Server Status Monitoring

Event Monitor 42 - Event Monitors trigger action and/or notification when an event does or does not occur. Event Monitors can be configured for Windows 7-10, and Windows Server 2008R2-2016.

4.1.1.1.1 Agent Monitor

The Agent Monitor performs regular checks on ELM Service Agents 94. If the Service Agent fails to respond or responds slowly, actions and notification options can be triggered.

- **Attempt to restart Service Agent if connection attempt fails** - When checked, attempts to restart a stopped Agent remotely by connecting to the Service Control Manager on the remote system.
- **Warn if QoS slower than** - Enter the number of seconds that are considered normal latency for socket sessions to the remote computer. If a socket communication session exceeds this value the **Quality of Service** Action will be triggered. If the Service Agent communicates with the ELM Server over slow or very busy network links, increase this value.
- **Execute configured Action(s) for every failure** - When checked, the **Failed** and **Quality of Service** Actions will be triggered for each interval if the condition is met. Leaving this box empty will create a monitor that generates a warning for the first failed or slow response time only.

- **Failed (Error) 5524** - The ELM Server was unable to connect to the ELM Agent on the monitored computer.
- **Success (Informational) 5525** - The ELM Server successfully re-connected to the ELM Agent after previously failing to connect.
- **Quality of Service (Warning) 5526** - The ELM Agent is responding very slowly.
-

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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

Scheduled Interval tab

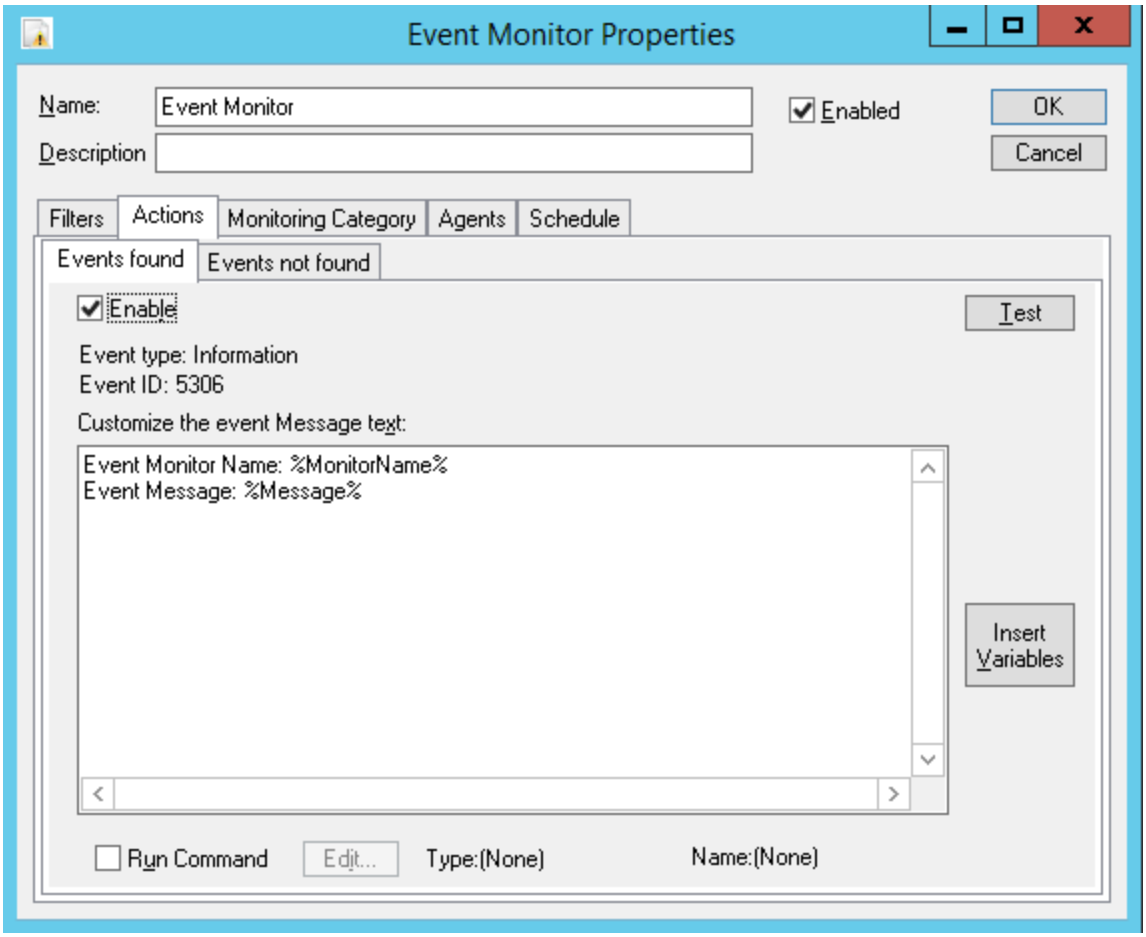
Specify the interval at which the monitoring, polling or action is to occur. Depending on the Monitor Item type, Items can be scheduled in interval increments of Seconds, Minutes, Hours and Days. The Scheduled Interval is relative to the top of the hour or top of the minute. For example, if a Scheduled 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, h1:00:00, 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:01:00, 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.

4.1.1.1.2 Event Monitor

Event Monitor looks at the event logs for a specified event, or lack of that event, within a given time period in order to trigger one or more actions.
When a new event occurs, it is checked against the Filters assigned to the Event Monitor. If it matches at least 1 Include Filter and no Exclude Filters, then the configured Action will be triggered. 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 Monitors, there are two important issues:

1. On very busy systems that generate many event log records, the Event Monitor 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 Monitor 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 Monitor 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 Monitor to monitor all events.

2. When using multiple Event Monitors or 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 Monitors and Event Collectors for the Agent, and then updating the bookmarks. In the case of Event Collectors, they check only their Event Criteria before deciding to process a new event. They do not check their Scheduled Hours. In the case of Event Monitors, they check both their Event Criteria and their Scheduled Hours before deciding to process a new event.

Note: *If ELM is running on Windows Server 2003 or Windows XP, and it's deployed a Virtual Agent to a Windows Vista or above version of Windows, the Event Collector will not be able to be assigned to it. The ELM Console will disallow the assignment due to the lack of support in Windows Server 2003 and Windows XP for Vista and newer Event Logs.*

- **Events not found (Warning) 5307** - An event matching the Event Filter Criteria was not found within the Scheduled time period.
- **Events found (Informational) 5306** - An event matching the Event Filter Criteria was found within the Scheduled time period.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, hh:01:15, etc.

Scheduled Hours tab

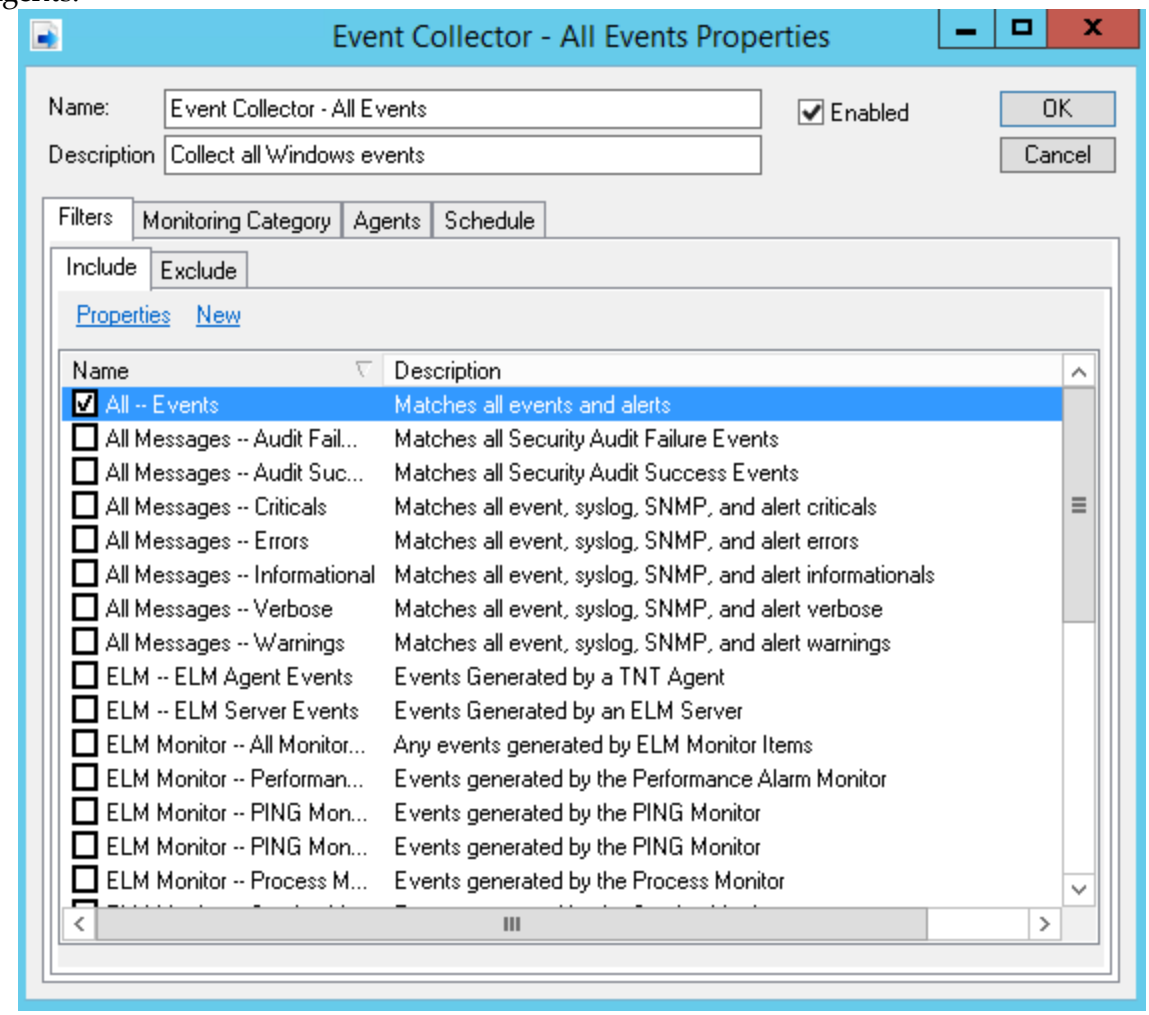
Select the days and/or hours this item is active. By default, the schedule is set to ON for all hours and all days. Mouse clicks toggle squares between ON and OFF. Clicking on an individual square will toggle the active schedule for that hour. Clicking on an hour at the top of the grid, or on a day of 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.

4.1.1.1.3 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 three important issues:

1. On very busy systems that generate many event log records, the Event Monitor 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 Monitor 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 Monitor 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 Monitor to monitor all events.

2. When using multiple Event Monitors or 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 Monitors and Event Collectors for the Agent, and then updating the bookmarks. In the case of Event Collectors, they check only their Event Criteria before deciding to process a new event. They do not check their Scheduled Hours. In the case of Event Monitors, they check both their Event Criteria and their Scheduled Hours before deciding to process a new event.

Note: *If ELM is running on Windows Server 2003 or Windows XP, and it's deployed a Virtual Agent to a Windows Vista or above version of Windows, the Event Collector will not be able to be assigned to it. The ELM Console will disallow the assignment due to the lack of support in Windows Server 2003 and Windows XP for Vista and newer Event Logs.*

Event Collectors do not trigger Actions like the other Monitor Items. For example Ping Monitors results will indicate if an ICMP echo request succeeds, Service Monitors results will indicate if a Windows service is started, etc. 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.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.4 Event File Collector

Event File Collector Monitor Items collect Event Log Files (.EVT and .EVTX) from the Agents being monitored.
The Event File Collector operates at a scheduled interval (the default is every 24 hours). At each interval, the Event File Collector will attempt to talk with the Log service, select the appropriate log files and then copy the specified Event Log Files from the assigned Agents to a defined storage location. The files will be stored by default under the ELM Enterprise Manager installation folder in a sub-directory named **EVT Files**. This location can be modified on the **Behavior** tab of the Event File Collector properties.

Displays the Available Logs the Collector is configured to copy and store. By default, the list of Selected Logs contains an asterisk, so the Monitor will collect all log files possible.

Specific logs can replace the asterisk to collect a subset of log files. Use the check boxes to select the logs you want collected.
To list logs from another system, click the **Choose log source** button and type the name of the server to retrieve the log list.

All events may be cleared from the selected logs after collection by checking the box labeled **Clear Logs after collection**.

Note

When clearing the event logs, if an Agent is also running any Event Collectors or Event Monitors, then the Event File Collector passes any un-read events to them for processing. This may result in events being collected outside of the configured Event Collector or Event Monitors Scheduled Interval.

On Windows 2008, Windows 7, and Vista systems, only logs under the registry key ***`HKLM\SYSTEM\CurrentControlSet\Services\Eventlog`*** *can be collected.*

Windows 2008, Windows 7, and Vista event logs can be collected, but if they are stored on an older Windows system, they cannot be read by the older Windows Event Viewer.

This tab configures where an how to store collected log files.

- The **Destination Folder** controls where to save collected Log files. This can be any existing folder local to the ELM Server.
- The setting **Minimum Free Space Allowed For Evt File Storage** protects free space on the drive hosting the Destination Folder. If the free space on the drive drops below this value, then the ELM Server will stop saving .evt files it receives from an Agent. When this happens, ELM will generate the error event 5595, with a message indicating it's unable to store the event file.
- Log Files may be compressed for storage by checking the **Compress Evt Files** checkbox**.**

A cryptographic hash may be created for collected log files to help verify the log file remains unchanged. Note that both the collected log file and the hash file should be secured from tampering.

- Check the box labeled **Create MD5 Hash File**.

ELM includes a tool to help verify hashed files. It is called **ELM Event File Verifier**, and it can be found in *Windows Start Menu > All Programs > ELM Enterprise Manager*, **or** in *ELM Dashboard > Menu > Tools*. Click to launch the tool.

There are two options:

- Enter a log file name in the File field to select a collected event log. You can also click the ellipsis button to browse to a file. Uncompress will unpack compressed .gz files.

- Enter an md5 file name in the .Md5 File field to select a companion hash file. You can also click the ellipsis button to browse to the file. Click the Verify button to test the file.

The hash value for a collected file can also be calculated with the **Microsoft File Checksum Integrity Verifier** tool. Please see Microsoft Knowledge Base article 841290 for more details.

Select the Monitor Action

- **Copy File Error (Error) 5576** - The selected Event Log file has NOT been successfully copied.
- **Copy File Success (Informational) 5575** - The selected Event Log file has been successfully copied.
- **Store File Error (Error) 5578** - The selected Event Log file has NOT been successfully stored.
- **Store File Success (Informational) 5577** - The selected Event Log file has been successfully stored.

Additionally, the Event File Collector may create one or more of the following events:

- **Agent Save File Error (Error) 5316** - The ELM Agent's install directory does not have enough free space. No event log files will be collected until this much space is available.
- **Store File Warning (Warning) 5594** - A cryptographic hash of the selected Event Log file has NOT been successfully created.
- **Store File Error (Error) 5595** - The selected Event Log file has NOT been successfully stored because of low disk space.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, hh:01:15, etc.

Scheduled Hours tab

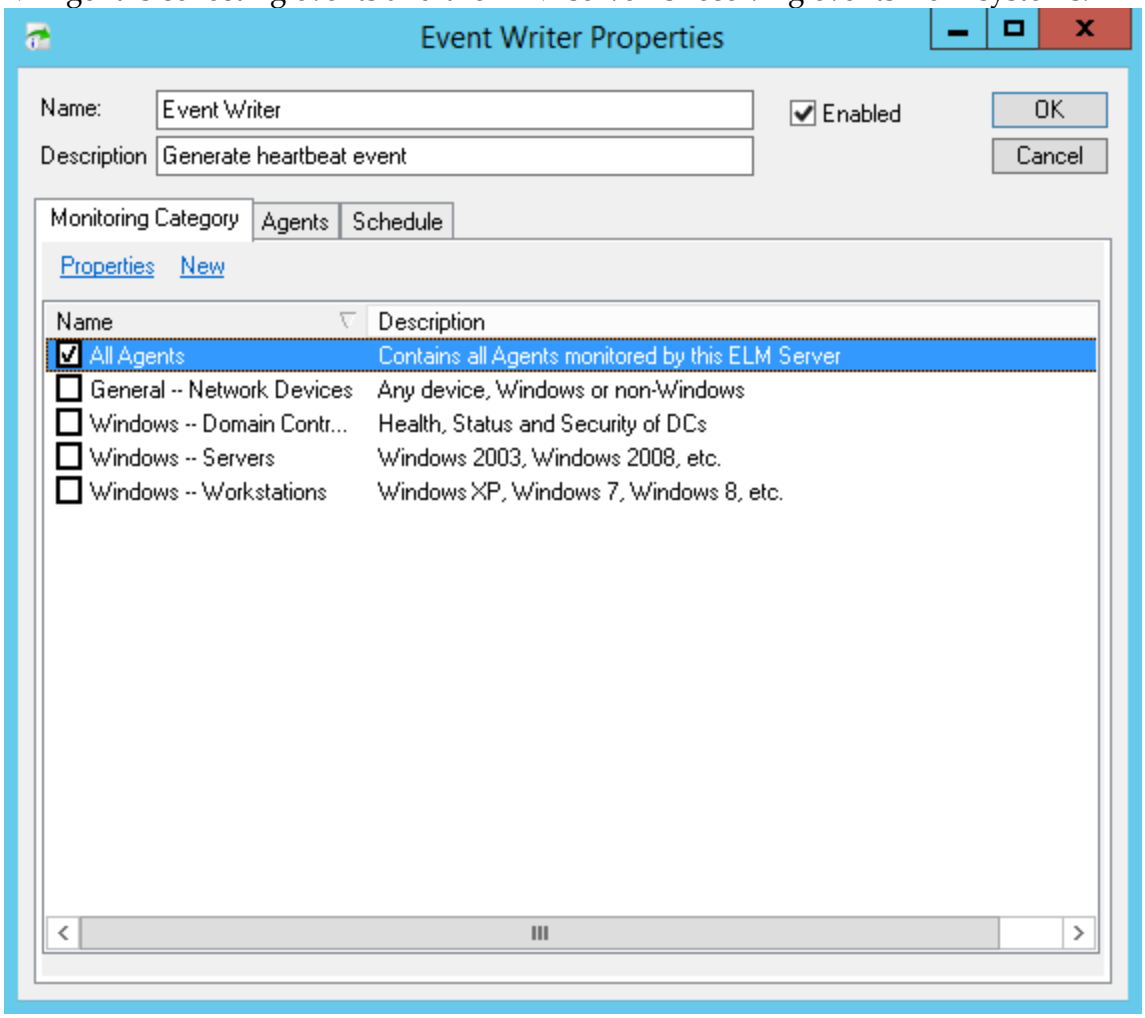
Select the days and/or hours this item is active. By default, the schedule is set to ON for all hours and all days. Mouse clicks toggle squares between ON and OFF. Clicking on an individual square will toggle the active schedule for that hour. Clicking on an hour at the top of the grid, or on a day of 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.

4.1.1.1.5 Event Writer

Heartbeat Event

The Event Writer monitor item allows the ELM Agent to generate a status event on an on-going basis. ELM can be configured to look for this event which helps to verify events are being collected and the system is functioning correctly. This can be used to ensure the ELM Agent is collecting events and the ELM server is receiving events from systems.



Displays the Monitoring Categories[96] to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.6 File Monitor

File Monitor monitors a log file, ASCII file, or text file (or a directory of ASCII or text files). File Monitors parse non-circular text files for words or strings, and notify when the search criteria is found.

Note

Only Service Agents can run a File Monitor, and only local file paths are supported. Virtual Agents, UNC paths and mapped drives are unsupported.

Unicode big endian format is not supported. An explanation of endian architecture can be found here.

If a new copy of a monitored file is created, the File Monitor will detect this and read it as a new file even though the file name has not changed. Windows file system tunneling can mask this change. See Microsoft Knowledge Base Article 172190 for more details.

On 64bit operating systems the File Monitor will use sysnative to access the System32 directory

When it gets to the end of the file, the File Monitor sets a bookmark. At the next Scheduled Interval it will begin reading new *lines* in the file after the bookmark. Since the File Monitor reads in a line-by-line fashion, a line that has additional text added to it after being bookmarked will have these characters skipped, and monitoring will begin on the line after the bookmark.

By default, when the File Monitor is first created, it skips to the end of each file it monitors and sets a bookmark. It then starts watching for character string matches in new lines

added to the file(s). To force File Monitor to search each file for matches from the beginning, add a checkmark next to **Do Actions on First Run**.

Each File Monitor supports one or more search paths. A search path can be a single file or, by using wildcards, a group of files. For example, to search all Internet Information Server logs, use a search path of C:\WINDOWS\SYSTEM32\LOGFILES*.LOG, and check the **Search Subfolders** checkbox. This will cause all log files (HTTP, SMTP, NNTP, and FTP) in all of the sub-directories to be searched for the strings specified.

Important

The File Monitor path must include a filename, or a wildcard pattern. For example:

```
C:\Windows\windowsupdate.log
C:\Windows\kb*.log
```

A path without a file name or pattern will cause the File Monitor to not do anything.

Each File Monitor supports one or more search paths. To add another file path, click the **Add** button.

Enter one or more character strings for the File Monitor search. Use the **Add** button to add a match, and use the **Delete** button to remove the selected match. Double-click any listed match string to edit it.

Note

There is an implied OR-operator between each line of the character strings. For example, given the following list of matches:

```
*error*
*root*
*paycheck*
```

*A line added to a monitored file and containing the string **root** will be found by the File Monitor.*

Enter the word or string you want to search for. You can click the **Insert Variable** button to insert a variable in the search string.

You can use the asterisk (*****) as a wildcard character, a pipe (**|**) as an OR operator, and an ampersand (**&**) as an AND operator. For example, to search a flat file for the word **error** OR the word **failed**, use the following syntax: ***error*|*failed***. Be sure to surround the character string with asterisks.

Click **OK** to save the match criteria.

Note
It is not possible to search for strings across multiple lines because the File Monitor reads in a line-by-line fashion. *For example, searching for *failed logon* will work if the text is all on one line but if the **failed** text is on one line, then there is a carriage return in the file with the text **logon** in the next line, then the File Monitor won't detect it.*
Each string match added to the **Matches** tab will add a corresponding sub-tab to the **Actions** tab. So File Monitor Actions can be customized for each string found.

- **Custom Action (Warning) 5532** - A custom action is added to the Actions list for each search string entered in the Match list (see Add Match above).

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.7 FTP Monitor

An FTP Monitor item monitors the status and availability of an FTP site. Any valid and accessible FTP server can be monitored by the ELM Enterprise Manager Server. An application-layer FTP connection to the FTP Server is made at your specified interval.

Anonymous or authenticated connections are supported. By default, port 21 is used, but the Monitor can be configured to use any port.
Because the ELM Enterprise Manager Server (and not an Agent) makes the FTP connection, you can monitor FTP server availability on any operating system running FTP server software (e.g., Unix, Linux, Novell, Solaris, etc.) Though an agent must be assigned to the FTP server.

- **Username** - Can be a specific username or can be set to anonymous.
- **Password** - Password for the account specified in the Username field. If you entered **anonymous** for the username, enter any SMTP address as the password.
- **FTP Port** - The port to which you want the FTP Monitor to connect. By default, TCP port 21 is used. However, you can specify any valid TCP port that is used by the FTP server.
- **Warn if QoS slower than __ seconds** - You may also monitor the FTP server's performance by monitoring how quickly a response is returned. By specifying a value for this field, you can cause a warning message to be generated whenever the response from the FTP server exceeds the threshold you specify here.
- **Execute configured Action(s) for every failure** - By default, ELM will notify you once when the FTP server is unavailable. By checking this box, you can specify that failure Actions be executed at each failure.

Note
The FTP Monitor doesn't have a FTP site setting, assign the FTP Monitor to the agent that is hosting the FTP Site.

- **Failed (Error) 5503** - The FTP Monitor was unable to connect to the configured FTP site.
- **Success (Informational) 5504** - The FTP Monitor was able to connect to the configured FTP site.
- **Quality of Service (Success) 5505** - The FTP Monitor was able to connect to the configured FTP site, but not within the configured QoS time period.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, hh:01:15, etc.

Scheduled Hours tab

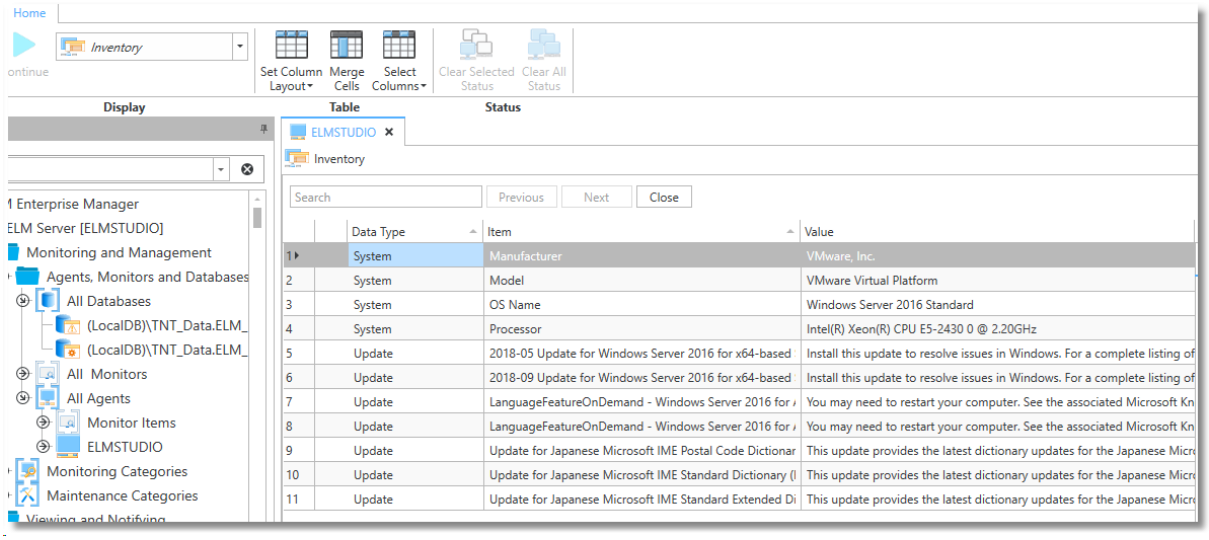
Select the days and/or hours this item is active. By default, the schedule is set to ON for all hours and all days. Mouse clicks toggle squares between ON and OFF. Clicking on an individual square will toggle the active schedule for that hour. Clicking on an hour at the top of the grid, or on a day of 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.

4.1.1.1.8 Inventory Collector

The Inventory Collector gathers data about the OS, installed applications, Windows updates and basic hardware information on each service-based Agent.
Note:
Applications installed on a per-user basis will not be collected by the Inventory Collector.

The Inventory Collector can also trigger Monitor Item Actions when an item is added to or removed from the inventory.

Inventory data is displayed in the ELM Management console by selecting the specific Agent document then choosing the Inventory display from the Ribbon Toolbar.



By default, all products will be included in the inventory.

- **Items Added (Warning) 5571** - An item was added to the inventory. For example, an application was installed.
- **Items Removed (Warning) 5572** - An item was removed from the inventory. For example, an application was uninstalled.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.9 Performance Monitor

A Performance Monitor is triggered when a selected performance counter, or instance of a counter, is less than, greater than, or equal to a specific value. Performance Monitors specify what action is to be taken when a performance counter or instance meets the specified criteria.

- **Object** - Use the dropdown to select the performance object to be monitored.
- **Counter** - Use the dropdown to select the performance counter to be monitored.
- **Monitored Instances** - Click the Add/Remove button to change the Instances of the counter to be monitored. Enter the instance(s) of the counter to be monitored. All instances listed in this field are monitored. Use an asterisk (*) or leave the instance field blank to monitor all detected instances of the counter. If no instances are entered, all instances are evaluated.
- **Condition** - Select the condition to be matched:

<	Less Than
<=	Less Than or Equal To
=	Equal To
>=	Greater Than or Equal To
>	Greater Than
<>	Does Not Equal

- **Value** - The threshold value with which the performance counter is compared. Enter only numbers and a decimal point in this field. Performance counters that use percentages (e.g., % Processor Time, % Free Disk Space, etc.), will be automatically translated. For example, 50.000000 in the Value field is translated to 50%.
- **Occurs __ Consecutive Times** - Enter the number of times **Value** must meet the specified Condition before triggering any enabled Actions.

Note

The Consecutive Times count is based on consecutive results after the initial Performance Monitor threshold has been met. For example, if the Scheduled Interval is 5 minutes and the Consecutive Times is 2, then it will be at least 10 minutes before the first Actions are triggered. After this, if results continue to be true, then Actions will be triggered every 5 minutes.

- **Warning 5527** - The monitored Performance Counter condition is true.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit

Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.10 Performance Collector

Performance Collectors are sets of one or more performance objects, counters and/or instances that are grouped together for collection and aggregation. ELM Enterprise Manager is pre-populated with a variety of Performance Collectors. These can be edited or custom Performance Collectors can be created. Each Performance Collector has three parts: the counters to be collected; the frequency of the collection (e.g., every 30 minutes, every hour, etc.); and the days on which collection occurs.

ELM is pre-populated with Performance Objects and Counters that are protected from editing. If the required object, counter or instance is not listed, it can be added from a Windows computer that publishes the counter.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect

individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.11 Ping Monitor

The Ping Monitor sends version 4 ICMP echo requests to the Agents being monitored. You may specify the size of the echo request packets and the number of packets that are sent. The Ping Monitor will execute the configured Actions, depending on the results of the Ping.
Even though the Ping Monitor is assigned to Agents, it is always executed by the ELM Server.

Packet Size (bytes) - Enter the size of the ICMP echo request (e.g., the size of each ping packet), in bytes, to send at each ping interval.
Repeat (packets) - Enter the number of packets to send at each interval.
Timeout (seconds) - Enter the time, in seconds, to wait for a response.

The Ping Monitor will execute the enabled Actions for various state changes.

Success

- **Success to Success (Informational) 5489** - All previous ICMP echo requests received a reply and all current requests returned a reply.
- **Warning to Success (Informational) 5492** - Some previous ICMP echo requests did not receive a reply and now all requests have been received.

- **Failed to Success (Informational) 5507** - All previous ICMP echo requests did not receive a reply but now all succeeded.

(Check Box) Run Command: If enabled the ELM server can execute scripts as part of the Success Action.

Warning

- **Success to Warning (Warning) 5508** - All previous ICMP echo requests received a reply and now some received a reply.
- **Warning to Warning (Warning) 5493** - Some previous ICMP echo requests did not receive a reply and are still not being recieved.
- **Failed to Warning (Warning) 5490** - All previous ICMP echo requests did not receive a reply but some were now received.

(Check Box) Run Command: If enabled the ELM server can execute scripts as part of the Warning Action.

Failed

- **Success to Failed (Error) 5506** - All previous ICMP echo requests received a reply and now NONE received a reply.
- **Warning to Failed (Error) 5491** - Some previous ICMP echo requests did not receive a reply and now none were received.
- **Failed to Failed (Error) 5488** - All previous ICMP echo requests did not receive a reply and all current attempts failed.

(Check Box) Run Command: If enabled the ELM server can execute scripts as part of the failed Action.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.12 Process Monitor

The Process Monitor monitors Windows processes when assigned to an Agent. The Process Monitor is multi-functional; it can notify you when a process has exceeded the threshold of CPU usage you specify and it can track when processes are started or terminated.
Each Process Monitor item supports multiple match criteria. Use the **Add** button to add a match criterion. Use the **Delete** button to remove a listed match criterion. Double-click any listed item to edit it.

Click the **Add** button to enter the name of the process or processes you want to monitor.
Note
The name of the process to monitor is derived from the Processes object in Windows. This name does not always match what you see in Task Manager. You should verify the name of the process you wish to monitor by using a utility such as Performance Monitor.
You may use the asterisk (*****) as a wildcard character, a pipe (**|**) as an OR operator, the ampersand (**&**) as an AND operator, and the exclamation point (**!**) as a NOT operator. Process names can be entered on separate lines for exclusion. For example, to exclude the **_Total** and **Idle** processes, you can enter them like this:

```
!_Total
!Idle
```

Click **OK** to save your changes.
Select a line in the **Processes to Monitor** window and click the **Delete** button to remove the line from the list.

Note
The Default pre configured Process Monitor is setup to watch all processes with the exception of _Total and Idle.

Enter threshold triggers for the Process Monitor.

CPU Usage

- **Warning when % Processor Time is greater than** - Executes the enabled CPU Warning Actions when the CPU utilization of a monitored process exceeds the value.
- **Error when % Processor Time is greater than** - Executes the enabled CPU Error Actions when the CPU utilization of a monitored process exceeds the value.

Note
The ELM Process Monitor recognizes multi-processor systems and calculates an overall system utilization. For example, given a quad-processor system and the processor utilizations shown, system utilization would be about one-third:

Processor 0 = 25% utilization
Processor 1 = 50% utilization
Processor 2 = 25% utilization
Processor 3 = 50% utilization
Total = 150%
Possible = 400%
System = 150/400 = 37.5% utilization

Number of Processes With the Same Name

- **Warning when the number is greater than** - Executes the enabled Process Count Warning Actions when the number of processes with the same name exceeds the value.
- **Error when the number is greater than** - Executes the enabled Process Count Error Actions when the number of processes with the same name exceeds the value.

Process Monitors can notify you when a process is started or terminated. These settings can be found on the **New Process** and **Process Ended** tabs of the Process Monitor's **Actions** dialog.

- **CPU Error (Error) 5534** - A monitored process is using more CPU than the **Error when % Processor Time is Greater Than** value specified under Thresholds (see above).
- **CPU Warning (Warning) 5533** - A monitored process is using more CPU than the **Warning when % Processor Time is Greater Than** value specified under Thresholds (see above).
- **New Process (Informational) 5535** - A new process was found in the list of monitored processes.
- **Process Ended (Warning) 5536** - A process disappeared from the list of monitored processes.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.13 Service Monitor

Service Monitor items monitor services and devices on Windows computers. The Monitor will trigger Actions when a service or device state changes (e.g., running to stopped, stopped to started, etc.). Service Monitor items also allow you to take action and/or be notified of services or devices that are set to Automatic startup but aren't running.
If a service or device is set to manual startup and its state changes from started to stopped, the Event Log Message that is generated is a Warning message. If a service or device is set to automatic startup and its state changes from started to stopped, the Event Log Message that is generated is an Error message.
If you have a service or device that is set to Automatic startup but not running, the Service Monitor item will generate an event to notify you about this condition. If you want to be repeatedly notified about this condition, put a check in the box labeled **Execute configured Action(s) at every scheduled interval for AutoStart services that are stopped**. This will cause the designated actions to be executed at each scheduled interval
Note
*A checkmark will not cause repeated action if a service or device is set to **Manual** startup and is not running. Repeated action is executed with this checkmark only when the service or device is set to **Automatic** startup and is not currently running.*

To add a service or device, enter the service or device name in the Service field. Wildcards are supported in this field. To monitor all services and devices enter an asterisk (*). You can use other Boolean operators, such as and (**&**) and Not (**!**). The Service Monitor looks for matches based on both the display name (long name) and the internal name (short name) of a service or device. For example, the long name of the Windows Web service is **World**

Wide Web Publishing and its short name is **W3SVC**. If a service's long name or short name matches the filter, it is added to the internal list of services and devices to monitor. Since both names are monitored, to exclude a service requires matches for both names. For example, to exclude the Windows Web service, enter strings that matches both its names. Service names can be entered on separate lines for exclusion. For example:

```
!*World*Wide*Web*Publishing*
!*W3SVC*
```

- **Running (Informational) 5530** - A service state has changed to a started status.
- **Stopped (Error) 5528** - A service state has changed to a stopped status.
- **Stopping (Error) 5529** - A service state has changed to a stopping (stop pending) status.
- **Starting (Informational) 5531** - A service state has changed to a starting (start pending) status.
- **Paused (Warning) 5573** - A service state has changed to a paused status.

Each Action also has an associated Run Command that is able to execute a script after a state change has occurred. Here is an example cmd script to restart failed services on a Service or Virtual agent:

```
:: Restart Failed Service on Service Agent or Virtual Agent
:: If the computer being monitored is the local computer
:: use NET START, otherwise use SM.EXE to restart
:: the service on the remote computer
if "%COMPUTER%"=="" goto failed
if "%SERVICE%"=="" goto failed
:: Check to see if the failed service is on the
:: local computer or a remote computer
if /I "%COMPUTER%"=="%COMPUTERNAME%" goto do_local
if /I NOT "%COMPUTER%"=="%COMPUTERNAME%" goto do_remote
:do_remote
SM.EXE \\%COMPUTER% "%SERVICE%" /START
goto finished
:do_local
NET START "%SERVICE%"
goto finished
:failed
echo A required environment variable is not defined. >.\Error.log
echo The service cannot be re-started. >>.\Error.log
goto finished
:finished
:: End
```

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect

individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.14 SMTP Monitor

SMTP Monitors watch SMTP hosts, gateways and services. If you are using a Service Agent, the Service Agent will periodically establish an SMTP connection to the server and port specified. If you are using a Virtual Agent or an IP Virtual Agent, the SMTP polling is done by the ELM Server. The SMTP Monitor connects to the SMTP Server and times the initiating conversation from "EHLO" to "250 OK." Enabled Actions are executed depending on successful, slow, or failed responses. Negative or slower-than-expected responses trigger a variety of notification options. Several settings are available for SMTP Monitors:

- **Port** - Enter the port to which the SMTP Monitor should connect on your SMTP server. By default, SMTP communication occurs over TCP port 25. You can specify any valid TCP port used by your SMTP server.
- **Warn if QoS slower than __ seconds** - You may monitor your SMTP server performance. By specifying a value for this field, a warning message will be generated whenever the response from the SMTP server exceeds the threshold you specify here. The maximum QoS allowed is controlled by the **HKEY_LOCAL_MACHINE \ SOFTWARE\ TNT Software \ ELM Enterprise Manager \ 7.5 \ Settings\SMTPMaxTimeoutInSeconds** registry key.
- **Execute configured Action(s) for every failure** - By default, ELM will notify you only the first time the SMTP server is unavailable. Check this box to have a message sent for each interval that the SMTP server is found to be unavailable.

- **Failed (Error) 5509** - The connection to the SMTP server could not be made, or the Monitor waited more than 2 QoS intervals.
- **Success (Informational) 5510** - The connection to the SMTP server could be made.
- **Quality of Service Warning (Warning) 5511** - The connection to the SMTP server could be made, but took longer than the Quality of Service time period.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.15 SNMP Monitor

The Simple Network Management Protocol (SNMP) communicates management information between network management stations and agents, and is defined in RFC 1157.

The ELM Server can listen for and receive SNMP traps from any SNMP-compliant system or device on your network. Traps are treated as events; they will appear in event views, they will be stored in the database, and you can assign notification

methods to trigger when any SNMP trap is received. By default, the Windows SNMP Service listens on UDP port 162, the default SNMP Trap port.
An ELM Agent can run an SNMP Monitor to query an SNMP Object ID (OID) and trigger an action if the value becomes greater than, less than or equal to a user configured value. The SNMP Monitor includes an object browser for you to query the namespace on an SNMP-capable device, and walk the SNMP tree to select the specific OID for monitoring.
See the ELM SNMP Notification Method 114 for details about using ELM to send an SNMP trap, or put an SNMP OID value.

Every SNMP-capable device includes manageable objects that are defined in one or more Management Information Bases (MIBs). Manageable objects include network identification, statistics, protocol information, performance data, and hardware and software configuration details. Each object within an MIB is identified by its object-identifier (OID), which is unique.
ELM Enterprise Manager includes an SNMP Monitor that will query an SNMP Object ID (OID) and then compare the result to a specified value. If the comparison yields a true, then the Warning Action is triggered. If the comparison yields a false, the Success Action is triggered. If the SNMP Monitor is unable to retrieve a value, the Failure Action is triggered. The SNMP Monitor includes an object browser and MIB browser for selecting the OID.

There are several settings for SNMP Monitors.

- **Host Computer** - The network name or IP address of the SNMP agent to be walked when the **Display Objects from computer/community** button is clicked.
- **Community** - The SNMP Community recognized by the SNMP agent. The Windows SNMP service on the ELM Server computer must be configured to use this Community as well.
- **Timeout (milliseconds)** - The amount of time the ELM SNMP Monitor will have the Windows SNMP Service wait for a response from the SNMP agent between retries.
- **Retries** - The number of attempts the ELM SNMP Monitor will have the Windows SNMP Service make contacting the SNMP agent before giving up and triggering the Failure Action.
- **Display Objects from computer/community** - Queries the specified Host Computer and Community for SNMP OIDs and values. Depending on network conditions, the SNMP Agent and the size of the namespace, the query may take several minutes. When complete, the root of the SNMP namespace will appear in the large Object Tree Browser window.

Note
*By adding the registry value **HKEY_LOCAL_MACHINE\SOFTWARE\TNT Software\ELM Enterprise Manager\7.5.0\Settings\SnmpRootOID** on the ELM Console computer, you can specify an OID root different from .1.3.6.1 when **Display Objects from a***

computer/community *is clicked in an SNMP Monitor Item or SNMP OID Notification Method. The root OID must be in numeric form.*

- **Object Tree Browser** - Once data is retrieved from the SNMP Agent, the tree can be expanded and collapsed by clicking on the plus (+) and minus (-) controls. When a branch or leaf node is selected, the Object Identifier is displayed. If a leaf node is selected, the value returned by the SNMP Agent is displayed.
- **Object Identifier** - When a branch or node is selected in the Object Tree Browser window, the corresponding Object Identifier (OID) is displayed here. If the OID is known, it can be entered into this field. It should be typed in dotted numeric format, typically starting with .1.3.6.1.
- **Condition** - The criterion used by the SNMP Monitors to compare the OID value with the specified value.
- **Value** - This field has two uses:
    - When a leaf node is selected in the Object Tree Browser window, the most recently retrieved value for that leaf node will be displayed here. To refresh the values, click the **Object Tree Browser** button again.
    - This field is used to enter the value used by the SNMP Monitor to evaluate the Condition.
- **Execute configured Action(s) for every warning and failure** - Check this box to configure the SNMP Monitor to trigger repeated Warning and Failure Actions.

During install, Windows copies a compiled MIB library called **MIB.bin** into the system32 directory. This file provides OID-to-name translation for a portion of the OID namespace tree. It does not generally include the namespace used by third-party SNMP agents. ELM can read vendor-provided MIB files and add to the namespace provided by the Windows SNMP service. When ELM is installed, it creates a **MibFiles** sub-directory for third-party MIB files. Place the vendor-supplied MIB file in the **MibFiles** folder, and use the **MIB Files** browser to select them. The **Add** button in the MIB Files Browser can also be used to put a copy of vendor-supplied MIB files in the **MibFiles** folder.

- **Success 5551** - The retrieved OID value comparison with the configured value yielded a false.
- **Warning 5552** - The retrieved OID value comparison with the configured value yielded a true.
- **Failure 5574** - The SNMP Monitor failed to retrieve the configured OID value.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.16 SNMP Collector

SNMP Collector Monitor Items can collect SNMP OID values from systems being monitored by an ELM Agent. Data can be collected based on one or more OIDs.

- The SNMP Collector requires the Windows **SNMP** and **SNMP Trap** services.

The SNMP Collector Monitor Item operates by polling the device at a scheduled interval and then writes this data to the ELM database.

SNMP Collectors behave like Performance Collectors. Performance Collectors query monitored Windows servers for defined statistics and return that data to the ELM Primary Database. An SNMP Collector's job is to collect the data provided by an SNMP Agent using the Simple Network Management Protocol and deliver the records to the ELM Server.

Displays the **OID**, **Translated Name**, and the **Community** fields. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent. After receiving an SNMP request, the SNMP agent compares the community string in the request to the community strings that are configured for the agent.

- The **Add OIDs** button opens the **SNMP OID Selector** window. This window provides the opportunity to select specific OIDs to monitor. OIDs may be browsed from a server or from a MIB file.

- The **Show OIDs** button on the **From Server** tab queries the specified Host Computer and Community for SNMP OIDs and values.
- The **Restore Defaults** button resets the **From Server** tab to the original settings.
- The **Add** button on the **From MIB** tab provides the ability to browse to a MIB file located elsewhere and add it to the list of MIB files available.
- The **Remove** button on the **From MIB** tab removes selected MIB files from the available list.
- The **Translate MIB** button on the **From MIB** tab converts the MIB file into the hierarchical tree format for browsing and selection of specific OIDs.

- The **Remove** button will delete any selected OIDs from the Collector window.

During install, Windows copies a compiled MIB library called **MIB.bin** into the system32 directory. This file provides OID-to-name translation for a portion of the OID namespace tree. It does not generally include the namespace used by third-party SNMP agents. ELM can read vendor-provided MIB files and add to the namespace provided by the Windows SNMP service. When ELM is installed, it creates a **MibFiles** sub-directory for third-party MIB files. Place the vendor-supplied MIB file in the MibFiles folder, and use the MIB Files browser to select them. The **Add** button on the **From MIB** tab is used to browse to the vendor-supplied MIB file.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.17 SNMP Receiver

The SNMP Receiver receives traps and translates them via a MIB file. ELM can receive **SNMP traps** sent from any SNMP management system or from another ELM Server. In order to receive **SNMP traps** on the ELM Server:

- **Windows SNMP Trap Services must Not be running**.
- **ELM Management Service must be running.**

SNMP Monitor

The default SNMP Receiver monitor item will translate OID values to names. To use this feature a MIB file for a device sending traps must be copied to the **MibFiles** sub-folder under the ELM install folder. When traps are received by ELM it will then translate the OID from numeric to text labels as defined in the MIB.

Auto Assign

By default, the SNMP Receiver monitor item will be automatically assigned to any agent that sends SNMP Traps to the ELM server. If unchecked, you must manually assign the monitor item to agents.

Event Filters

By default, the SNMP Receiver defaults to collecting all SNMP Traps when there isn't an Include Filter assigned to it. See Event Filters for further information.

Categories

Displays the Monitoring Categories 96 to which the Monitor is assigned. Click to select or deselect Monitoring Categories. Right click or click the New link to create or edit Monitoring Categories.

Displays the Agents to which the Monitor is assigned. Click to select or deselect Agents. Right click or click the New link to deploy a new agent.

4.1.1.1.18 SQL Monitor

Using SQL Monitors, you may periodically execute SQL queries against a database and generate a variety of notification options. SQL Monitors support default and named instances, and Windows and SQL Server authentication, making it easy to fit into your existing SQL security environment.

SQL Monitor Settings

- **Query** - Enter a SQL query to be executed by the monitor. An event will be triggered if the results are different from the last time the query was run. Enter the SQL instance name in the **Instance Name** field if necessary. Otherwise leave blank for the default instance.
- **Logon** - The SQL Monitor supports SQL Authentication and Mixed Mode Authentication.
  - If you are using integrated (Windows) authentication, then check the **Use Integrated Logon** checkbox.
  - If you are using SQL authentication, un-check the **Use Integrated Logon** checkbox, and enter the username and password ELM is to use when executing the Query.

Actions

- **Warning 5538** - The SQL query results are different from the results the last time the query ran.

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, hh:01:15, etc.

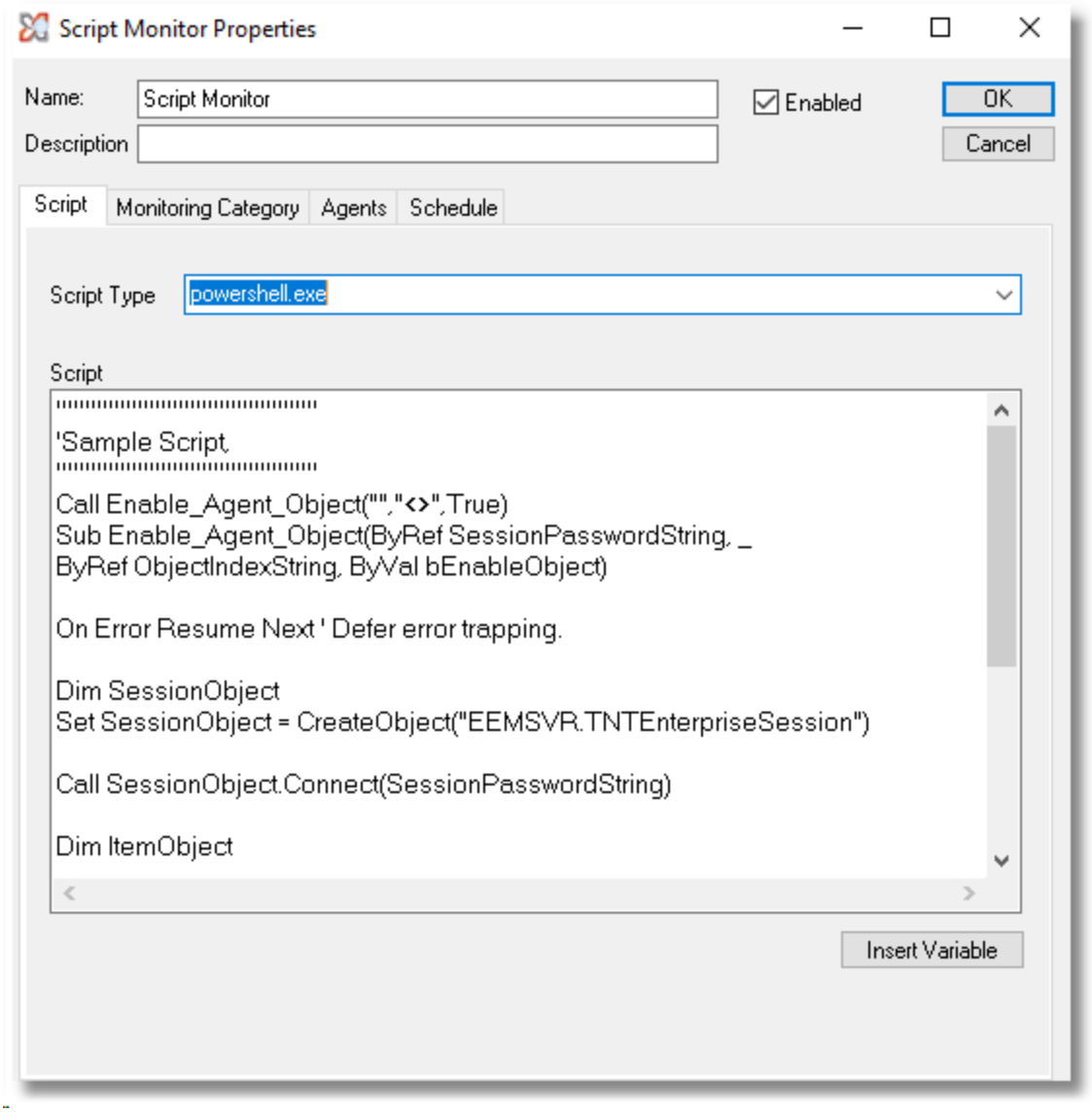
Scheduled Hours tab

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.

4.1.1.1.19 Script Monitor

The script monitor allows you to execute scripts in the context of the ELM Agent on a scheduled interval. Default scripting language includes cscript.exe, cmd.exe and powershell.exe. Additional scripting languages may be used by providing a full path to the executable in the Script Type field. Because of the nature of this monitor item, results of the script actions are not returned to the ELM console. It is the responsibility of the scripts author to confirm the script was successful run or to include output to standard Windows event that can then be collected by the ELM Event Collector.



Event ID:

The following event id's and category are available for use within any custom scripts.
5051 - Ex: Informational
5052 - Ex: Warning
5053 - Ex: Error
Category: 124 (Script Monitor)

Usage Examples:

- Connect to a RestAPI, perform an action and then generate an event with the results.
- Centralize cloud based log files into syslog msgs and send them to ELM for processing.

Sample Script:

Powershell: Check a specified directory for the existence of a specific file or file type, output to Windows event.

```
$MyPath = "c:\Dumps\*.dmp"
$FileExists = Test-Path $MyPath
If ($FileExists -eq $True)
{
$file = Get-ChildItem -Path $MyPath -Recurse -Filter "*.dmp" | Sort-Object LastWriteTime -Descending | Select-Object -First 1
Write-Eventlog -Source "ELMAgent" -LogName Application -EventId 5051 -Category 124 -EntryType Informational -Message "Dump File $($file.Name) was found on server %Computer%. Script run by ELM Server Monitor item: %MonitorName%"
}
```

Note: If the script monitor has been assigned to an Agent, you may need to adjust the ELM Agent service account username and password to have proper security to execute your script. When running Powershell scripts, ELM uses an "Exit" command following each run to prevent multiple instances of Powershell starting each time the script is executed. Best practice would be to include these types of exits in every type of script you choose to run.

4.1.1.1.20 Syslog Receiver

Syslog

The Syslog Receiver is based on RFC 3164 and listens for Syslog messages. By default, the Receiver listens for Syslog on UDP port <%SYSLOG_UDP_PORT%> ***or*** TCP port <% SYSLOG_TCP_PORT%>.

Auto Assign

By default, the Syslog Receiver monitor item will be automatically assigned to any agent that sends syslog messages to the ELM server using the specified protocol and port number. If unchecked, you must manually assign the monitor item to agents.

Event Filters

By default, the Syslog Receiver defaults to collecting all syslog messages when there isn't an Include Filter assigned to it. See Event Filters for further information.

Categories

Displays the Monitoring Categories 96 to which the Monitor is assigned. Click to select or deselect Monitoring Categories. Right click to create or edit Monitoring Categories.

Agents

Displays the Agents to which the Monitor is assigned. Click to select or deselect Agents. Right click or click the New link to deploy a new agent.

Syslog Device Configuration

Before ELM receives any Syslog messages, the device sending Syslog has to be configured, and usually this is done in a syslog.conf file. A common format for this file designates facility, severity, and destination.

Generic Examples:

facility.severity[;facility.severity]	destination	Meaning
kern.*	@PDC1	Send all messages from the kernel facility to server PDC1.
*.err	@redmond	Send all messages with a severity of error to server REDMOND
cron.warning;ntp.alert	@corp3	Send messages from the cron facility with a severity of warning and from the ntp facility with a severity of alert to the server CORP3.

These are generic examples, please consult the documentation for your specific device for details about its Syslog functionality.

Syslog to Event Log Record

When ELM receives Syslog messages, the Syslog record format is converted to a Windows event log record style format.
Syslog messages have the following fields which ELM maps to the corresponding event record fields listed:

Syslog Message	Event Record
Facility	Category
Severity	Event Type
Priority	Event ID
Header	Message
Message	Message

Syslog messages have 24 Facilities. These are converted to event categories by ELM according to the following mapping:

Number	Syslog Facility	Event Category
0	Kernel	kern
1	User	user
2	Mail	mail
3	Daemon	daemon
4	Auth	auth
5	Syslog	syslog
6	Lpr	lpr
7	News	news
8	UUCP	uucp
9	Cron	cron
10	Security	authpriv
11	FTP Daemon	ftp
12	NTP	ntp
13	Log Audit	audit
14	Log Alert	alert
15	Clock Daemon	clock
16	Local0	local0
17	Local1	local1
18	Local2	local2
19	Local3	local3
20	Local4	local4
21	Local5	local5
22	Local6	local6
23	Local7	local7

Syslog messages have 8 Severities or Levels. These are converted to event types by ELM according to the following mapping:

Number	Syslog Severity	Event Type
0	Emergency	Error
1	Alert	Error
2	Critical	Error
3	Error	Error
4	Warning	Warning
5	Notice	Warning
6	Info	Informational
7	Debug	Informational

Syslog messages have 192 Priorities. The lower the number, the higher the priority. These are calculated from the Facility and Level according to the following formula, and are used by ELM for the Event ID:

Facility * 8 + Severity = Priority (Event ID)

Examples:

Facility	* Multiplier	+ Severity	= Priority (Event ID)
Mail (2)	* 8	+ Error (3)	= 19
Clock Daemon (15)	* 8	+ Warning (4)	= 124
Kernel (0)	* 8	+ Emergency (0)	= 0

Parsing Syslog messages

The syslog receiver has the ability to parse messages and insert that information into an event log format for use with Event Views and Reporting.

In order to use this functionality you will first need to export a syslog receiver to xml and then open the file in a text editor. By default the following properties/modifiers examples are empty but you can customize them with regular expressions for parsing of message field information.

TimeModifier="MessageRegularExpression=end="([^"]*)"

In this example when the keyword "end" is found followed by an = sign then the time stamp following, that is contained in quotes is extracted and inserted into the time generated event message field.

ComputerModifier="MessageRegularExpression=dhost="([^"]*)"

In this example when the keyword "dhost" is found followed by an = sign then the word following, that is contained in quotes is extracted and inserted into the computer name event message field.

LogModifier=""

CustomCategory=""

EventIdModifier=""MessageRegularExpression=eventid="([^"]*)"

In this example when the keyword "eventid" is found followed by an = sign then the number following, that is contained in quotes is extracted and inserted into the Event ID event message field.
MessageModifier=""
UserModifier="MessageRegularExpression=suser="([^"]*)"
In this example when the keyword "suser" is found followed by an = sign then the word following, that is contained in quotes is extracted and inserted into the User event message field.
CategoryModifier="MessageRegularExpression=name="([^"]*:)"
In this example when the keyword "name" is found followed by an = sign then the word following, that is contained in quotes is extracted and inserted into the Category name event message field.

4.1.1.1.21 TCP Port Monitor

You can monitor any valid TCP port using a TCP Port Monitor item. Because the ELM Server (and not an Agent) makes the actual connection to the port, you can monitor TCP port availability on any operating system (e.g., Unix, Linux, Novell, Solaris, Windows, etc.), provided that you have TCP/IP connectivity to that system from the ELM Server. Each TCP Port Monitor can poll a single port.

TCP Port Monitor

- **TCP Port** - The TCP port you want to monitor.
- **Warn if QoS slower than __ seconds** - You may monitor the port's response time. By specifying a value for this field, a warning message will be generated whenever the response from the port exceeds the threshold you specify here.
- **Execute configured Action(s) for every failure** - By default, ELM will notify you only the first time the port is unavailable. Check this box to have a message sent for each interval that the port is unavailable.

Actions

- **Failed (Error) 5521** - The connection to the TCP port could not be made.
- **Success (Informational) 5522** - The connection to the TCP port could be made.
- **Quality of Service Warning (Warning) 5523** - The connection to the TCP port took longer than the Quality of Service time period.
-

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect

individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.22 Web Page Monitor

Web Page Monitors are used to monitor HTTP or HTTPS URLs. The ELM Enterprise Manager Server periodically establishes an HTTP connection to the server and port specified. If the response is negative, slower than expected, or if the content has been changed, a variety of notification options can be triggered. Note that multiple Web Page Monitors can be assigned to the ELM Server or to Service Agents. Therefore, you may create Web Page Monitors independent of the number of Agent licenses you have purchased. You must assign the Web Page Monitors to a licensed Agent, however, if you want an Agent to execute the Web Page Monitor.

Web Page Monitor

- **URL** - The URL you want to monitor. By default, HTTP communication occurs over TCP port 80. If you are using a different port, you can specify that port as part of the URL. For example, to monitor a web page on www.firemtsoftware.com that is listening on port 8080, you would use the following URL: http://www.firemtsoftware.com:8080.
- **Warn if QoS slower than __ seconds** - You can monitor your Web server's performance. By specifying a value for this field, a warning message will be generated whenever the response from the Web server exceeds the quality of service threshold you specify here.
- **Username** - If you must enter a username and password to access the URL listed in the URL field, enter that username in this field.

Note

If you are accessing the URL through a proxy server, this is NOT the username used for Proxy

server or firewall authentication. This username is for the Web server that contains the URL being monitored only.

- **Password** - The password for the account specified in the **Username** field.
- **Execute configured Action(s) for every failure** - By default, ELM will notify you only the first time the Web server is unavailable. Check this box to have a message sent for each interval that the Web server is unavailable.
- **Warn if content changes** - Check this box to cause a warning to be generated if the content of the monitored URL is different from the last time the Web Page Monitor retrieved the URL.
- **Run At Server** - Check this box to have the Web Page Monitor always executed on the ELM Server by the ELM Server service account. If you leave the box unchecked, the Web Page Monitor will be executed on the assigned Agents by the Agent's service account.
- **Proxy Server** - If the ELM Server or Agent needs to access the monitored URL through a proxy server, enter the name, fully-qualified domain name or IP address of the proxy server in the **Proxy Server** field. Enter the appropriate port for the proxy server in the **Proxy Port** field.

Actions

- **Failed (Error) 5517** - The web page could not be found or retrieved.
- **Success (Informational) 5518** - The web page was retrieved within the quality of service time period.
- **Quality of Service Warning (Warning) 5519** - The web page was not retrieved within the quality of service time period.
- **Content has changed (Warning) 5520** - The web page was retrieved, but the content has changed.
-

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.1.23 WMI Monitor

If you are using Windows Management Instrumentation (WMI) -- the Microsoft implementation of Web-Based Enterprise Management (WBEM) -- you can use WMI Monitors to query a WMI namespace and database. WMI monitor items periodically query the Windows Management Instrumentation database and generates events when the results of the query change.

- **Namespace** - Enter the name of the WMI namespace to query. This is usually **root/cimv2**.
- **Query** - Enter the query to execute. This query is the base query which retrieves zero or more records from the WMI repository.

- **Warning 5537** - The results of the WMI query are different from the results the last time the query ran.
-

Displays the Monitoring Categories 96 to which the Monitor item is assigned. Click to select or deselect Monitoring Categories. Click New to create or Properties to Edit Monitoring Categories.

Displays the Agents to which the Monitor item is assigned. Click to select or deselect individual agents. Click New to deploy an agent or Properties to View/Edit an existing agent.

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, h1:00:00, 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:01:00, 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.

4.1.1.2 All Agents

4.1.1.2.1 Agent Installation

Installing Agents From ELM Console

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. Three types of agents are available:

IP Virtual Agents: monitor Windows and non-Windows systems such as firewalls remotely from the ELM Server. They can run Monitor Items to monitor TCP based services like FTP, TCP ports, or listen for syslog and SNMP information.

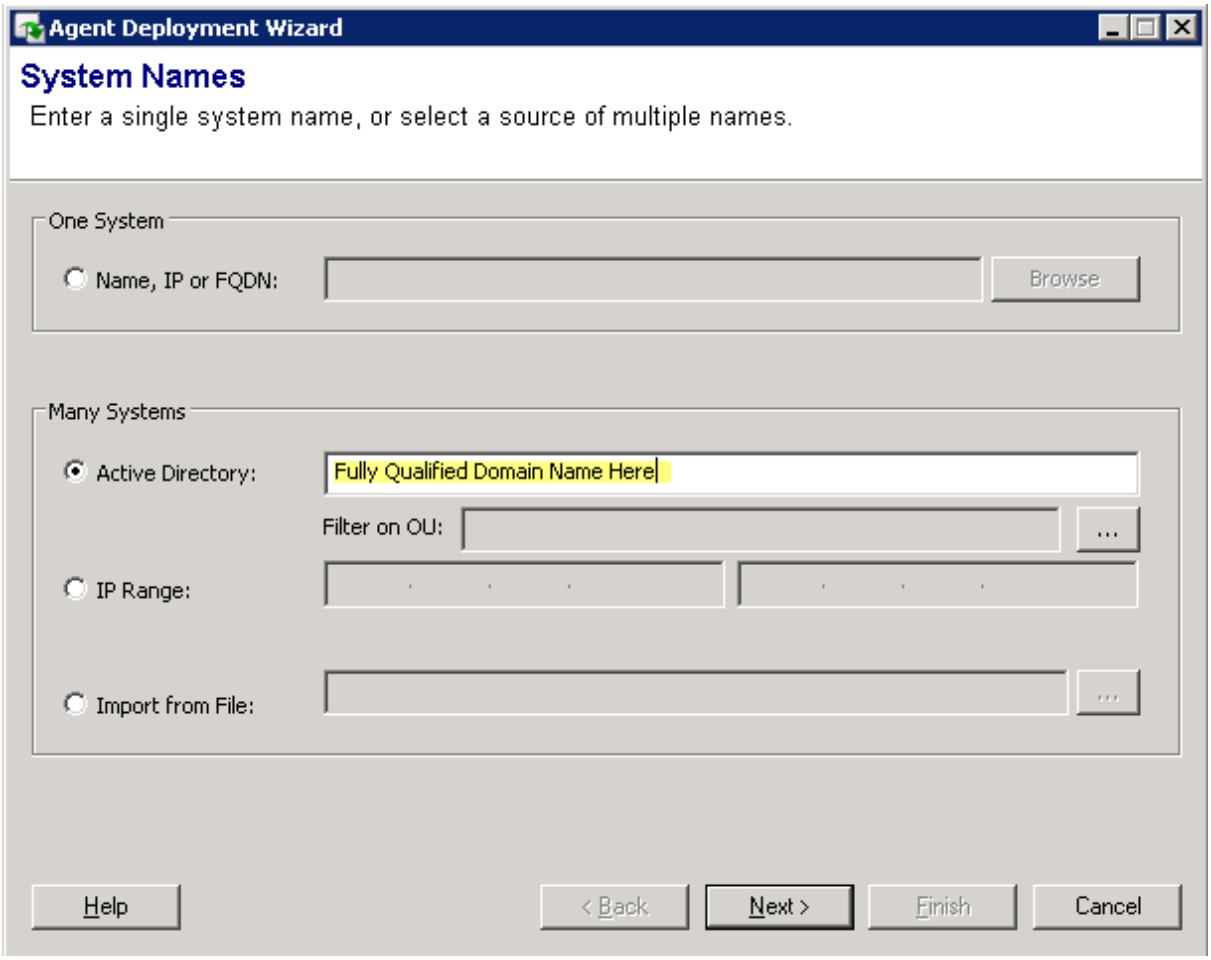
Virtual Agents: monitor Windows systems monitored remotely from the ELM Server, without installing software on the monitored system.

Service Agents 94 (ELM Standard): monitor Windows systems with the ELM Agent service installed on the monitored system.

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 87 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.



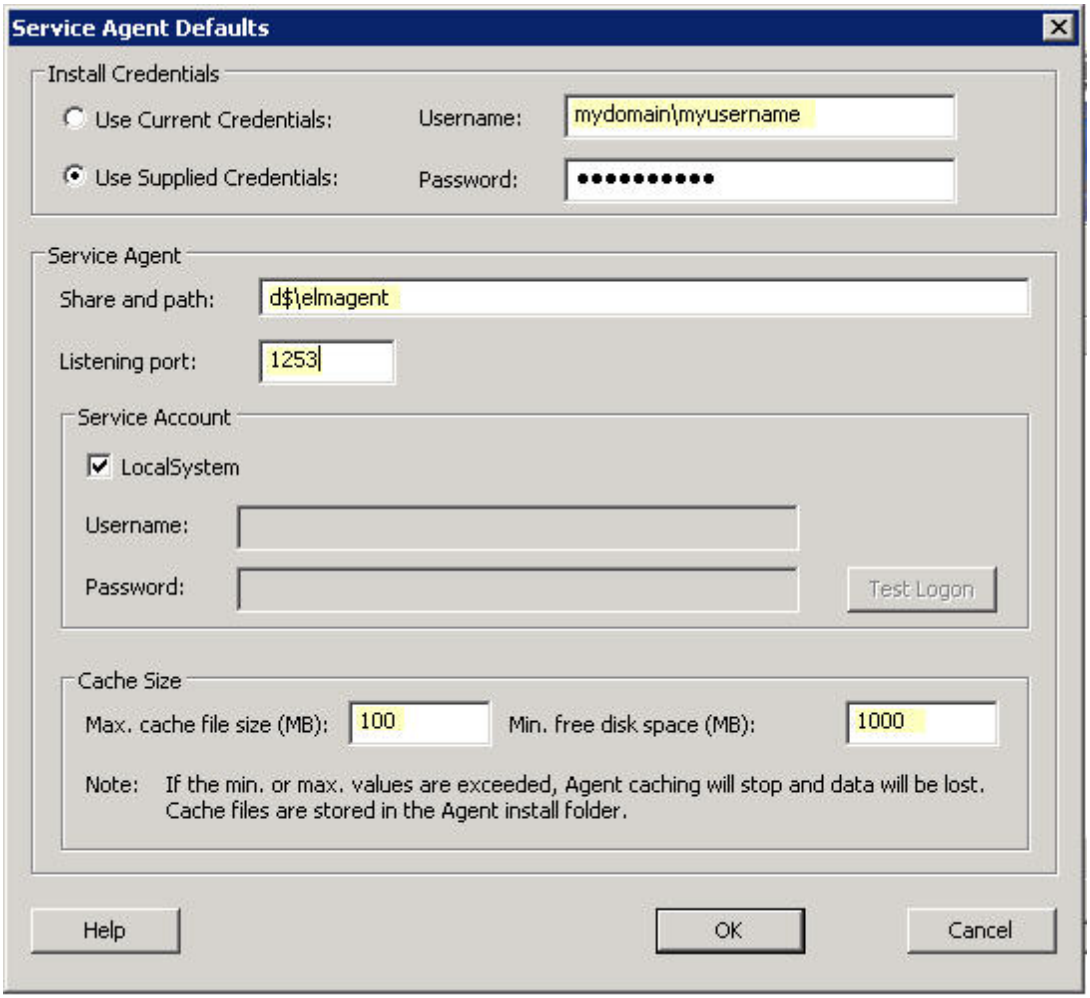
2. From the **System Names** dialog box, there is the option of installing ***One System*** or ***Many Systems***.
3. In the ***Many Systems*** area, there are three options: **Active Directory, IP Range,** and **Import from File**.
   - **Active Directory**: Specify the Active Directory domain to search. Selecting the **...** in the box marked **Filter on OU:** allows you to further specify particular Organizational Units within the domain to search.
   - **Scan IP Range**: Specify a range of IP addresses to search for computers or devices. The ELM Server will query port 139 and look for responses.
   - **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. After the import, the **Agent Deployment Wizard** will determine if it what type of agent to install.

   The CSV file has the following syntax:

   Agent1,
   Agent2,
   Agent3,

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. The directory must already exist.
- 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.

5. 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.

6. 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.**

7. 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 **Monitoring Categories** dialog is used to assign agents to Monitoring Categories 96. 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 40. 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 a 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 ELM Enterprise Manager Setup:

1. Double-click the **ELM7.50_*nnn*.exe** file you downloaded (where ***nnn*** is the build number). The Setup Wizard will launch.
2. Make sure the Service Logon is correct, and type in the password you wish to use for the Local ELM Database, if applicable.
3. Select the components you wish to install and check the box agreeing to the licensing terms.
4. Click **Install** to start the Service Agent install process.
5. 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.
6. 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.
7. The **Monitoring Products** dialog box will appear. Put a check in the box to the left of the type of Monitoring Product 40 you want this agent to have. Click **Next** to continue.
8. The **Monitoring 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.
9. Click **Finish** to close the install wizard.

To install an agent using EAM Agent-Only MSI Package:

1. From an Administrative command prompt, navigate to the folder the .msi package is in and type its name to start Setup.
2. Click Next and accept the License Agreement.
3. Click Next again and verify Agent is only component being installed. Change directory path if necessary.
4. Verify path and click Install.

To uninstall a Service Agent that was installed using setup:

1. Open the Windows Control Panel and double-click '**Uninstall A Program**' then select ELM Enterprise Manager (or ELM Agent, if only an agent is installed) and click **Uninstall**'.
2. Select the 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, deselect the check-box for each component you wish removed. Any ELM components installed on this system that you do not wish to remove should have a checked check-box. select '**Repair/Modify'** and the unchecked components will be removed. **(EAM Agent .msi Only:** 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.**)**

4.1.1.2.1.1 Agent Properties

To view the properties of an Agent right click on the Agent name and select Properties.

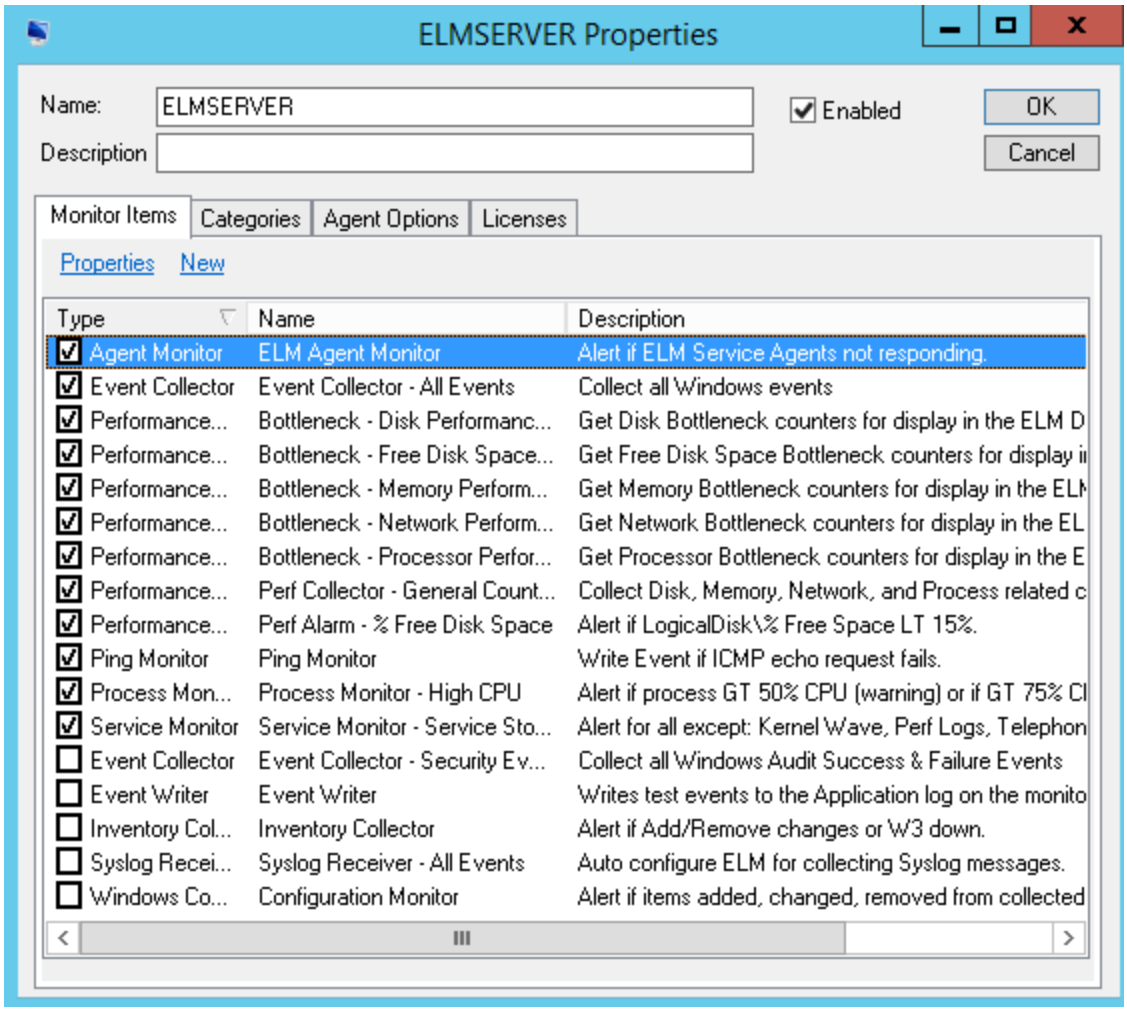
The Name Field provides the name of the agent configured. This should be a valid Netbios name or IP Address.

The description Field provides a note area for a system administrator to describe the system being monitored.

The Enabled check box allows you to disable an agent from collecting any information from its assigned monitor items. If an Agent is not enabled it will still use a license until it is deleted.

Monitor Items

The Monitor items tab displays all Monitors available to an Agent. The list of Monitor Items available is determined by the total population of Monitor Items created plus the licenses assigned to the Agent. Monitor items that are already assigned to agent are indicated by a check mark next to the Monitor item name.

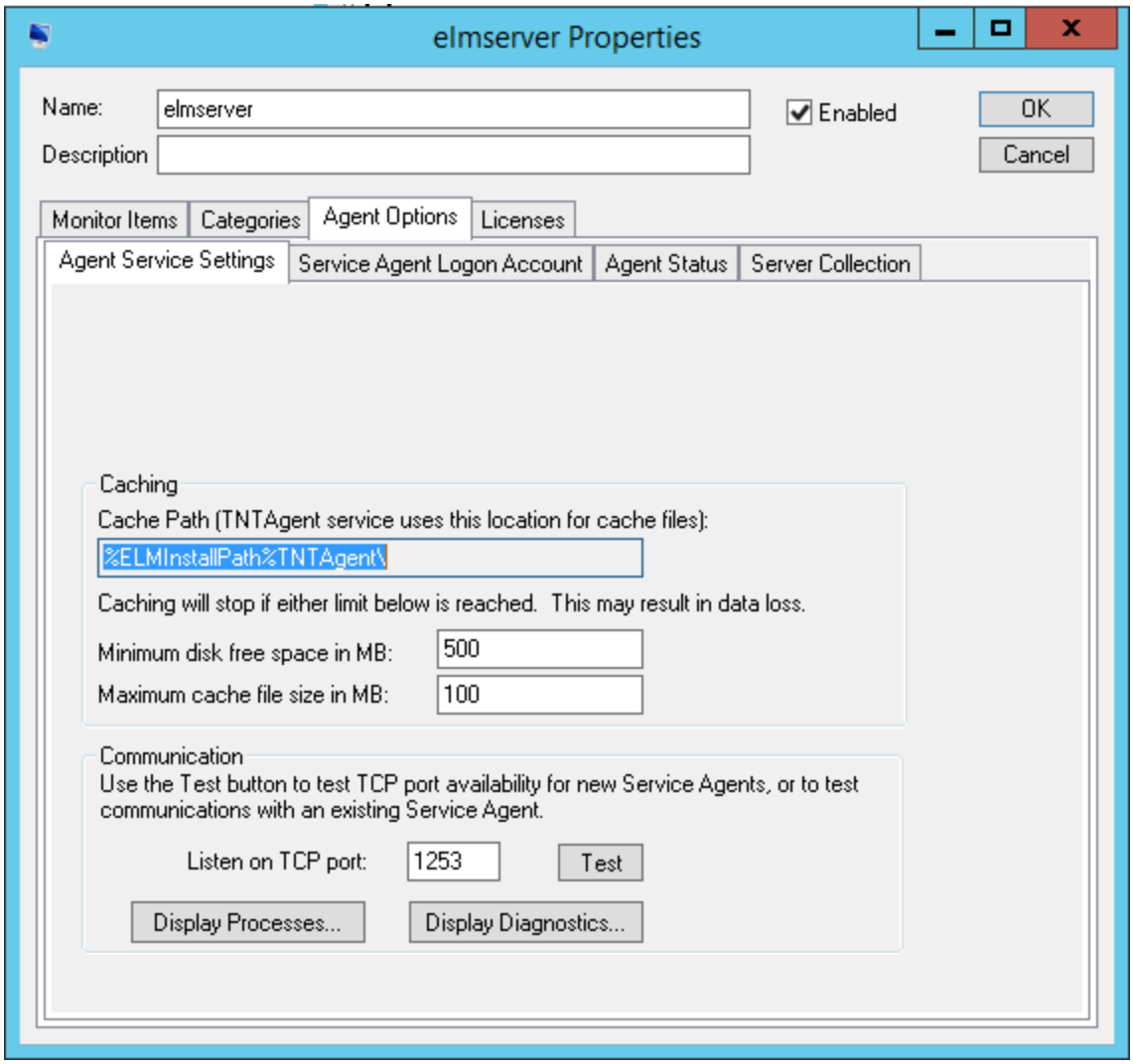


Categories

The Categories tab displays all Agent Monitoring or Maintenance category groups currently assigned or available to the agent. A category may be assigned or unassigned by checking the box next to the category name.

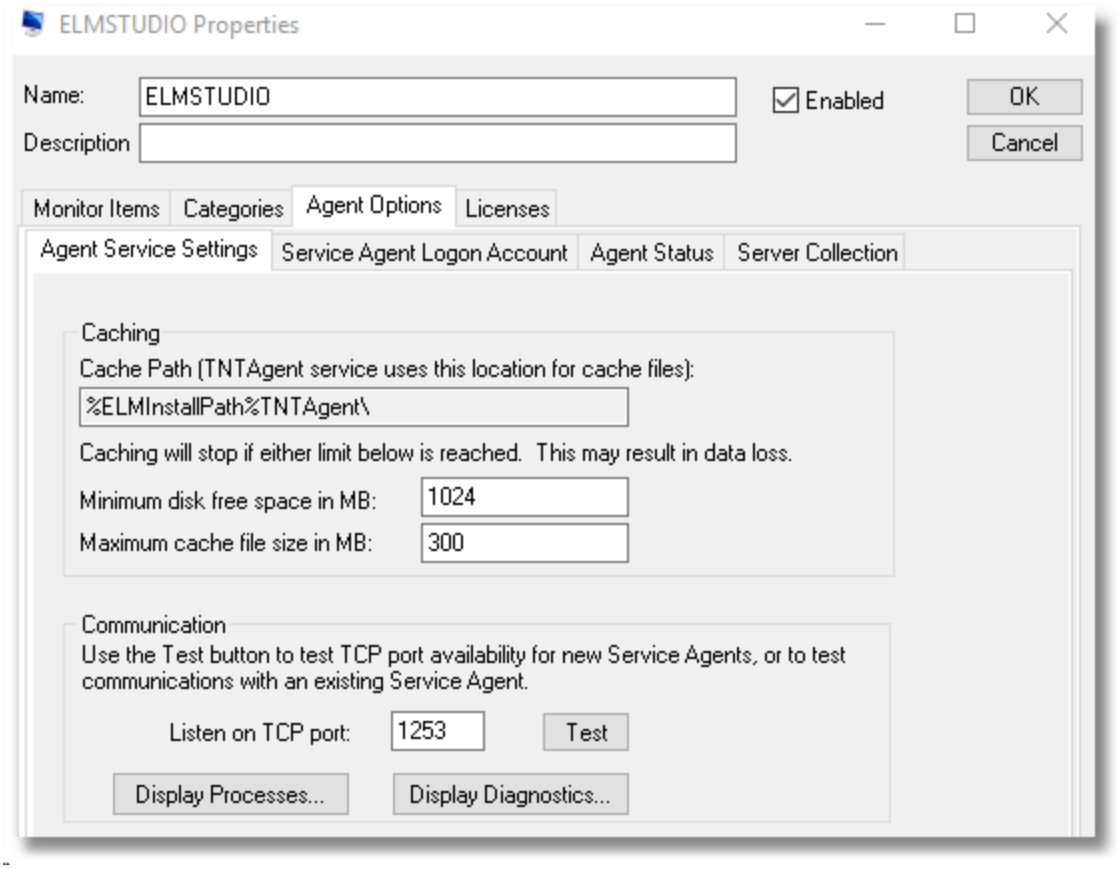
Agent Options

The Agent Options tab displays the following information:



Agent Service Settings Tab

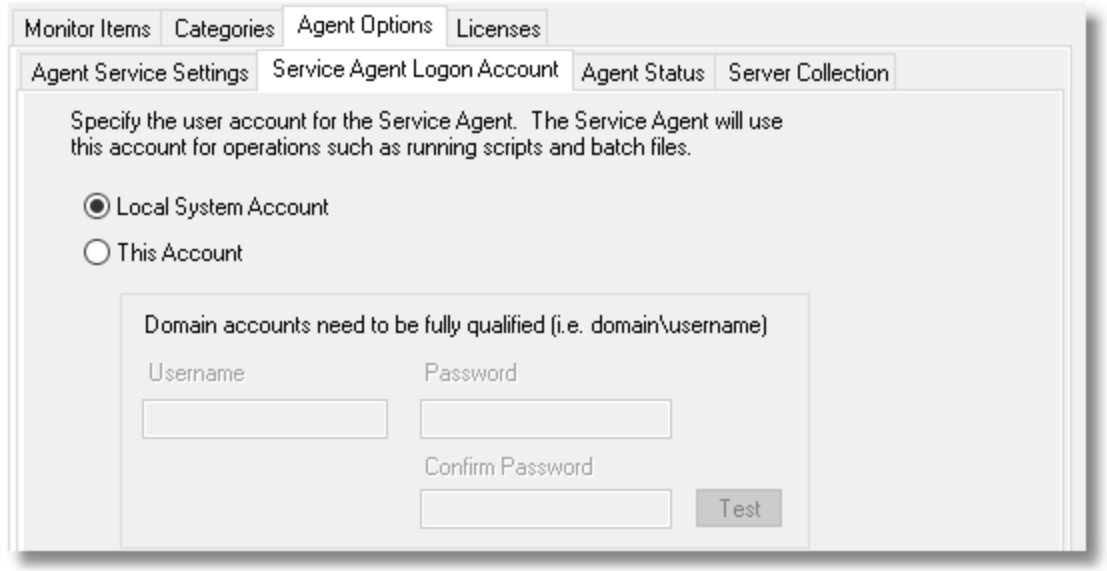
Click the **Test** button to test the Agent's port. A successful test will produce the following message with the agent name in it:



Click the **Display Processes** button for a live view of the current processes on this Agent.
Click the **Display Diagnostics** button to generate a text file containing diagnostic and module information.

Service Agent Logon Account Tab

Enter the credentials required to run privileged operations on your Service Agent. Certain operations such as scripts, SQL queries, or other processes may require different permissions than those required by LocalSystem.
This account will take precedence over the account listed in the service.
You may enhance security by running the Service Agent with an account that has minimum permissions to perform its operations.The account you specify on this dialog will appear in the properties of the **ELM Agent** service.



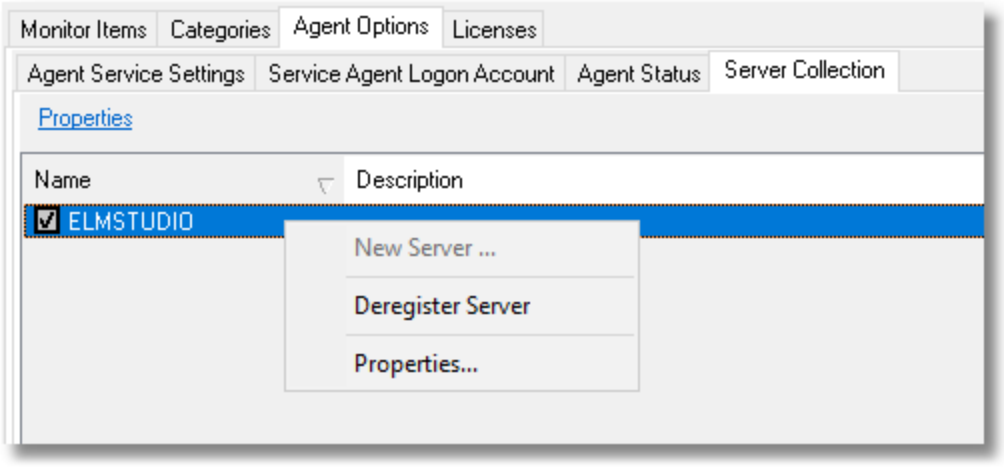
Agent Status Tab

Agent status displays details about the currently active Agent process, TNTAgent.exe. The **Active Configuration Settings** section lists the Monitor Items active on the Agent, followed by time-stamped activities. This provides important details to verify that an Agent is operating as desired.

Agent Status is one of the first places to look for suspected reporting or communication problems between a Service Agent and an ELM Server. Use your mouse to select data in this dialog box (drag-select or right-click and **Select All**), then copy and paste it into a file or email message.

Server Collection Tab

Displays a list of the ELM Servers that are monitoring this Service Agent. Double-click on a listed ELM Server to display details about the ELM Server. Right-click the ELM Server and deregister it from this Agent if you no longer want it to monitor this Agent.



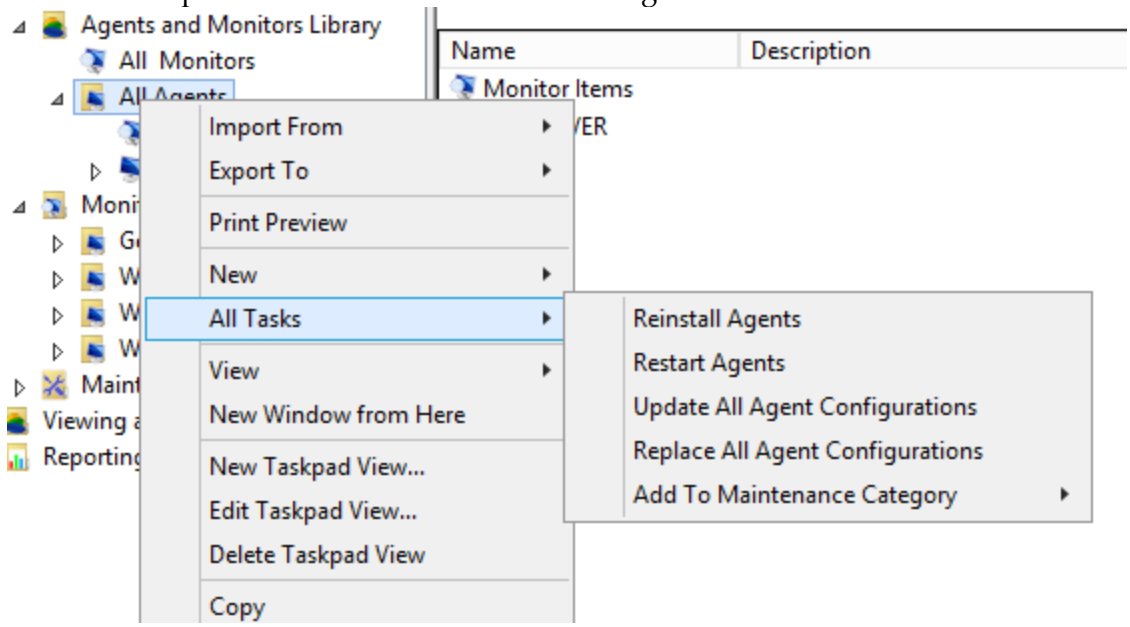
Licenses

Shows the currently assigned licenses, and allows an administrator to change the licenses assigned to the Agent

4.1.1.2.1.2 Service Agents

4.1.1.2.2 Agent Tasks

Agent 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, Monitoring Categories, or multiple Agents as illustrated below. Not all operations are relevant for Virtual Agents.



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.

This operation will restart the ELM Agent service.
This operation applies only to Service Agents. It will fail if the Service Agent is not running.

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 5 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 5 minutes.
This operation applies only to Service Agents.

Similar to the Update Agent Configuration, the **Replace Agent Configurations** operation allows an ELM administrator to manually refresh the configuration without waiting the default 5 minutes however using this option will delete the old configuration (tntagent.dat) and replace it with a new copy.
This operation applies only to Service Agents.

This options allows you to assign All or selected agents to a Maintenance category 97.

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 does not affect the NetBIOS name of the agent.
Resolution for an agent is based on the following order:

The ELM Server first checks to see what was last successful, this could be the agent name or the ip address.
If resolution fails, it then checks the agent name.
If that fails, it then checks the FQDN in the aliases list.
If that fails, it then checks the IP address in the aliases list.

This operation applies to Service Agents, Virtual Agents, and IP Virtual Agents.

4.1.2 Monitoring Categories

Monitoring 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.

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

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 2008 could be in the following categories:

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

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) can be assigned to Monitoring 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. If the agent cannot run the Monitor, for example a Windows XP agent in a category with a Cluster Server monitor, nothing will happen. The agent will ignore the monitor and there is no adverse effect.

To create a new Monitoring 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 **Monitoring 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.

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.

4.1.3 Maintenance Categories

Maintenance Categories group Agents for easy management during schedule maintenance periods such a Windows service pack installations. By utilizing the maintenance window you are able to schedule dates/times when notifications can be disabled automatically at regular intervals.

To create a new Maintenance Category

1. Right click on the Maintenance Category container and select **New | Maintenance Category**. The New Category Wizard will appear. Click **Next** to continue.
2. 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. Maintenance Categories can be created and assigned to agents at any time.

3. The Maintenance Schedule will appear where you can specify the start date/time, duration and recurrence pattern. Once, Daily, Weekly or Monthly are available recurrence patterns. Click Next to continue.
4. The **Item Name and Description** dialog will appear. Enter the **Name** for the new Category, and an optional **Description**. Click **Finish** to create the maintenance category.

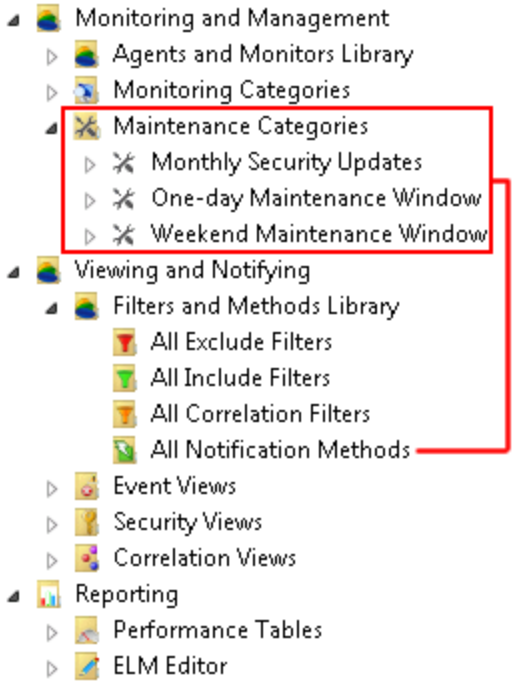
You can also create a new category from the **Monitoring Categories** tab inside the properties of an **Agent**, or from the **Categories** tab inside the properties of a **Monitor Item**. To do this, right-click anywhere in the tab dialog, select **New Agent Category**, and complete steps 2-5 above.

Agents Tab

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

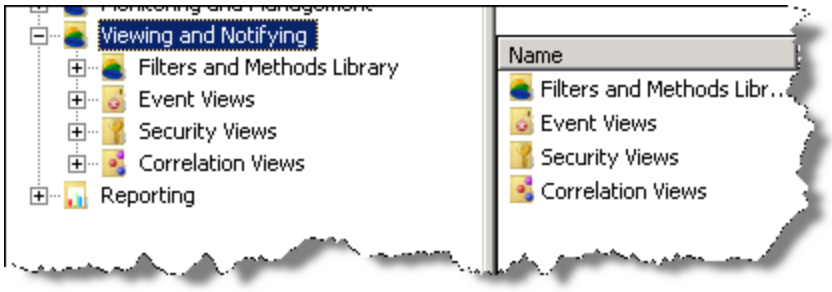
Maintenance Tab

In the properties of a Maintenance Category, the Maintenance tab will show the current Maintenance schedule.



4.2 Viewing and Notifying

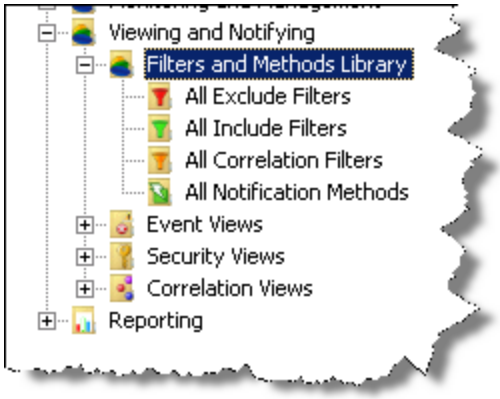
The Viewing and Notifying container in ELM is where Filters, Views, and Notifications within ELM reside. Event Views, Security Views and Correlation Views organize the large amounts of event log information collected from systems into common groups based on matching criteria in the assigned filters.



See More:
Filters and Methods Library 99

4.2.1 Filters and Methods Library

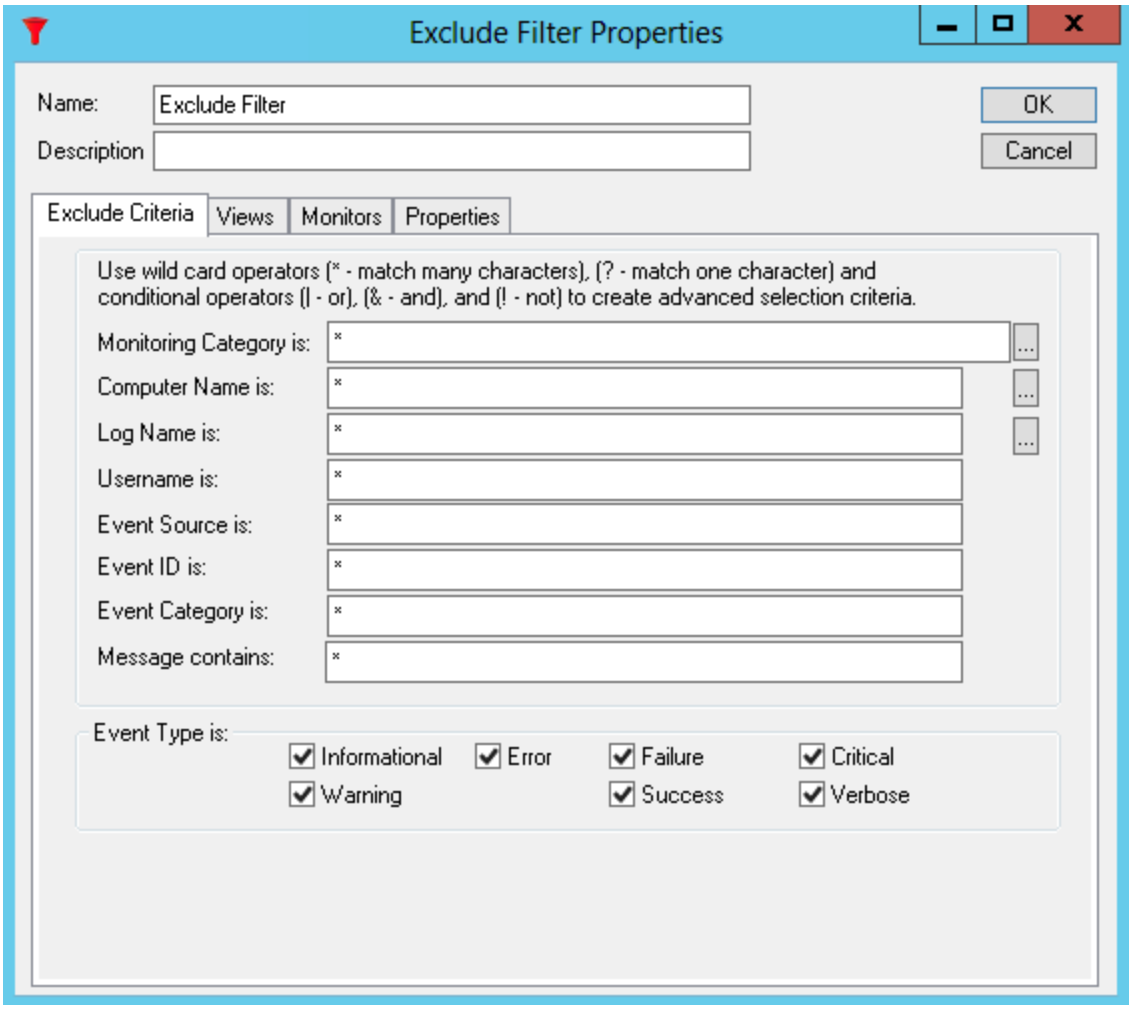
The Filters and Methods Library within ELM contains Event Filters and Notification Methods which can be assigned to Event Views. Event Filters are common objects within ELM and can also be assigned to Event Collectors, Syslog Monitors, SNMP Monitors and Event Monitors.



See More:
All Exclude Filters 99
All Include Filters 103
All Correlation Filters 106
All Notification Methods 111

4.2.1.1 All Exclude Filters

Exclude Event Filters are common objects within ELM and can be assigned to Event Views 118, Security Views 125 or Correlation Views 130 to have specific events excluded from the View. In addition they can be assigned to Monitor item types Event Collector 45, Event Writer 50, Syslog * 75 or SNMP * 71 to exclude events from Agent collection. The Filter criteria entered by the user controls what events are excluded from collection and displaying.



- **Name** - Enter a unique name.
- **Description** - Enter a description (optional).

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 deleting or archiving, however these Filters will not be available in the Event Filter collections.
The following fields are available for filtering purposes:

- Agent Category is
- 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 **Agent Category, Computer Name is**, **Log Name is**, and **Event Source is** fields browse and display the agent category names, 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.

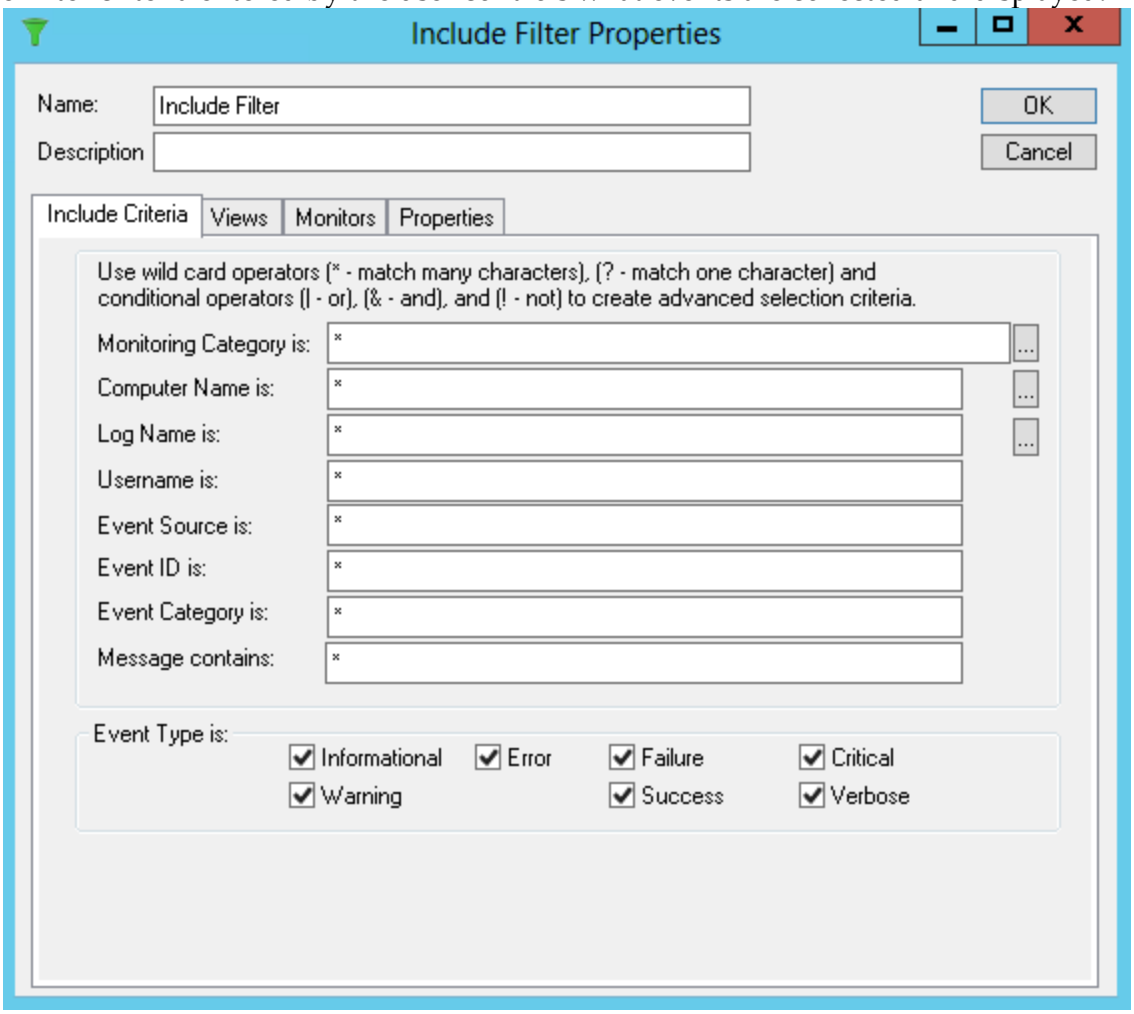
Views

Shows the Views associated with this Exclude Event Filter. Select **New** to create or **Properties** to edit a highlighted View.

Shows the Monitor Items of type Event Collector[45] associated with this Event Filter using an Include relationship. Right click to create or edit an Event Collector[45].

4.2.1.2 All Include Filters

Include Event Filters are common objects within ELM and can be assigned to Event Views 118, Security Views 125 or Correlation Views 130 to display specific events. In addition they can be assigned to Monitor item types Event Collector 45, Event Writer 50, Syslog * 75 or SNMP * 71 to include events from Agent collection.
The Filter criteria entered by the user controls what events are collected and displayed.



- **Name** - Enter a unique name.
- **Description** - Enter a description (optional).

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 deleting or archiving, however these Filters will not be available in the Event Filter collections.
The following fields are available for filtering purposes:

- Agent Category is
- 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 **Agent Category, Computer Name is**, **Log Name is**, and **Event Source is** fields browse and display the agent category names, 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.

Views

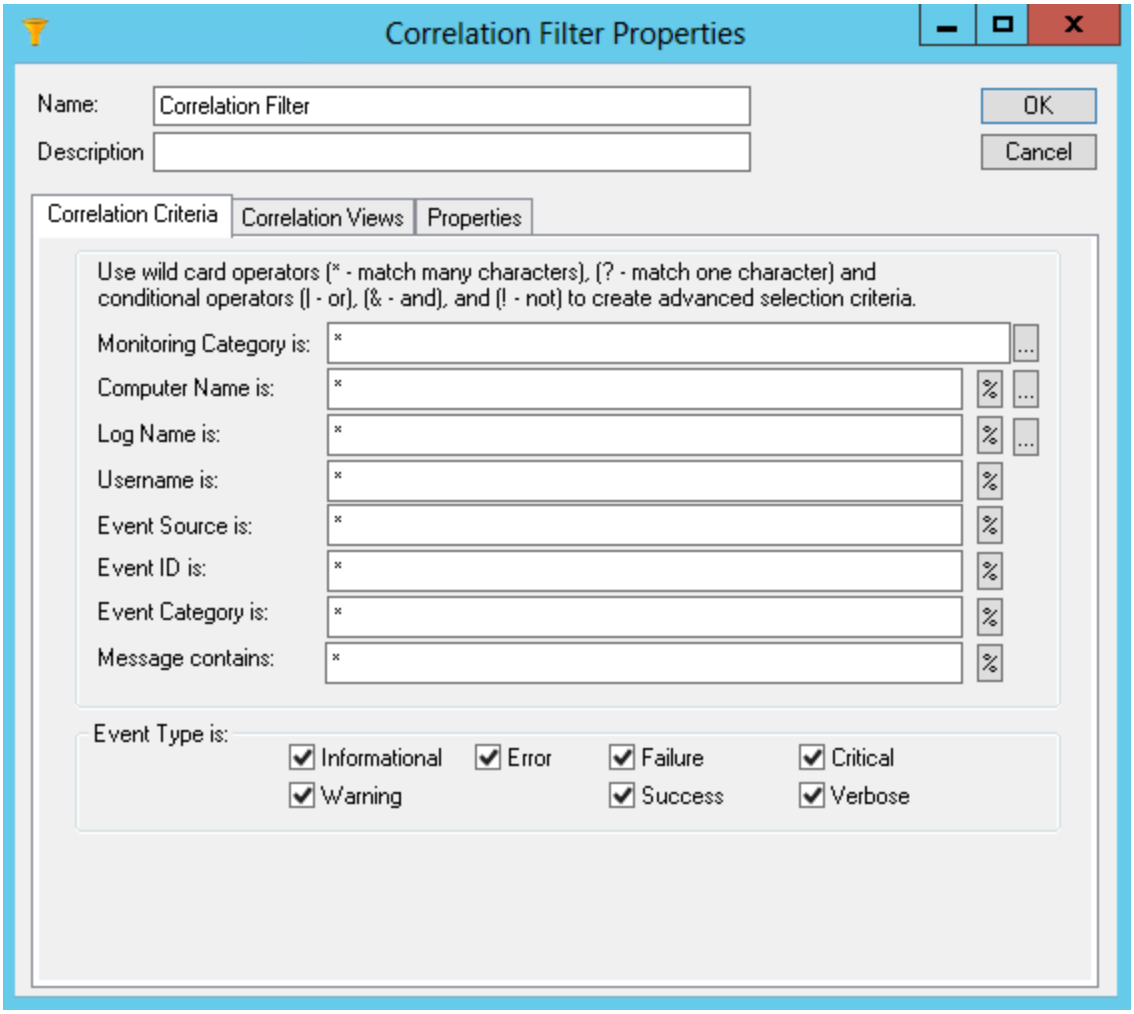
Shows the Views associated with this Event Filter using an Include or Exclude relationship. Select **New** to create or **Properties** to edit a highlighted Event View 118.

Shows the Monitor Items of type Event Collector 45 associated with this Event Filter using an Include relationship. Right click to create or edit an Event Collector 45.

4.2.1.3 All Correlation Filters

Correlation Filters

ELM Correlation Filters are used only by ELM Correlation Views 130. These Filters are designed to watch for the ending event in a pair of correlated events. The Correlation Criteria can be hardcoded, or can use environment variables which resolve to values found in the Start events. In addition, the Message field can use regular expressions to allow sophisticated filtering patterns when watching for pairs of correlated events.



- **Name** – Enter a unique name.
- **Description** – Enter a description (optional).

Correlation Filter Criteria

Correlation Filters provide a mechanism for isolating specific events, and multiple Correlation Filters can be combined to create a complex set of criteria. The same Filter can include or exclude events.

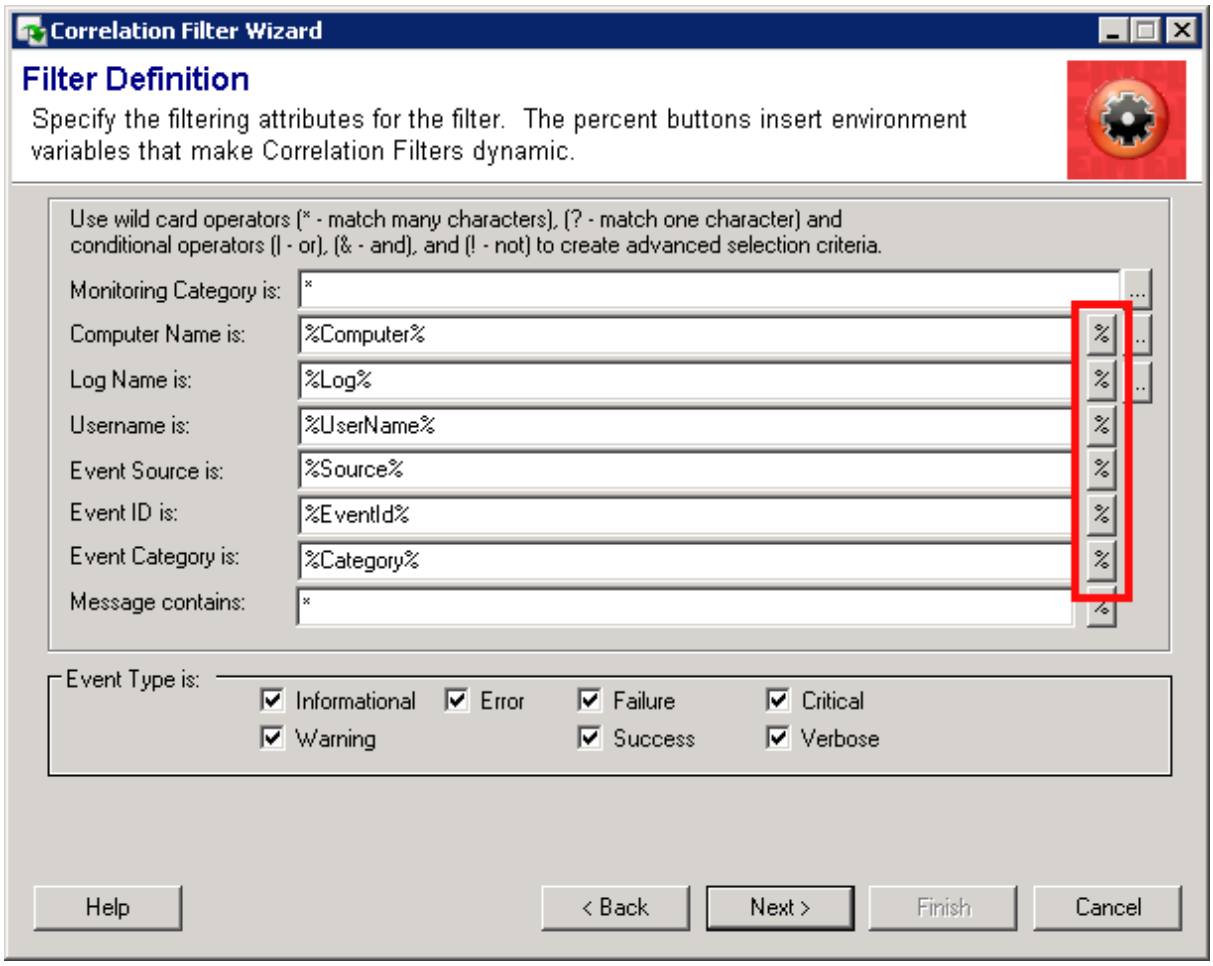
The following fields are available for filtering purposes:

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

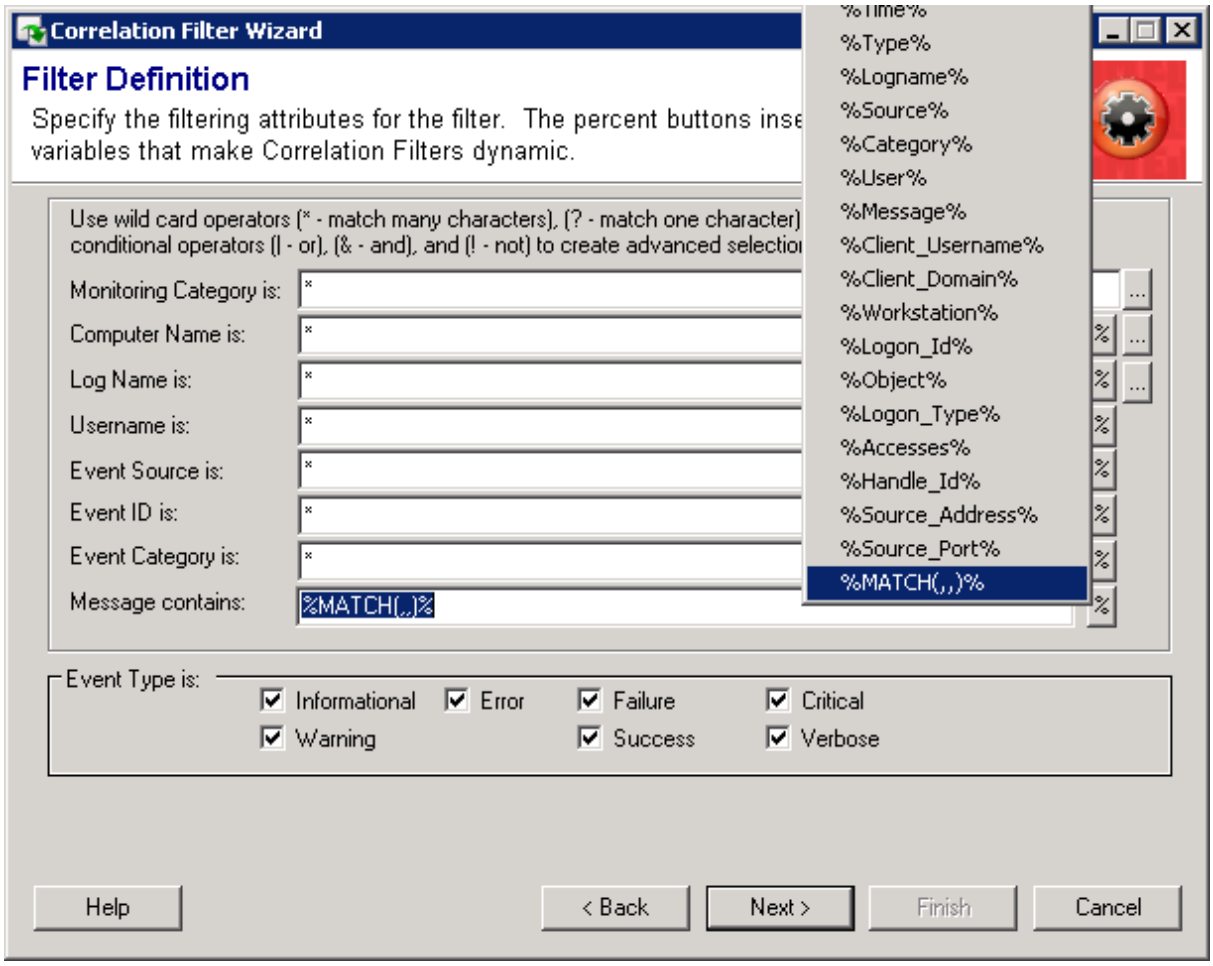
This dialog box has a dynamic menu behavior. The ellipsis button next to the **Agent Category**, **Computer Name**, and **Log Name** fields browse and display the agent category names, computer names, and event log names. If the **Computer Name** field is left blank, the list of event Logs and Sources 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 button for the **Log Name** or **Event Source** fields, the list of event Logs and Sources from that system will be displayed.

Environment Variables

The percent button for most fields will put the matching environment variable in the field. This variable will use the value from the "start" event and look for a matching value in the "end" event.



The Message field can use a variety of environment variables. Like the other fields, the environment variable takes the value from the "start" event and looks for that value in the "end" event. Additionally, it can use a custom regular expression match variable for advanced match criteria.



The MATCH variable uses the ECMAScript grammar provided by TR1 Regular Expressions. Microsoft documentation can be found here: http://msdn.microsoft.com/en-us/library/bb982727.aspx. Inside the parentheses, the MATCH variable requires 3 parameters:

1. A regular expression to capture a string from the "start" event
2. Reuse of one or more strings to look for in the "end" event
3. True or false, require case sensitive matching

For example:

%MATCH("username: (.+)","\0","false")%

This match pattern searches for a "start" event that contains "username" followed by a colon, a space, and one-or-more characters. The one-or-more characters pattern (period followed by a plus-sign) is inside parentheses, so these characters are captured. These captured characters are reused by the 2nd parameter via the \0 characters. So the "end" event must have the same username. The 3rd parameter (false) makes this match case in-sensitive.

Another example:

%MATCH("handle id:[:blank:]+([:w:]+)","handle id:[:blank:]+\0","FALSE")%

This match pattern searches for a "start" event that contains "handle id" followed by a colon, one-or-more blanks (spaces or tabs), and one-or-more alphanumerics. The one-or-more alphanumerics pattern (open square bracket, colon, w, colon, close square bracket) is inside parentheses, so these characters are captured. These captured characters are reused by the 2nd parameter via the \0 characters. So the "end" event must have "handle id" followed by a colon, one-or-more blanks, and the same handle id value as the "start" event. The 3rd parameter (false) makes this match case in-sensitive.

A 3rd example:

%MATCH("The (.*) service .* stopped","The \0 service .* running","FALSE")%

This match pattern searches for a "start" event that contains the letters "The" followed by a space. Then it captures everything upto a space followed by the letters "service" and followed by another space. Then anything, followed by a space, and followed by the letters "stopped". The end result is the name of the stopped service is captured. These captured characters are reused by the 2nd parameter via the \0 characters. Similar to the first parameter, the 2nd parameter looks for the service name followed by the word "running." The 3rd parameter (false) makes this match case in-sensitive.

Note: Regular expressions are supported only in the custom MATCH variable in the Message Contains field.

Leading and trailing wildcards (*) and character position wildcards (?) are supported, as are the Boolean operators Or (|), And (&), and Not (!). 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.

Correlation Views

See Correlation Views 130

4.2.1.4 All Notification Methods

Notification methods are how administrators learn of events. To create a new Notification method, select the **New** Notification Method link when the **All Notification Methods** container in the ELM Console is selected under **Results -> Event Views**.
Notification Methods are triggered by assigning them to an Event View 118, Security View 125 or as a **Match/Timeout** notification in Correlation Views 130. 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 setting

Desktop Notification Methods

The list below describes the methods designed for use at the desktop computer.
Dashboard Notifications 113 - Send updates to the Dashboard when triggered.
ELM Advisor Notification 117 - Send event information to ELM Advisor clients.
Mail Notification 117 - Send event information to email addresses.

Server Notification Methods

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

Command Script 112 - Process event information using scripts and custom programs.
Forward Event 113 - Send event information to another ELM Server.
SNMP V1, V2, V3 114 - Send event information to an SNMP management system or SNMP agent.
Syslog Message 115 - Send event information to a syslog server.

4.2.1.4.1 Command Script

The Command Script Notification runs a script on the ELM Server.
The script runs in the security context of the account under which the ELM Server is running. The script can be a batch command script, an executable or command line application, or a script.
Event information is available to the command script through Environment Variables, allowing you to use information from the event, such as the computer name or the message details field in any batch files, scripts, or other programs.
ELM supports the Windows Script Host (cscript.exe), command line (cmd.exe), or any executable, including custom-written programs. To use another type of script (e.g., a Perl script, or PowerShell), enter the name of the script engine in the Type field (e.g., perl.exe, or powershell.exe).

- Script Name - Enter a name for the script. The name is used for information purposes only.
- Type - Select script engine processor executable filename. If the filename is in not the path of the account the ELM Server is running under, enter the full path to the executable file local to the ELM Server. If you are executing a VB Script, use cscript.exe. If you are executing a Perl script, enter perl.exe for Type. If you are using a custom program, enter the name of that executable file.
- Timeout - Enter a value for the script. If the script does not complete within the timeout period, it will be considered a failed notification.
- Script - Enter the text of the Script you want executed in this field. By default the field contains a sample script. The script text will be copied to a temporary file in the file system and then passed to the script engine as an argument on it's command line.

Use the Test button to test the script.
Caution
When you click the Test button, the script will be executed.

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.

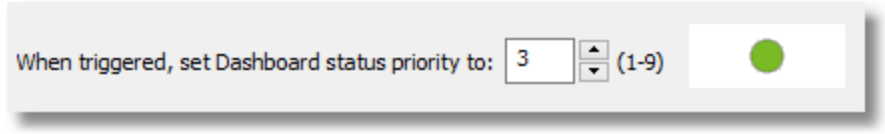
4.2.1.4.2 Dashboard Notification

The dashboard notification method will send status updates to the ELM Dashboard when triggered. Its primary purpose is to provide a visual representation of an agents current status. This is represented in Red light/Green light type manner on the gauge.

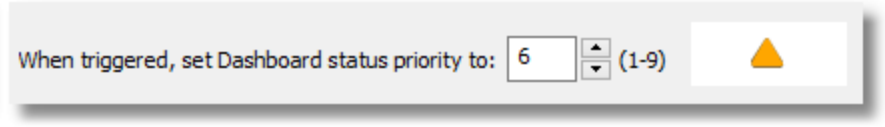
- Message - Enter the text you want displayed in the message portion of the dashboard. You may use the Insert Variable button to insert Environment Variables that will be populated when the notification is created.

When triggered the status is assigned a value of 1-9.

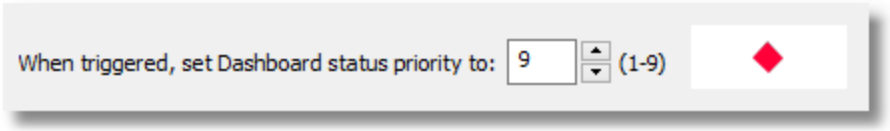
Values 1-3: Dashboard indication will be set to a Green color



Values 4-6: Dashboard indication will be set to a Yellow color



Values 7-9: Dashboard indication will be set to a Red color



- **Enable Timeout** - This allows for resetting the last message priority to a different level after the specified time period has lapsed. Ex: Change the dashboard from a priority 9 back to a 1 if the condition has not occurred recently.

Lists the Event Views[118] that the Dashboard Notification Method is assigned to. Select the **New** link to add an Event View[118]. Highlight an Event View[118] and select **Properties** to modify the Event View[118].

4.2.1.4.3 Forward Event

The Forward Event Notification sends event information from one ELM Server (the sending server) to another ELM Server (the receiving server). Use this notification to link one or more ELM Servers. Forwarding events to an upstream ELM Server allows you to create a tiered monitoring system, an industry standard for monitoring multiple locations. Forward

Event also has a caching mechanism. If the sending ELM Server cannot deliver the notification, it will cache it and attempt to resend after a few minutes.

- Names - This is the list of receiving ELM Servers.
- TCP Port - The port on which the receiving ELM Server is listening. By default, ELM Servers listen on port 1251. Set this value before adding a receiving ELM Server name to the list.
- Add - Click the Add button to add a server. The Select Computer dialog box will appear. You may enter the server name in the Computer Name field or browse the network and select the server. Click OK to add the server. Repeat this step for each server you wish to add.
- Remove - Select an ELM Server in the Names list and click the Remove button to delete it from the list.
- Remove All - You may use the Remove All button to remove all ELM Servers from the Names list.

Click the Test button to test the notification. A test message will appear in the Events view of the receiving ELM Server with the name of the sending ELM Server.

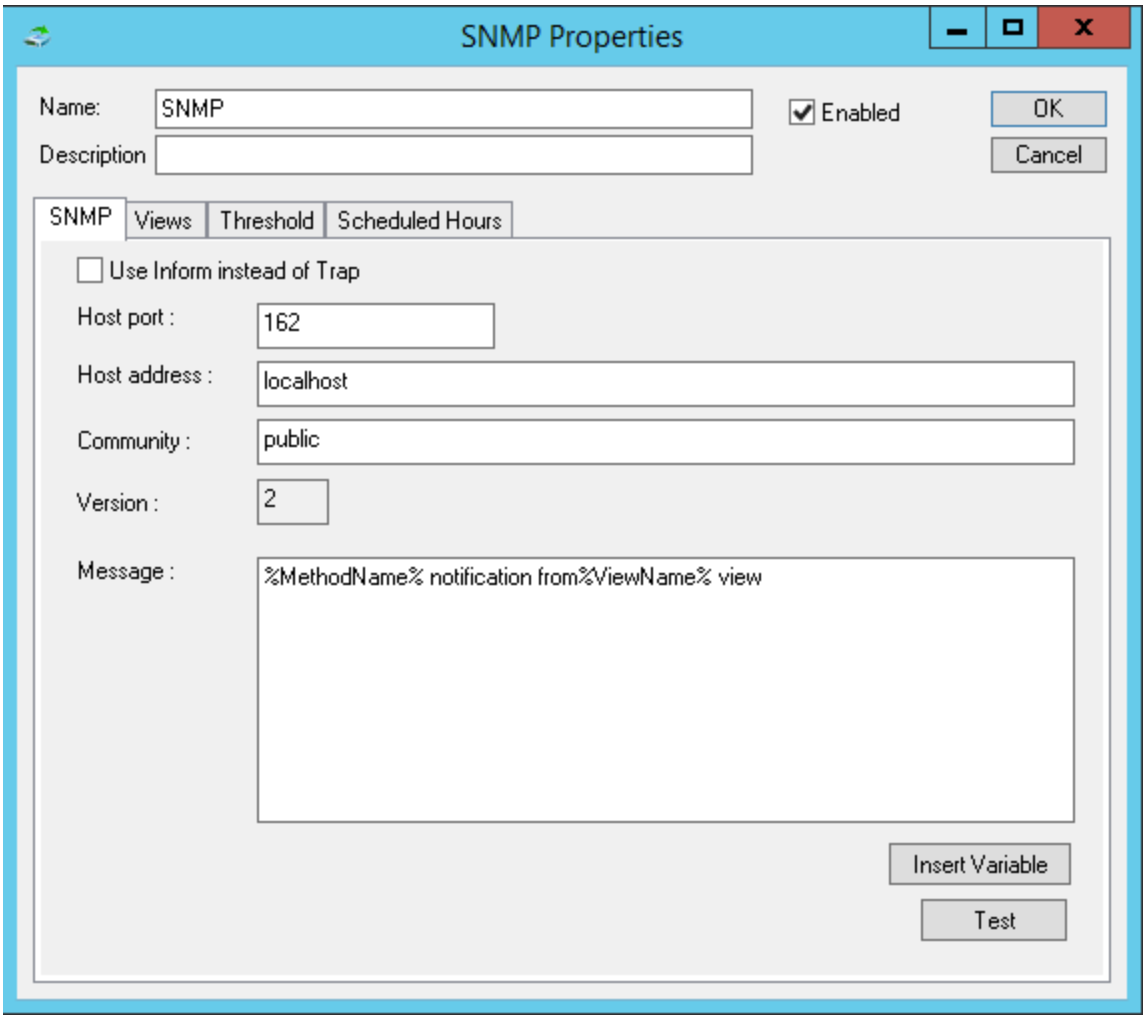
Note

The receiving ELM Server must have the IP address of the sending ELM Server before it will accept forwarded notifications. The IP address is entered in the ELM Control Panel applet, on the ***Forwarded Events*** *tab, of the receiving ELM Server.*

4.2.1.4.4 SNMP

ELM supports SNMPv1, SNMPv2c, and SNMPv3 traps as notification types.

The SNMP Trap Notification sends event information as an SNMP Trap to an SNMP management system. An ELM MIB is provided in the MibFiles folder under the ELM Server installation folder. It is used by the SNMP management system to translate the SNMP Trap.



Click the Test button to test the trap generation and settings.

4.2.1.4.5 Syslog Message

The Syslog notification sends event information to a syslog server.

- Syslog Server Host Name - Enter the host name, IP address or fully-qualified domain name of the syslog server.
- Port - Select the port on which the syslog server is listening. By default this is UDP port <% SYSLOG_UDP_PORT%> ***or*** TCP port <%SYSLOG_TCP_PORT%>
- Sockets Type - Select the protocol the syslog server is using (TCP or UDP).

- Message - Enter the text you want displayed in the message portion of the Syslog event. Event information is available to the command script through the Environment variables, enabling you to use information from the event, such as the computer name or the message details field in any batch files, scripts, or other programs.

Click the Test button to test the notification.

4.2.1.4.6 Mail Notification (SMTP)

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

- 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.

- SMTP Server - Enter the name or 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.
- **Priority** - Sets the priority or importance of the email message: High, Normal, Low

- 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.

Lists the Event Views[118] that the SMTP Notification Method is assigned to. Select the **New** link to add an Event View[118].

Highlight an Event View[118] and select **Properties** to modify the Event View[118].

- 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.

4.2.1.4.7 ELM Advisor Notification

The ELM Advisor Notification sends event information to desktop computers that are running the ELM Advisor client.

ELM Advisor provides the user with an instant notification that does not disrupt work flow. The ELM Advisor desktop tool is a component that is selected during setup or can be installed separately.

- All connected ELM Advisor users - Enable (check) this option to send the event information to all ELM Advisor users who are currently connected. Users must have read access to the ELM Server to connect.
- Users - Enter a list of the Usernames who will be using the ELM Advisor desktop utility. This option is disabled if All connected ELM Advisor users is enabled.
  - Browse - Click the Browse button to select users from a list of domain accounts.
  - Add - Click the Add button to add the user to the list.
  - Remove - Click the Remove button to remove selected users from the list.
- Message - Enter a message to be sent to currently connected users. You may use the Insert Variable button to insert Environment Variables that will be populated when the notification is created.

Note

ELM Advisor is closely associated with a single desktop session (i.e. logged on user). So if a user is not logged on, then ELM Advisor Notifications will not be received by the ELM Advisor Taskbar Tool. Also, if the same username has multiple simultaneous desktops, for example multiple remote desktop sessions, then deleting Notification Messages, or marking them as read, will not be reflected in the ELM Advisor UI in other desktop sessions.

4.2.2 Event Views

Event views are modified in the MMC however viewing the results is more efficient using the ELM Management Console. 16

Administrators can quickly diagnose problems by using **Event Views** to organize large amounts of event log information. **Event Views** allow you to group events that match Include 103 and/or Exclude 99 Filters with the options to notify or report based on that **Event View**. 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.

Records in Event Views are generically referred to as "Events." Events originate from several sources:

- Event log entries collected from Windows-based systems.
- Syslog messages received from Syslog clients.
- SNMP Traps received from SNMP-capable systems and devices.
- ELM Server generated Events.
-

An **Event View** has two display modes:

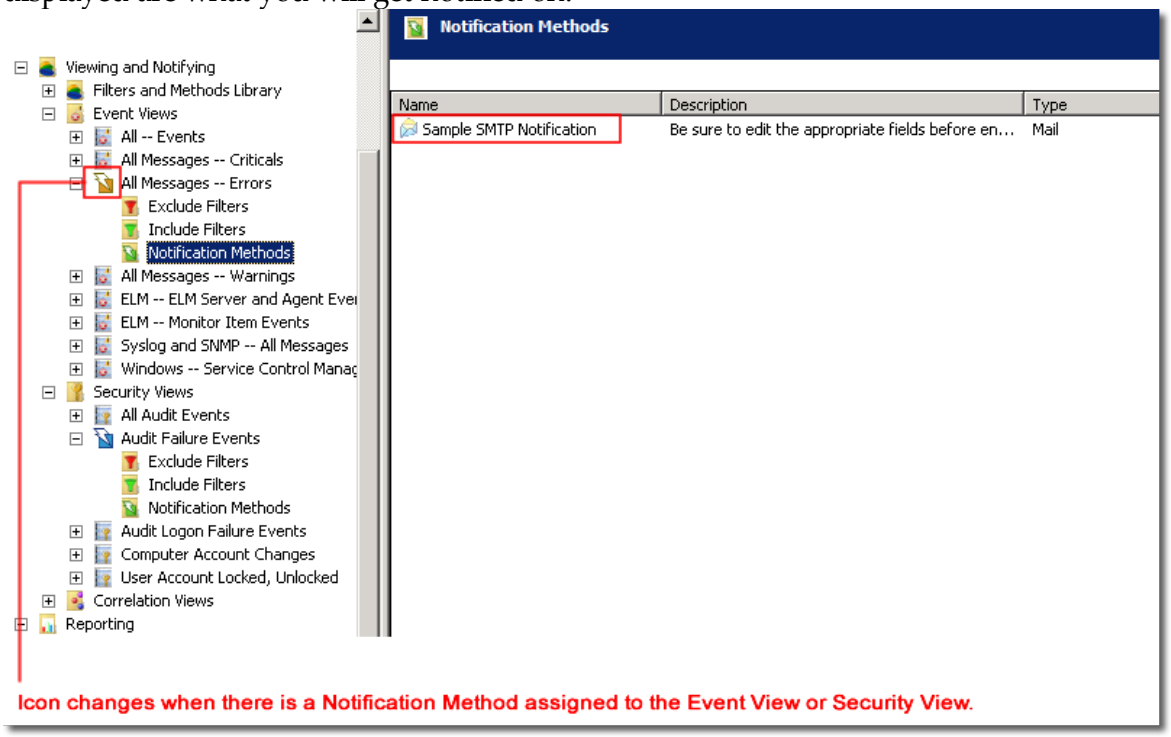
- Detail Event View mode (default) which shows each event on a single line in the Event View.

- Summary Event View mode displays a summary roll-up (i.e., count of events). This **Event View** display mode is very useful to determine the busiest events across multiple systems by sorting on the **Count** column heading.

ELM comes pre configured with a variety of **Event Views** and are sorted into logical groupings. **Event Views** beginning with All represent general events grouped by type or protocol. Names can be modified for the requirements of a specific environment.

Notifications

When the Notification Method is applied to the **Event View**, the events that are displayed are what you will get notified on.



Excluding Events

Select the event that you want to exclude.

Select an event in the **Event View**, select **Create View** to automatically create an Event Filter and navigate through the **Create Event View Wizard**.

Create Filter

Select an event in the **Event View**, select **Create Filter** to automatically create an Event Filter and navigate through the **Create Event Filter Wizard**.

Event View Properties

Event View Settings 121

Exclude Filters 99

Include Filters 103

Notification Methods 111

Reports from an Event View

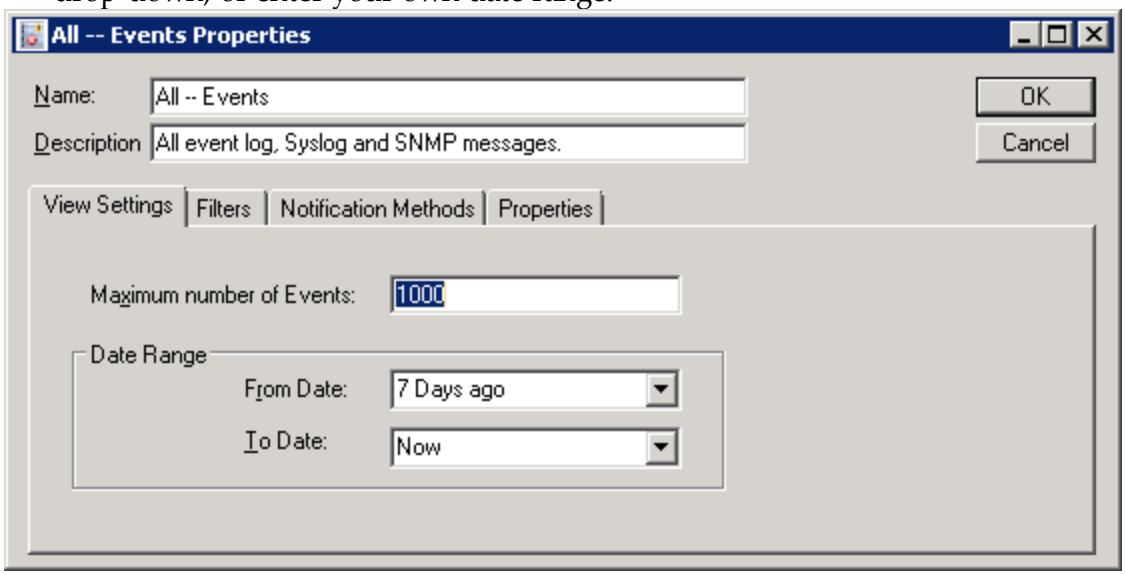
Beginning with ELM 7.5 reports from Event views are exclusive to the ELM Management console.

4.2.2.1 Event View Properties

Maximum number of Events 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 and the longer the query will take to return results.

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.



The Event Filters[99] determine what events are going to be filtered in or out of the Event View.

Include Event Filters

Select the Include Event Filters[103] that identify events to be displayed in this Event View.

- New - Opens the **Event Filter Wizard** to create a new Event Filter.
- Properties - Select the filter and click Properties to edit or view the properties of an Event Filter.

Exclude Event Filters

Exclude Filters[99] 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 focuses subset of the events you want to isolate.

- New - Opens the **Event Filter Wizard** to create a new Event Filter.
- Properties - Select the event filter and click Properties to edit or view the properties of an event filter.

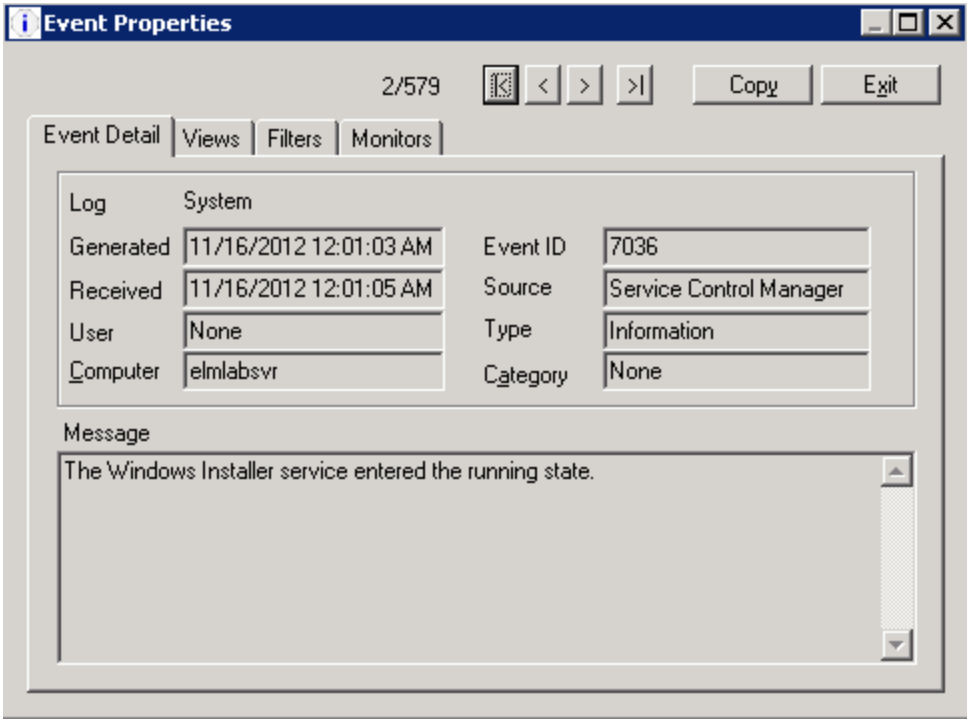
The Notification Method determines where the events in the Event View are going to be delivered to.

This is a way to use multiple Notification Methods.

- New - Opens the **Notification Method Wizard** to select a Notification Method.
- Properties - Select the Notification Method and click Properties to edit or view the properties of a Notification Method.

4.2.2.2 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.
Use the Database Retention Policy to configure deleting and/or 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.

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 event.
- **Message** - Determined by the application or process that created the event.

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.

Displays a list of Event Filters that display this event.

Displays a list of Monitor items where this event is collected.
To view properties of an Event View, right click on the Event View and select Properties from the menu.

4.2.3 Security Views

Security views are modified in the MMC however viewing the results is more efficient using the ELM Management Console. 16

Administrators can track security issues by using Security Views. Security Views allow you to group events that match Exclude and/or Include Filters with the options to notify or report based on that Security View. Security Views differ from Event Views slightly by design in that only security-related events (audit success and audit failure events) are displayed in the view. The Security View also uses 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.

Records in Security Views are generically referred to as "Events." Events generate from several sources:

- Event log entries collected from Windows-based systems.
- Syslog messages received from Syslog clients
- SNMP Traps received from SNMP-capable systems and devices
- ELM Server generated Events

A Security View has two display modes:

- Detail View mode (default) which shows each event on a single line in the Security View.
- Summary Event mode displays a summary roll-up (i.e., count of events). The Summary View display mode is very useful to determine the busiest events across multiple systems by sorting on the Count column heading.

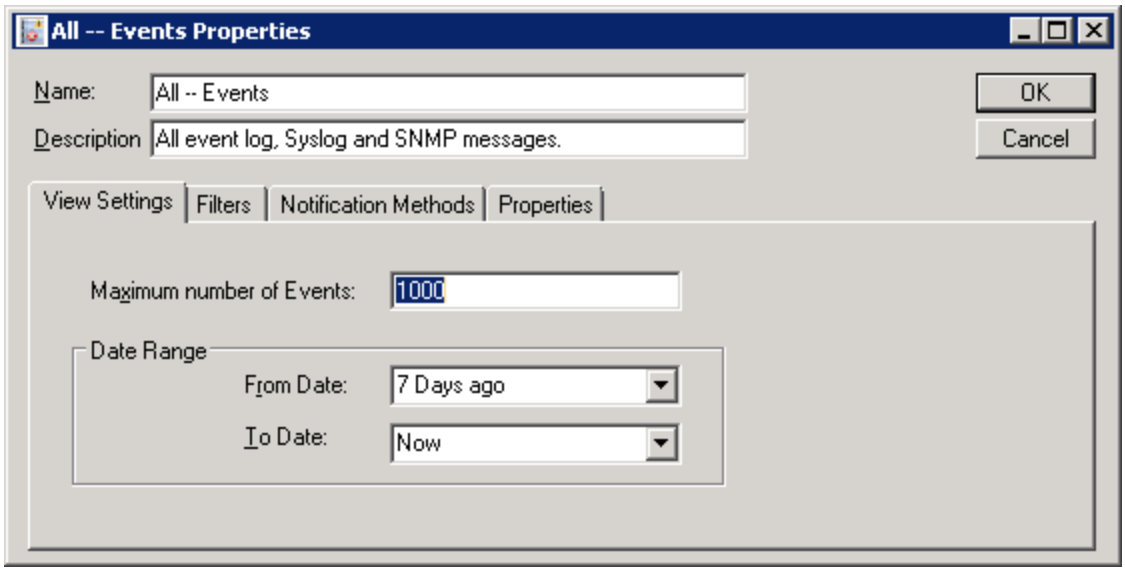
Pausing Event Views – On busy servers, thousands of events can stream into the Security View making it difficult to read a specific event. Pause the Security View to get more detail on the event or to exclude the event from the Security View.

4.2.3.1 Event View Properties

Maximum number of Events 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 and the longer the query will take to return results.

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.



The Event Filters[99] determine what events are going to be filtered in or out of the Event View.

Include Event Filters

Select the Include Event Filters[103] that identify events to be displayed in this Event View.

- New - Opens the **Event Filter Wizard** to create a new Event Filter.
- Properties - Select the filter and click Properties to edit or view the properties of an Event Filter.

Exclude Event Filters

Exclude Filters[99] 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 focuses subset of the events you want to isolate.

- New - Opens the **Event Filter Wizard** to create a new Event Filter.
- Properties - Select the event filter and click Properties to edit or view the properties of an event filter.

The Notification Method[111] determines where the events in the Event View are going to be delivered to.

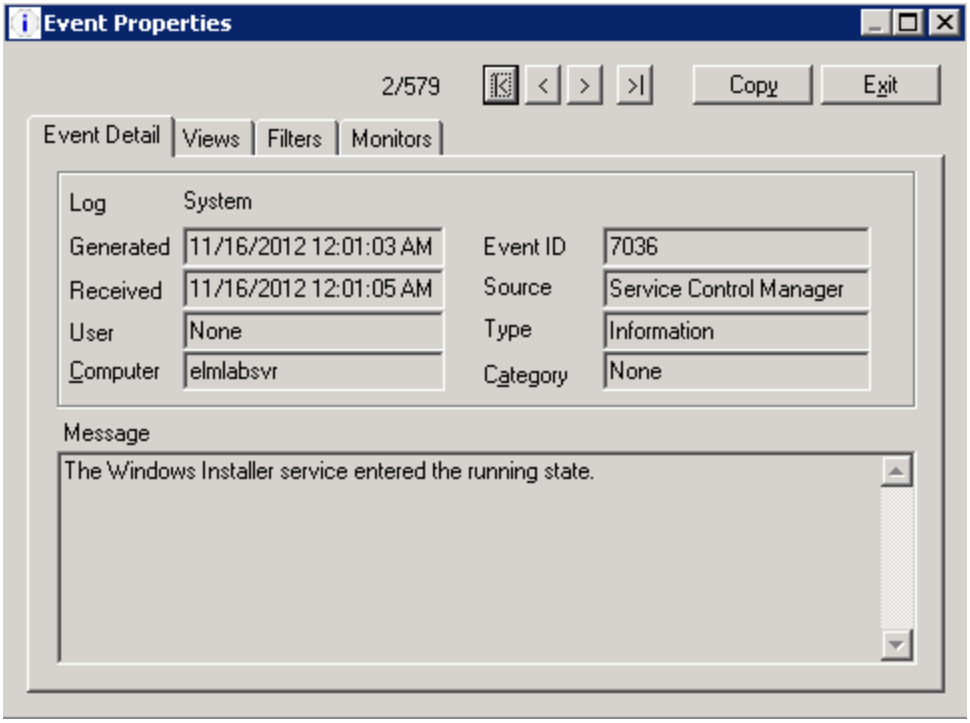
This is a way to use multiple Notification Methods[111].

- New - Opens the **Notification Method Wizard** to select a Notification Method[111].

- Properties - Select the Notification Method and click Properties to edit or view the properties of a Notification Method.

4.2.3.2 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.
Use the Database Retention Policy to configure deleting and/or 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.

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 event.
- **Message** - Determined by the application or process that created the event.

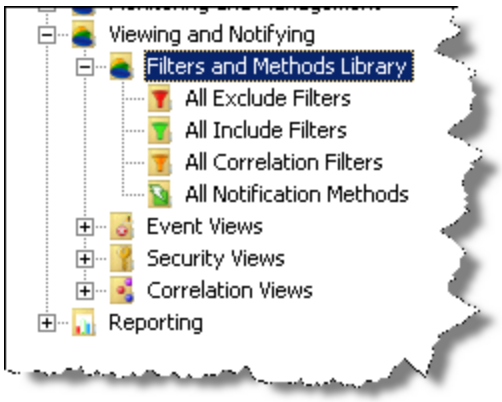
Displays a list of Event Views that will display this event. Event Filters determine which Event Views will display the event. Editing Event Filters after the event has been received and processed by the ELM server may change the results displayed in this list.

Displays a list of Event Filters that display this event.

Displays a list of Monitor items where this event is collected.
To view properties of an Event View, right click on the Event View and select Properties from the menu.

4.2.3.3 Event Filters

The Filters and Methods Library within ELM contains Event Filters and Notification Methods which can be assigned to Event Views. Event Filters are common objects within ELM and can also be assigned to Event Collectors, Syslog Monitors, SNMP Monitors and Event Monitors.



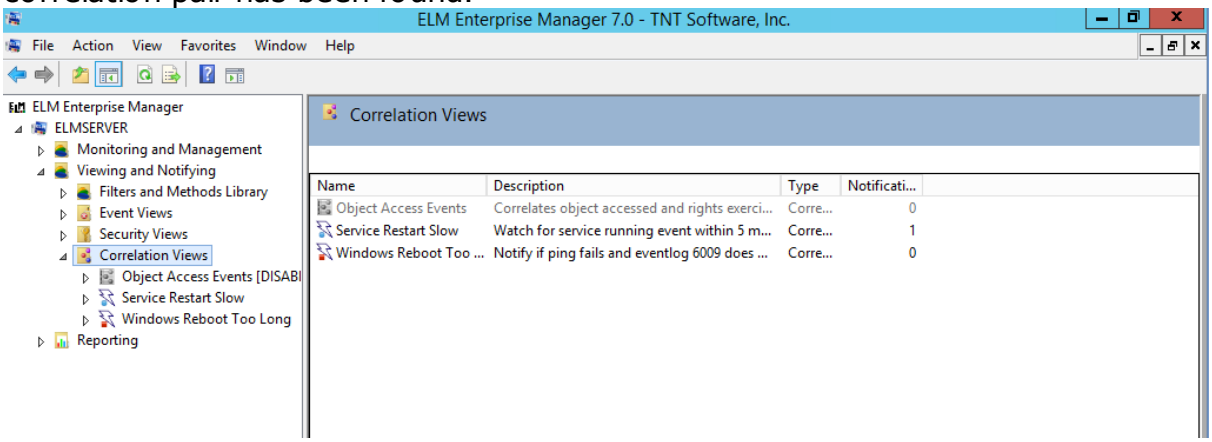
See More:

All Exclude Filters 99
All Include Filters 103
All Correlation Filters 106
All Notification Methods 111

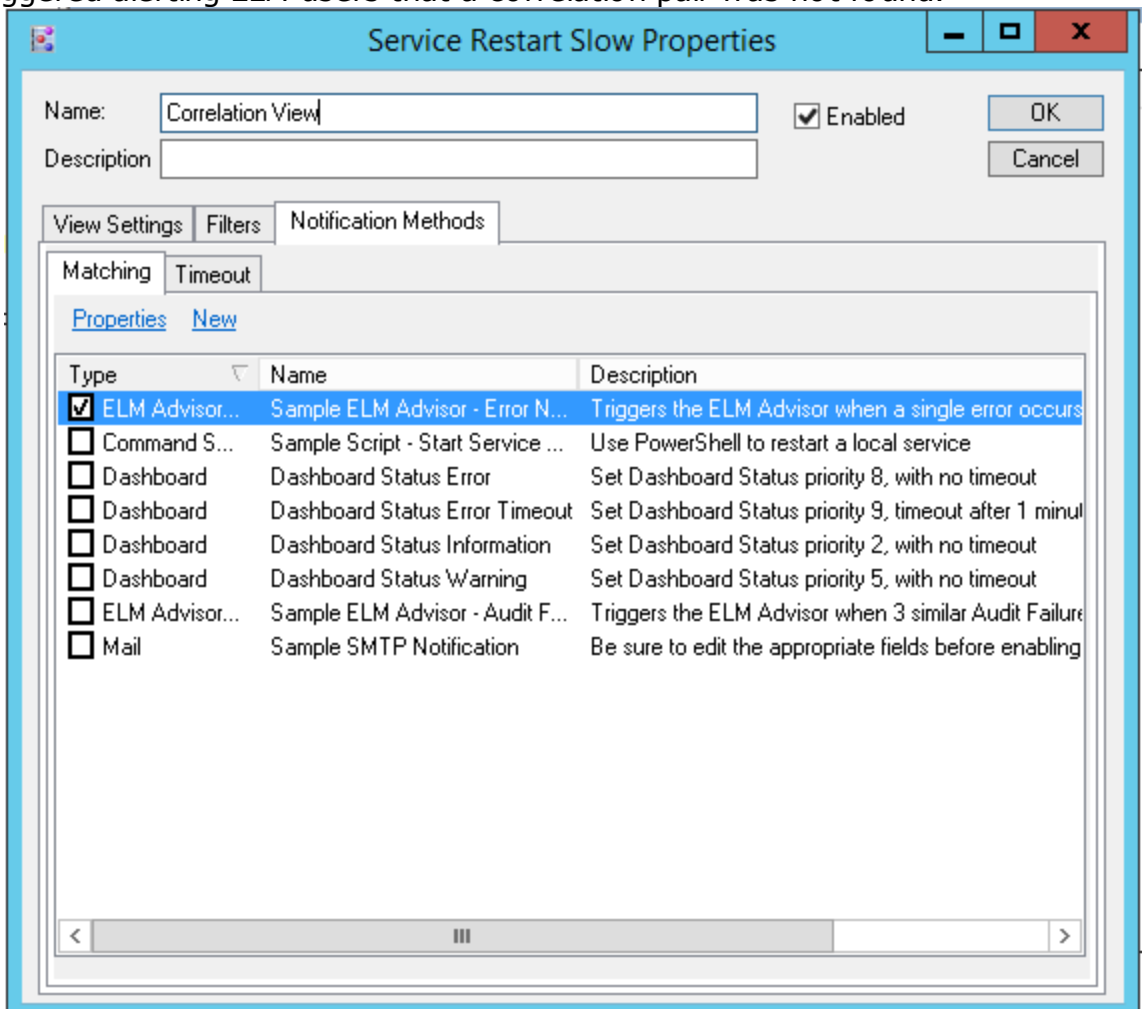
4.2.4 Correlation Views

Event views are modified in the MMC however viewing the results is more efficient using the ELM Management Console. 16

ELM Correlation Views watch for specific pairs of event. The most basic configuration requires an Include Filter, a Correlation Filter, and a timer setting. When an event matches the Include Filter, it is designated as the "start event" and the timer begins counting down. If an event matching the Correlation Filter is found before the timer expires, then it is designated as the "end event" and a correlation pair has been found.



The basic Correlation View described above can have a Notification Method assigned, so ELM users can be alerted to the occurrence of a correlation pair. If the timer counts down to zero, then a separate Notification Method can be triggered alerting ELM users that a correlation pair was not found.



Note

Correlation View Icons will change depending on the assignment of Notification Methods.

- No Notification Methods assigned to the View

- One or more Notification Methods assigned to only the Matching result.

- One or more Notification Methods assigned to only the Timeout result.

- One or more Notification Methods assigned to both the Matching and Timeout results.

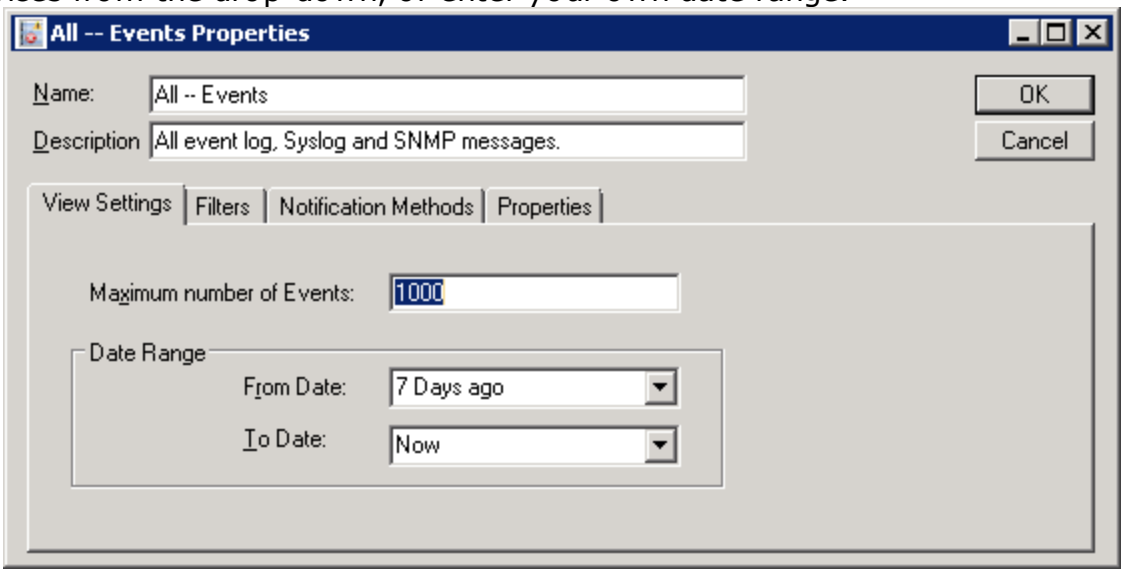
4.2.4.1 Correlation View Properties

Maximum number of Events

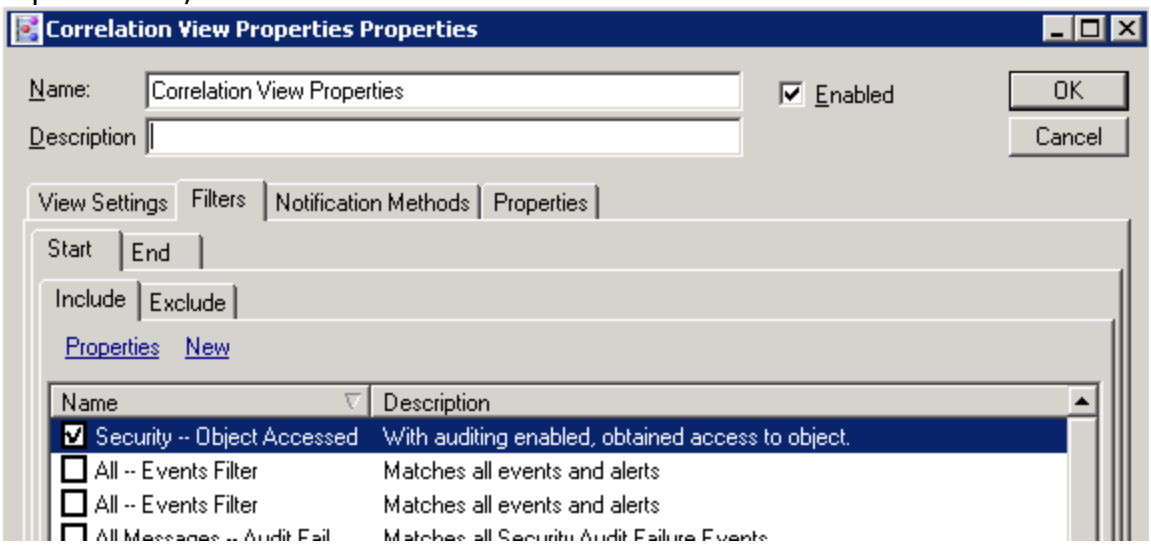
- Specifies the maximum number of rows displayed in the **Event View**. You may select any value from 1 through 50000. The larger the number, the more memory the mmc.exe process will consume and the longer the query will take to return results.

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.



Events matching the combination of Include and Exclude Filters will start the Correlation View timer. If subsequent events matching the combination of Filters are processed, then the Correlation View timer will be re-started.



Start - Include Filters 103

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

- New - Opens the Include Filter Wizard to create a new Include Event Filter.
- Properties - Select the filter and click Properties to edit or view the properties of an Event Filter.

Start - Exclude Filters 99

Exclude Filters are evaluated before the Include Filters. An Exclude 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.

- New - Opens the Exclude Filter Wizard to create a new Event Filter.
- Properties - Select the Exclude Filter and click Properties to edit or view the properties of an Exclude Filter.

End - Correlation Filters 106

Events matching any of the End Correlation Filters within the time period will trigger all assigned Matching Notification Methods.

Watch for correlating event within this time period - This sets the duration for how long a Correlation View will watch for a Matching End event once a Start event has initiated the timer.

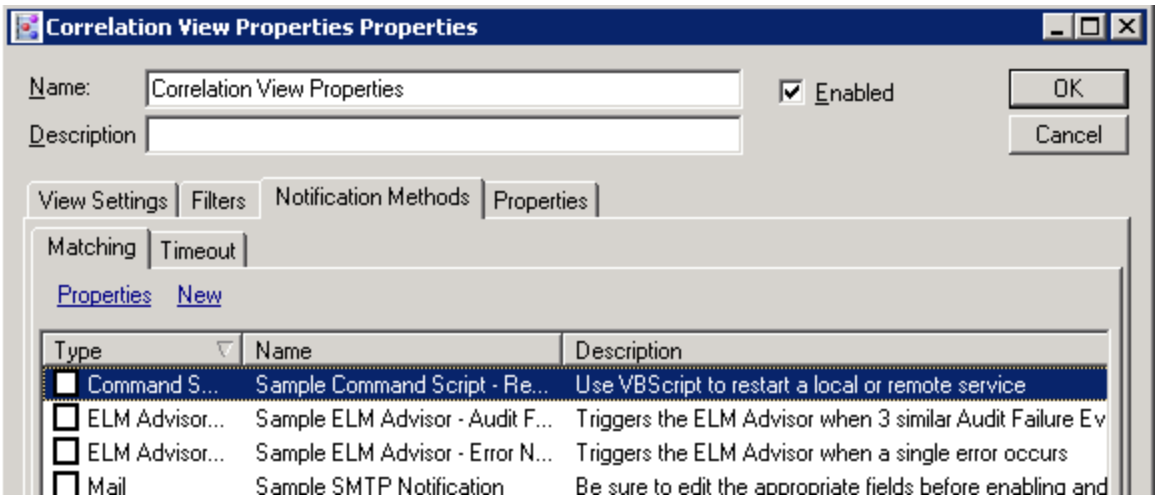
- New - Opens the Correlation Filter Wizard to create a new End Event Filter.
- Properties - Select the Correlation Filter and click Properties to edit or view the properties of an Correlation Filter.

If an Event matches any of the Correlation Filters within the time period, assigned Matching Notification Methods will be triggered, and the View itself will generate event 5708. If no Event is found within the time period, the assigned Timeout Notification Methods will be triggered, and the View itself will generate event 5707.

Notifications can be triggered if correlating End events are found, or if they are not found, within the configured time period. The time period begins when an event matches the combination of Include and Exclude Filters assigned to the View.

Matching

The assigned Notification Methods are triggered if a correlating End event is found within the time period configured on the Filters End tab.



- New - Opens the **Notification Method Wizard** to select a Notification Method.
- Properties - Select the Notification Method and click Properties to edit or view the properties of a Notification Method.

Timeout

The assigned Notification Methods are triggered if a correlating End event is not found within the time period configured on the Filters End tab.

- New - Opens the **Notification Method Wizard** to select a Notification Method.
- Properties - Select the Notification Method and click Properties to edit or view the properties of a Notification Method.

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

Server Properties

5 Server Properties

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

Licensing

If you are running ELM in evaluation or with a temporary license, the **Licensing** tab will indicate when the evaluation period expires. If you have purchased ELM, you will receive a Serial Number which must be entered into the **ELM Server Properties - Licensing** tab. Enter the information exactly as it appears on your Software License Agreement. If you did not receive an SLA with your purchase, or if you cannot locate your SLA, please contact Sales@firemtsoftware.com
You must activate your license **within 7 days** after your Serial Number has been entered. If the product is not activated within 7 days, the product is locked until it is activated. If you have Internet access on your ELM Console computer, you may activate over the Web. If you don't have Internet access from your ELM Console, you may call or email Fire Mountain Software to request an activation file for your license. We will send a TNTKEY file to you to activate the license.

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.

Note

If the evaluation period has expired or if you received a temporary serial number which has expired, you must close and re-open the ELM Console after entering a valid serial number for the unlock procedure to complete.

ELM will automatically activate your license. If you do not have internet access or have disabled this option then you can manually update your license by following the procedure below.

To manually activate your license:

1. Open the **Licensing** tab.
2. To enter your Serial Number, select **Edit/Activate**.
3. If you have Internet access, select **Web Activation**, and click the **Activate** button.

If you do not have Internet access:

1. Contact Fire Mountain Software at Sales@firemtsoftware.com or by telephone at **360-546-0878**.
2. Fire Mountain Software will email you a **TNTKEY** file. Save this file to the file system.
3. Select **File Activation** and use the **Browse** button to select the TNTKEY file.

4. Click the **Activate** button.

Once activated, the number of Agents in-use and total number of Agents for the license, by class, are displayed in the Licensing dialog. In the example figure below, this license allows various quantity available and also shows that 2 licenses are in use for Class I Core. This indicates 8 Class I Core licenses are still available along with all other licenses.

License	Quantity	In Use
Cr Class I Core (Cr I)	10	2
Ev Class I Event (Ev I)	10	0
Nt Class II Network (Nt II)	3	0
Sy Class I System (Sy I)	3	0
Lg Class I Log (Lg I)	3	0
Pf Class I Performance (Pf I)	3	0

If you have any licensing or registration questions, please contact Fire Mountain Software's Sales Department: Sales@firemtsoftware.com.

Modules

This tab displays module (DLL), process, thread, and other diagnostic information about the ELM Server and ELM Console. Fire Mountain Software's Product Support Group may request this information.

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.

Technical Resources

6 Technical Resources

Database Settings Reference

Database Settings Entries 19

Event Reference

ELM Server and ELM Agent Events 147

Registry Settings

ELM Server Registry Entries 160
ELM Console Registry Entries 158
ELM Service Agent Registry Entries 167

Command Line Reference

ELM Server Command Line Options 175

Online References

Fire Mountain Software Support
(http://www.firemtsoftware.com/support)
Support Knowledge Base
(http://www.firemtsoftware.com/support/kba)
Software Prerequisites and Downloads
(http://www.firemtsoftware.com/elmsupport/supplementaldownloads.aspx)
Online Tutorials
(http://www.firemtsoftware.com/elmsupport/tutorials/default.aspx)

6.1 Security Guide

The ELM Security Guide provides ELM administrators details on the following topics:

Introduction 142
Security Guidelines 144
Configuring ELM Server Security 146

6.1.1 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
- ELM Advisor

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

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.

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 ELM 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).

Management Console -

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

Data Encryption - ELM incorporates proprietary data encryption. All data sent between the following components is encrypted using this mechanism:

- Communication between a Service Agent and an ELM Server.
- Communication between two ELM Servers (via the Forward Event Notification Method 113)

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

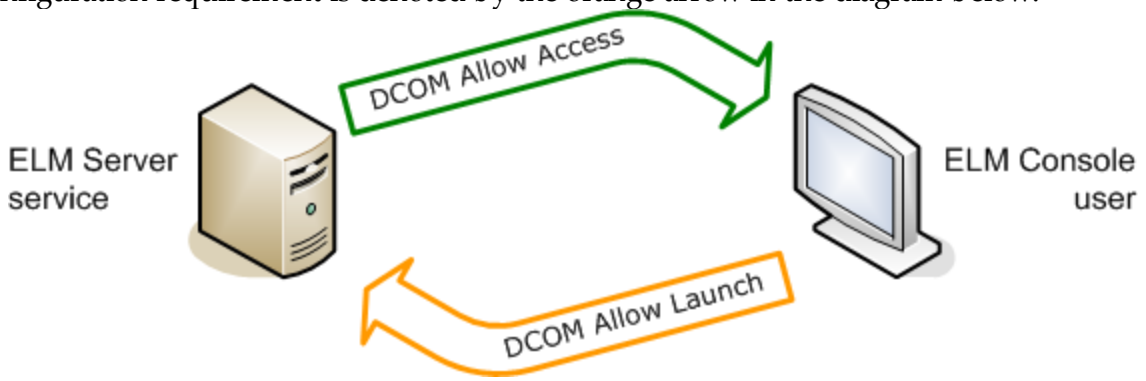
Integrated Auditing - ELM supports auditing of access and modification to ELM Server objects. This enables administrators to audit configuration changes to ELM Server objects.

6.1.2 Security Guidelines

ELM uses integrated Windows Security (NTLM or Kerberos depending on the Server and Agent OS) to authenticate users. Some of the functions won't work (such as killing a task or managing services) unless you have administrative rights on the monitored computer. ELM supports object and item-level security through the snap-in UI. You may apply Windows Access Control Lists (ACLs) to objects in your ELM Console.

DCOM Permissions

Communication between the ELM Server and the ELM Console or ELM Advisor is done with Distributed COM (DCOM). The ELM Server service requires DCOM Allow Access permissions to the ELM Console and ELM Advisor. In turn, users running the ELM Console or ELM Advisor require DCOM Allow Launch permissions to the ELM Server. DCOM Allow Access permissions are granted to the **Authenticated Users** group by the ELM setup program when the ELM Console is installed. This automatic configuration is denoted by the green arrow in the diagram below. DCOM Allow Launch permissions need to be granted on the ELM Server computer by an Administrator. This manual configuration requirement is denoted by the orange arrow in the diagram below.



These permissions may be viewed and edited via the DCOM Configuration Utility (DCOMCNFG.exe). To manage these permissions, use the steps below.

These steps should be done automatically by ELM setup.

In Windows XP, Vista, Windows 7, Windows 2003, or Windows 2008:

1. Launch DCOMCNFG.
2. Expand Component Services, then Computers, then My Computer, and finally DCOM Config.
3. Scroll down to ELM.Advisor.exe.
4. Right-click and select Properties.
5. Select the Security tab.
6. In the Access Permission area, click the Edit button.
7. Verify that Authenticated Users has Allow for Local Access and Remote Access.
8. Repeat steps 3-7 for MMC Application Class.

Note

In some cases, the ELM Setup package does not have permissions to the MMC Application Class DCOM application. *When this happens you will typically see the* Use Default *radio button selected, and* Authenticated Users *will be granted Access at the* ***My Computer*** *level.*

9. Close DCOMCNFG.

You may have to reboot each system in order for the DCOM security changes to take effect.

These steps need to be manually verified and completed, as necessary.

In Windows XP, Vista, Windows 7, Windows 2003, or Windows 2008:

1. Launch DCOMCNFG.
2. Expand Component Services, then Computers, then My Computer, and finally DCOM Config.
3. Scroll down to TNT **Software** .
4. Right-click and select Properties.
5. Select the Security tab.
6. In the Launch and Activation Permissions area, select the Custom radio button, and click the Edit button.
7. Verify that ELM Console users, or an equivalent group, have Allow for Local and Remote, Launch and Activation.
8. Close DCOMCNFG.

You may have to reboot each system in order for the DCOM security changes to take effect.

Note

Because communication between an ELM Server and an ELM Console is COM-based, TCP port 135 (RPC endpoint mapper) must be open between the communicating end-points. DCOM also uses RPC dynamic port allocation. By default, RPC dynamic port allocation randomly selects port numbers above 1024. You can control which ports RPC dynamically allocates for incoming communication and then configure your firewall to confine incoming external communication to only those ports (and TCP/UDP port 135).

NetBIOS/RPC

When using a Virtual Agent to monitor a Windows system (e.g., to collect events, monitor services, etc.), monitoring is performed by the ELM Server. The ELM Server makes RPC

Win32 API calls to execute Monitor Items and collect data. There must be NetBIOS and RPC connectivity between the ELM Server and the Virtual Agent.

Firewalls and Port Blocking

If you intend to use Virtual Agents in a firewall environment (IE putting a firewall between the ELM Server and ELM Virtual Agent), or put a firewall between the ELM Server and ELM Console, network communication is RPC based. TCP port 135 (RPC endpoint mapper) must be open between the communicating end-points. DCOM also uses RPC dynamic port allocation. By default, RPC dynamic port allocation randomly selects port numbers above 1024. You can control which ports RPC dynamically allocates for incoming communication and then configure your firewall to confine incoming external communication to only those ports (and TCP/UDP port 135).
For more information on DCOM and firewalls, see Microsoft's White Paper about Using DCOM with Firewalls.

6.1.3 Configuring ELM Server Security

ELM integrates with Windows security to provide item-level security on objects and items within the ELM Console. This enables you to selectively set security on the individual objects and containers, including:

- ELM Server
- Agents
- Monitoring Categories
- Monitor Items
- Event Filters
- Notification Methods
- Event Views
- Performance Data container
- Performance Counters

To view or configure security on an item:

1. Right-click on the item you wish to secure and select Security. If Security is not an option on the context menu, you are not able to secure this item.
2. The permissions for the item and the list of Access Control Entries (ACEs) will be displayed.

    - Click the Add button to add a user or group to the list of ACEs.
    - Click the Remove button to remove the selected user or group from the list of ACEs.
    - Click the Advanced button to view and modify advanced security settings such as Special Access and Inheritance.

ELM supports auditing of access and modification to ELM Server Objects. When ELM is installed, the ELM Server service account user is added to the "Generate security audits" Security Policy. This is so if auditing is turned on for ELM objects, and "Audit object access" is turned on in the Audit Policy settings, ELM will write out an audit trail for ELM object changes. In order to audit activity on ELM Server Objects, you must enable File and

Object Access auditing on the ELM Server. On a Windows system, this is typically done using a security-policy snap-in (e.g., the Local Security Policy snap-in).

Note

As a failsafe mechanism, an ELM Server ignores all security settings when the ELM Console is run in the security context of the ELM Server service account. This is done intentionally to prevent administrators from inadvertently locking themselves out of objects. If you log on to the ELM Server using the ELM Server service account, you will be able to configure all objects, settings and features. Security will not be enforced for the session.

To view or configure auditing on an item:

1. Right-click on the item you wish to secure and select Security. If Security is not an option on the context menu, then you are not able to secure or audit access to this item.
2. Click the Advanced button.
3. Select the Auditing tab.
4. Click the Add button to add a user, group, or multiple users/groups to the list of Audit entries, then click OK. Click the Edit button to edit an existing entry, or the Remove button to remove an existing entry.
5. The Auditing Entry dialog will appear. Select the items for Success and/or Failure that you wish to audit by clicking the desired checkboxes so that they are checked.
6. Select whether the audit level should apply to this object, or to this object and all child objects, from the Apply onto dropdown list.
7. Click OK to save the changes, then click Apply to apply them.
8. Click OK twice to exit the Security dialogs.

6.2 Server and Agent Events

The tables in this section lists the events that the server and ELM Agent processes can log. All events created from Monitor Item Actions are written to the ELM database. All events logged by the ELM Agent process will set the Event Source field to **TNTAGENT**. All events logged by the server process will set the Event Source field to .

ELM event numbers are grouped into ranges with the following descriptions:

- General purpose messages (5050-5099) 147
- Service or Process Related Messages (5100-5199) 149
- Session Related Messages (5200-5299) 149
- Agent Related Messages (5300-5399) 150
- Notification Related Messages (5400-5499) 151
- Monitor Related Messages (5500-5599) 152
- Performance Data Collector Related Messages (5600-5699) 156
- Event Engine Related Messages (5700-5799) 156
- Report Related Messages (5800-5899) 156
- Common Messages (5900-5999) 157

6.2.1 Event IDs 5050 - 5099

Below are **general purpose** events from the server or ELM Agent process.

Event Type:

I = Informational W = Warning E = Error

Event ID	Event Type	Message
5050	I[4]	%1 (reserved)
5051	I	%1 (reserved) Script Monitor Informational
5052	I	%1 (reserved) Script Monitor Warning
5053	I	%1 (reserved) Script Monitor Error
5054	I	%1 (reserved)
5055	E	%1 (reserved)
5056	W	%1 (reserved)
5057	E	%1 (reserved)
5058	E	The item has not been locked for write access.
5059	E	Access denied because another caller has the item open and locked.
5060	E	Access denied because the caller has insufficient permission, or another caller has the file open and locked.
5061	E	An item with this name already exists.
5062	E	The action could not be carried out because the software evaluation period has expired.
5063	I	The software license for this product indicates that it has not been registered.
5064	I	An attempt was made to WriteLock %1 which cannot be modified. Its properties will be shown in a Read Only state.
5065	E	An attempt was made to connect to the server from %1. Connection denied.
5066	E	%1 service is restarting itself for the following reason: • VIRTUAL MEMORY MAX EXCEEDED • THREAD COUNT MAX EXCEEDED • HANDLE COUNT MAX EXCEEDED • MONITOR JOB QUEUE TERMINATED • MONITOR JOB QUEUE UNABLE TO ENUMERATE SERVERS • MONITOR JOB QUEUE UNABLE TO GET MASTER MONITOR COLLECTION
5067	E	%1 is missing one or more binary files. Please use the Repair option in Add/Remove Programs.
5068	E	Error. Install complete, but Agent offline. Intervention required.
5069	E	Error. Install Skipped, Agent is not enabled.
5070	E	Error. A Conflicting product is already installed.
5071	E	An SEH Exception was caught. Details: %1
5072	E	The proxy server requires authentication and authenticated proxy connections are not supported.
5073	E	Caught exception in %1 %2

5074	E	Assigned license quantities exceed quantities currently allowed. Please Activate license and adjust quantities. Contact Fire Mountain Software Sales with questions.
5075	W	Your license will expire in less than 12 days. Please Activate your updated license to prevent license expiration. Contact Fire Mountain Software Sales with questions
5076	E	Your license will expire in less than 4 days. Please Activate your updated license to prevent license expiration. Contact Fire Mountain Software Sales with questions.

6.2.2 Event IDs 5100 - 5199

Below are **service or processor** related events from the server or ELM Agent process.
Event Type:
I = Informational W = Warning E = Error

Event ID	Event Type	Message
5100	I[1]	%1 service running
5101	I[2]	User requested %1 service shutdown
5102	I[1]	%1 service stopping
5103	E	An Error occurred accessing the %1 of %2. This Error indicates incompatible Microsoft Data Access Components (MDAC) could be installed. Please refer to the software compatibility checklist for further information.
5104	E	An Error occurred queuing the %1 job named %2. The maximum job queue entries for an individual item cannot exceed %3. For more information please contact technical support at support@firemtsoftware.com.
5105	I	The ELM Server has been shutdown.

6.2.3 Event IDs 5200 - 5299

Below are **session** related events from the server or ELM Agent process.
Event Type:
I = Informational W = Warning E = Error

Event ID	Event Type	Message
5200	E[3]	Error opening configuration file: %1
5201	E	Fatal Error in %1 for stream %2

5202	E	Error connecting to database: %1
5203	E	Database access error %1
5204	E	Critical failure: failed loading configuration data from %1.%r Contact Fire Mountain Support for assistance, or try these steps:%r 1. Move the above dat file to another folder.%r 2. Make a copy of %2.%r 3. Rename the copy to %3.%r 4. Start the ELM Server.
5205	E	The %1 service failed to initialize
5206	E	The service failed to initialize a session for %1. %2
5207	E	The service failed to initialize a session because the software license quota has been exceeded.
5208	E	Critical failure: failed storing configuration data to %1
5209	E	Critical failure: failed writing to registry. Check the registry permissions on the service account.
5210	E	The XML import feature is not available in evaluation mode.
5214	W[1]	A critical database failure occurred and the temporary database %1 has been enabled. Data in this temporary file will be merged with the configured database when it becomes available.
5215	E	A critical failure occurred while enabling fail-over to temporary database %1. This failure could result in loss of data.
5216	I[1]	The configured database has returned on-line. Temporary data written to %1 is now being merged with the database.
5217	I[1]	%1, recovery attempt completed for the database. %2
5218	I	%1 prune %2 %3 event records completed.
5219	E	%1, errors occurred attempting to purge event records. %2
5220	E	%1 %2 The Primary and Failover databases configured for ELM are not available. At least one of the configured databases needs to be available for the ELM Server service to start.
5221	I[1]	%1 The Primary database configured for ELM has returned on-line.
5222	E	Failed to drop the database %1. Error %2. Please make sure the SQL server is connectable.
5223	E	Error running database SQL script %1 %2
5225	W	

6.2.4 Event IDs 5300 - 5399

Below are **Agent** related events from the server or ELM Agent process.

Event Type:

I = Informational W = Warning E = Error

Event ID	Event Type	Message
5300	E	%1
5301	I[1]	%1 running
5302	I[1]	%1 stopped
5303	I[2]	%1 started monitoring
5304	I[2]	%1 stopped monitoring
5305	I[2]	%1 configuration updated
5306	I	%1 events found
5307	W	%1 events not found
5308	E	The Agent is unable to contact the ELM server.
5309	I	%1 TNTAgent service binaries updated.
5310	E	Deleting corrupted Agent cache file: %1
5311	E	Deleting Agent Service because %1
5312	E	Failed to listen on any of the configured tcp ports
5313	E	Agent version is out of date
5314	E	Cache directory %1 does not have at least %2 MB free. Data may be irretrievably lost until either ELM Server communication is reestablished or disk free space is increased.
5315	E	Cache directory %1 is not available. Data may be irretrievably lost until either ELM Server communication is reestablished or the directory becomes available.
5316	E	The ELM Agents install directory does not have %1 MB free space. No Evt Files will be collected until this much space is available.
5317	I	Switching Agent to Home Server %1.
5318	I	Switching Agent to Standby Server %1.
5319	E	Staging unlicensed ELM Agents found in dat file.
5320	E	File monitor error. %r %1%r File: %2.
5321	E	At least one of the licenses (%1) being assigned to the agent %2 is not valid for the agent.

6.2.5 Event IDs 5400 - 5499

Below are **Notification** related events from the server or ELM Agent process.
Event Type:

I = Informational W = Warning E = Error

Event ID	Event Type	Message

5400	E	%1 is up but the service is not responding
5401	E	Error connecting, %1 is not currently on the network or the network is down or there is no connectivity to TCP port %2
5402	I	Notification Sent: %1 The notification method sent successfully
5403	E	Notification Error: %1 %2
5404	W	Notification script timeout: %1 The following file could not be removed: %2
5488	E	PING monitor %2 failed. Previous state was failure
5489	I	PING monitor %2 succeeded. Previous state was success.
5490	W	PING %2 warning, quality of service may be degraded. Previous state was failure.
5491	E	PING monitor %2 failed. Previous state was warning.
5492	I	PING monitor %2 succeeded. Previous state was warning.
5493	W	PING %2 warning, quality of service may be degraded. Previous state was warning.
5496	I	The service Agent %1 successfully restarted the ELM Server service
5497	E	The service Agent %1 could not restart the ELM Server service
5498	I	The ELM Server successfully restarted the ELM Agent service on %1
5499	E	The ELM Server could not restart the ELM Agent service on %1

6.2.6 Event IDs 5500 - 5599

Below are **Monitor** related events from the server or ELM Agent process.
Event Type:

I = Informational W = Warning E = Error

Event ID	Event Type	Message
5500	E	Monitor item '%1' failed on %2 %3.
5501	I	Monitor item '%1' on %2 is operating.
5502	E	Event monitor failed to connect to agent %1 %2.
5503	E	%1 FTP monitor failed to connect to %2.
5504	I	%1 FTP monitor connected to %2.
5505	W	%1 FTP quality of service is degraded on %2.
5506	E	%1 PING monitor %2 failed.
5507	I	%1 PING monitor %2 succeeded.
5508	W	%1 PING %2 quality of service may be degraded.
5509	E	%1 SMTP monitor failed to connect to %2.
5510	I	%1 SMTP monitor connected to %2.
5511	W	%1 SMTP quality of service is degraded on %2.

5512	W	%1 The SMTP monitor connected to %2.
5513	E	%1 POP3 monitor failed to connect to %2.
5514	I	%1 POP3 monitor connected to %2.
5515	W	%1 The POP3 monitor connected to %2.
5516	W	%1 POP3 quality of service is degraded on %2.
5517	E	%1 Web Page Monitor failed.
5518	I	%1 Web Page Monitor succeeded.
5519	W	%1 Web Page Monitor quality of service is degraded.
5520	W	%1 Web Page Monitor detected a change to the web page on %2.
5521	E	%1 TCP PORT monitor failed to connect to %2.
5522	I	%1 TCP PORT monitor connected to %2.
5523	W	%1 TCP PORT monitor quality of service is degraded on %2.
5524	E	%1 Agent monitor failed to connect to %2.
5525	I	%1 Agent monitor connected to %2.
5526	W	%1 Agent monitor quality of service is degraded on %2.
5527	W	%1 Performance Monitors monitor triggered on %2.
5528	E	%1 Service state has changed on %2, the service is stopped.
5529	E	%1 Service state has changed on %2, the service is stopping.
5530	I	%1 Service state has changed on %2, the service is started.
5531	I	%1 Service state has changed on %2, the service is starting.
5532	W	%1 File Monitor detected a match on %2.
5533	W	%1 Process Monitor detected a process on %2 using excessive CPU time.
5534	E	%1 Process Monitor detected a process on %2 using an excessive amount of CPU time.
5535	I	%1 Process Monitor detected a new process started on %2.
5536	W	%1 Process Monitor detected a process has ended on %2.
5537	W	%1 WMI Monitor detected a change in the WMI Query on %2.
5538	W	%1 SQL Monitor detected a change in the SQL Query on %2.
5539	I	%1 Cluster Monitor event on %2.
5540	W	%1 Cluster Monitor Warning on %2.
5541	E	%1 Cluster Monitor Error on %2.
5542	E	%1 Exchange Monitor Error.
5543	W	%1 Exchange Monitor Warning.
5544	I	%1 Exchange Monitor Success.
5545	E	Exchange Monitor could not logon to the administrator mailbox %1 on %2.
5546	E	Exchange Monitor could not access the message store on %1.
5547	I	Exchange Monitor successfully logged on to the administrator mailbox %1 on %2.

5548	E	Exchange Monitor services are unavailable because MAPI is not installed.
5549	I²	Exchange Monitor services restored.
5550	E	Exchange Monitor services are unavailable because there is no MAPI admin profile.
5551	I	The following SNMP object has a value outside the indicated range: %1.
5552	W	The following SNMP object has a value in the indicated range: %1.
5553	W	Process Monitor detected a number of instances of a monitored process on %2 which exceeds the warning threshold. %1.
5554	E	%1 Process Monitor detected a number of instances of a monitored process on %2 which exceeds the error threshold.
5555	W	%1 Link Monitor average response time is above QoS threshold.
5556	W	%1 Link Monitor detected a broken link.
5557	W	IIS Monitor detected a change in the status of the following services %1.
5558	E	IIS Monitor detected a broken path referenced in the IIS Metabase %1.
5559	W	IIS Monitor detected a failed URL request in the log files %1.
5560	W	IIS Monitor Blocked Address Connection Attempt %1.
5561	I	%1 Link Monitor succeeded .
5562	I	Event Monitor successfully connected to %1.
5563	E	%1 ELM Server Monitor failed to connect to %2.
5564	I	%1 ELM Server Monitor connected to %2.
5565	W	%1 ELM Server Monitor quality of service is degraded on %2.
5566	E	The Bookmark for the %1 event log on %2 rolled over. To prevent the loss of more events, please increase the size of your event log. See the Best Practices section of the ELM Help file for more information.
5567	I	The application %1 version %2 has been installed on %3. The inventory record for this Agent has been updated to reflect this change.
5568	I	The application %1 version %2 has been uninstalled on %3. The inventory record for this Agent has been updated to reflect this change.
5569	W	The application %1 on %2 is unavailable. An event log entry indicates there is a problem and the application may not be working correctly.
5570	I	The application %1 on %2 experienced a problem at %3. The outage lasted about %4. The application appears to be working properly now.
5571	W	%1 Items have been added to the Inventory on computer %2.
5572	W	%1 Items have been removed from the Inventory on computer %2.
5573	I	%1 Service state has changed on %2, the service is paused.

5574	E	Failure trying to retrieve MIB value: %1.
5575	I	%1 EVT File Collector successfully copied file.
5576	E	%1 EVT File Collector failed to copy the file.
5577	I	%1 EVT File Collector successfully stored the file.
5578	E	%1 EVT File Collector failed to store the file.
5579	W	%1 EVT File Collector lost events.
5580	I	Monitor %1 on Agent %2 reported error %3.
5581	I	Evt File Collector Log Settings Changed. LogName: %1 MaxSize: %2 Retention: %3
5582	I	%1 Configuration Changes Detected.
5583	I	%1
5584	E	%1
5585	E	%1
5586	I	%1
5587	E	%1
5588	E	%1
5589	I	%1
5590	E	%1
5591	E	%1
5592	E	Environmental collector %1 had an error %2 aggregating environmental data.
5593	I	Environmental collector %1 successfully aggregated environmental data.
5594	W	Unable to md5 hash the Evt Files Error Message: %1 Computer: %2 Log: %3 Evt Full File Path: %4
5595	E	Unable to store the Evt File. The minimum free space of %1 MB is less than the minimum acceptable free space level of %2 MB. Agent: %3 Log: %4 Storage Directory: %5
5596	W	%1 Configuration Monitor Detected Item(s) Added.
5597	W	%1 Configuration Monitor Detected Item(s) Changed.
5598	W	%1 Configuration Monitor Detected Item(s) Removed.

6.2.7 Event IDs 5600 - 5699

Below are **Performance Data Collector** related events from the server or ELM Agent process.

Event Type:

I = Informational W = Warning E = Error

Event ID	Event Type	Message
5600	E	Error: Receiving performance collection data from %1 a %2 %3
5601	E	Performance collector %1 had an error %2 aggregating performance collection data
5602	I	Performance collector %1 successfully aggregated performance collection data

6.2.8 Event IDs 5700 - 5799

Below are **Event Engine** related events from the server or ELM Agent process.

Event Type:

I = Informational W = Warning E = Error

Event ID	Event Type	Message
5700	E	Error: Receiving event data from %1 a %2
5701	E	Error: Creating event in function %1
5702	E	Error: Streaming event in function %1
5703	E	Error: Handling new event from Agent
5704	I	%1
5705	I	%1
5706	E	%1 Error. %2
5707	W	Correlation Timeout: A Start event was found, but no End event was found within the allowed time period.
5708	I	Correlation Match: A matching pair of Start and End events were found within the allowed time period.

6.2.9 Event IDs 5800 - 5899

Below are **Report** related events from the server or ELM Agent process.

Event Type:

I = Informational W = Warning E = Error

Event ID	Event Type	Message
5800	E	Report failed to run %1
5801	I	Report ran successfully %1

6.2.10 Event IDs 5900 - 5999

Below are **Common** related events from the server or ELM Agent process.
Event Type:
I = Informational W = Warning E = Error

Event ID	Event Type	Message
5900	E	Warning: Cannot add NULL dispatch to ELM Properties collection
5901	E	Error initializing %1 %2
5902	E	%1 API failed %2
5903	E	%1 failed to create socket %3
5904	E	%1 failed to bind socket %3
5905	E	Unable to query the server service performance data. The error code returned by the service is %1.
5906	E	When searching events, at least one event type is required. Please use the back button on your browser to select an item type.
5907	E	The installation was staged
5908	E	The agent was not installed
5909	E	Unable to start the deployment another deployment is already in progress.
5910	E	The specified file does not appear to be of csv or xml file format.
5911	E	An error occurred stopping the agent service.
5912	E	An error occurred copying files.
5913	E	An error occurred opening the remote registry.
5914	E	An error occurred writing to the remote registry.
5915	E	An error occurred opening the service control manager on the computer.
5916	E	An error occurred starting the agent service.
5917	E	Windows NT 4.0 not supported.

6.3 Registry Entries

The tables in this section list registry settings for the Server, ELM Wizard, Service Agent, and Console.
ELM Wizard Registry Entries 158

ELM Service Agent Registry Entries 167
ELM Console Registry Entries 158
ELM Server Registry Entries 160

6.3.1 ELM Wizard 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**).

HKEY_CURRENT_USER \ SOFTWARE\ TNT Software \ ELM Enterprise Manager\ 7.5.0 \ Wizards\Settings

Name	**ADWAgentWaitTimeout**
Type	REG_DWORD
Default Value	20
Restart Required	Console Restart
Description	Value is set in minutes. This setting determines how long the deployment wizard will wait for data from a new agent.
Name	**MaxNumAgentWizardThreads**
Type	REG_DWORD
Default Value	5
Restart Required	Console Restart
Description	Number Agents being deployed at any one time.

HKEY_CURRENT_USER \ SOFTWARE\ TNT Software \ ELM Enterprise Manager\ 7.5.0 \ Wizards\Agent Deployment Wizard

Name	**PreferTCPOverRPCReinstall**
Type	REG_DWORD
Default Value	1
Restart Required	Console Restart
Description	Connect via agent port first.

6.3.2 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**).

HKEY_CURRENT_USER \ SOFTWARE\ TNT Software \ \ 7.5.0 \ Snapin \ Settings

Name	**DefaultEventViewIsDetail**
Type	REG_DWORD
Default Value	0
Restart Required	No
Description	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 Views.
Name	**MaxNumAdvises**
Type	REG_SZ
Default Value	5000
Restart Required	No
Description	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 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	**SnapinAdviseTimerInMilliseconds**
Type	REG_DWORD
Default Value	50
Restart Required	ELM Console restart required
Description	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	**SplashScreen**
Type	REG_DWORD
Default Value	1
Restart Required	ELM Console restart required
Description	Display (1) or do not display (0) Fire Mountain Software splash screen when opening the ELM Console.

6.3.3 ELM Server Registry Entries

HKEY_LOCAL_MACHINE \ SOFTWARE\ TNT Software \ \ 7.5.0 \ Settings
OR if 64bit Operating System
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TNT Software\ELM Enterprise Manager\7.5.0\Settings

Name	**AgentHeartbeatInSeconds**
Type	REG_DWORD
Default Value	60 (seconds)
Restart Required	ELM Server restart required
Description	This sets the interval used by ELM Agent for checking in with the ELM Server. The ELM Server uses this heartbeat check to provide At-a-Glance Agent status information.
Name	**AutoAddParsedAgents**
Type	REG_DWORD
Default Value	0
Restart Required	ELM Server restart required
Description	This automatically adds virtual agents to the ELM server when parsing computer names from Syslog messages. A license is required for each computer name parsed.
Name	**CacheDataTrigger**
Type	REG_DWORD
Default Value	60 (minutes)
Restart Required	ELM Server restart required
Description	Interval for cached data window in minutes. Applies to EEM, ELM, and EVM only.
Name	**ContinuePruneOnArchiveError**
Type	REG_DWORD
Default Value	0
Restart Required	ELM Server restart required
Description	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**	**ForwardELMServerNotification_Category** String Value null ELM Server restart required This setting allows you to re-write an Event category when using a Forward to ELM server notification method. Replace "ForwardELMServerNotification" with the name of your pre-configured Forward to ELM Server notification method. Ex: You setup a Forward to ELM Server type notification method called "Forward to Central Office". The registry entry would then be ***Forward to Central Office_Category*** and the value would be set to how you want the category re-written.
Name **Type** **Default Value** **Restart Required** **Description**	**ForwardEventLicense** String Value null ELM Server restart required Assigns a specific license type to Auto Add agents. Default is null. ex: 7521 = Network license
Name **Type** **Default Value** **Restart Required** **Description**	**FTPMonitorTakeActionAtEachInterval** REG_DWORD 0 ELM Server restart required This modifies the default behavior of the FTP Monitor. By creating this key and setting the value to 1, you can force the FTP Monitor to execute its configured Action(s) at each interval, regardless of state changes. <%REG_VIRTUAL_SERVICE%>
Name **Type** **Default Value** **Restart Required** **Description**	**LicenseEventInXml** REG_DWORD 0 No If set to 1, changes the event output for license changed (Event ID 5226), Agent added (Event ID 5229), and Agent deleted (Event ID 5230) to XML format for debugging purposes.
Name **Type** **Default Value** **Restart Required** **Description**	**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).
Name **Type** **Default Value** **Restart Required** **Description**	**MaxNumRecordsReadBeforeForceSend** REG_DWORD 1000 No This value is used for Event Monitors and Event Collectors. This is the maximum number of event log records that will be read in a single monitor item interval. <%REG_VIRTUAL_SERVICE%>
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**	**MaxSyslogMessageQueueSize** REG_DWORD 500000 No This key controls the number of TCP or UDP syslog messages the ELM Syslog Receiver will hold in memory. Limiting this queue will limit how much virtual memory (perfmon: process/private bytes) ELM will use. When the queue limit is reached, the queue is purged and informational event 5050 from EEMSVR is generated: SyslogMessageQueue reached max size, syslog message not accepted.
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**	**NumSyslogEventsDroppedBeforeLoggingEvent** REG_DWORD 10 ELM Server restart required This key controls the number of syslog messages that will be dropped before the ELM Server writes event log message 5050. It can be used to minimize the number of events the ELM Server writes if many syslog messages are dropped from the syslog message queue. Restarting the ELM Server or changing this registry entry will reset the internal counter. The first time a syslog message is dropped, an event 5050 is generated. After that, the counter starts.
Name **Type** **Default Value** **Restart Required** **Description**	**PortMonitorTakeActionAtEachInterval** REG_DWORD 0 ELM Server restart required This modifies the default behavior of the TCP Port Monitor. By creating this key and setting the value to 1, you can force the Port Monitor to execute its configured Action(s) at each interval, regardless of state changes. <%REG_VIRTUAL_SERVICE%>
Name **Type** **Default Value** **Restart Required** **Description**	**RealTimeEventViewUpdates** REG_DWORD 1 ELM Server restart required

	This value is set through the *Options* 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 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.
Name **Type** **Default Value** **Restart Required** **Description**	**ServerName** REG_SZ < NetBIOS Name of the ELM Server computer > 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.
Name **Type** **Default Value** **Restart Required** **Description**	**ShowServerMonitor** REG_DWORD 0 ELM Server restart required If set to 1, the ELM Server monitor item is displayed in the Console.
Name **Type** **Default Value** **Restart Required** **Description**	**SMTPEmailNotificationTimeOut** REG_DWORD 60 ELM Server restart required Specifies the number of seconds the ELM Server will wait for a SMTP Server to respond when using the SMTP e-mail Notification Method. The minimum timeout is set to 5 seconds. The maximum timeout value is specified by the **SMTPMaxTimeoutInSeconds** registry key.
Name **Type** **Default Value** **Restart Required** **Description**	**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 minimum timeout is set to 5 seconds. The maximum timeout value is 4,294,967,295 seconds.
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**	**SQLExpressMaxSizeR2** REG_DWORD 10140 No Specified in MB, any SQL Express 2008 R2 or SQL Express 2012 database of this size or larger will be rolled over to a new database. This number can be reduced to roll over the database earlier to avoid conflicts with SQL Express reaching its maximum size limit.
Name **Type** **Default Value** **Restart Required** **Description**	**SyslogMaxNumThreads** REG_DWORD 10 Yes The number of workers threads that processes the syslog queue. Set the value to number of worker threads.
Name **Type** **Default Value** **Restart Required** **Description**	**TrustedServers** REG_SZ <IP Address> No This value is set through the *Forwarded Events* 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.
Name **Type** **Default Value**	**UseShellExecuteForScripts** REG_DWORD 0

Restart Required	No
Description	This value will alter the method used by the **Run** Action in Monitor Items assigned to Virtual Agents and the **Command Script** Notification Method. Setting it to 1 will enable script execution on a remote system, but will disable environment variable expansion.
Name	**ValidateTablesOnCreation**
Type	REG_DWORD
Default Value	1
Restart Required	ELM Server restart required
Description	If set to 1, the SQL validation scripts will only be run at database creation, except for INTERNAL.PR_MaintainAllPartitions.sql.
Name	**ViewListSendAdvises**
Type	REG_String
Default Value	No Value
Restart Required	ELM Server restart required
Description	Semicolon delimited string of Event View names to receive real time ELM console updates.
Name	**WarnIfLessThanNumLicenses**
Type	REG_DWORD
Default Value	0
Restart Required	No
Description	Set the value that an event should be written if X is exceeded. So, if you have 20 licenses, and you set it to 5, after the 6th is taken it'll write an event out.
Name	**WebPageMonitorCaseInsensitive**
Type	REG_DWORD
Default Value	0
Restart Required	No
Description	Specifies whether the fetched web pages are treated as case-sensitive (0) or not (1). <%REG_VIRTUAL_SERVICE%>
Name	**WriteEventOnAgentAdd**
Type	REG_DWORD
Default Value	0
Restart Required	No
Description	If set to 1, if an Agent is added to the Server, an event will be written out.
Name	**WriteEventOnAgentDelete**
Type	REG_DWORD
Default Value	0
Restart Required	No
Description	If set to 1, if an Agent that is reporting to the Server is deleted, an event will be written out.

6.3.4 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**).

HKEY_LOCAL_MACHINE \ SOFTWARE \ TNT Software \ ELM Manager Agent \ 7.5.0 \ Settings
OR if 64bit Operating System
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TNT Software\ELM Manager Agent\7.5.0\Settings

Name	**AllowSecondsCorrelationTimeOut**
Type	REG_DWORD
Default Value	0
Restart Required	MMC Restart required.
Description	When set to a value of 1 this key allows the use of seconds in correlation views. Changing this value to allow seconds can result is false timouts and is generally not recommended..
Name	**CacheDataMaxSize**
Type	REG_DWORD
Default Value	104,857,600 (100MB)
Restart Required	Service Agent restart required
Description	This value is set through the Agent properties. Controls the maximum size of the ELM Agent cache file size.
Name	**CachePath**
Type	REG_SZ
Default Value	%systemroot%\TNTAgent
Restart Required	Service Agent restart required
Description	This value is set through the Agent properties. Controls the destination of the ELM Agent cache file on the local computer. Also see MinDiskFreeSpaceInMBToContinueCaching.

Name	**MinDiskFreeSpaceInMBToContinueCaching**
Type	REG_DWORD
Default Value	20 MB
Restart Required	Service Agent restart required
Description	Controls the minimum free space in MB before a ELM 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.
Name	**MonitorNumLoggingChars**
Type	REG_DWORD
Default Value	512
Restart Required	Service Agent restart required
Description	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.
Name	**ProcessCollectedEvtFiles**
Type	REG_DWORD
Default Value	1
Restart Required	Service Agent restart required
Description	This key stores the latest copy of evt(x) file in cache path for agent.
Name	**RemoteAgentInstall**
Type	REG_DWORD
Default Value	1
Restart Required	No
Description	Users should not change this registry entry. This value is set internally by ELM. This value indicates if the Service Agent was installed through the ELM Console (1) or using Windows Installer (0).
Name	**RestartHandleCountMax**
Type	REG_DWORD
Default Value	4000
Restart Required	Service Agent restart required
Description	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.
Name	**RestartThreadCountMax**
Type	REG_DWORD
Default Value	

Restart Required	400
Description	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.
Name	**RestartVirtualMemoryMaxMb**
Type	REG_DWORD
Default Value	400
Restart Required	Service Agent restart required
Description	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.
Name	**SMTPMaxTimeoutInSeconds**
Type	REG_DWORD
Default Value	300
Restart Required	Service Agent restart required
Description	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. 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. 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. <% REG_VIRTUAL_SERVICE%>
Name	**TCPAgentPort**
Type	REG_DWORD
Default Value	1253
Restart Required	Service Agent restart required
Description	This ADDS a listening port, which can be verified by using netstat. Changing TCPAgentPort to 1353 will result in both 1253 and 1353 to being listened to.
Name	**UseShellExecuteForScripts**
Type	REG_DWORD
Default Value	0

Restart Required	No
Description	This value will alter the method used by the **Run** Action in Monitor Items assigned to Service Agents. Setting it to 1 will enable script execution on a remote system, but will disable environment variable expansion.
Name	**WebPageMonitorCaseInsensitive**
Type	REG_DWORD
Default Value	0
Restart Required	Service Agent restart required
Description	Specifies whether the fetched web pages are treated as case-sensitive (0) or not (1). To use this with Virtual Agents this entry must be manually entered in the registry of the ELM Server computer. Applies to EEM only.

6.4 Command Line Switches

The tables in this section list command line options for the Server and ELM Service Agent.
ELM Server Command Line Options 175
ELM Agent Command Line Options 177

6.4.1 Silent Install

All the ELM 7.5.0 components can be installed silently by providing appropriate command line switches to the ELM .exe setup install package. All switches must be provided as a single line, and will typically wrap in a command prompt window.
Syntax Conventions 170
Silent Install 171

Syntax conventions are based on the style used in SQL Server Books Online.

Convention	Used for
UPPERCASE	Installer switch.
italic	User supplied values.
Monospaced	Values that must be typed exactly as shown.
Bold font	Default value used by the installer if the switch is omitted.
| (vertical bar)	Separates syntax items enclosed in brackets or braces. Use only one item in the list.
[ ] (brackets)	Optional syntax items. Do not type the brackets.
{ } (braces)	Required syntax items. Do not type the braces.
[,...n]	The preceding values can be repeated *n* number of times. MSI values are comma separated. Do not allow spaces around any

	commas.
[;...n]	The preceding values can be repeated *n* number of times. ELM values are semicolon separated. Do not allow spaces around any semicolons.

Syntax for all switches requires the switch name, an equals sign, and values enclosed in quotation marks.
For example: REMOVE="ELMServerFeature"

Switch	InstallMode
Values	**"{Install|Repair|Remove}"**
Description	The overall action to be performed by the ELM setup package.
Default	None. Required for all installs.
Switch	InstallFolder
Values	"*drive letter:path*"
Description	The drive and path to use for installing the ELM Server.
Default	**C:\Program Files\ELM Enterprise Manager** on 32-bit systems. **C:\Program Files\ELM Enterprise Manager (x86)** on 64-bit systems.
Switch	AddFeatures
Values	**"{[ELMServerFeature]|[ELMConsoleFeature] |[ELMDashboardFeature]|[ELMAdvisorFeature]|[ELMAgentFeature]}[,...n]"**
Description	Specify one or more features to install using a comma separated list.
Default	None.
Switch	RemoveFeatures
Values	**"{[ELMServerFeature]|[ELMConsoleFeature] |[ELMDashboardFeature]|[ELMAdvisorFeature]|[ELMAgentFeature]}[,...n]"**
Description	Specify one or more features to uninstall using a comma separated list.
Default	None.
Switch	ReinstallFeatures
Values	**"{[ELMServerFeature]|[ELMConsoleFeature] |[ELMDashboardFeature]|[ELMAdvisorFeature]|[ELMAgentFeature]}[,...n]"**
Description	Specify one or more features to Reinstall using a comma separated list.
Default	None.
Switch	AgentDefaultLicense
Values	**"{7510|7511|7512|7513|7514|7515|7516|7517}[;...n]"**
Description	Product licenses that will be assigned to a Service Agent. 7510 = System Class I 7511 = System Class II

	7512 = Log Class I 7513 = Log Class II 7516 = Event Class I 7517 = Event Class II 7518 = Core Class I 7519 = Core Class II 7521 = Network Class II
Default	7510. Switch required only if an Agent is installed.
Switch	SilentServer
Values	*"elm_server_name"*
Description	This is the ELM Server to which the Service Agent will report.
Default	None. Switch required if installing **ELMAgentFeature**.
Switch	ServerDefaultPort
Values	*"port_number"*
Description	Port number of the ELM Server the Service Agent will use.
Default	None. Switch required if installing **ELMAgentFeature**. ex: 1251
Switch	AgentDefaultPort
Values	*"port_number"*
Description	Listening port for the Service Agent.
Default	None. Switch required if installing **ELMAgentFeature**. ex: 1253
Switch	AgentDefaultCategories
Values	*"category_name[;...n]"*
Description	The Categories to which the Agent should be added. These must match existing ELM Server categories.
Default	None. New Agents are always added to the **All Agents** Category.
Switch	FailoverServer
Values	*"server[\named_instance]"*
Description	The instance name of the ELM failover database.
Default	(LocalDB)\TNT_Data. Switch required if installing **ELMServerFeature**.
Switch	FailoverDatabase
Values	*"database_name"*
Description	The name of the ELM failover database. Using only alpha, numeric, and underscore characters is recommended.
Default	ELM_Failover_00001. Switch required if installing **ELMServerFeature**.
Switch	FailoverSQLUser
Values	*"sql_username"*
Description	SQL username when SQL Authentication is used.
Default	None. Required if using **ELMServerFeature** and **FailoverWindowsAuthentication = 0**.

Switch	FailoverSQLPassword
Values	*"sql_password"*
Description	Password for SQL Authentication.
Default	None. Required if using **ELMServerFeature** and **FailoverWindowsAuthentication = 0**.
Switch	FailoverWindowsAuthentication
Values	**"{0|1}"**
Description	Use SQL or Windows authentication. 1 = Windows authentication. 0 = SQL authentication.
Default	None. Required if using **ELMServerFeature**.
Switch	PrimaryServer
Values	*"server[\named_instance]"*
Description	The instance name of the ELM primary database.
Default	(LocalDB)\TNT_Data. Switch required if installing **ELMServerFeature**.
Switch	PrimaryDatabase
Values	*"database_name"*
Description	The name of the ELM primary database. Using only alpha, numeric, and underscore characters is recommended.
Default	ELM_Primary_00001. Switch required if installing **ELMServerFeature**.
Switch	PrimarySQLUser
Values	*"sql_username"*
Description	SQL username when SQL Authentication is used.
Default	None. Required if using **ELMServerFeature** and **PrimaryWindowsAuthentication = 0**.
Switch	PrimarySQLPassword
Values	*"sql_password"*
Description	Password for SQL Authentication.
Default	None. Required if using **ELMServerFeature** and **PrimaryWindowsAuthentication = 0**.
Switch	PrimaryWindowsAuthentication
Values	**"{0|1}"**
Description	Use SQL or Windows authentication. 0 = Windows authentication. 1 = SQL authentication.
Default	**0**
Switch	DeleteDatabasesCheckbox
Values	**"{0|1}"**
Description	Delete all databases during uninstall.
Default	**0**
Switch	AdvisorCheckbox
Values	**"{0|1}"**
	Install or do not install the ELM Advisor. 1 = Installing ELMAdvisorFeature. 0 = Not installing ELMAdvisorFeature. Should be

Description	**1** if ADDLOCAL includes **ELMAdvisorFeature**. Otherwise, omitted.
Default	1. Required only when ADDLOCAL includes ELMAdvisorFeature.
Switch	AgentCheckbox
Values	"{0|1}"
Description	Install or do not install a Service Agent. 1 = Installing ELMAgentFeature. 0 = Not installing ELMAgentFeature. Should be **1** if ADDLOCAL includes **ELMAgentFeature**. Otherwise, **0**.
Default	1. Required for all installs.
Switch	ConsoleCheckbox
Values	"{0|1}"
Description	Install or do not install the ELM Console. 1 = Installing ELMConsoleFeature. 0 = Not installing ELMConsoleFeature. Should be **1** if ADDLOCAL includes **ELMConsoleFeature**. Otherwise, omitted.
Default	1. Required only when ADDLOCAL includes ELMConsoleFeature.
Switch	DashboardCheckbox
Values	"{0|1}"
Description	The overall action to be performed by the ELM setup package.
Default	1. Required for all installs.
Switch	ServerCheckbox
Values	"{0|1}"
Description	Install or do not install an ELM Server. 0 = Install ELMServerFeature. 1 = Do not install ELMServerFeature. Should be **1** if ADDLOCAL includes **ELMServerFeature**. Otherwise, **0**.
Default	1. Required for all installs.
Switch	EulaAcceptCheckbox
Values	"{0|1}"
Description	Accept End User agreement. 1=Accept
Default	0. Required for all installs.
Switch	TraceFile
Values	"*drive letter:path*"
Description	The drive and path to use for generating an install trace.
Default	**[TempFolder]TntTrace.txt**
Switch	ServiceUser
Values	*"domain\username"*
Description	The service account used by the ELM Server and ELM Report Scheduler services.
Default	None. Required only if using **ADDLOCAL = "ELMServerFeature" = 1**.
Switch	ServicePassword
Values	*"strong_password"*

Description	The password for the ServiceUser service account.
Default	None. Required only if using **ADDLOCAL = "ELMServerFeature" = 1**.

6.4.2 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.

Switch	Usage Examples	Description
/? /help	eemsvr.exe /help	Show the ELM Server command line help.
/GetTraceFiles	eemsvr.exe /GetTraceFiles /Host=Hostname /From=YYMMDD_HHmm /To=YYMMDD_HHmm	This can retrieve trace files from remote ELM server. Files are stored in a "Hostname Logs" in the ELm program directory.
/ImportEVT=*file* [/LogName=*logname*]	eemsvr.exe /importevt=dns_events.evt /logname="dns server" eemsvr.exe /importevt="c:\temp\file replication service.evt"	Imports events from an EVT file into the ELM Server database. The ELM Server must have the following for the computer providing the EVT file: • ELM Agent(s) for the computername(s) in the EVT file • RPC Connectivity to the computer • Read permissions to the registry on the computer • Read permissions to the file system on the computer • Remote Registry Service running on the computer Either file or logname must match the event log name as displayed in Windows Event Viewer. If file or logname is not specified correctly, then some of the events messages may be incomplete. At least 1 Event View must have a Date Range that encompasses all the desired historical events. Date Range is in the properties of an Event View. Recent events can trigger Notification Methods. See Disable...for Cached (old) data and CacheDataTrigger 160 for more details.

		Also note the default database pruning will delete older events.
/LoadXML[=file]	eemsvr.exe /loadxml	Import an XML file from an ELM 3.1 or later export. If *file* is not specified, the ELM server will use a filename based on the Server executable.
/RegServer /regservice /service	eemsvr.exe /regserver	Register the ELM Server as a COM server and as a Windows service.
/ReinstallAgents	eemsvr.exe /ReinstallAgents /Host=hostname /Port=1251	Tells a remote ELM server (Or local server if no host is is used) to reinstall agents. This can be useful after an update/upgrade is installed.
/SendBinaries	eemsvr.exe /SendBinaries=sendfiles.txt /Host=hostname	Upgrades/updates 7.5 to 7.5 or 7.0 ELM servers and can be used to send individual patched dll files. Hostname can be a text file. One line per hostname and use a comma to specify ELM server port.
/SendXML	eemsvr.exe /SendXML=xmlfilelist.txt /Host=hostname Optional: /70Type=NM,MI,MC,CV,SV,EV,CF,EF,IF /Port=1251 /ClearType=NM,MI,MC,CV,SV,EV,CF,EF,IF	Can send updated configuration files to 7.5 or 7.0 ELM servers. Filelist.txt should have one line per xml file listed using relative path to eemsvr.exe or full path to xml file. The xmlfilelist.txt can also be replaced with a path to an individual xml file. /70Type required for ELM 7.0. /ClearType will delete specified items before import.
/Restart	eemsvr.exe /restart	Restart the ELM Server service.
/SaveXML[=file]	eemsvr.exe /savexml	Saves all ELM Server configuration data to an XML file. If *file* is not specified, the ELM server will use a filename based on the Server executable.
/Start	eemsvr.exe /start	Start the ELM Server service.
/Stop	eemsvr.exe /stop	Stop the ELM Server service.
/UnRegServer /UnRegService	eemsvr.exe /unregserver	Remove the ELM Server service and unregister the ELM Server as a COM server.

6.4.3 TNT Agent Command Line Options

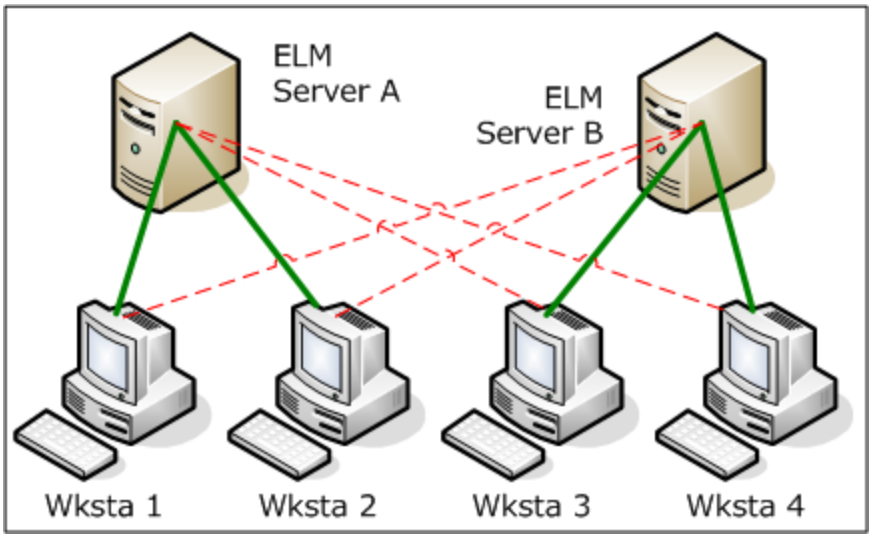
The table below lists command line switches that are recognized by ELM Agents. Some switches have equivalents, but only 1 switch needs to be used.

Switch	Usage Examples	Description
/?	`tntagent.exe /help`	Show the ELM Agent command line help.
/help		
/Install	`tntagent.exe /install`	Creates the ELM Agent service.
/Register	`tntagent.exe /register`	Displays the wizard dialog to connect the agent to an ELM Server.
/Remove	`tntagent.exe /remove`	Deletes theELM 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	`tntagent.exe /restart`	Stops and restarts the ELM Agent service
/Start	`tntagent.exe /start`	Starts the ELM Agent service
/Stop	`tntagent.exe /stop`	Stops the ELM Agent service.
/Trust="nnn.nnn.nnn.nnn"]	`tntagent.exe /trust="192.168.1.10"`	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.nnn"]	`tntagent.exe /trust="192.168.1.10"`	Removes the specified TCP/IP address from the list of trusted servers.

6.5 Home and Standby

ELM provides additional Fault Tolerance by providing the option to employ a Standby ELM Server which will accept data (Events, Performance Data) from Agents should the primary (now referred to as the Home) ELM Server become unavailable for an extended period of time.

The Standby server may be another active ELM Server on the network servicing its own group of Agents, or may be simply another server on the network with an idle instance of ELM running. In the active-active ELM Server scenario, each ELM Server may be configured as the Standby server for the other. However, each Agent can have only 1 Home ELM Server, and 1 Standby ELM Server. This is illustrated below: ELM Server A is the Home Server for Workstations 1 and 2, plus it is the Standby Server for Workstations 3 and 4. ELM Server B is the Home Server for Workstations 3 and 4, and the Standby Server for Workstations 1 and 2.



Active-Active ELM Servers

Only ELM Service Agents can be configured to Switchover and Switchback to the ELM Standby Server. Virtual Agents and IP Virtual Agents cannot be configured for use with this feature.

The ELM Standby Server must have sufficient unallocated licenses available to accommodate the Agents it receives during Switchover from the ELM Home Server. Note that these licenses are allocated on a first-come, first-served basis. Any Agents that attempt to Switchover without an unallocated license will fail to Switchover and will remain in staged Mode.

All Agents should be deployed from their Home ELM Server. To configure Agents with Home/Standby properties, the following keys must be edited in the appSettings.xml file, found in the ELM installation directory on the Home ELM Server:

1. StandbyELMServerName
2. StandbyELMServerIPAddresses
3. StandbyELMServerPort
4. StandbyELMServerIndex - This can be found on the Standby ELM Server, in the following registry key:
   HKLM\SOFTWARE\TNT Software\ELM Enterprise Manager\7.5.0\Settings::Console Item Index
5. StandbyELMServerLicenseKey - This can be found on the Activation 138 tab of the Standby ELM Server.
6. StandbyELMServerAgentCategoryName - All agents switching over to the standby server will be assigned to this category. This appSettings key is optional on the Standby Server, and the home server ignores this key. The category will be created by the standby ELM server when Agents switchover. If not present, Agents in Standby mode will appear only in the **All Agents** container in the Standby ELM Server Console.
7. HomeELMServerAgentCategoryName - This Category will be created by the ELM Home Server when it is restarted, and all agents assigned to this Category will have Home and Standby properties.
8. HomeELMServerCacheDurationInMinutes - See Switchover 179 for more details.
9. HomeELMServerRetryIntervalInMinutes - See Switchback 179 for more details.

The following sample appSettings.xml entries can be found near the bottom of the file. In a default ELM install, the keys are commented-out. The Home Server keys in the example below are commented-in to facilitate copy/paste.

```
<!--        ELM Home/Standby server keys
                The below keys must all be set in the Home Server's appSettings file
                to enable the Home/Standby feature. Search for 'Standby' in the Help
                file for more information.
-->
        <add key="StandbyELMServerName"      value="NetBIOS Name of Standby Server" />
        <add key="StandbyELMServerIPAddresses" value="000.000.000.000" />
        <add key="StandbyELMServerPort"      value="1251" />
        <add key="StandbyELMServerIndex" value="{00000000-0000-0000-0000-000000000000}" />
        <add key="StandbyELMServerLicenseKey" value="{00000000-0000-0000-0000-
000000000000}" />
        <add key="HomeELMServerAgentCategoryName" value="This Category will be created, and
agents put in it will have the      Home/Standby behavior" />
        <add key="HomeELMServerCacheDurationInMinutes" value="1" />
        <add key="HomeELMServerRetryIntervalInMinutes" value="1" />


        <!-- optional for the standby server appSettings file -->
        <!-- add key="StandbyELMServerAgentCategoryName"  value="If this category exists, agents
switching to the standby on this server will exist in this category" / -->
```

All Agents desired to Switchover to the Standby server must be placed in the Category defined in the "HomeELMServerAgentCategoryName" appSettings.xml key. After restarting the Home ELM Server, this Category will be created and visible in the ELM Console.

Tip

*After editing **appSettings.xml**, open it using Internet Explorer to verify there are no xml formatting errors.*

Both ELM Server services must be restarted to activate changes to appSettings.xml.

Switchover

The ELM Service Agent caches for HomeELMServerCacheDuration (this value could be zero). This timer is started when a cache file is created. If this duration has been exceeded before adding data to the cache file, the Agent will attempt to open a socket connection to the Standby server. If it fails to open a connection it will continue to cache as normal. If the socket connection succeeds and it can get a license, then the agent informs the Standby server that it is switching over (which may involve sending some configuration information). The Agent then sets its server properties to point to the Standby server and begins sending the cache to the Standby server. Sending configuration to the Standby ELM Server requires that the Agent know the Standby ELM Server's Index, and does not depend on the AutoAdd flag on the Standby server. A 5318 150 event is written to the Agent's Application event log.

Switchback

Each time at least HomeELMServerRetryIntervalInMinutes has elapsed and there is data to send or an Agent Heartbeat occurs, the agent tries to connect to the Home ELM Server. This

timer is started when the Agent successfully switches over to the Standby Server. If the HomeELMServerRetryIntervalInMinutes is set to zero, Agents will wait for the Home server to initiate switchback. Switchback can be initiated by running **Update Agent Configuration** for one or more Agents. When switching back to the Home server, the Agent must first tell the Standby server that it has re-established communication with its Home server (this causes the Agent to release its license on the Standby Server and be marked as staged). A 5317 event is written to the Agent's Application event log.

Blackout condition

If an ELM Service Agent is unable to contact either the Home or the Standby server, it enters Blackout mode. It will go into cache mode, and begin caching data for the currently configured server (Home or Standby).

Deleting an ELM Standby Agent

Before deleting an Agent configured for Home/Standby operation, make sure the following criteria are met:

- The Agent is reporting to the Home Server.
- The Agent is deleted from the Home Server Console or from **Add or Remove Programs** on the Agent computer.

Deleting an Agent when in Standby mode, or from the Standby Server will leave Agent components behind.

This page is intentionally left blank.
Remove this text from the manual
template if you want it completely blank.

- A -

Agent Monitor 41
Agent Types 39
Anonymous Connections 53
Application and Server Status Monitoring 40
Application monitoring 40
Archive 24
Archiving 24
ASCII files 51
Authenticated Connections 53

- C -

Categories 96
CMD 112
Command Script 112
Compressed 47
Copyright Notice 8
Correlation Views 130
Counter 57, 58
CPU Usage 61
create new report 30
Cross Platform Monitoring 40

- D -

Data Collector and Real-Time Monitors 40
Display Diagnostics 94
Display Processes 94

- E -

ELM Advisor 117
Engine ID 24
Event File Collector 47
Event View Settings 118, 121, 125, 131
Event Views 118
Evt files 47
Evtx files 47
Exclude Filters 45

- F -

File Monitor 51
Forward Events 113
Forwarded Events 24
FTP Monitor 53
FTP site 53

- H -

HTTP 79
HTTPS 79

- I -

ICMP Echo Requests 59
IIS Logs 51
Include Filters 45
Installed Applications 55
Internet Service Monitoring 40
Inventory Collector 55
IP Virtual Agents 83

- L -

Legal Notice 8

- M -

Mail 117
Maintenance Categories 97
MD5 Hash 47
MIB Browser 66
Monitor Items 38, 40, 96
Monitoring Categories 96
Monitoring Products 39

- N -

New Process 61
Notification Methods 111, 118
Number of Processes 61

- O -

Object 57, 58
OID Values 66, 69, 114
Operating Systems 55

- P -

Packet Size 59
Performance Collectors 58
Performance Counter 57, 58
Performance Monitor 57
Ping Monitor 59
Ports 24
Process Ended 61
Process Monitor 61

- Q -

Quality of Service 41, 59, 65, 78, 79
Queries Database 71

- R -

Retention 24
RFC 1157 66

- S -

Scheduled hours 40, 111
Scheduled Interval 40, 111
Server Activation 138
Service Agents 39, 41, 83, 94, 96
Service Monitor 63
Service Paused 63
Service Started 63
Service Stopped 63
Simple Network Management Protocol 66
SMTP 117
SMTP Gateways 65
SMTP Hosts 65
SMTP Monitors 65
SMTP Services 65
SNMP 66
SNMP Collector 69
SNMP Trap 114
SNMP Traps 71
Socket 41, 63, 78
SQL Logs 51
SQL Monitors 71
String Matching 51
Syslog 75, 115

- T -

TCP Port 41, 78
TCP Port Monitor 78
Text Files 51
Thresholds 61, 111

- U -

Uncompressed 47

- V -

Virtual Agents 39, 83

- W -

WBEM 81
Web Page Monitor 79
Web-Based Enterprise Management 81
Windows Management Instrumentation 81
Windows Processes 61
WMI 81