

# **24x7 Event Server™ 2.0**

## **User's Guide**

## Table of Contents

|   |           |
|---|-----------|
| <b>ABOUT THIS GUIDE</b> .....                           | <b>5</b>  |
| CONVENTIONS USED IN THIS DOCUMENT.....                  | 5         |
| ABBREVIATIONS AND TERMS.....                            | 5         |
| TRADEMARKS .....  | 6         |
| <b>CHAPTER 1: GETTING STARTED</b> .....                 | <b>7</b>  |
| OVERVIEW.....   | 7         |
| SYSTEM REQUIREMENTS .....                               | 7         |
| NT SECURITY-RELATED ISSUES .....                        | 7         |
| REGIONAL AND LANGUAGE SPECIFIC ISSUES.....              | 8         |
| PRODUCT CONFIGURATION.....                              | 8         |
| ADMINISTRATIVE ALERTS .....                             | 8         |
| <b>CHAPTER 2: INSTALLATION AND UNINSTALLATION</b> ..... | <b>9</b>  |
| INSTALLATION .....                                      | 9         |
| AUTOMATING THE INSTALLATION PROCESS; SILENT SETUP ..... | 10        |
| UNINSTALLATION.....                                     | 11        |
| <b>CHAPTER 3: EVENT SERVER MANAGEMENT CONSOLE</b> ..... | <b>12</b> |
| OVERVIEW.....   | 12        |
| EVENT WIZARD.....                                       | 13        |
| WORKING WITH EVENTS.....                                | 13        |
| ADDING/REMOVING EVENT MANAGEMENT PACKS.....             | 14        |
| MANAGING EVENT SERVER STATE .....                       | 15        |
| CONFIGURING CENTRALIZED EVENT LOGGING.....              | 15        |
| Step 1 – Selecting Database System .....                | 16        |
| Step 2 – Configuring Database Connection.....           | 17        |
| Step 3 – Creating Event Log Tables .....                | 17        |
| Scheduling Periodic Purge of Event Log Tables.....      | 18        |
| CONFIGURING SYSTEM OPTIONS .....                        | 19        |
| RUNNING EVENT TRACKING AND ANALYSIS REPORTS .....       | 19        |
| Built-in Reports .....                                  | 19        |
| Overview .....  | 19        |
| Event Summary .....                                     | 20        |
| Event Detail.....                                       | 20        |
| Top 10 Events.....                                      | 21        |
| Event Trends (All Events) .....                         | 21        |
| Event Trends (Top 10 Events) .....                      | 21        |
| Event Trends (Selected Events) .....                    | 22        |
| Warnings and Errors in System Event Logs.....           | 22        |
| Warnings and Errors in Application Event Logs.....      | 23        |
| Security Failure Audit.....                             | 23        |
| Application and Service Failures.....                   | 24        |
| System Performance Issues .....                         | 25        |
| Database Performance Issues.....                        | 26        |
| Database Downtime.....                                  | 27        |
| Web and Network Services Downtime.....                  | 27        |
| Computer Downtime .....                                 | 28        |
| User-defined Reports.....                               | 29        |
| Overview .....  | 29        |
| Event Log Tables and Event Data .....                   | 29        |
| Microsoft Access Example .....                          | 36        |
| Microsoft Excel Example.....                            | 43        |

|   |           |
|---|-----------|
| <b>CHAPTER 4: EVENT MONITORS AND FILTERS.....</b>   | <b>49</b> |
| EVENT MONITOR METHODS.....                          | 49        |
| EVENT MONITOR TYPES.....                            | 49        |
| EVENT FILTERS.....                                  | 52        |
| EVENT MONITOR SCHEDULES.....                        | 53        |
| REAL-TIME EVENTS.....                               | 54        |
| Process start.....                                  | 54        |
| Process termination.....                            | 54        |
| Dial-up connection start.....                       | 54        |
| Dial-up connection termination.....                 | 55        |
| New SNMP trap.....                                  | 55        |
| New SysLog record.....                              | 56        |
| System shutdown.....                                | 58        |
| 24x7es.....   | 58        |
| POLLED EVENTS.....                                  | 60        |
| Windows appearance.....                             | 60        |
| Windows disappearance.....                          | 61        |
| Screen saver activation.....                        | 62        |
| Screen saver deactivation.....                      | 62        |
| Service start.....                                  | 62        |
| Service stop.....                                   | 62        |
| Process hung.....                                   | 63        |
| Process crash.....                                  | 63        |
| Dr. Watson error.....                               | 63        |
| New NT Event Log record.....                        | 65        |
| New text log file record.....                       | 66        |
| Server downtime.....                                | 67        |
| TCP service downtime (FTP, HTTP, SMTP, etc...)..... | 67        |
| Web server slow response.....                       | 68        |
| New file.....                                       | 69        |
| File deletion.....                                  | 69        |
| File change (size or time).....                     | 70        |
| Folder changes (generic event).....                 | 70        |
| File size threshold.....                            | 71        |
| NT Event Log size threshold.....                    | 71        |
| New e-mail message.....                             | 72        |
| New fax received.....                               | 74        |
| New fax sent.....                                   | 75        |
| User logon.....                                     | 76        |
| User logoff.....                                    | 76        |
| Database downtime.....                              | 77        |
| Database startup.....                               | 77        |
| Database data change.....                           | 78        |
| Database performance threshold.....                 | 78        |
| System performance threshold.....                   | 80        |
| Disk free space threshold.....                      | 83        |
| Registry change.....                                | 83        |
| WMI event.....                                      | 84        |
| USER-DEFINED EVENTS.....                            | 87        |
| <b>CHAPTER 5: EVENT ACTIONS.....</b>                | <b>89</b> |
| AUTOMATING EVENT RESPONSES.....                     | 89        |
| ACTION PROPERTIES AND PARAMETERS.....               | 90        |
| Event-specific Parameters.....                      | 91        |
| System Parameters.....                              | 91        |
| Special Symbols.....                                | 92        |
| SUPPORTED ACTIONS.....                              | 92        |
| Write to text log file.....                         | 92        |
| Write to Windows Event Log.....                     | 92        |

|   |            |
|---|------------|
| Display non-blocking GUI window .....   | 93         |
| Send e-mail .....   | 93         |
| Send SNMP trap.....   | 94         |
| Run Program .....   | 94         |
| Run 24x7 Scheduler job .....  | 95         |
| Restart system.....   | 95         |
| <b>CHAPTER 6: OPTIONAL EVENT MANAGEMENT PACKS.....</b>                                    | <b>96</b>  |
| <b>CHAPTER 7: EXAMPLES .....</b>  | <b>97</b>  |
| OVERVIEW.....   | 97         |
| EXAMPLE 1 – "NEW FILE" MONITORING AND AUTOMATION.....                                     | 97         |
| EXAMPLE 2 – WINDOWS NT EVENT LOG MONITORING AND CONVERTING ERROR MESSAGES TO SNMP TRAPS.. | 100        |
| EXAMPLE 3 – SYSLOG MONITORING AND CONVERTING ALERT MESSAGES TO SNMP TRAPS .....           | 103        |
| EXAMPLE 4 – DATABASE DATA CHANGE MONITORING AND NOTIFICATION.....                         | 106        |
| EXAMPLE 5 – HUNG APPLICATION MONITORING AND RESTARTING .....                              | 109        |
| EXAMPLE 6 – LOW DISK SPACE MONITORING AND ALERTING.....                                   | 112        |
| EXAMPLE 7 – TEXT LOG FILE MONITORING AND ALERTING.....                                    | 115        |
| EXAMPLE 8 – INCOMING EMAIL MONITORING AND LOADING EMAIL ATTACHMENTS INTO A DATABASE ..... | 118        |
| <b>APPENDIX 1: TECHNICAL SUPPORT.....</b>   | <b>122</b> |
| <b>APPENDIX 2: LICENSING .....</b>  | <b>123</b> |

## About This Guide

This user's guide describes features of the 24x7 Event Server. Information in this manual applies to the 24x7 Event Server v2.0.1.16 running on all supported systems. This manual contains information for both beginning and experienced users of the 24x7 Event Server. Both the print and the on-line documentation assume that you have a working knowledge of standard mouse and keyboard actions and understand basic computer processing concepts. This manual is provided so that the reader can understand how 24x7 Event Server functions. It also contains information on the following topics:

- Installation and configuration instructions
- Supported event monitors and their parameters
- Supported event response actions and their parameters
- Task-oriented guidelines to all interactive 24x7 Event Server functionality
- Descriptions of optional Event Management Packs

## Conventions Used in This Document

This section describes the style conventions used in this document.

### *Italic*

An *italic* font is used for filenames, URLs, emphasized text, and the first usage of technical terms.

### Monospace

A monospaced font is used for code fragments and data elements.

### **Bold**

A **bold** font is used for important messages, names of options, names of controls and menu items, and keys.

### User Input

Keys are rendered in **bold** to stand out from other text. Key combinations that are meant to be typed simultaneously are rendered with "+" sign between the keys, such as:

#### **Ctrl+F**

Keys that are meant to be typed in sequence will be separated with commas, for example:

#### **Alt+S, H**

This would mean that the user is expected to type the Alt and S keys simultaneously and then to type the H key.

### Graphical marks



- This mark is used to indicate product specific options and issues and to mark useful tips.



- This mark is used to indicate important notes.

## Abbreviations and Terms

This guide uses common abbreviations for many widely used technical terms including ASP, JSP, HTTP, and other.

## Trademarks

24x7 Automation Suite, 24x7 Event Server, 24x7 Scheduler, DB Audit, DB Audit Expert, DB Mail for Oracle, DB Tools for Oracle are trademarks of SoftTree Technologies, Inc.

Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP are registered trademarks of Microsoft Corporation. UNIX is registered trademark of the X/Open Consortium. Sun, SunOS, Solaris, SPARC are trademarks or registered trademarks of Sun Microsystems, Inc. HP-UX is a trademark of Hewlett-Packard Co. IRIX is a trademark of Silicon Graphics, Inc. AIX is a trademark of International Business Machines, Inc. Microsoft SQL Server is a registered trademark of Microsoft Corporation. Oracle is a registered trademark of Oracle Corporation. IBM, DB2, UDB are registered trademarks of International Business Machines Corporation

All other trademarks appearing in this document are trademarks of their respective owners. All rights reserved.

## CHAPTER 1: Getting Started

### Overview

24x7 Event Server is designed for system and application events monitoring and automated processing. The term “monitoring” means here detecting occurrence of a particular event (such as CPU usage reaching pre-defined threshold level, appearance of a specific GUI window, startup of a new RAS connection, and so on). The term “processing” means here automatically performing of a single action or multiple actions in response to an event occurrence (such as writing to a log file, sending an alert, starting of a batch process and so on).

24x7 Event Server can be also configured to log all detected events and performed actions to a centralized database which allows you to monitor and control multiple computers and the entire network from a single location as well as to add another global set of customized event filters and monitors for analyzing network conditions and overall usage. You can also run pre-built or create your own detailed reports on all detected events, system event logs, system and application performance, services, user activity and a lot more.

24x7 Event Server provides straight-forward wizard-driven user interface which is easy to use and quick to learn. No special training is required.

The following are some common applications for the 4x7 Event Server:

- Network Administration
- Help Desk Support
- Application Support
- Backup Monitoring
- Security Monitoring and Auditing

### System requirements

Currently supported operating systems:

- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows 2003

### NT security-related issues

24x7 Event Server is designed to operate as Windows NT service running under the Local System security account in a non-interactive mode. This gives the program access to all required system resources.

Also, all event actions are executed in the same security context as the program is running in, i.e. in the context of the Local System account.

## Regional and language specific issues

As the program operates under Local System account, all regional and language –specific issues are handled in accordance with the system-wide settings of the hosting computer.

## Product configuration

24x7 Event Server reads configuration data on the start up from an externally provided configuration file. In this file you can specify any set of events you want to monitor and actions to be performed in response to each event.

Configuration file has the standard Windows INI-file format. Each section begins with [<Section Name>] line and each element is defined by a line in the format: <Name>=<Value>. Complex elements may contain multiple simple elements separated with semicolons.

Sections describing events must have their names in [event <Event ID>] format. The file can have at most one [Globals] section and any number of [event <Event ID>] sections. The [Globals] section defines general settings and must be the first section in the configuration file.

All settings in the configuration file are case-sensitive.

You can use 24x7 Event Server Management Console to edit the configuration file. Do not modify this file directly unless you are instructed to do so by SoftTree Technologies technical support.

## Administrative Alerts

The 24x7 Event Server tracks its internal state during the execution and reports detected events to the Windows NT Application Event Log. These events are called Administrative Events. Among them are both informative events and events about issues that can affect the 24x7 Event Server processing. For more information see [CHAPTER 4, Real-Time Events topic, 24x7es Event Type](#) description.

In addition to default logging administrative events to the Windows NT Application Event Log based logging, administrative alerts can be emailed to system administrators.

The administrative email alerts can be enabled and configured in the system options. To open system Options dialog use **Event Server / Options** menu available in the 24x7 Event Server Management Console. Use "Error Handling Options" and "SMTP Email Server Options" sections within the Options dialog.



### Important Note:

**You must restart 24x7 Event Server in order for the changes in the system Options to take effect.**

The other way to define actions for Administrative Events is a regular real-time event with the type "24x7es". See [24x7es](#) topic In CHAPTER 4 for details including list of properties available for Administrative Events.



## CHAPTER 2: Installation and Uninstallation

### Installation

The 24x7 Event Server setup program provides intuitive and simple installation method. Simply run the setup program and follow prompts displayed on the screen.



#### Important Notes:

- Before installing the 24x7 Event Server, make sure that you are logged-on using an account that is a member of the local Administrators group.
- A computer restart is required after the installation in case if you are going to monitor process start/termination events and/or SNMP messaging.
- The 24x7 Event Server service can be configured to start automatically whenever the computer is started and it can run continuously in the background, regardless of whether a user is logged on or not.
- Programs and batch scripts run by the 24x7 Event Server inherit the security attributes of the 24x7 service. This gives them the same security permissions as the operating system.
- In order to create event monitors for various database-related events you must have ODBC interface installed on the system as well as appropriate ODBC database drivers. Contact your database vendor to obtain such drivers. To configure the data sources use the standard Windows ODBC Administrator program that can be found in the Control Panel's Administrative Tools.
- You can reconfigure the 24x7 schedule service to a certain extent using the Control Panel services applet. Before you make any changes, make sure you understand the Windows NT service concepts. You should refer to the following Microsoft knowledge base articles for more information:

Q124184 - Service Running as System Account Fails Accessing Network.

Q132679 - Local System Account and Null Sessions in Windows NT.

Q152451 - Applications Run from the Schedule Service Fail to Print.

- If you are planning to use WMI events on Windows NT4 computer the following steps must be performed before installing 24x7 Event Server:
  1. Install "MSSCE". This is a prerequisite for WMI on NT4 and can be obtained here <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/SCM/SCESP4I.EXE>
  2. Run SCESP4I.EXE to unpack the first level of the package to your hard drive. Then manually unpack the cab file to the same directory using pkunzip, WinZip or similar zip/unzip utility. When this is done, launch the unpacked copy of mssce.exe to begin the installation.

Download and install the WMI core. This can be obtained from the following address here <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=AFE41F46-E213-4CBF-9C5B-FBF236E0E875>
  3. Restart your computer as and when requested by the installers.



#### Tip: To install 24x7 Event Server on a Windows Server through Terminal Services:

- 1 Set up a Windows 2000/XP/2003 Server computer as a Terminal Services Host and configure it to allow both administrator and non-administrator access.

- 2 Run the installation program on this machine logged on as an Administrator. The 24x7 Event Server should be installed in Terminal Services' Install mode. Use the command line "change user /install" or use Add/Remove Programs in the Control Panel. This is required so that Terminal Services can appropriately manage the registry for each user.



**Tip: In order to make behavior of 24x7 Event Server and accompanying products installed on Windows Terminal Server consistent with other installations**, the 24x7 Event Server creates HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Compatibility\Applications\24X7ES value, which consists of the following flags:

- Windows 32-bit application: 0x00000008
- Disable registry mapping for application: 0x00000100
- Do not substitute user Windows folder: 0x00000400

## Automating the Installation Process; Silent Setup

If you plan to install the 24x7 Event Server using the same installation settings on a large number of computers, you can record the installation process on one computer and then play it back on the others. This allows you to run the Setup program on the other computers automatically, without user input ("silent" installation). A silent installation does not prompt the user for input.

The Setup program accepts optional command line parameters. These can be useful to system administrators, and to other programs calling the Setup program.

### **/SILENT, /VERYSILENT**

Instructs Setup to be silent or very silent. When Setup is silent the wizard and the background window are not displayed but the installation progress window is. When a setup is very silent this installation progress window is not displayed. Everything else is normal so for example error messages during installation are displayed and the startup prompt is

If a restart is necessary and the '/NORESTART' command isn't used (see below) and Setup is silent, it will display a Reboot now? message box. If it's very silent it will reboot without asking.

### **/NORESTART**

Instructs Setup not to reboot even if it's necessary.

### **/LOADINF="filename"**

Instructs Setup to load the settings from the specified file after having checked the command line. This file can be prepared using the '/SAVEINF=' command as explained below.

Don't forget to use quotes if the filename contains spaces.

### **/SAVEINF="filename"**

Instructs Setup to save installation settings to the specified file. Don't forget to use quotes if the filename contains spaces.

### **/DIR="x:\dirname"**

Overrides the default folder name displayed on the Select Destination Folder wizard page. A fully qualified pathname must be specified.

### **/GROUP="folder name"**

Overrides the default folder name displayed on the Select Start Menu Folder wizard page.

### **/NOICONS**

Instructs Setup not to create icons and shortcuts in the Windows Programs Start menu.

### **/NOGUI**

Instructs Setup not to install 24x7 Event Server Management Console.

### **/NOSNMP**

Instructs Setup not to install and register SNMP Extension Agent

### **/NOHELP**

Instructs Setup not to install 24x7 Event Server Documentation.

### **/COMPONENTS="comma separated list of component names"**

Overrides the default components settings. Using this command line parameter causes Setup to automatically select a custom type.

### **/SERVICE <account> <password>**

Instructs Setup to automatically install 24x7 Event Server service under the specified account. By default the service is installed under **LocalSystem** account. To install the service under another account specify the full service account name including domain for user authentication and password. To authenticate user on the local computer specify dot. For example: 247es\_setup.exe /service .\Administrator adminpass.

If account name or password includes spaces enclose it in double quotes. The **/service** option can be used along with other setup options, however it must be specified as the last option following by the account and password.



**Tip:** If you are installing 24x7 Event Server on multiple computers, you may want to copy the same configuration information to all of them.

#### **To copy configuration information:**

- 1 Install the 24x7 Event Server on the first computer, recording the installation as described above.
- 2 Configure the 24x7 Event Server using the **File/Options** menu.
- 3 Configure events to monitor and actions to perform in response to these events
- 4 Copy 24X7ES.INI file from the first computer to other computers

## Uninstallation

The 24x7 Event Server supports standard uninstallation mechanism for removing program files from the computer.

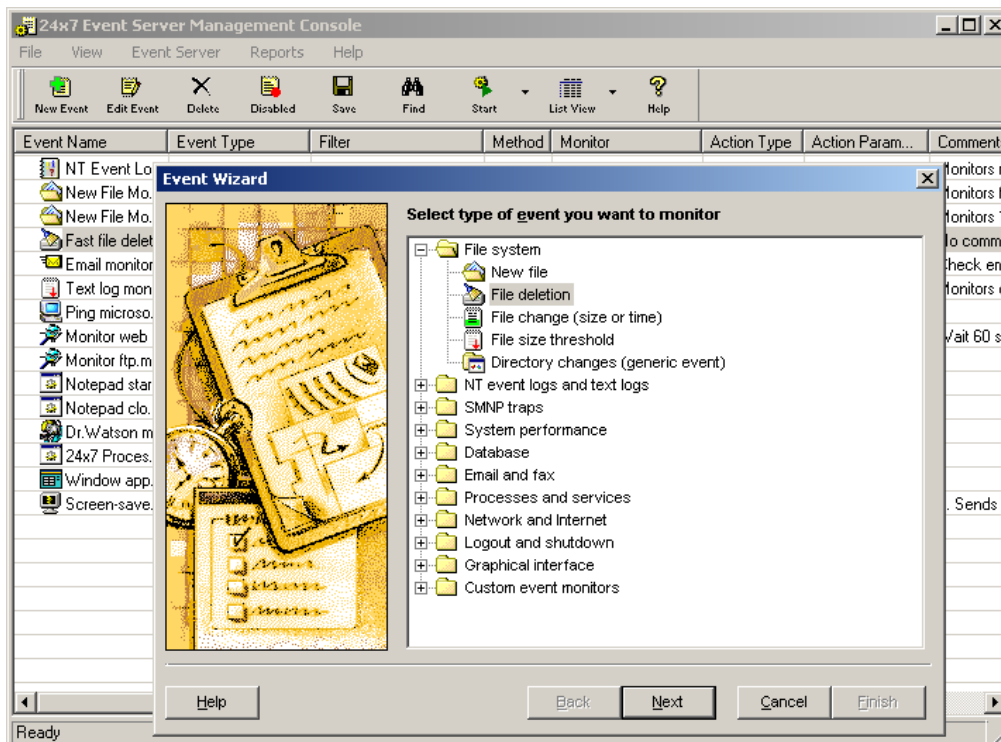
To uninstall the 24x7 Event Server:

- 1 Click Windows **Start** button, from the Start Menu select **Settings**, then **Control Panel**.
- 2 Double-click **Add/Remove Programs**.
- 3 Select the **24x7 Event Server** item in the programs list, click the **Add/Remove** button.

## CHAPTER 3: Event Server Management Console

### Overview

The 24x7 Event Server Management Console can be started from the Windows Start menu. On startup the Management Console reads 24x7 Event Server configuration file and displays configured events in a graphical user-friendly format. Below is a sample screenshot of the Management Console.



The configured events can be displayed in several different formats. Use the **View** menu commands to customize the display. The following formats are supported:

**List View** - Displays event items a list including detailed information event definitions.

**Large Icons** - Displays event items by using large icons.

**Small Icons** - Displays event items by using small icons.

**Tree** - Displays event items by using Explorer style small folders and icons.

The Management Console also provides access to event tracking and analysis reports and also to the event monitoring and processing engine.

Use the **Event Server** menu to control state of the event monitoring and processing engine.

Use the **Reports** menu to run event tracking and analysis reports.

Use the **File/Options** menu to configure global options.

For detailed information on supported reports and options and how to use them see [CHAPTER 3, Event Tracking and Analysis Report](#) topic.

## Event Wizard

The Event Wizard is the tool you use to create new event monitors and modify properties of existing event monitors. The Event Wizard consists of a series of dialog windows. The Event Wizard asks you questions and then, using your answers, updates the event properties. The Event Wizard uses different event properties for the different event types. The Event Wizard shows only properties appropriate for the event type you have selected.

You can change event properties, including event type, at any time. Use the **Next** and **Back** buttons displayed at the bottom of the Event Wizard window to move between the property pages. To cancel changes, click the **Cancel** button at any time. Alternatively, you can use the following keyboard shortcuts:

- **Next** - ALT+N or CTRL+TAB
- **Back** - ALT+B or SHIFT+CTRL+TAB
- **Finish** - ALT+F
- **Cancel** - Escape or ALT+C

To navigate between individual properties you can use your mouse or use TAB or SHFIFT+TAB keyboard shortcuts.

For more information on available properties and how to create and modify events see the following:

- [CHAPTER 3, Working With Events](#) topic
- [CHAPTER 4, Event Monitors and Filters](#)
- [CHAPTER 5, Event Actions](#)

## Working With Events

### To add a new event

1. Click the **File/New Event** menu item or press CTRL+N keyboard shortcut. The Event Wizard will appear.
2. Select event type in the event tree and click the Next button.
3. Fill in event filter parameters and click the Next button.
4. If the selected event type is a real-time event, click the Next button again, otherwise customize event monitor schedule parameters and click the Next button.
5. Select desired event response actions and complete their parameters.
6. Enter event name and optional description and then click the Next button.
7. Review event definition and it looks correct Click the **Finish** button otherwise click the Back button and make the necessary changes. Repeat steps 2 to 7 as needed.



**Tip:** To save the created event permanently in the 24x7 Event Server configuration file click the **File/Save** menu item or press CTRL+S keyboard shortcut.

### To delete an event

1. Select the desired event in the event list (or tree)
2. Click the **File/Delete Event** menu or press CTRL+D keyboard shortcut.



**Tip:** To save your changes permanently in the 24x7 Event Server configuration file click the **File/Save** menu item or press CTRL+S keyboard shortcut.


### To disable or enable a previously disabled event

1. Select the desired event in the event list (or tree).
2. Click the **File/Disable/Enable Event** menu item or press F8 keyboard shortcut to toggle event Disabled/Enabled state.

 **Tip:** To save your changes permanently in the 24x7 Event Server configuration file click the **File/Save** menu item or press CTRL+S keyboard shortcut.

#### To modify properties of an existing event

1. Double-click the desired event in the event list (or tree) or alternatively select the event and then click the **File/Edit Event** menu item or press CTRL+E keyboard shortcut. The Event Wizard will appear.
2. If the event type is correct click the Next button to advance to the Event filter properties, otherwise select a different event type and click the Next button.
3. If necessary modify event filter parameters and then click the Next button.
4. If the selected event type is a real-time event, click the Next button again, otherwise necessary modify event monitor schedule parameters and click the Next button.
5. If necessary modify event response actions and their parameters.
6. If necessary modify event name and optional description and then click the Next button.
7. Review event definition and it looks correct Click the **Finish** button otherwise click the Back button and make the necessary changes. Repeat steps 2 to 7 as needed.

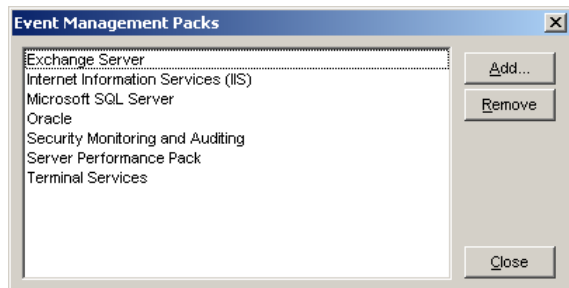
 **Tip:** To save your changes permanently in the 24x7 Event Server configuration file click the **File/Save** menu item or press CTRL+S keyboard shortcut.

#### To find an event in the event list

1. Click the **File/Find Event** menu item or press CTRL+F keyboard shortcut. The Search Options dialog will appear.
2. Enter the string you want to find and choose which event properties you want to search.
3. Check Case-sensitive option to find only events whose properties have the capitalization used in the Find Text box.
4. Click the Find Next button. The next found event is automatically highlighted. Click the Find Next button again to find next other events whose properties contain the search string. Please note that the search continues at the beginning of the event list when the end of the list is reached.
5. Click the Close button on the Search Options dialog to close that dialog.

## Adding/Removing Event Management Packs

Event Management Packs contain pre-built event monitors and processing rules that can react to events, thresholds and alerts monitored by 24x7 Event Server. Event Management Packs are targeted to monitor specific applications and also give IT staff expert advice on how to handle specific problems by automatically responding to common application problems.



#### To add a new or delete previously added Event Management Pack

1. Click the **File/Event Management Packs** menu item. The Event Management Packs dialog will appear.

2. To remove (uninstall) previously installed Event Management Pack, select the desired Management Pack name from the list and then click the Remove button. This will delete all events from the configuration file belonging to the selected pack.
3. To add a new Event Management Pack, click the Add button. The select file dialog will appear. Select the desired pack name and click the OK button to add (install) it.



**Tip:** To save your changes permanently in the 24x7 Event Server configuration file click the **File/Save** menu item or press CTRL+S keyboard shortcut.

## Managing Event Server State

You can use Event Server Management Console to start, stop, pause and resume Event Server service engine. Use the **Event Server** top-level menu to perform the following operations:

- Start – this command starts Event Server engine if it is not already running. On startup the engine reads the configuration file.
- Stop – this command stops Event Server engine. Use this to stop the engine while you are making changes in events for which you do not want the Event Server to respond.
- Pause – this command temporarily pauses Event Server engine. In this state the Event Servers stops monitoring and responding to new event but the program is still loaded into computer memory and can be quickly resumed. Note that all events occurring while the engine is being paused are completely missed. If you resume the engine it will not process such events.
- Resume – this command resumes previously paused Event Server engine.

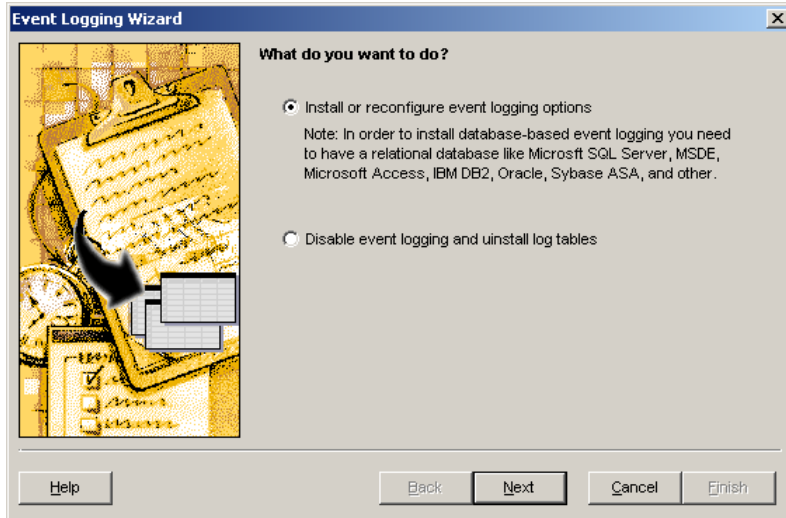


**Important Note:** When you save changes in the configuration file Event Server automatically restarts the engine forcing it to reload the latest event configuration file. However if the engine is stopped or paused before the save it is not restarted automatically. You have to restart it manually if you want the engine to reload the event configuration file containing your recent changes.

## Configuring Centralized Event Logging

24x7 Event Server can log all detected events to a relational database. If the selected database is file-based such as Microsoft Access it must reside locally on the same computer or be accessible on a shared network drive. If the selected database is server-based such as Microsoft SQL Server, Oracle, etc... the database server can reside on any computer on your network. You can configure 24x7 Event Server running on multiple computers to log events to the same centralized database thus creating a single point of event monitoring and analysis. You can then use either built-in event tacking and analysis reports or your custom reports to analyze log data. For more information on event tacking and analysis reports see the following topics in this CHAPTER.

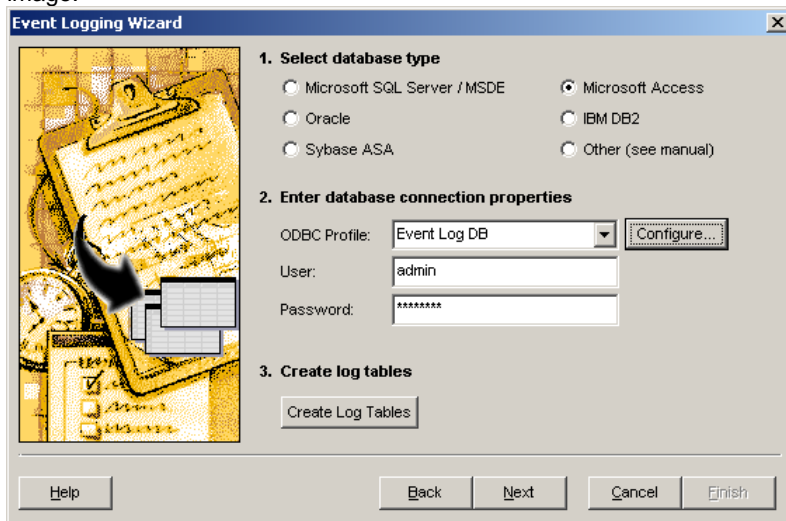
To install or uninstall event logging use **Event Server/Event Logging...** menu. This will start the Event Logging Wizard as displayed on the following image.



Follow instructions provided by the wizard when installing, changing or uninstalling event logging service.

## Step 1 – Selecting Database System

The Event Logging Wizard supports a number of widely used database systems. When installing the logging service make sure to select the correct database when prompted for the database information as displayed on the following image.



**Important Notes:** Not every relational database system can be used as a backend database for event logging. Only database systems that meet the following requirements can be used for event logging:

- Support standard ANSI database data types: INTEGER, VARCHAR, TIMESTAMP.
- Support long VARCHAR columns able to store at least 4000 characters and allow simple updates for such columns (not using BLOB like updates).
- Support table primary keys.
- Support basic ANSI syntax for CREATE TABLE command.
- Support ODBC 3.0 compliant database driver.

For example, the following database systems cannot be used for event logging: SQL Server 6.5 and prior, Oracle 7.3 and prior, Sybase SQL Server and Sybase ASE 12.0 and prior. All the databases do not support table columns



having VARCHAR(4000) database. You must use later versions of these databases that support longer VARCHAR type columns.

## Step 2 – Configuring Database Connection

The Event Logging service uses standard Open Database Connectivity (ODBC) interface available in all modern Windows systems. To configure a database connection you need to specify is the ODBC profile name (you can select it from the **ODBC profile** drop-down list or type it in), your database user name and password just as you use them in other database programs.

If you do not have a ready to use ODBC connection, you need to do the following basic steps to prepare the 24x7 Event Server to work with your database:

1. Install the ODBC database driver. The driver can be obtained from your database vendor, or a third party company. Many drivers are available directly from Microsoft. The driver must be compliant with ODBC Level 1 or higher ODBC 1.x, 2.x or 3.0
2. Define the ODBC data source. To define a new data source you can use ODBC Driver Manager which you can start from Control Panel or alternatively you can click the **Configure** button in the Event Logging Wizard.
3. Test if necessary troubleshoot the database connection.

In case if you experience problems with the configured data source you can use the ODBC Driver Manager Trace tool to troubleshoot the problem. The ODBC Driver Manager Trace tool records information about the ODBC API calls made by the Event Logging service while connected to an ODBC data source. ODBC Driver Manager Trace writes its output to a file named SQL.LOG (by default) located in the Windows home folder or to a log file that you specify. You can view the ODBC Driver Manager Trace log at any time by using any text editor.


## Step 3 – Creating Event Log Tables

If you have installed 24x7 Event Server on multiple computes and already created centralized event log tables using one of these installations you should skip step 3.

Normally the Event Logging Wizard will use database specific SQL commands to create the logging tables. If you select the **"Other"** option for the database type in step 1 and then click the **Create Log Tables** button in step 3, the Event Logging Wizard will attempt to execute the following two CREATE TABLE commands in order to create the required logging tables:

```
CREATE TABLE event_log_header
(
    event_id INTEGER NOT NULL,
    computer VARCHAR(50) NOT NULL,
    client_time TIMESTAMP NOT NULL,
    db_time TIMESTAMP default CURRENT_TIMESTAMP,
    event_name VARCHAR(255),
    event_type VARCHAR(20),
    user_name VARCHAR(50),
    PRIMARY KEY (event_id, computer)
);
```

```
CREATE TABLE event_log_detail
(
    event_id INTEGER NOT NULL,
    computer VARCHAR(50) NOT NULL,
    param_name VARCHAR(20) NOT NULL,
    param_value VARCHAR(4000),
    PRIMARY KEY (event_id, computer, param_name)
);
```

 **Tip:** If you receive an error in step 3 try creating these tables outside of the Logging Wizard using native database utilities like ISQL and other. You can also try modifying the default data-types (for example use `TIMESTAMP` keyword instead of `DATETIME`, `TEXT` instead of `VARCHAR`, etc...) and if you are successful in creating these two tables you should simply skip step 3 and click the Next button to continue. In case if you are unable to create these tables please contact your database administrator for assistance and to verify your database meets the minimum requirements listed in "Step 1 – Selecting Database System."

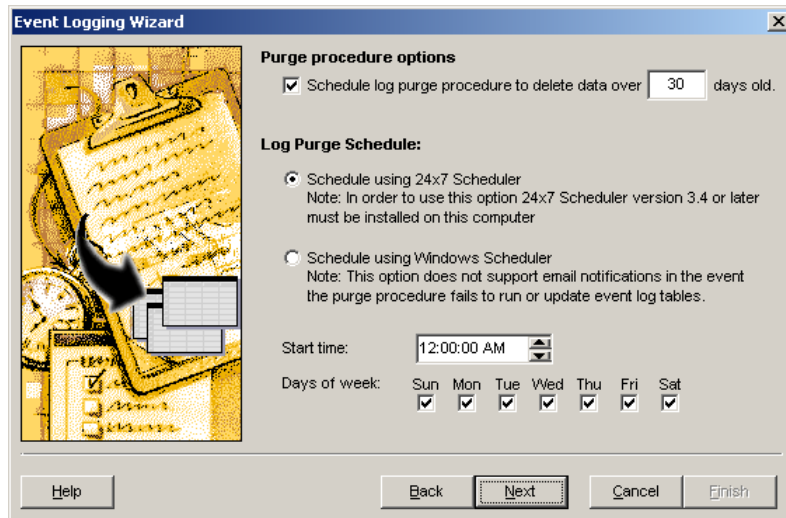
 **Important Notes:**

- You must have `CREATE TABLE` database privileges in order to create event logging tables.
- If your database system supports multiple databases on a single server, the Event Server Wizard will create event logging tables in the default database assigned to the user specified in the database connection properties in step 2. If you do not want to use the current default database either alter user's settings and assign a different database or create a new user for event logging with a different default database.

## Scheduling Periodic Purge of Event Log Tables

The Event Logging Wizard can schedule an optional procedure to periodically purge old data from event log tables. If you have limited space requirements this procedure will help you to control size of the event log tables. In case if you

are not concerned about space usage or you already scheduled this procedure to run on another computer you should uncheck the **Schedule log purge** option and click the Next button to continue. Otherwise, choose how many days of history you want to keep in the logging tables, select the appropriate schedule method and timing and click the Next button to schedule the purge procedure and advance to the next step.



The screenshot shows the 'Event Logging Wizard' dialog box. The 'Purge procedure options' section has a checked checkbox for 'Schedule log purge procedure to delete data over' followed by a text box containing '30' and the text 'days old.'. The 'Log Purge Schedule:' section has two radio button options: 'Schedule using 24x7 Scheduler' (selected) and 'Schedule using Windows Scheduler'. Below these are 'Start time:' (12:00:00 AM) and 'Days of week:' (Sun, Mon, Tue, Wed, Thu, Fri, Sat) with checkboxes for each day, all of which are checked. At the bottom are buttons for 'Help', 'Back', 'Next', 'Cancel', and 'Finish'.

## Configuring System Options

24x7 Event Server system options can be accessed using **Event Server/Options** menu.

24x7 Event Server presently supports 2 types of options:

1. Default event monitoring options - this group of options controls how often Event Server engine checks for different event types. This options affect all events based on the polling method. For more information see [CHAPTER 4, Polled Events](#) topic.
2. Error handling and event notification options - this two groups of options control how Event Server responds to various event processing errors. By default Event Server writes all run-time errors to the Windows NT Application Event Log. In addition to default error logging Event Server can send optional administrative email alerts to a single person or a group of people. The email is send using SMTP protocol so that no third-party email client software is required for this option. For more information about administrative alerts and event types see [CHAPTER 1, Administrative Alerts](#) topic.



### Important Note:

You must restart 24x7 Event Server in order for the changes in the system options to take effect.

## Running Event Tracking and Analysis Reports

Event Server can collect the event data from your servers and store it in a relation database. This data can be then analyzed using either built-in reports or user-defined reports. For instructions on how to configure event logging see [Configuring Centralized Event Logging](#) topic in CHAPTER3.

### Built-in Reports

#### Overview

Built-in Reports are accessed using Reports menu in the 24x7 Event Server Management Console. There are two types of reports:

- Generic Reports
- Special Reports

Generic reports analyze and display common data and charts for all logged events regardless of event type while Special reports analyze and display more targeted information for specific event types.

The following reports are available:

#### Generic Reports

- [EVENT SUMMARY](#)
- [Event Detail](#)
- [Top 10 Events](#)
- [Event Trends \(All Events\)](#)
- [Event Trends \(Top 10 Events\)](#)
- [Event Trends \(Selected Events\)](#)

### Special Reports

- [Warnings and Errors in System Event Logs](#)
- [Warnings and Errors in Application Event Logs](#)
- [Security Failure Audit](#)
- [Application and Service Failures](#)
- [System Performance Issues](#)
- [Database Performance Issues](#)
- [Database Downtime](#)
- [Web and Network Services Downtime](#)
- [Computer Downtime](#)

All reports but 3 generic reports (Event Summary and 2 Top 10 Events) allow you to select report filter parameters such as event originating computer name, event type, event dates and some other. After you select a report in the Reports menu, 24x7 Event Server Management Console displays **Report Filter Parameters** dialog. Enter optional report filter parameters. For example, if you want to filter by event type only select desired type from the **Event Type** drop-down list leaving all other parameters blank. If you do not want to filter events and include all of them simply do not enter anything and click the **OK** button to display the selected report.

### Event Summary

The "Event Summary Report" displays summary statistics by different event types and event sources (source: computer name and user name) as well as a pie chart presenting event occurrence totals by event type. To run the report, select **Reports/Generic Reports/Event Summary** menu.

The following columns are displayed on the report:

1. **Computer** – Name of the 24x7 Event Server computer.
2. **User Name** – Name of the user logged on to the computer (user account used for the 24x7 Event Server service) when events occurred.
3. **Event Type** – Name of event type. For a list of supported event types and their descriptions see [Event Monitor Types](#) topic in CHAPTER 4.
4. **Total Events** – Total number of events detected for a computer and/or event type.
5. **Sub-total** – Sum of values in Total Events column.



**Chart by Event Type** – this chart graphically shows all totals by event type. All event types that generated less than 10% of all events are combined together and displayed as the "Other" slice.

### Event Detail

The "Event Detail Report" displays individual records for all logged events. To run the report, select **Reports/Generic Reports/Event Details...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.

The following columns are displayed on the report:

1. **Computer** – Name of the 24x7 Event Server computer.
2. **User Name** – Name of the user logged on to the computer (user account used for the 24x7 Event Server service) when events occurred.
3. **Event Name** – Name of event.
4. **Event Type** – Event type name. For a list of supported event types and their descriptions see [Event Monitor Types](#) topic in CHAPTER 4.
5. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
6. **Database Log Time** – System time on the database server computer at the time of event logging to the database.



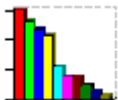
**Tip:** System time can differ on different computers, especially when computers are running in different time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## Top 10 Events

The "Top 10 Events Report" displays summary statistics for 10 most frequently occurring events as well as a bar chart presenting event occurrence totals. To run the report, select **Reports/Generic Reports/To 10 Events** menu.

The following columns are displayed on the report:

1. **Event Rank Number** – Event frequency rank. The most frequent event has rank 1, the least frequent event, among top 10 events, has rank 10.
2. **Computer** – Name of the 24x7 Event Server computer.
3. **Event Name** – Name of event.
4. **Total Events** – Total number of events detected for a computer and/or event type.
5. **Sub-total** – Sum of values in Total Events column.



**Top 10 Events Chart** – this chart graphically shows all totals by event type. All event types that generated less than 10% of all events are combined together and displayed as the "Other" slice.

## Event Trends (All Events)

The "Event Trends (All Events) Report" displays event occurrence trends for all logged events. To run the report, select **Reports/Generic Reports/Event Trends (All Events)** menu.



The chart shows how many events occurred as a function of time. It also shows a trend line displayed as a blue dashed line. The trend line is built using simple linear regression model.




**Tip:** The trend line is only accurate if sufficient number of events is recorded during a continuous time interval. For best results at least a few hundred events should be recorded.

## Event Trends (Top 10 Events)

The "Event Trends (Top 10 Events) Report" displays event occurrence trends for top 10 most frequently occurring events. To run the report, select **Reports/Generic Reports/Event Trends (Top 10 Events)** menu.



The chart shows how many events occurred as a function of time. It also shows a trend line displayed as a blue dashed line.


 **Tip:** The trend line is only accurate if sufficient number of events is recorded during a continuous time interval. For best results at least a few hundred events should be recorded.

### Event Trends (Selected Events)

The "Event Trends (Selected Events) Report" displays event occurrence trends for selected events. This report is similar to "Event Trends (All Events) Report" except it allows you to filter which event(s) to include. To run the report, select **Reports/Generic Reports/Event Trends (Selected Events)** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to select which event(s) to include. If you don't enter anything the result will be the same as running "Event Trends (All Events) Report."



The chart shows how many events occurred as a function of time. It also shows a trend line displayed as a blue dashed line. The trend line is build using simple linear regression model.

 **Tip:** The trend line is only accurate if sufficient number of events is recorded during a continuous time interval. For best results at least a few hundred events should be recorded.

### Warnings and Errors in System Event Logs

The "Warnings and Errors in System Event Logs Report" displays individual records for all events that capture warning and error messages written to Windows NT System Event Logs. The following event types are used with this report:

- [New NT Event Log record](#)

To run the report, select **Reports/Special Reports/ Warnings and Errors in System Event Logs...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.

#### **Important Notes:**

- The report shows only events whose data is saved in the event log tables; it does not query actual System Event Log files. If you do not have event(s) configured to monitor warning and errors do not expect to find them in this report.
- It is recommended to setup a catch-all event monitor for the Windows NT System Event Log so that every message written to the log file is also copied to event log database. In this scenario the report can provide accurate information on all system errors and warnings. If you have 24x7 Event Server installed on multiple computers you can then use this report to get a summary picture of all enterprise-wide system failures.
- If you have multiple event monitors configured to monitor system errors and warnings and event monitor filters do overlap then you can get multiple records for the same physical event being saved in the event log tables. As a result you may see duplicate records displayed on the report.

The following columns are displayed on the report:

1. **Computer** – Name of the 24x7 Event Server computer.
2. **Event ID** – Event number as it appears in the Windows NT Event Viewer.
3. **Source** – Event source as it appears in the Windows NT Event Viewer.
4. **Event Type** – Event type, either ERROR or WARNING.
5. **Message** – Event message text as it appears in the Windows NT Event Viewer.
6. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
7. **Database Log Time** – System time on the database server computer at the time of event logging to the database.

 **Tip:** System time can differ on different computers, especially when computers are running in different

time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## Warnings and Errors in Application Event Logs

The "Warnings and Errors in Application Event Logs Report" displays individual records for all events that capture warning and error messages written to Windows NT Application Event Logs. The following event types are used with this report:

- [New NT Event Log record](#)

To run the report, select **Reports/Special Reports/ Warnings and Errors in Application Event Logs...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.



### Important Notes:

- The report shows only events whose data is saved in the event log tables; it does not query actual Application Event Log files. If you do not have event(s) configured to monitor warning and errors do not expect to find them in this report.
- It is recommended to setup a catch-all event monitor for the Windows NT Application Event Log so that every message written to the log file is also copied to event log database. In this scenario the report can provide accurate information on all application-specific errors and warnings. If you have 24x7 Event Server installed on multiple computers you can then use this report to get a summary picture of all enterprise-wide application failures.
- If you have multiple event monitors configured to monitor system errors and warnings and event monitor filters do overlap then you can get multiple records for the same physical event being saved in the event log tables. As a result you may see duplicate records displayed on the report.

The following columns are displayed on the report:

1. **Computer** – Name of the 24x7 Event Server computer.
2. **Event ID** – Event number as it appears in the Windows NT Event Viewer.
3. **Source** – Event source as it appears in the Windows NT Event Viewer.
4. **Event Type** – Event type, either ERROR or WARNING.
5. **Message** – Event message text as it appears in the Windows NT Event Viewer.
6. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
7. **Database Log Time** – System time on the database server computer at the time of event logging to the database.



**Tip:** System time can differ on different computers, especially when computers are running in different time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## Security Failure Audit

The "Security Failure Audit Report" displays individual records for all events that capture audit failure messages written to Windows NT Security Event Logs. The following event types are used with this report:

- [New NT Event Log record](#)

To run the report, select **Reports/Special Reports/ Security Failure Audit...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.

**Important Notes:**

- The report shows only events whose data is saved in the event log tables; it does not query actual Security Event Log files. If you do not have event(s) configured to monitor security failures do not expect to find them in this report.
- By default Windows systems are not configured to perform security audit. If you want to monitor security-related events you must either configure Network Domain Security Policy rules on your network primary domain server or configure Local Security Policy on each individual computer running 24x7 Event Server. Note that domain rules always override local computer rules. For information on how to configure security audit see examples available in the [New NT Event Log record](#) topic in CHAPTER 4.
- It is recommended to setup a catch-all event monitor for the Windows NT Security Event Log so that every message written to the log file is also copied to event log database. In this scenario the report can provide accurate information on all security violations. If you have 24x7 Event Server installed on multiple computers you can then use this report to get a summary picture of all enterprise-wide security problems and detect any anomalies such as hacker unauthorized access, hacker attacks, and other security breaches.
- Because amount of data generated by audit events can be huge it is recommended to audit only failure events.
- If you have multiple event monitors configured to monitor system errors and warnings and event monitor filters do overlap then you can get multiple records for the same physical event being saved in the event log tables. As a result you may see duplicate records displayed on the report.

The following columns are displayed on the report:

1. **Computer** – Name of the 24x7 Event Server computer.
2. **Event ID** – Event number as it appears in the Windows NT Event Viewer.
3. **Source** – Event source as it appears in the Windows NT Event Viewer.
4. **Event Type** – Event type, always AUDIT FAILURE.
5. **Message** – Event message text as it appears in the Windows NT Event Viewer.
6. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
7. **Database Log Time** – System time on the database server computer at the time of event logging to the database.



**Tip:** System time can differ on different computers, especially when computers are running in different time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## Application and Service Failures

The "Application and Service Failures Report" displays individual records for all events that capture various application and service failures. The following event types are used with this report:

- [New NT event log record](#)
- [Dr. Watson error](#)
- [Process hung](#)
- [NT Service stop](#)

To run the report, select **Reports/Special Reports/Application and Service Failures...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.

**Important Notes:**

- The report shows only events whose data is saved in the event log tables; it does not query actual Windows Event Log files or any other files and logs. If you do not have 24x7 Event Server configured to monitor types of events described above do not expect to find them in this report.



- It is recommended to setup a catch-all event monitors described events in case if you want to capture every possible failure. If you have 24x7 Event Server installed on multiple computers you can then use this report to get a summary picture of all enterprise-wide application problems.
- If you have multiple event monitors configured to monitor types of described events and event monitor filters do overlap then you can get multiple records for the same physical event being saved in the event log tables. As a result you may see duplicate records displayed on the report.

The following columns are displayed on the report:

1. **Computer** – Name of the 24x7 Event Server computer.
2. **Event Type** – Event type, such APPLICATION ERROR, PROCESS HUNG, SERVICE STOP and other.
3. **Application/Service** – Name of failed application or service.
4. **Additional Information** – Additional information describing event failure (if available).
5. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
6. **Database Log Time** – System time on the database server computer at the time of event logging to the database.



**Tip:** System time can differ on different computers, especially when computers are running in different time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## System Performance Issues

The "System Performance Issues Report" displays individual records for all events that capture various system performance issues. The following event types are used with this report:

- [System performance threshold](#)

To run the report, select **Reports/Special Reports/System Performance Issues...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.




### Important Notes:

- The report shows only events whose data is saved in the event log tables; it does not query real-time performance statistics or any other files and logs. If you do not have 24x7 Event Server configured to monitor types of events described above do not expect to find them in this report.
- If you have multiple event monitors configured to monitor types of described events and event monitor filters do overlap then you can get multiple records for the same physical event being saved in the event log tables. As a result you may see duplicate records displayed on the report.
- **Event Logging Database Limitations:** This report is not supported in Microsoft Access! To use this report move your log database to a database server supporting CASE expressions compliant with ANSI/ISO: 1999 standard.

The following columns are displayed on the report:

1. **Computer** – Name of the 24x7 Event Server computer.
2. **Performance Counter** – Name of the performance counter used in the event monitor, for example, \PROCESSOR(\_TOTAL)% PROCESSOR TIME, \MEMORY\AVAILABLE MBYTES,\OBJECTS\PROCESSES, \ACTIVE SERVER PAGES\ERRORS DURING SCRIPT RUNTIME, and other.
3. **Value** – Actual value of the performance counter at the time of the event occurrence.
4. **Event Description** – Additional information describing how the event monitor filter is setup, for example, for a CPU usage monitor, the value in this column could show something like VALUE 84 REACHED OR EXCEEDED 75% PERFORMANCE THRESHOLD.

5. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
6. **Database Log Time** – System time on the database server computer at the time of event logging to the database.

 **Tip:** System time can differ on different computers, especially when computers are running in different time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## Database Performance Issues

The "Database Performance Issues Report" displays individual records for all events that capture various database performance issues. The following event types are used with this report:

- [Database performance threshold](#)


To run the report, select **Reports/Special Reports/Database Performance Issues...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.

### **Important Notes:**

- The report shows only events whose data is saved in the event log tables; it does not query real-time performance statistics or any other files and logs. If you do not have 24x7 Event Server configured to monitor types of events described above do not expect to find them in this report.
- If you have multiple event monitors configured to monitor types of described events and event monitor filters do overlap then you can get multiple records for the same physical event being saved in the event log tables. As a result you may see duplicate records displayed on the report.
- **Event Logging Database Limitations:** This report is not supported in Microsoft Access! To use this report move your log database to a database server supporting CASE expressions compliant with ANSI/ISO: 1999 standard.

The following columns are displayed on the report:

1. **Computer : DB** – Name of the 24x7 Event Server computer following by the name of ODBC Profile used for connections to the monitored database.
2. **Performance Query** – Text of SQL query used for database monitoring.
3. **Value** – Actual value returned by the query at the time of the event occurrence.
4. **Event Description** – Additional information describing how the event monitor filter is setup, for example, for a user connections monitor, the value in this column could show something like VALUE 105 REACHED OR EXCEEDED 100 CONNECTIONS THRESHOLD.
5. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
6. **Database Log Time** – System time on the database server computer at the time of event logging to the database.

 **Tip:** System time can differ on different computers, especially when computers are running in different time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## Database Downtime

The "Database Downtime Report" displays individual records for all events that capture database availability issues. The following event types are used with this report:

- [Database downtime](#)

To run the report, select **Reports/Special Reports/Database Downtime...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.



### Important Notes:

- The report shows only events whose data is saved in the event log tables; it does not attempt to connect and validate database connections or query any other files and logs. If you do not have 24x7 Event Server configured to monitor types of events described above do not expect to find them in this report.
- If you have multiple event monitors configured to monitor types of described events and event monitor filters do overlap then you can get multiple records for the same physical event being saved in the event log tables. As a result you may see duplicate records displayed on the report.

The following columns are displayed on the report:

1. **Computer : DB** – Name of the 24x7 Event Server computer following by the name of ODBC Profile used for connections to the monitored database.
2. **Event Description** – Event description such as DATABASE NOT AVAILABLE.
3. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
4. **Database Log Time** – System time on the database server computer at the time of event logging to the database.



**Tip:** System time can differ on different computers, especially when computers are running in different time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## Web and Network Services Downtime

The "Web and Network Services Downtime Report" displays individual records for all events that capture various web and network service availability issues. The following event types are used with this report:

- [Web server slow response](#)
- [TCP service downtime](#)

To run the report, select **Reports/Special Reports/Web and Network Services Downtime...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.




### Important Notes:

- The report shows only events whose data is saved in the event log tables; it does not attempt to connect and validate any service statuses or query any files and logs. If you do not have 24x7 Event Server configured to monitor types of events described above do not expect to find them in this report.
- If you have multiple event monitors configured to monitor types of described events and event monitor filters do overlap then you can get multiple records for the same physical event being saved in the event log tables. As a result you may see duplicate records displayed on the report.
- **Event Logging Database Limitations:** This report is not supported in Microsoft Access! To use this report move your log database to a database server supporting CASE expressions compliant with ANSI/ISO: 1999 standard.

The following columns are displayed on the report:

1. **Computer** – Name of the 24x7 Event Server computer.
2. **Web/Network Service** – Name of monitored web or network service as it is entered in the event properties. This name could be one of the following: computer name, web service name, TCP/IP address. For [Web server slow response](#) event types this name also includes name of the monitored resource.
3. **Event Description** – Event description such as TCP SERVICE DOWNTIME.
4. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
5. **Database Log Time** – System time on the database server computer at the time of event logging to the database.

 **Tip:** System time can differ on different computers, especially when computers are running in different time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## Computer Downtime

The "Computer Downtime Report" displays individual records for all events that capture database availability issues. The following event types are used with this report:

- [System shutdown](#)
- [Server downtime](#)


To run the report, select **Reports/Special Reports/ Computer Downtime...** menu. The **Report Filter Parameters** dialog will appear. If you wish you may enter the optional report filter to limit the amount of data retrieved from the event log tables.

### **Important Notes:**

- The report shows only events whose data is saved in the event log tables; it does not attempt to connect and validate any computer/system state or query any files and logs. If you do not have 24x7 Event Server configured to monitor types of events described above do not expect to find them in this report.
- If you have multiple event monitors configured to monitor types of described events and event monitor filters do overlap then you can get multiple records for the same physical event being saved in the event log tables. As a result you may see duplicate records displayed on the report.

The following columns are displayed on the report:

1. **Computer** – Name of the 24x7 Event Server computer.
2. **Not Available Computer** – Name of monitored computer which is not available. For [Server downtime](#) event types this name could be one of the following: computer name, web service name, TCP/IP address. The name is reported exactly as it is entered in the event properties. For [System shutdown](#) event types this name is always the same as name of the computer running 24x7 Event Server (which always matches the name displayed in the first **Computer** column).
3. **Event Description** – Event description, either SERVER DOWNTIME or SYSTEM SHUTDOWN.
4. **Computer Time** – System time on the computer running 24x7 Event Server at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.
5. **Database Log Time** – System time on the database server computer at the time of event logging to the database.

 **Tip:** System time can differ on different computers, especially when computers are running in different time zones. That's why only the **Database Log Time** column can be using to compare event timing for events occurred on different systems.

## User-defined Reports

### Overview





User-defined report can be created in any software that supports database access. The following topics describe how the event information is stored in the database as well as provide step-by-step instructions for creating user-defined reports using Microsoft Access and Microsoft Excel.


### Event Log Tables and Event Data

Event log data is stored in 2 database tables **EVENT\_LOG\_HEADER** and **EVENT\_LOG\_DETAIL**. The first table stores event record header data – 1 record for every logged event. The second table stores event detail records – as many records as many properties are supported by the type of the logged event.


For instructions on how to configure event logging to a relational database system and how to create event log tables see [Configuring Centralized Event Logging](#) topic in CHAPTER3.

**EVENT\_LOG\_HEADER** table contains the following columns:

| Column      | Description   |
|-------------|---|
| event_id    | A numeric column whose value uniquely identifies the logged event on the originating computer. It can be used together with the value in the <b>computer</b> column as a global unique identifier for the logged event.   |
| computer    | A text column whose value is the name of the event originating computer. It can be used together with the value in the <b>event_id</b> column as a global unique identifier for the logged event.<br><br> <b>Tip:</b> Don't confuse the event originating computer with the computer where the actual event occurs. In most cases they are the same, but in some cases they could be different. For example, on computer A running 24x7 Event Server you have configured event monitor watching performance of your web server running on computer B then A is the originating computer.   |
| client_time | A date/time column whose value stores system time on the event originating computer at the time of event logging to the database. This time should be virtually the same as the time of the event occurrence. There could be a slight difference caused by the time required to establish a new database connection for the event logging process.<br><br> <b>Tip:</b> This value can be used to sort events in chronological order as they occurred on the event originating computer whose name is stored in the <b>computer</b> column (in other words, from the originating computer local point of view).<br> <b>Tip:</b> System time can differ on different computers, especially when computers are running in different time zones. Use <b>db_time</b> column when analyzing and reporting data from multiple computers. |
| db_time     | A date/time column whose value stores system time on the database server computer at the time of event logging to the database.<br><br> <b>Tip:</b> This value can be used to sort events in chronological order as they occurred on the entire network (in other words, from the global point of view). Use this column in your reports instead of the <b>client_time</b> column if you have multiple computers logging to a centralized database system.   |
| event_name  | A text column whose value is the name of the logged event as it is defined on the event   |

|            |  |
|------------|--|
|            | <p>originating computer.</p> <p> <b>Tip:</b> Same event name can be used on multiple computers for different events. Unless you run 24x7 Event Server on all computers using the same event configuration file don't use event name as common value for event grouping.</p> |
| event_type | A text column whose value is the type of the logged event. See the following table for a list of supported event types.  |
| user_name  | A text column whose value is the name of a user account running 24x7 Event Server on the event originating computer at the time of event occurrence.   |

**EVENT\_LOG\_DETAIL** table contains the following columns:

| Column      | Description   |
|-------------|---|
| event_id    | <p>A numeric column whose value uniquely identifies the logged event on the originating computer. For more details see description of this column in the header table.</p> <p> <b>Tip:</b> Use <b>event_id</b> and <b>computer</b> columns together to join data the detail table with the data in the header table.</p> |
| computer    | A text column whose value is the name of the event originating computer. For more details see description of this column in the header table.   |
| param_name  | A text column whose value stores names of the logged event parameters. For more information on supported parameter names and their descriptions see the following table.  |
| param_value | A text column whose value stores values of the logged event parameters. For more information on supported parameter names and their descriptions see the following table.   |

**Event types, parameters and their descriptions:**

| EVENT TYPE                  | PARAMETER        | PARAMETER NAME         | PARAMETER DESCRIPTION   |
|-----------------------------|------------------|------------------------|---|
| New NT event log record     | ev_log           | Event Log Name         | Windows NT event log name. You can either select one of the default names or type in any other valid log name.  |
|                             | ev_id            | Event ID               | The event ID, as seen in the Event Viewer Event column.   |
|                             | ev_type_name     | Event Type             | The event type, as seen in the Event Viewer "Type" column.  |
|                             | ev_category_name | Event Category         | The event category, as seen in the Event Viewer "Category" column.  |
|                             | ev_source        | Event Source           | The source of the record, as seen in the Event Viewer "Source" column.  |
|                             | ev_computer      | Event Computer         | The name of the computer where event has been reported, as seen in the Event Viewer "Computer" column.  |
|                             | ev_desc          | Event Message Contains | This is the substring that you want to search in the event message text. Leave this blank to trigger event action for any text. If used as macro-parameter action definition, it returns the complete event message text. |
|                             | ev_time_gen      | Record Submit Time     | The event generation time (time when the event was submitted)   |
|                             | ev_time_wr       | Record Write Time      | The event logging time (time when the event was written to the log)   |
|                             | ev_number        | Record Number          | The unique number identifying event record in the log.  |
| NT event log size threshold | source           | Event Log Name         | Windows NT event log name. You can either select one of the default names or type in any other valid log name.  |

|                              |                 |                           |  |
|------------------------------|-----------------|---------------------------|--|
|                              | threshold_value | Size Threshold (bytes)    | Event log size threshold (bytes)   |
|                              | size            | Current File Size (bytes) | Current event log size (bytes)   |
| New SysLog message           | hostname        | Event Source              | The device or computer that generated the event.   |
|                              | addr            | Event Address             | UDP address of the computer or device from where the event has been forwarded, in <IP address>:<port> format.  |
|                              | facility        | Event Facility            | Message facility number as it appears in the syslog.   |
|                              | severity        | Event Severity            | Event severity level as it appears in the syslog.  |
|                              | msg             | Event Source              | This is the substring that you want to search in the event message text. Leave this blank to trigger event action for any text. If used as macro-parameter action definition, it returns the complete event message text.  |
|                              | timestamp       | Message Sent Time         | The event generation time (time when the syslog message was sent)  |
| System performance threshold | name            | Counter Name              | Performance Counter name. You can either select one of the default names or type in any other valid counter name.  |
|                              | threshold_value | Threshold Value           | Event action is triggered when specified threshold value is reached during specified period of time  |
|                              | threshold_type  | Threshold Type            | If threshold value is specified enter comparison type such as less (<), greater (>), less or equal (<=), greater or equal (>=), equal (=), not equal (<>), between and not between. The threshold value must be entered as two comma separated numbers if between or not between is specified for the comparison type. |
|                              | duration        | Duration (seconds)        | Period of time during which threshold value is constantly violated.  |
|                              | value           | Counter Value             | Current value of the Performance Counter.  |
| Disk free space threshold    | name            | Disk Name                 | Disk name, for example C:, D:, E:  |
|                              | threshold_value | Size Threshold (Mbytes)   | Minimum amount of available free space threshold (Mbytes)  |
|                              | value           | Disk Free Space (Mbytes)  | Current amount of available free space (Mbytes).   |
| Process hung                 | process         | Process Module Name       | Name of the executable file for the hung process. If blank, all processes are monitored.   |
|                              | pid             | System Process ID         | System process Id as it appears in the Windows Task Manager  |
| Process start                | process         | Process Module Name       | Name of the executable file for the started process  |
|                              | event           | Event Type                | Process event type   |
|                              | pid             | System Process ID         | System process Id as it appears in the Windows Task Manager  |
| Process termination          | process         | Process Module Name       | Name of the executable file for the terminated process   |
|                              | event           | Event Type                | Process event type   |
|                              | pid             | System Process ID         | System process Id as it appears in the Windows Task Manager  |
| New file                     | file            | File Mask                 | Name of the file to monitor. You can standard wildcards to specify file mask for multiple files. Leave this parameter blank to trigger event action for any new file.  |

|                              |                 |                        |   |
|------------------------------|-----------------|------------------------|---|
|                              | root            | File Path              | File path to the base directory   |
|                              | event           | File Event             | File event type   |
| File deletion                | file            | File Mask              | Name of the file to monitor. You can standard wildcards to specify file mask for multiple files. Leave this parameter blank to trigger event action for any deleted file.   |
|                              | root            | File Path              | File path to the base directory   |
|                              | event           | File Event             | File event type   |
|                              | file            | File Mask              | Name of the file to monitor. You can standard wildcards to specify file mask for multiple files. Leave this parameter blank to trigger event action for any changed file.   |
| File change                  | root            | File Path              | File path to the base directory   |
|                              | event           | File Event             | File event type   |
| File size threshold          | path            | File Name              | Full file name including path   |
|                              | threshold_value | Size Threshold (bytes) | File size threshold (bytes)   |
|                              | size            | Current File Size      | Current file size (bytes).  |
| Text log file size threshold | path            | File Name              | Full file name including path   |
|                              | threshold_value | Size Threshold (bytes) | File size threshold (bytes)   |
| New text log file record     | file            | File Name              | File name NOT including path  |
|                              | root            | File Path              | File path to the base directory   |
|                              | data            | Message Contains       | This is the substring that you want to search in the message text. Leave this blank to trigger event action for any text. If used as macro-parameter action definition, it returns the complete message text (e.g. the complete text line). |
| Directory changes            | root            | File Path              | File path to the base directory   |
|                              | file            | File Mask              | Name of the file to monitor. You can standard wildcards to specify file mask for multiple files. Leave this property blank to monitor all files.  |
|                              | event           | Change Type            | Change type to monitor  |
| New SNMP trap                | gen_trap        | Generic Trap           | Identifier of the generic trap.   |
|                              | spec_trap       | Specific Trap          | Identifier of the specific trap.  |
|                              | ent_oid         | Enterprise OID         | OID of the enterprise that generated the trap.  |
|                              | time            | Trap Time              | The trap time.  |
|                              | src_ip          | Source IP              | IP address of the agent that generated the trap. This information is retrieved from the network transport.  |
|                              | agent_ip        | Agent IP               | IP Address of the agent that generated the trap. This information is retrieved from the SNMP protocol data unit (PDU).  |
|                              | community       | Community              | Community string of the trap.   |
|                              | vars            | Variables              | Partial or full values of trap variables.   |
| Database                     | db              | ODBC Profile           | Name of the ODBC profile for this database connection.  |



|                                |                 |                      |  |
|--------------------------------|-----------------|----------------------|--|
| downtime                       | user            | Database User        | Name of the database user.   |
|                                | password        | Password             | User's password.   |
|                                | timeout         | Connection Timeout   | Connection timeout threshold.  |
|                                | event           | Database Event       | Database event type  |
| Database startup               | db              | ODBC Profile         | Name of the ODBC profile for this database connection.   |
|                                | user            | Database User        | Name of the database user.   |
|                                | password        | Password             | User's password.   |
|                                | timeout         | Connection Timeout   | Connection timeout threshold.  |
|                                | event           | Database Event       | Database event type  |
| Database data change           | db              | ODBC Profile         | Name of the ODBC profile for this database connection.   |
|                                | user            | Database User        | Name of the database user.   |
|                                | password        | Password             | User's password.   |
|                                | query           | SQL Query            | SQL query to run. Must be a valid SQL SELECT query returning only single value of numeric or string data type  |
|                                | timeout         | Query Timeout        | Query execution timeout.   |
| Database performance threshold | db              | ODBC Profile         | Name of the ODBC profile for this database connection.   |
|                                | user            | Database User        | Name of the database user.   |
|                                | password        | Password             | User's password.   |
|                                | query           | SQL Query            | SQL query to run. Must be a valid SQL SELECT query returning only single value of numeric or string data type. Tip: to call stored procedures and other SQL commands create user-defined database functions and call them using a SELECT-type query.   |
|                                | threshold_value | Threshold Value      | Threshold value. If this parameter is not specified any change in returned value triggers event action.  |
|                                | threshold_type  | Threshold Comparison | If threshold value is specified enter comparison type such as less (<), greater (>), less or equal (<=), greater or equal (>=), equal (=), not equal (<>), between and not between. The threshold value must be entered as two comma separated numbers if between or not between is specified for the comparison type. |
|                                | duration        | Threshold Duration   | Period of time the threshold must be consistently reached before event action is triggered. If duration is not specified the action is triggered as soon as the returned value reaches the specified threshold.  |
|                                | timeout         | Query Timeout        | Query execution timeout.   |
|                                | value           | Query Result         | Query result.  |
| New email message              | address         | Mailbox Address      | POP3 email mailbox to watch on, in "<user>[:<password>]<server>[:<port>]" format. Password and port values are optional.   |
|                                | Subject         | Subject Contains     | This is the substring that you want to search in the email subject. Leave this parameter blank to trigger event action for any text.   |

|                          |                  |                       |   |
|--------------------------|------------------|-----------------------|---|
|                          | From             | Message Sender        | This is the substring that you want to search in the email sender address. Leave this parameter blank to trigger event action for any sender.       |
|                          | To               | Message Recipient     | This is the substring that you want to search in the email recipient address. Leave this parameter blank to trigger event action for any recipient. |
|                          | X-Mailer         | Email Program         | Name of the email program that produced the message.  |
|                          | X-Priority       | Message Priority      | Email message priority. Leave this blank for any message. Note that value 3 is most commonly used as "Normal" priority, 1 as "High" and 2 as "Low." |
|                          | Content-Type     | Content Type          | Message content type such as "multipart/alternative", "text/plain", "text/html" and other.  |
|                          | X-Originating-IP | Sender IP             | This is network IP address or computer name of the message sender.  |
|                          | message          | Message Contains      | This is the substring that you want to search in the email message text. Leave this parameter blank to trigger action for any text.                 |
|                          | attachments      | Has Attachments       | Message contains attachments (Yes/No)   |
| New fax message received | fax_name         | TIFF File Name        | Fax file name (TIFF file)   |
|                          | fax_from         | Fax From              | Fax sender number or name as it appears in the Received Faxes folder (usually C:\Documents and Settings\All Users\Documents\My Faxes)               |
|                          | fax_caller_id    | Caller ID             | Fax calling station identifier. This is usually includes sender's fax number.   |
|                          | fax_to           | Fax To                | Fax recipient number  |
|                          | fax_pages        | Number of Pages       | Number of pages received  |
|                          | fax_tr_time      | Fax Transmission Time | Fax transmission time   |
|                          | fax_device_name  | Modem Device Name     | Fax device name (this is usually name of modem used for transmission)   |
| New fax message sent     | fax_sender       | Sender Name           | Name of the fax sender  |
|                          | fax_sender_comp  | Sender Company Name   | Name of the fax sender company  |
|                          | fax_sender_dept  | Sender Department     | Name of the fax sender department   |
|                          | fax_billing_code | Fax Billing Code      | Fax billing code. This is usually the account to pay the cost of sending faxes.   |
|                          | fax_rec_name     | Recipient Name        | Name of fax recipient   |
|                          | fax_rec_num      | Recipient Number      | Destination fax number  |
|                          | fax_pages        | Number of Pages       | Number of pages sent  |
|                          | fax_tr_time      | Fax Transmission Time | Fax transmission time   |
|                          | fax_device_name  | Modem Device Name     | Fax device name (this value usually contains name of the modem used for transmission)   |
| Dr. Watson error         | title            | Title Text            | Title text of the Dr. Watson window. This text normally contains name of the crashed process.   |

|                           |           |                                 |   |
|---------------------------|-----------|---------------------------------|---|
| NT Service start          | service   | Service Name                    | Service display name (as displayed in the services applet)  |
|                           | event     | Service Event                   | Service event type  |
|                           | service   | Service Name                    | Service display name (as displayed in the services applet)  |
|                           | event     | Service Event                   | Service event type  |
| User logon                | account   | Account Name                    | User account name   |
|                           | event     | Event Type                      | Event type  |
| User logout               | account   | Account Name                    | User account name   |
|                           | event     | Event Type                      | Event type  |
| TCP service downtime      | host      | Host Computer                   | Name or IP address of monitored computer.   |
|                           | port      | Port Name or Number             | Name or number of TCP port or service. You can either select one of the default names or type in any other valid port name or number. |
|                           | timeout   | Response Timeout (milliseconds) | Host response timeout in milliseconds.  |
| Web server slow response  | host      | Web Server Name or IP           | Name or IP address of monitored web server computer.  |
|                           | port      | HTTP port number                | HTTP service port number (by default use standard port 80)  |
|                           | resource  | Resource                        | Name of the resource, in other words URL of web page or file not including server name (/ by default)                                 |
|                           | timeout   | Server Response Threshold       | Maximum accepted web server response time in milliseconds.  |
| Server downtime           | host      | Host Computer                   | Name or IP address of monitored computer.   |
|                           | timeout   | Response Timeout (seconds)      | Maximum allowed wait time for response from host in seconds.  |
| Dial-up connection stop   | entry     | RAS Entry Name                  | RAS connection name (as it appears in the Network and Dial-up Connections folder)   |
|                           | event     | Event Type                      | RAS event type  |
| Dial-up connection start  | entry     | RAS Entry Name                  | RAS connection name (as it appears in the Network and Dial-up Connections folder)   |
|                           | event     | Event Type                      | RAS event type  |
| Screen saver activation   | status    | Event Type                      | Activation of a password-protected screen-saver   |
| Screen saver deactivation | status    | Event Type                      | Deactivation of a password-protected screen-saver   |
| Window appearance         | process   | Process Module Name             | Name of the process main executable file  |
|                           | wnd_class | Window Class Name               | Window class name (see Windows programming manuals for more info)   |
|                           | wnd_text  | Window Caption                  | Window caption (title text)   |
|                           | child     | Window Type                     | Top-level or child window   |
|                           | event     | Event Type                      | Event type  |

|                      |                 |                     |  |
|----------------------|-----------------|---------------------|--|
| Window disappearance | process         | Process Module Name | Name of the process main executable file   |
|                      | wnd_class       | Window Class Name   | Window class name (see Windows programming manuals for more info)  |
|                      | wnd_text        | Window Caption      | Window caption (title text)  |
|                      | child           | Window Type         | Top-level or child window  |
|                      | event           | Event Type          | Event type   |
| WMI event            | namespace       | WMI-namespace Name  | WMI-namespace to connect to.   |
|                      | query           | WMI query           | WMI SQL SELECT query. Must be a valid SQL query written in WMI dialect and returning only values of numeric or string and date/time data types.  |
|                      | credentials     | User Credentials    | Name of the domain user and password to run the WMI query. If not empty the value must be specified in one of the following formats:<br>ntlm/domain:<br><domain>:<user_name>:<password><br>Kerberos:<br><principal_name>:<user_name>:<password><br><br>[<domain>]<user_name>:<password><br><br>If this value is empty, credentials of the user account running the Event Server are used with the query. |
| Custom event monitor | cmd_line        | Command Line        | Name of the executable file, batch file or script file to run following by optional command line parameters.   |
|                      | timeout         | Process Timeout     | Process execution timeout. Process is automatically killed if it takes longer to run and the event is ignored.   |
|                      | threshold_value | Process Exit Code   | Process exit code. The following parameter ("Exit Code Condition") determines how the returned exit code value is treated.   |
|                      | threshold_type  | Exit Code Condition | Process exit code condition. This condition defines how to evaluate process exit code and which exit codes indicate event occurrence. In case if the specified process completes with an exit code not satisfying the Exit Code Condition then it is considered as an event, otherwise if the Exit Code Condition is satisfied it is considered as a non-event.  |

### Microsoft Access Example

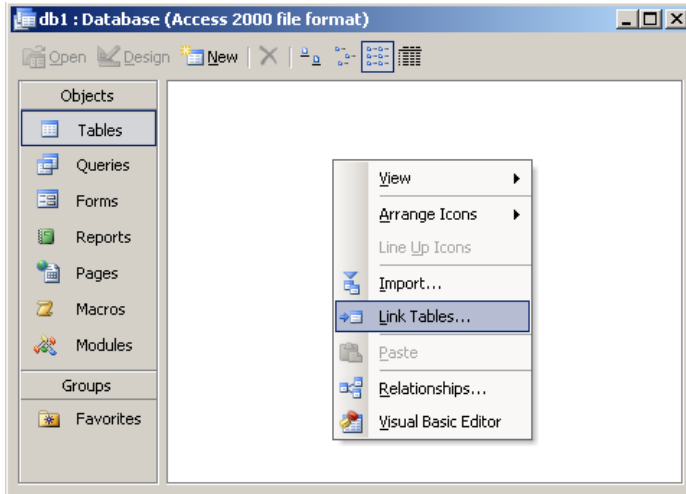
This example demonstrates how to create a user-defined report using Microsoft Access.



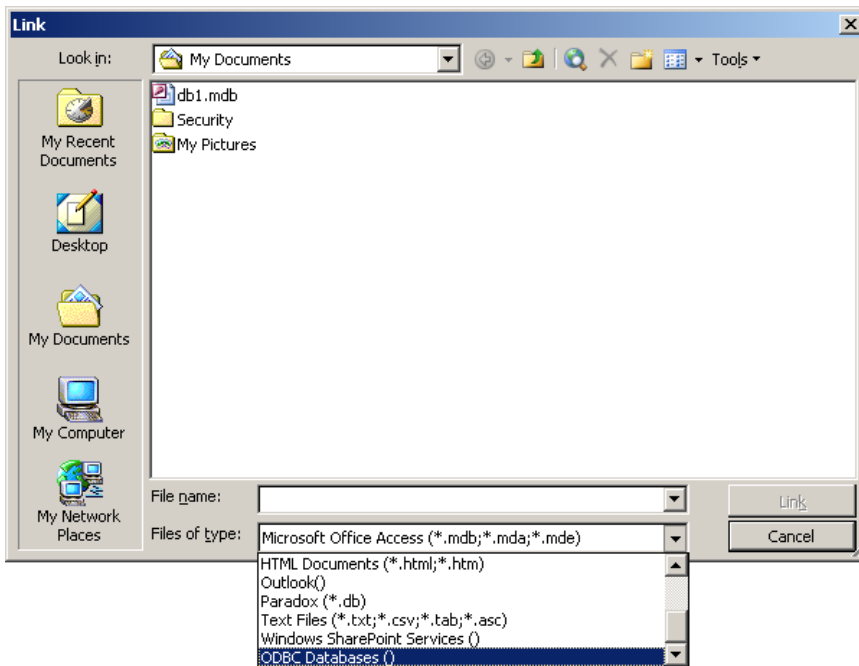
**Note:** If the event log data is stored in a local Microsoft Access database skip the first step and proceed directly to step 2.

1. Link to log tables stored in an external database.

Activate **Tables** View. Right-click within workspace and then select **Link Tables** option from the popup menu.



The **Link** dialog box will appear.

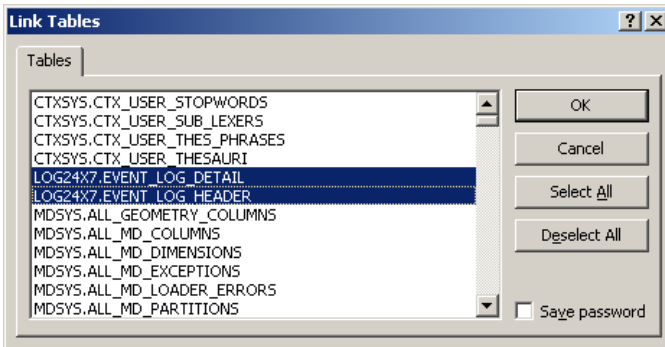


From the **Files of type** drop-down box on the bottom of the dialog select **ODBC Databases()** item. This will open **Select Data Source** dialog. Select name of the ODBC profile for your event log database. If you do not a profile yet click the **New** button and add a new profile. Click the **OK** button.

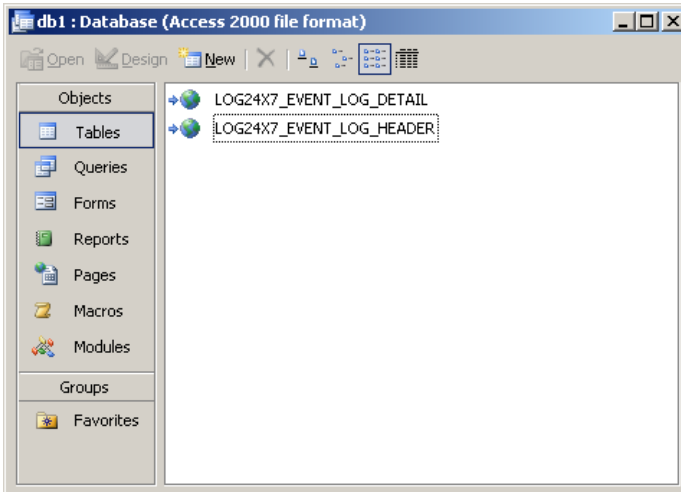
If your database requires user and password for the connection another dialog will appear prompting you to enter the required password for the connection. For example, the following dialog appear when connection to Oracle 8i databases.



After you connect successfully to the event log database Microsoft Access will display names of all available tables.

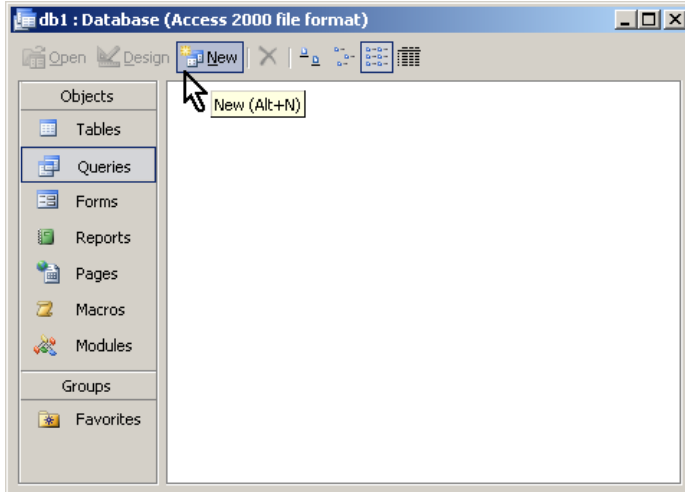


Select `EVENT_LOG_HEADER` and `EVENT_LOG_DETAIL` tables and click the **OK** button. Microsoft Access will add linked tables to the workspace.

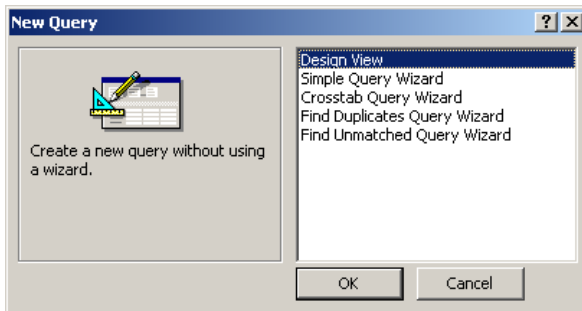


2. Design SQL Query returning data for your report.

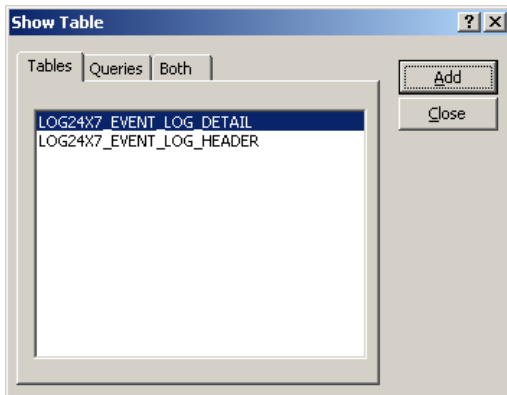
Activate **Queries** View. Click the **New** button.




Microsoft Access will display the **New Query** dialog.

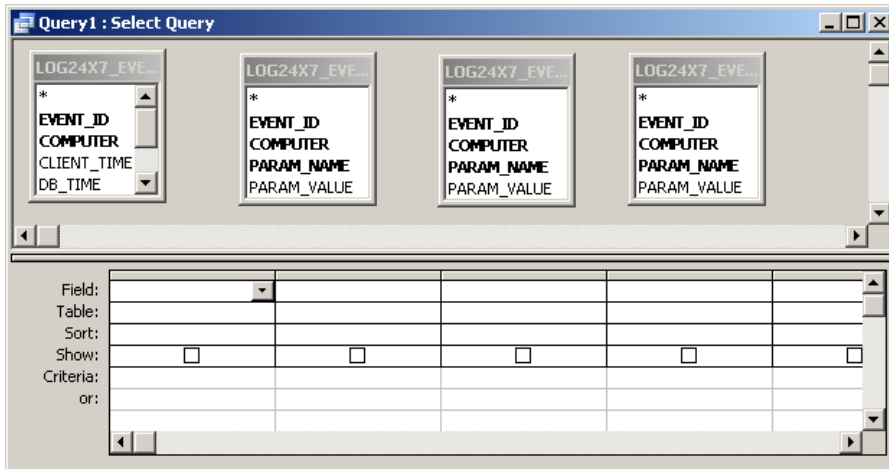


Select the first item **Design View** and click the **OK** button to continue. This will display 2 dialog windows - the **Query1: Select Query** dialog in the background and the **Show Table** dialog in the foreground.



 **Tip:** If you are familiar with SQL and Microsoft Access you can cancel the **Show Table** dialog and then open the SQL view where you can quickly type or paste the required SQL. If you are not familiar with SQL or simply prefer to design queries interactively read the following paragraphs.

In the **Show Table** dialog select **EVENT\_LOG\_HEADER** table and click the **Add** button then select **EVENT\_LOG\_DETAIL** table and click the **Add** button as many times as many event parameters you will need to use for your report. For example you have events monitoring performance of several web servers using "Web server slow response" event type. To create a report returning web server name, name of monitored resource, and event timeout value you will need to add 3 instances of the **EVENT\_LOG\_DETAIL** table as on the following picture.

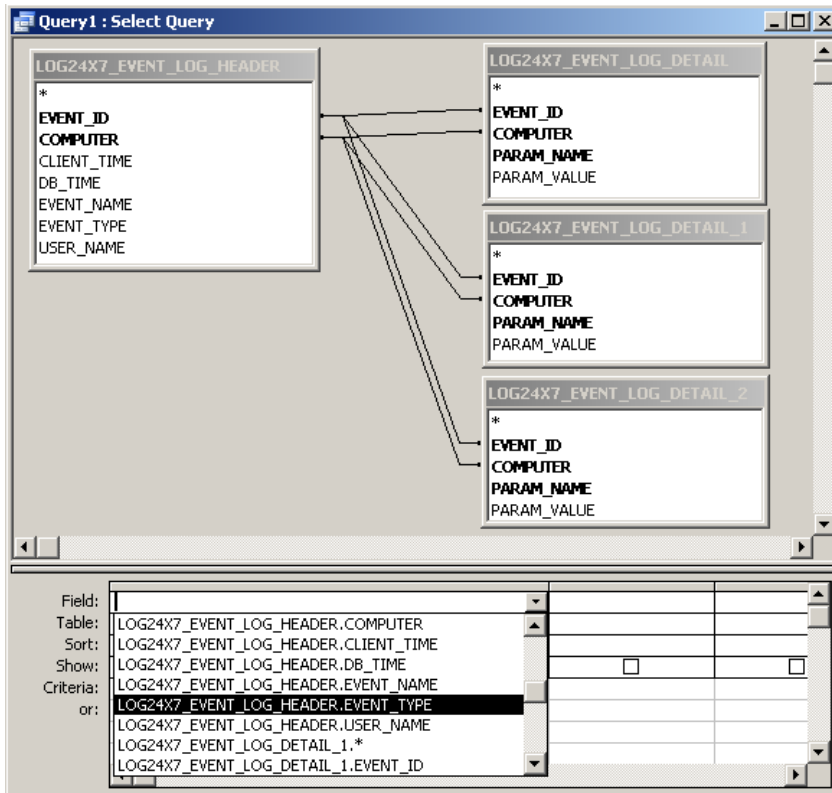


Using mouse resize the **Query1: Select Query** dialog and make it larger; resize top and bottom panes to have a larger workspace and also resize and rearrange table boxes so you can see complete table names and their columns. This will make it convenient for you to link tables together as instructed in the following paragraph.

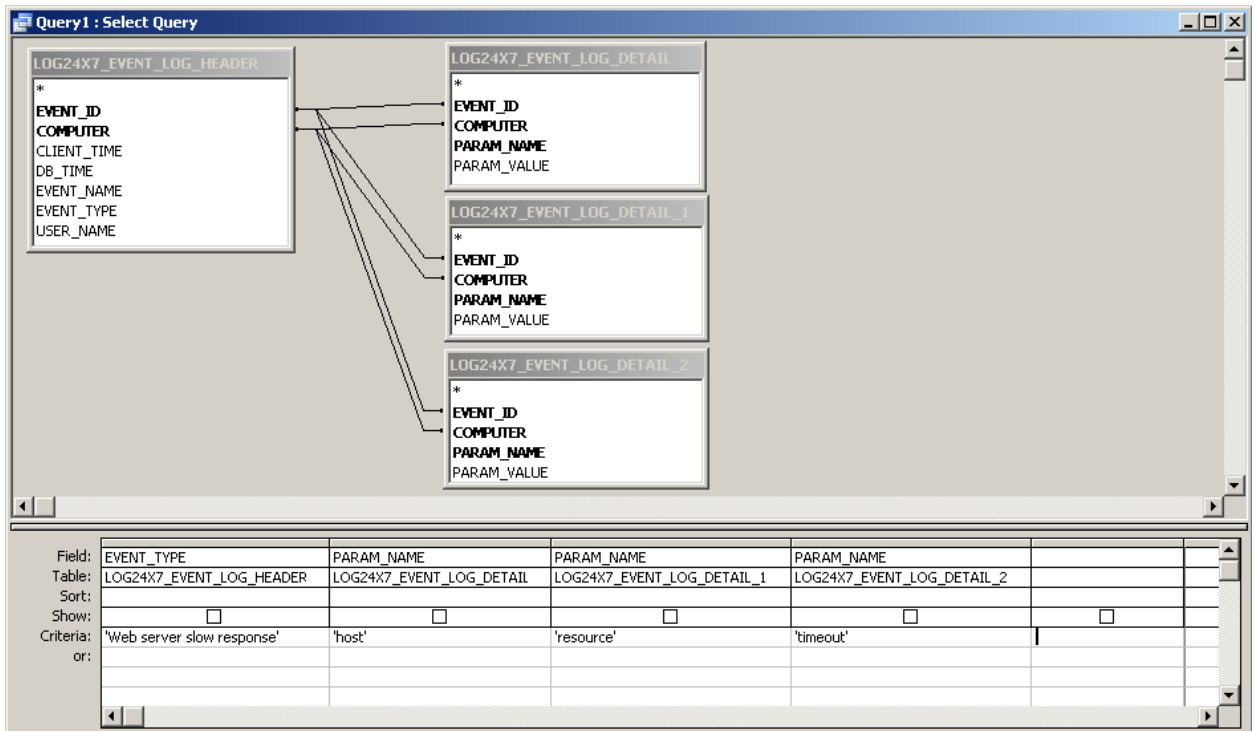
Drag-and-drop **EVENT\_ID** column from the **EVENT\_LOG\_HEADER** table to the **EVENT\_ID** column of the first **EVENT\_LOG\_DETAIL** table. Microsoft Access will draw a line between these 2 columns indicating a SQL JOIN. Drag-and-drop **COMPUTER** column from the **EVENT\_LOG\_HEADER** table to the **COMPUTER** column of the first **EVENT\_LOG\_DETAIL** table. Another line will be displayed. Repeat this for the 2 remaining detail tables. The result should look like as on the following picture.

In the Design Query grid select the first **Field** column and then from the drop-down box with the available field names select **EVENT\_TYPE** from the **EVENT\_LOG\_HEADER** table. Alternatively you can drag-and-drop this column from table box displayed above the grid. Drag-and-drop the **EVENT\_NAME** column from each **DETAIL** table into the **Field** box of the next column.



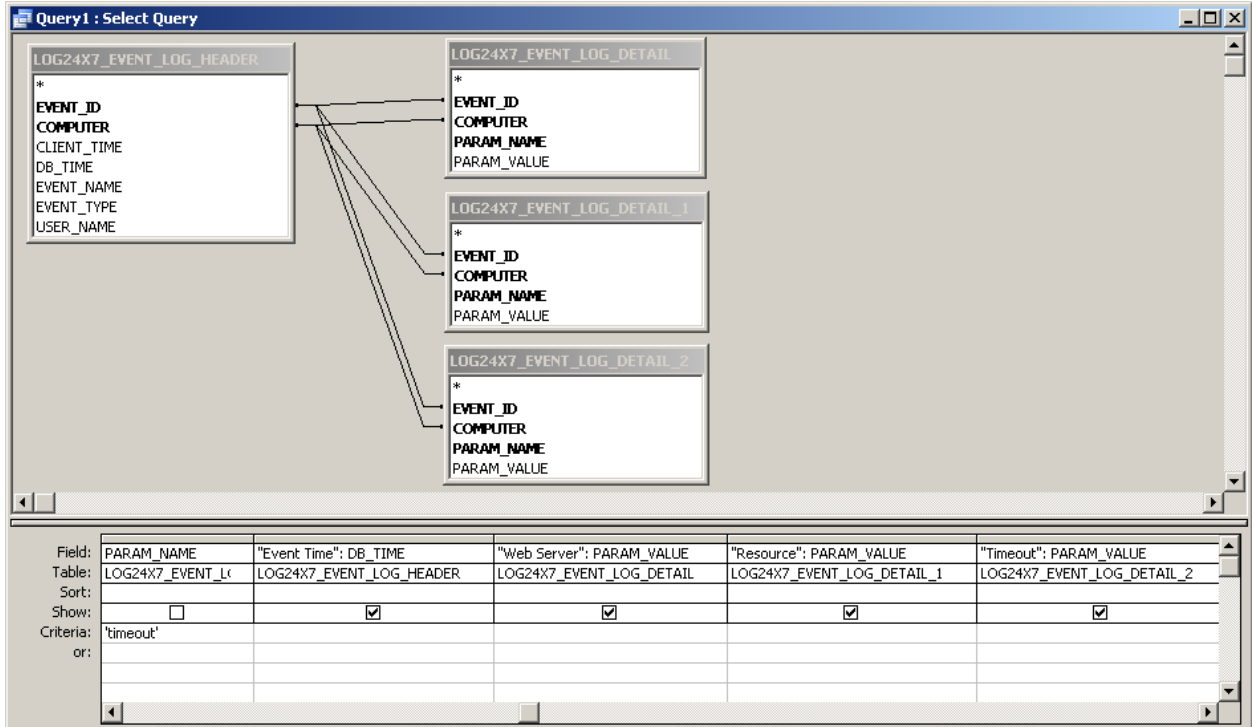


After dragging all 4 columns uncheck the **Show** box in each column and then enter event type ( 'Web server slow response' ) in single quotes into the **Criteria** box of the EVENT\_TYPE column. After that enter sequentially 'host', 'resource', and 'timeout' values into **Criteria** box of PARAM\_NAME columns as on the following picture.



Now you are ready to select which data you want to display on the report. For our example let's display Web server name, monitored resource and used timeout value as well as event time. To do that scroll the Design Query grid to the right and then drag-and-drop DB\_TIME column from the header table to the grid following by PARAM\_VALUE columns from each of the detail tables.

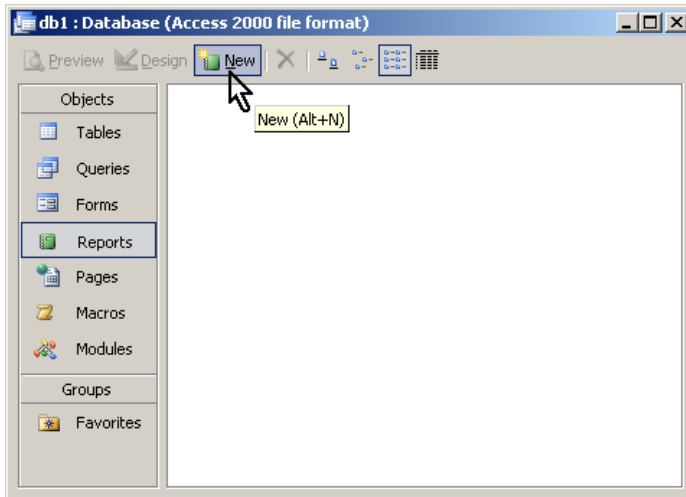
Add column aliases describing actual values instead of default generic column names. For example to rename DB\_TIME column to "Event Time" click on the **Field** cell containing DB\_TIME text and in front of that text type **Event Time:** text. Same way add **Web Server:**, **Resource:** and **Timeout:** text to the next 3 columns. The result should look as on the following picture.



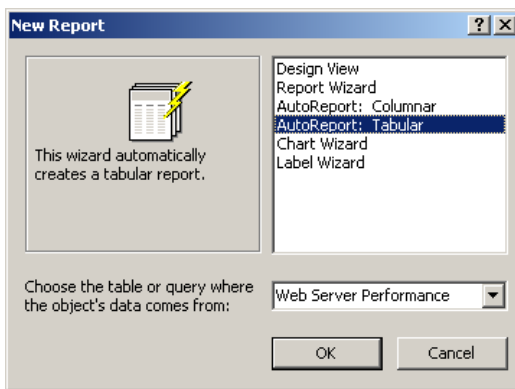
Click the **View/Datasheet View** menu to verify if the created query returns correct results. If you are satisfied click the **File/Close** menu and when prompted to save the created query choose Yes and then when prompted for the query name enter "Web Server Performance" then click the **OK** button to save the created query.

3. Design report layout.

Activate **Reports** View. Click the **New** button. This is the same button that you used in the step 2.




The **New Report** dialog will be displayed. Select **AutoReport: Tabular** in the list box and then select **Web Server Performance** item in the **tables and queries** drop-down box as on the following picture.



Click the **OK** button. Microsoft Access will automatically create new report using your **Web Server Performance** query as a data source and will automatically layout report columns and headers and other elements. Customize report layout as desired. Click **File/Save** menu to save the new report as a complete object that you can run at any time later by simply double-clicking on the report name in the **Reports** View. For information on how to customize report layout see your Microsoft Access manual.

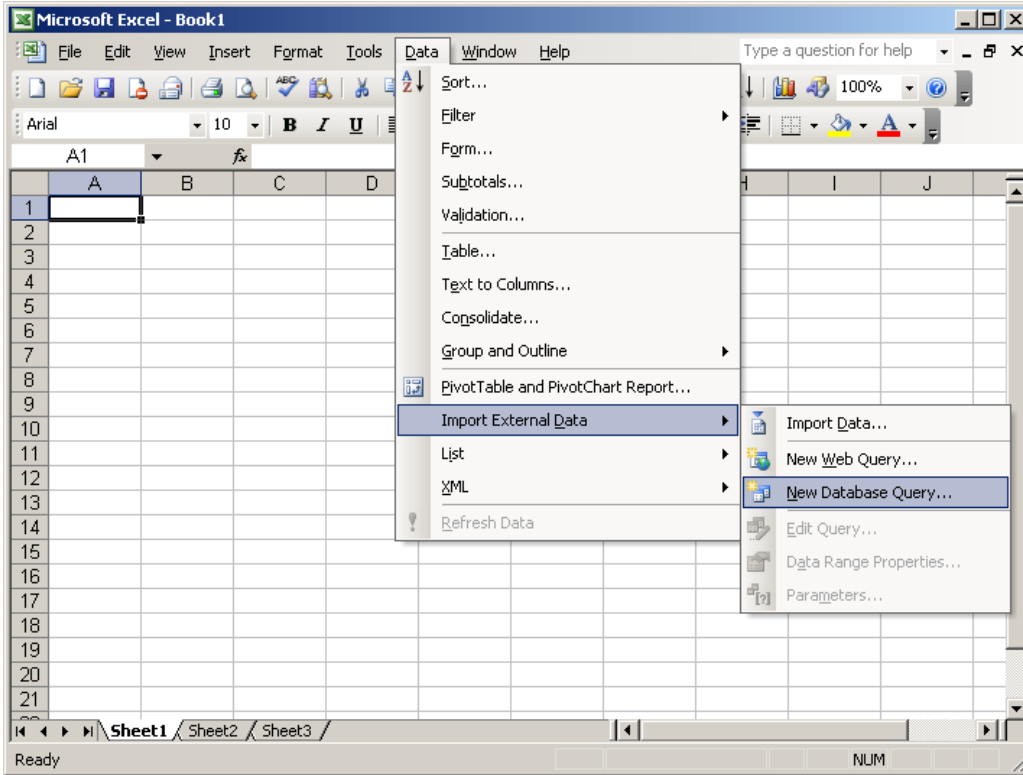
## Microsoft Excel Example

This example demonstrates how to create user-defined report using Microsoft Excel.

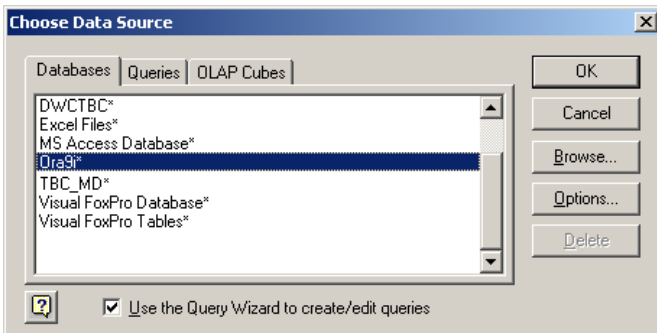
 **Notes:** In different Excel versions names and locations of referenced menu items and options may be different. In order to use Excel as a reporting tool for a relation database you must also have Microsoft Query component installed as part of your Microsoft Office installation.

1. Design SQL Query returning data for your report.

In Microsoft Excel click **Data/Import External Data/New Database Query** menu.

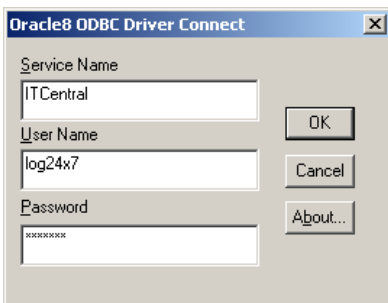


The **Choose Data Source** dialog will appear. The first tab page will display all available ODBC data sources.

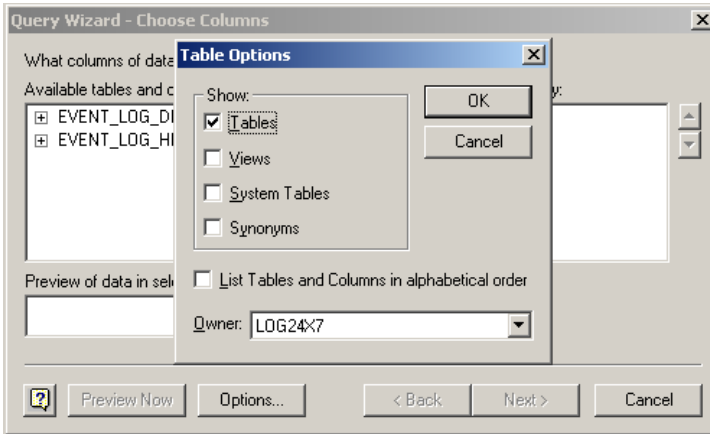


Select name of the ODBC profile for your event log database. Click the **OK** button.

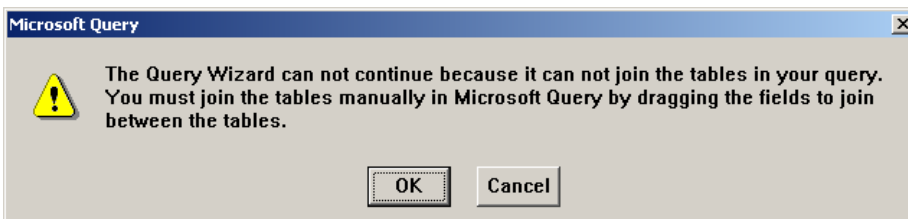
If your database requires user and password for the connection another dialog will appear prompting you to enter the required password for the connection. For example, the following dialog appear when connection to Oracle 9i databases.



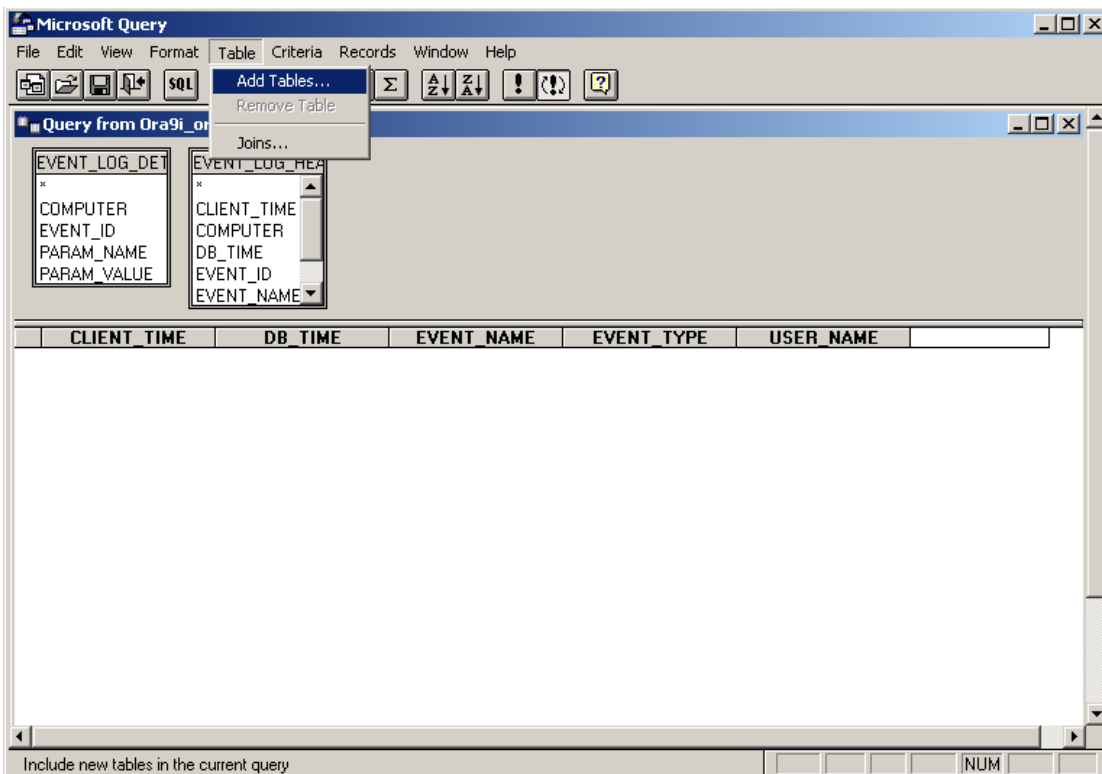
After you click the **OK** button the **Query Wizard – Choose Columns** dialog will appear. Click the **Options** button and choose to display only tables from the LOG24x7 schema or from the other schema where you previously created log tables in the log database.



Select the **EVENT\_LOG\_HEADER** table click the ">" button to select all columns from that table. Repeat this for the **EVENT\_LOG\_DETAIL** table. Click the next button. You should get the following warning:



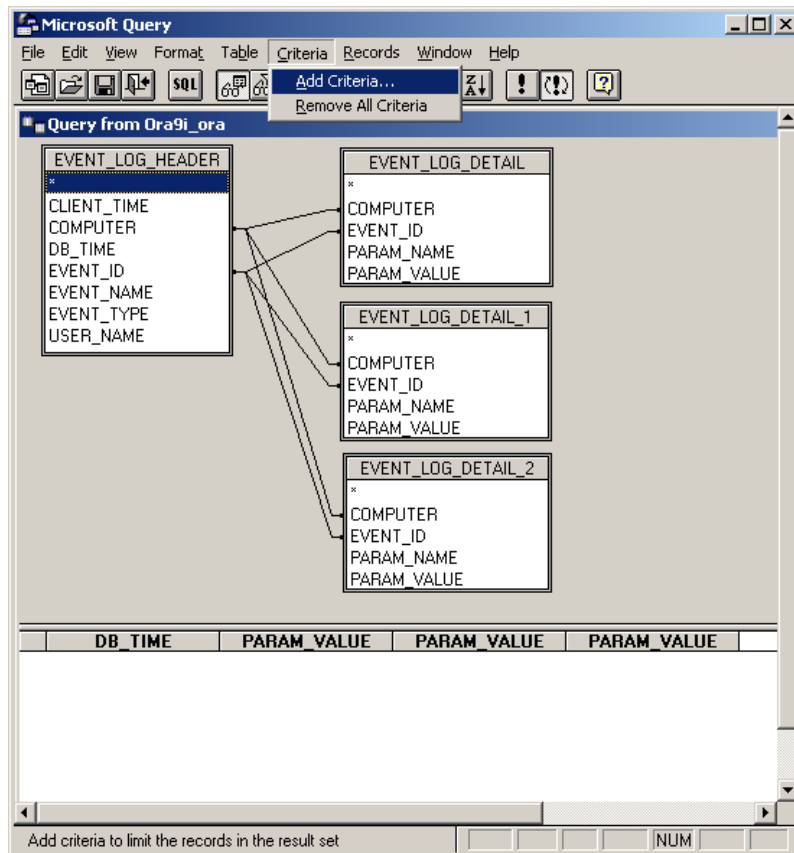
Click the **OK** button to continue. The Microsoft Query window will appear on the screen.



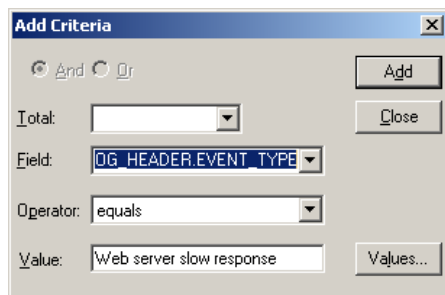
In order to create a report similar to the one described in Microsoft Access example in the previous topic use **Table/Add Tables** menu to add 2 more detail tables. The design steps for a new query in Microsoft Query are similar to design steps in Microsoft Access although the graphical interface is slightly different. Read second step instructions in the previous the Microsoft Access example for more information.

 **Tips:**

- Resize table boxes, workspace and columns so that you can see them completely
- To delete a column from the query display select column header in the bottom part of the Design Query window and then press the Delete key.
- To add columns to the display drag-and-drop columns from the table boxes to the bottom part.
- To join tables drag-and-drop columns from the EVENT\_LOG\_HEADER table to the EVENT\_LOG\_DETAIL table. The result should like on the following picture.



- To enter the report criteria click **Criteria/Add Criteria** menu. The **Add Criteria** dialog will appear.



In the **Field** field select EVENT\_LOG\_HEADER.EVENT\_TYPE and the enter **Web server slow**

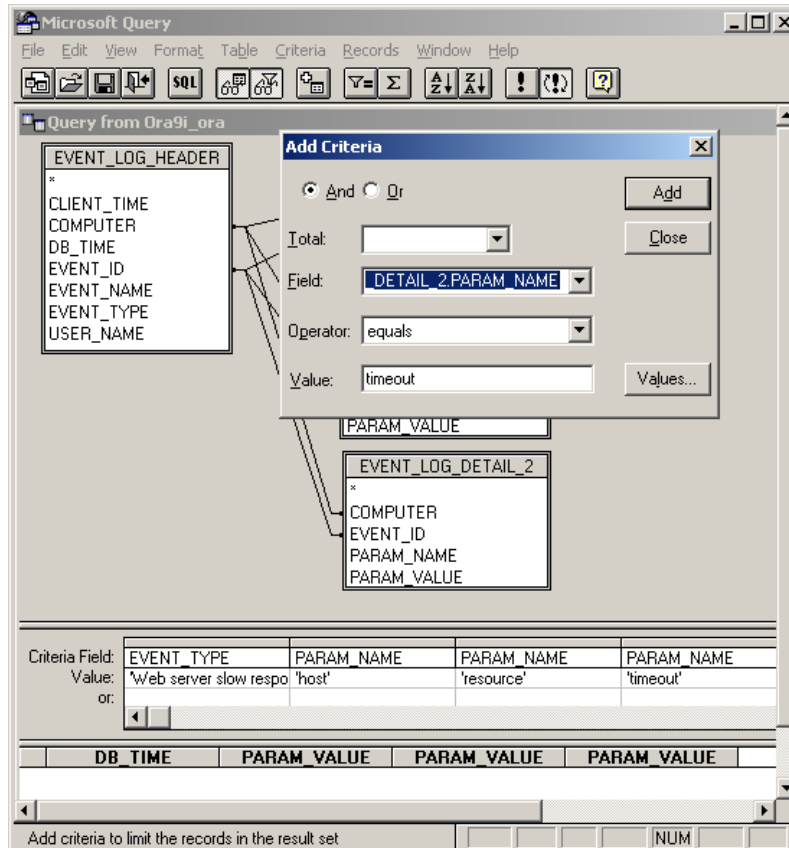
**response** into the **Value** field. Click the **Add** button.

Select **EVENT\_LOG\_DETAIL.PARAM\_NAME** for the field name and **host** for the value. Click the **Add** button.

Select **EVENT\_LOG\_DETAIL\_1.PARAM\_NAME** for the field name and **resource** for the value. Click the **Add** button.

Select **EVENT\_LOG\_DETAIL\_2.PARAM\_NAME** for the field name and **timeout** for the value. Click the **Add** button.

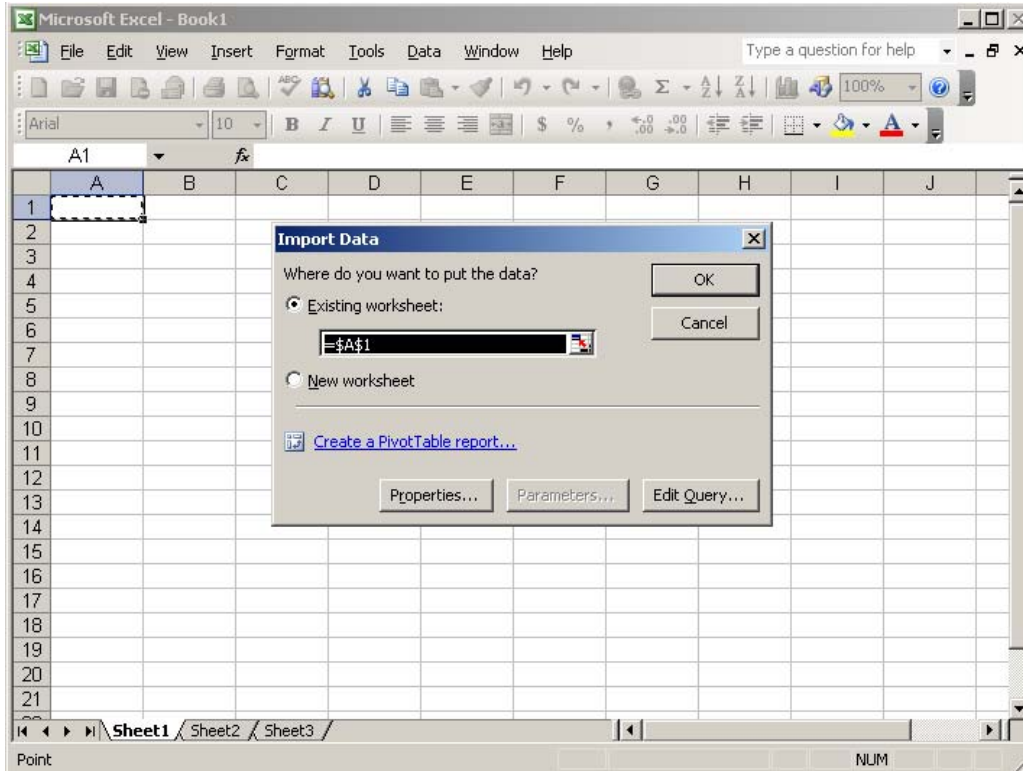
The result should look like on the following picture:



Click the **Close** button. You are done with the query design and you can now close the Microsoft Query window.

2. Select place where you want to display reports data.

After the Microsoft Query window is closed Microsoft Excel will prompt you to select report data location. If you are creating a new report simply click the **OK** button and Microsoft Excel will start with the first cell \$A\$1.



### 3. Customize report display options.

You can now customize report display. Pick desired data formats, alignments, resize columns and headers rows as needed. Customize report layout as desired. Click **File/Save** menu to save the new report as an Excel file. For information on how to customize Excel see your Microsoft Excel manual.




## CHAPTER 4: Event Monitors and Filters

### Event Monitor Methods


24x7 Event Server supports two event-monitoring methods:

- Real-time event monitoring
- Periodic event polling

Real-time event monitors are implemented using system-level drivers and notification hooks. They trigger associated response actions during event occurrences.





 **Tip:** Real-time event monitors act as an integral part of the operation system. They allocate persistent system resource, which may affect the overall system performance. Running small number of real-time event monitors normally provides low overhead and should not cause any performance problems while running large number of real-time monitors on a slow-processor system may significantly affect your system performance. Systems with faster processors can run real-time event monitors faster and so they can run more event monitors than slower systems. Consider upgrading to a faster system if you experience significant performance issues.















Event-polling monitors are implemented as multithreaded processes, which periodically run and check event conditions. Event-polling monitors trigger associated response actions when they find event conditions satisfied. Because of the periodic polling method there could be time lag between time of event occurrence and time of event detection.













 **Tip:** Event-polling monitors run periodically. They affect system performance during event condition checking times only. Between checks all event-polling monitors remain in an efficient sleep mode. Using low event checking frequency decreases the system performance hit. On the other hand, using higher event checking frequency decreases event response latency (time between event occurrence and event detection). When choosing event checking frequencies use balanced approach to achieve optimal system performance and acceptable latency. A balanced system takes into account the needs of the applications and matches them with available computing power.






### Event Monitor Types

The following table describes event types based on event functional purpose. For detailed descriptions of event monitors and supported filters see their named event topics. If you are reading this document on-line you can click on the event monitor name to jump to the linked topic.

| Category   | Event Type   | Method  | Brief Description                                 |
|--|--|---------|---|
|  <b>File system</b> |  |         |   |
|  |  <a href="#">New file</a>                   | Polling | Appearance of a new file in the monitored folder. |
|  |  <a href="#">File deletion</a>              | Polling | Disappearance of a file in the monitored folder.  |
|  |  <a href="#">File change (size or time)</a> | Polling | Change of a file in the monitored folder.         |

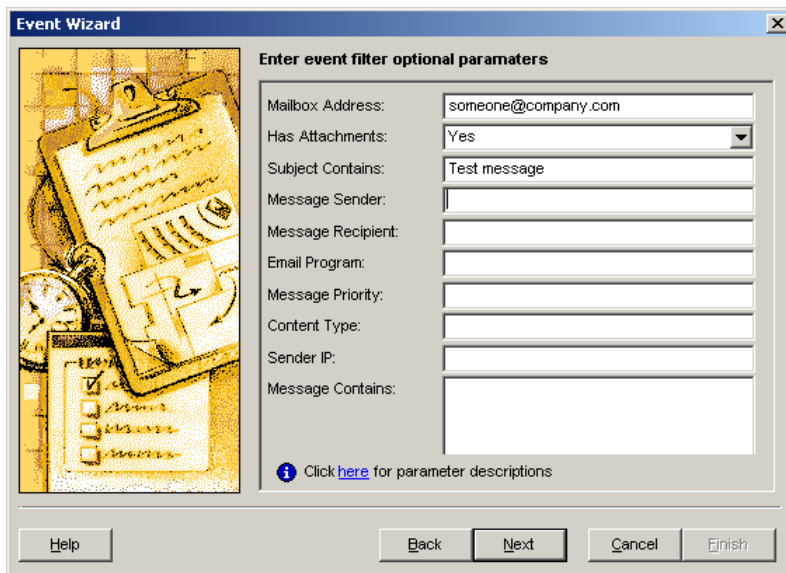
|  |           |  |
|--|-----------|--|
|  <a href="#">File size threshold</a>                                  | Polling   | Size of a file reaches or exceeds certain value.   |
|  <a href="#">Folder changes (generic event)</a>                       | Polling   | Creation, deletion, or change of a file contents or file attributes in the monitored folder.   |
|  <b>NT event logs and text logs</b>                                   |           |  |
|  <a href="#">New NT event log record</a>                              | Polling   | New record added to the monitored Windows NT Event Log file.   |
|  <a href="#">NT event log size threshold</a>                          | Polling   | Size of the monitored Windows NT Event Log file reaches certain value.   |
|  <a href="#">New text log file record</a>                             | Polling   | New record added to the monitored text-based log file.   |
|  <a href="#">Text log file size threshold</a>                         | Polling   | Size of the monitored text log file reaches certain value.   |
|  <b>SNMP traps</b>  |           |  |
|  <a href="#">New SNMP trap</a>  | Real-time | Receiving of a SNMP trap.  |
|  <b>System performance</b>  |           |  |
|  <a href="#">System performance threshold (CPU, disk I/O, etc...)</a> | Polling   | Current value of a Windows Performance Counter (such as CPU usage, disk I/O, ASP errors, etc...) crosses threshold value and constantly remains below or above that value during user specified time interval. |
|  <a href="#">Disk free space threshold</a>                          | Polling   | The event is triggered when the amount of free space on the monitored disk drops below user specified threshold value and constantly remains below that value during at least 10 seconds.                      |
|  <b>Database</b>  |           |  |
|  <a href="#">DATABASE DOWNTIME</a>                                  | Polling   | A database becomes not available (i.e. database connection fails)  |
|  <a href="#">Database startup</a>                                   | Polling   | A database becomes available (i.e. database connection stops failing and can be now established)   |
|  <a href="#">Database data change</a>                               | Polling   | Value returned by a user supplied SQL query changes from between runs.   |
|  <a href="#">Database performance threshold</a>                     | Polling   | Database performance metric reaches certain threshold.   |
|  <b>Email and fax</b>   |           |  |
|  <a href="#">New e-mail message received</a>                        | Polling   | Appearance of a new email message in the specified mailbox.  |
|  <a href="#">New fax message received</a>                           | Polling   | A fax message is received through the local Windows Fax Server.  |
|  <a href="#">New fax message sent</a>                               | Polling   | A new fax message is sent through the local Windows Fax Server.  |

|   |           |  |
|---|-----------|--|
|  <b>Processes and services</b>   |           |  |
|  <a href="#">Process start</a>   | Real-time | Start of a Windows process.  |
|  <a href="#">Process termination</a>                                       | Real-time | Termination of a Windows process.  |
|  <a href="#">Process hung</a>  | Polling   | Hanging of a Windows process.  |
|  <a href="#">Process crash</a>   | Polling   | Crashing of a process generating a Dr. Watson error message.                                       |
|  <a href="#">Dr. Watson error</a>  | Polling   | Crashing of a process generating a Dr. Watson error message  |
|  <a href="#">NT Service start</a>  | Polling   | Start of a Windows NT service.   |
|  <a href="#">NT Service stop</a>   | Polling   | Stop of a Windows NT service.  |
|  <b>System registry</b>  |           |  |
|  <a href="#">Registry changes</a>  | Polling   | Changes in the system registry.  |
|  <b>Network and Internet</b>   |           |  |
|  <a href="#">New SysLog message</a>  | Real-time | New syslog message received.   |
|  <a href="#">User logon (network user logon)</a>                          | Polling   | A user's logon to the local computer.  |
|  <a href="#">User logout (network user logout)</a>                       | Polling   | A user's logoff from the local computer.   |
|  <a href="#">TCP service downtime (remote FTP, Telnet, HTTP, etc...)</a> | Polling   | TCP/IP-based service is not available.   |
|  <a href="#">Web server slow response (HTTP request)</a>                 | Polling   | Unavailability or unacceptable performance of the monitored resource on the monitored HTTP-server. |
|  <a href="#">Server downtime</a>   | Polling   | Server computer or net service is not available.   |
|  <a href="#">Dial-up connection start</a>                                | Real-time | Start of a dial-up or RAS connection.  |
|  <a href="#">Dial-up connection termination</a>                          | Real-time | Termination of a dial-up or RAS connection.  |
|  <b>Logout and shutdown</b>  |           |  |
|  <a href="#">System shutdown</a>   | Real-time | Initiation of the system shutdown process.   |
|  <b>Graphical interface</b>  |           |  |
|  <a href="#">Window appearance</a>                                       | Polling   | Appearance of a new graphical window on the screen.  |

|   |           |   |
|---|-----------|---|
|  <a href="#">Window disappearance</a>                            | Polling   | Disappearance of a graphical window from the screen.  |
|  <a href="#">Screen saver activation</a>                         | Polling   | Activation a password-protected screen-saver.   |
|  <a href="#">Screen saver deactivation</a>                       | Polling   | Deactivation a password-protected screen-saver  |
| <b>WMI event monitors</b>   |           |   |
|  <a href="#">WMI event</a>                                       | Real-time | Change of a system parameter, creation of a process, addition of a new event log record, etc... Event type is determined by the user-defined WMI query. |
| <b>Custom event monitors</b>  |           |   |
|  <a href="#">Custom event monitor (script, batch or program)</a> | Polling   | User-defined event monitor  |

## Event Filters


Each event monitor has a set of properties (called filters) that are associated with it. These properties differ for different event types. Depending on the complexity of the event monitor there could just a few or there could be many properties available for use as event filters. 24x7 Event Server uses standard “AND” Boolean logic for evaluating event filters. For example, if event filter properties A, B and D are specified and properties C and E are left blank the 24x7 Event Server will trigger associated event actions when it evaluates that event conditions satisfy all A and B and D properties while conditions for C and E are not evaluated and could be any. Below is a sample dialog page containing filters for “New Email” Event Monitor.



Event filters can be used to specify which events to ignore and which events to process. Multiple event monitors with different event filters can be setup for the same event type. Virtually in all events all filter properties are optional. For unspecified filter properties 24x7 Event Server either uses a default value or assumes that any value is good for the event. The actual behavior depends on the property type. For example, if you leave the "Duration" property blank in the Process Hanging event monitor, the 24x7 Event Server will use the default value of 10 seconds. If you leave the

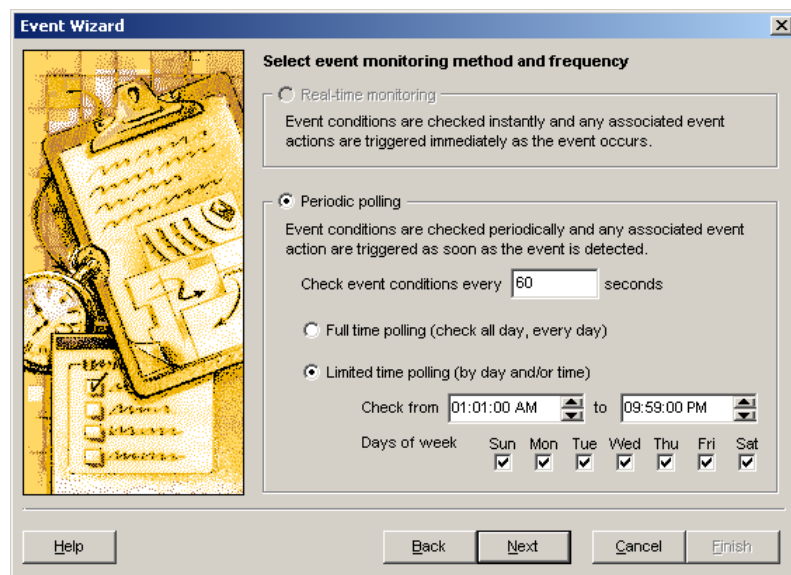
"Process Module Name" property blank, the 24x7 Event Server will assume that any hanged process should trigger event response actions for such event.

Be aware that if you can configure multiple event monitors with filters overlapping each other all these events will be processed simultaneously and all associated event actions will be triggered at the same time, which potentially can cause double processing, concurrent file access locks, and other undesired effects. For example, if you create 2 Window Watcher events, one with a filter to monitor window appearances whose caption contains word "Microsoft \*" and another event with a filter to monitor window appearances whose caption contains word "\* Word" and then start Microsoft Word program you will end up with both events firing their associated event actions at the same time.

 **Tip:** When creating events and entering event filter properties try to be as specific as possible. Too broad filters definitions (filters with many properties left blank) may cause the system to react to a large number of unnecessary events causing unnecessary event processing.

## Event Monitor Schedules


Event monitors based on the polling method support time schedules specifying what days/hours the monitor should run. This can be handy in avoiding false event detection and responses during event blackout times. For example if you want to monitor your database availability using Database State monitor and your database is shutdown every night from 10:00 PM to 1:00 AM for a cold backup you can schedule this monitor to run only between 1:01 AM and 9:59 PM. Below is a sample dialog page for such schedule.



The **Event check** is used to specify how often you want 24x7 Event Server to check for event conditions. This is also called "polling interval". Specify this value in seconds.


Use the **Full time polling** option for events that must be checked all day every day. If this option is selected there are no other options that need to be configured.

Use the **Limited time polling** option for events that should be checked periodically on certain days and times only. If this option is selected you can then configure event-checking start and end time using **Check from** and **Check to** edit fields.

 **Note:** Time entered in the **Check from** field must be less then time entered in **Check to** field (for example, 1:00 AM to 5:00 AM). In case if you need to specify a time interval that starts on one day and ends on the next day (for

example, 8:00 PM to 6:00 AM) create 2 separate event monitors, one for the first day (for example, from 8:00 PM to 11:59 PM) and another for the second day (for example, from 12:00 AM to 6:00 AM)

Use the **Days of week** options to select days of week when you want to run the event monitor.

 **Note:** Within the same event monitor you cannot use different **Check from** and **Check to** values for different days of week. In case if you want to check an event during different times on different days of week create as many separate event monitors as many time intervals you need.

## Real-Time Events

The following event types use notification-based real-time event monitors.


### Process start

**Event Type:** ProcessEvent.

**Event Description:** Start of a Windows process.

**Event Filter Properties:**

| Property            | Required?                           | Fixed?                              | Description  |
|---------------------|-------------------------------------|-------------------------------------|--|
| Process Module Name | <input type="checkbox"/>            | <input type="checkbox"/>            | Name of the executable file without path. If the file name is not specified then event response action is fired for every newly started process. |
| Event Type          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Process event type. This property cannot be modified and is always set to "start."   |

 **Tip:** [WMI Event](#) type can be also used to monitor for process start and termination.


### Process termination

**Event Type:** ProcessEvent.

**Event Description:** Termination of a Windows process.

**Event Filter Properties:**

| Property            | Required?                           | Fixed?                              | Description   |
|---------------------|-------------------------------------|-------------------------------------|---|
| Process Module Name | <input type="checkbox"/>            | <input type="checkbox"/>            | Name of the executable file without path. If the file name is not specified then event response action is fired for every terminated process. |
| Event Type          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Process event type. This property cannot be modified and is always set to "stop."   |

 **Tip:** [WMI Event](#) type can be also used to monitor for process start and termination.

### Dial-up connection start

**Event Type:** RasConnect

**Event Description:** Start of a dial-up or RAS connection.

**Event Filter Properties:**

| Property       | Required?                           | Fixed?                              | Description   |
|----------------|-------------------------------------|-------------------------------------|---|
| RAS Entry Name | <input type="checkbox"/>            | <input type="checkbox"/>            | RAS connection name (as it appears in the Network and Dial-up Connections folder). If the name is not specified then event response action is fired for every newly started connection. |
| Event Type     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connection event type. This property cannot be modified and is always set to "connected."   |



**Tip:** [WMI Event](#) type can be also used to monitor for connection state changes.

**Dial-up connection termination**

**Event Type:** RasConnect

**Event Description:** Termination of a dial-up or RAS connection.

**Event Filter Properties:**

| Property       | Required?                           | Fixed?                              | Description  |
|----------------|-------------------------------------|-------------------------------------|--|
| RAS Entry Name | <input type="checkbox"/>            | <input type="checkbox"/>            | RAS connection name (as it appears in the Network and Dial-up Connections folder). If the name is not specified then event response action is fired for every terminated connection. |
| Event Type     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Connection event type. This property cannot be modified and is always set to "disconnected."   |



**Tip:** [WMI Event](#) type can be also used to monitor for connection state changes.

**New SNMP trap**

**Event Type:** SNMPTrap

**Event Description:** Receiving of a SNMP trap

**Event Filter Properties:**

| Property       | Required?                | Fixed?                   | Description  |
|----------------|--------------------------|--------------------------|--|
| Generic Trap   | <input type="checkbox"/> | <input type="checkbox"/> | Indicator of a generic trap. If not specified, any trap with and without this indicator can fire event response actions.   |
| Specific Trap  | <input type="checkbox"/> | <input type="checkbox"/> | Indicator of a specific trap. If not specified, any trap with and without this indicator can fire event response actions.  |
| Enterprise OID | <input type="checkbox"/> | <input type="checkbox"/> | The OID of the enterprise that generated the SNMP trap. If not specified, any trap can fire event response actions.  |
| Source IP      | <input type="checkbox"/> | <input type="checkbox"/> | IP address of the agent that generated the trap. This information is retrieved from the network transport. If not specified, trap from any source can fire event response actions. |

|           |                          |                          |   |
|-----------|--------------------------|--------------------------|---|
| Agent IP  | <input type="checkbox"/> | <input type="checkbox"/> | IP address of the agent that generated the SNMP trap (this information is retrieved from the SNMP protocol data unit PDU). If not specified, trap from any agent can fire event response actions. |
| Community | <input type="checkbox"/> | <input type="checkbox"/> | Community string of the generated SNMP trap. If not specified, trap with any community string can fire event response actions.  |
| Variables | <input type="checkbox"/> | <input type="checkbox"/> | Partial or full values of trap variables. If not specified, trap with any message and variables can fire event response actions.  |

### New SysLog record

**Event Type:** SyslogEvent

**Event Description:** New record added to Unix/Linux syslog.

**Event Filter Properties:**

| Property        | Required?                                | Fixed?                   | Description  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
|-----------------|--|--------------------------|--|-----------------|-------------|---|-----------------|---|---------------------|---|-------------|---|----------------|---|---------------------------------|---|--|---|------------------------|---|------------------------|---|----------------|---|--------------|----|---------------------------------|----|------------|----|---------------|----|-----------|
| Event Source    | <input type="checkbox"/>                 | <input type="checkbox"/> | Event computer or device (such as routers, switches, firewalls, etc..) that generated this event. You can use standard wildcard symbols for LIKE filters. If not specified, any event computer can fire event response actions. An empty value is the same as using "*" wildcard.  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| Event Address   | <input type="checkbox"/>                 | <input type="checkbox"/> | UDP address of the computer or device from where the event has been forwarded, This value must be specified in <IP address>:<port> format, for example, 198.162.0.10:514<br><br>If not specified, any syslog producer forwarding syslog messages using standard syslog port 514 can fire event response actions.   |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| Event Facility  | <input type="checkbox"/>                 | <input type="checkbox"/> | Message facility number as it appears in the syslog. If not specified, syslog message with any facility can fire event response actions.<br><br>Below is a list of standard Unix/Linux facilities <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>Facility Number</th> <th>Description</th> </tr> </thead> <tbody> <tr><td>0</td><td>kernel messages</td></tr> <tr><td>1</td><td>user-level messages</td></tr> <tr><td>2</td><td>mail system</td></tr> <tr><td>3</td><td>system daemons</td></tr> <tr><td>4</td><td>security/authorization messages</td></tr> <tr><td>5</td><td>messages generated internally by syslogd</td></tr> <tr><td>6</td><td>line printer subsystem</td></tr> <tr><td>7</td><td>network news subsystem</td></tr> <tr><td>8</td><td>UUCP subsystem</td></tr> <tr><td>9</td><td>clock daemon</td></tr> <tr><td>10</td><td>security/authorization messages</td></tr> <tr><td>11</td><td>FTP daemon</td></tr> <tr><td>12</td><td>NTP subsystem</td></tr> <tr><td>13</td><td>log audit</td></tr> </tbody> </table> | Facility Number | Description | 0 | kernel messages | 1 | user-level messages | 2 | mail system | 3 | system daemons | 4 | security/authorization messages | 5 | messages generated internally by syslogd | 6 | line printer subsystem | 7 | network news subsystem | 8 | UUCP subsystem | 9 | clock daemon | 10 | security/authorization messages | 11 | FTP daemon | 12 | NTP subsystem | 13 | log audit |
| Facility Number | Description                              |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 0               | kernel messages                          |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 1               | user-level messages                      |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 2               | mail system                              |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 3               | system daemons                           |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 4               | security/authorization messages          |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 5               | messages generated internally by syslogd |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 6               | line printer subsystem                   |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 7               | network news subsystem                   |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 8               | UUCP subsystem                           |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 9               | clock daemon                             |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 10              | security/authorization messages          |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 11              | FTP daemon                               |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 12              | NTP subsystem                            |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |
| 13              | log audit                                |                          |  |                 |             |   |                 |   |                     |   |             |   |                |   |                                 |   |  |   |                        |   |                        |   |                |   |              |    |                                 |    |            |    |               |    |           |



|                        |  |                          | <table border="1"> <tr><td>14</td><td>log alert</td></tr> <tr><td>15</td><td>clock daemon</td></tr> <tr><td>16</td><td>local use 0 (local0)</td></tr> <tr><td>17</td><td>local use 1 (local1)</td></tr> <tr><td>18</td><td>local use 2 (local2)</td></tr> <tr><td>19</td><td>local use 3 (local3)</td></tr> <tr><td>20</td><td>local use 4 (local4)</td></tr> <tr><td>21</td><td>local use 5 (local5)</td></tr> <tr><td>22</td><td>local use 6 (local6)</td></tr> <tr><td>23</td><td>local use 7 (local7)</td></tr> </table>  | 14       | log alert   | 15 | clock daemon                  | 16 | local use 0 (local0)                    | 17 | local use 1 (local1)          | 18 | local use 2 (local2)    | 19 | local use 3 (local3)        | 20 | local use 4 (local4)                     | 21 | local use 5 (local5)                  | 22 | local use 6 (local6)        | 23 | local use 7 (local7) |
|------------------------|--|--------------------------|---|----------|-------------|----|-------------------------------|----|---|----|-------------------------------|----|-------------------------|----|-----------------------------|----|--|----|---------------------------------------|----|-----------------------------|----|----------------------|
| 14                     | log alert                                |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 15                     | clock daemon                             |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 16                     | local use 0 (local0)                     |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 17                     | local use 1 (local1)                     |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 18                     | local use 2 (local2)                     |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 19                     | local use 3 (local3)                     |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 20                     | local use 4 (local4)                     |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 21                     | local use 5 (local5)                     |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 22                     | local use 6 (local6)                     |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 23                     | local use 7 (local7)                     |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| Event Severity         | <input type="checkbox"/>                 | <input type="checkbox"/> | <p>Event severity level as it appears in the syslog.</p> <p>If not specified, message with any severity can fire event response actions.</p> <p>Below is a list of message severity levels</p> <table border="1"> <thead> <tr> <th>Severity</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Emergency: system is unusable</td> </tr> <tr> <td>1</td> <td>Alert: action must be taken immediately</td> </tr> <tr> <td>2</td> <td>Critical: critical conditions</td> </tr> <tr> <td>3</td> <td>Error: error conditions</td> </tr> <tr> <td>4</td> <td>Warning: warning conditions</td> </tr> <tr> <td>5</td> <td>Notice: normal but significant condition</td> </tr> <tr> <td>6</td> <td>Informational: informational messages</td> </tr> <tr> <td>7</td> <td>Debug: debug-level messages</td> </tr> </tbody> </table> | Severity | Description | 0  | Emergency: system is unusable | 1  | Alert: action must be taken immediately | 2  | Critical: critical conditions | 3  | Error: error conditions | 4  | Warning: warning conditions | 5  | Notice: normal but significant condition | 6  | Informational: informational messages | 7  | Debug: debug-level messages |    |                      |
| Severity               | Description                              |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 0                      | Emergency: system is unusable            |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 1                      | Alert: action must be taken immediately  |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 2                      | Critical: critical conditions            |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 3                      | Error: error conditions                  |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 4                      | Warning: warning conditions              |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 5                      | Notice: normal but significant condition |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 6                      | Informational: informational messages    |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| 7                      | Debug: debug-level messages              |                          |   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |
| Event Message Contains | <input type="checkbox"/>                 | <input type="checkbox"/> | Text to search in the event message. If not specified, any event can fire event response actions.   |          |             |    |                               |    |   |    |                               |    |                         |    |                             |    |  |    |                                       |    |                             |    |                      |



**Notes:**

- 24x7 Event Server listens for syslog messages sent to the 24x7 Event Server computer on UDP port 514.
- **IMPORTANT:** You must configure system loggers on your devices and Unix/Linux computers to forward syslog messages to the computer running 24x7 Event Server. By default **syslogd** will not forward messages. See the following **Tip** section for instructions on how to configure the forwarding.
- All messages are processed as defined by the section “4.3 Relayed syslog Packets” of the RFC3164 <http://www.ietf.org/rfc/rfc3164.txt>
- Syslog message priorities can be calculated using the following formula: Priority = Facility \* 8 + Severity



**Tip: Configuring devices and computers to forward syslog messages**

To forward syslog messages, a device (such as router, switch, firewall, etc...) or a Unix/Linux computer must have an entry in its system logger configuration file **syslog.conf** that maps syslog messages to the IP address of the computer running 24x7 Event Server.

1. If you don't know the IP of the 24x7 Event Server computer run **ipconfig** at a DOS command prompt. This will print the IP address of the computer.

2. Update the `syslog.conf` file on the source device or computer to forward syslog messages to the 24x7 Event Server computer. The `syslog.conf` file must contain an entry for each message type that is forwarded, as well as the IP address of the 24x7 Event Server computer that will receive the syslog messages. In the `syslog.conf` file, tabs separate the message type and the IP address. The message type is of the form `facility.level`, such as `kern.error`, which signifies a kernel error.

Note: A good practice is to forward only selected events to 24x7 Event Server. Therefore, instead of sending all events to 24x7 Event Server, only events with a certain priority level are sent.

The following example sends syslog messages with a priority of **error (or higher)** to the 24x7 Event Server computer identified by the IP address 198.162.0.91:

```
*.err @198.162.0.91
```

The following example sends syslog user messages with a priority of **alert (or higher)** to the 24x7 Event Server computer that has an IP address of 198.162.0.91:

```
user.alert @198.162.0.91
```

Consult your system documentation for additional `syslog.conf` file help

3. **IMPORTANT:** You must restart the system logger daemon (**syslogd**) after changes are made in the `syslog.conf` configuration file. The command to kill and restart the daemon may differ on different systems. Below is a generic command compatible with most Unix systems; this command finds the syslog process ID, and then restart the system logger:

```
ps -A | grep syslog kill -HUP <pid>
```

Consult your source device documentation for additional information about the `syslogd` daemon.

4. Your system is now ready to forward syslog messages to 24x7 Event Server. When the 24x7 Event Server receives the syslog message, the 24x7 Event Server creates an event, applies selected event filters (if any) and if the event is validated as positive, 24x7 Event Server fires the associated event response actions.

**IMPORTANT:** Multiple devices and computers they can forward syslog messages to the same 24x7 Event Server computer.

## System shutdown

**Event Type:** SystemShutdown

**Event Description:** Initiation of the system shutdown process.

**Event Filter Properties:** None.




**Note:** Windows restricts the set of actions that can be performed during system shutdown. Only actions that don't change system state can be used with this event monitor. For example, it's possible to write to a file but it's impossible to start a new process/application.

## 24x7es

**Event Type:** 24x7es

**Event Description:** 24x7 Administrative Event. 24x7 Event Server generates this event internally whenever system errors or other abnormal conditions are detected. This event type is used internally for executing various actions used to notify system administrators about such errors or conditions. To configure notification methods and recipients use System Options as described in [CHAPTER 3, Configuring System Options](#) topic.

There is a close relation between Administrative Event and NT Event Log events. So, Administrative Events have mostly the same properties as "[New NT Event Log](#)" events.

 **Note:** Because this event is an internal event 24x7 Event Server does not provide graphical interface for this event. Event monitors for this event type can be only directly entered to the 24x7 Event Server configuration file. However you **should not modify this file directly** unless you are instructed to do so by SoftTree Technologies technical support.

**Event Filter Properties:**

| Property       | Required?  | Fixed?                   | Description  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
|----------------|--|--------------------------|--|---|---------|----|---|----|---|----|---|----|-------------------------------|----|--|----|---|----|------------------------------|----|---|----|----------------------------|----|----------------------------|----|-----------------------------|----|-----------------------------------|----|---------------------------------------|
| Event ID       | <input type="checkbox"/>   | <input type="checkbox"/> | <p>Event number as it appears in the Windows NT Event Viewer. If not specified, administrative event with any number can fire event response actions. Event number can be one of the following:</p> <table border="1"> <thead> <tr> <th>#</th> <th>Message</th> </tr> </thead> <tbody> <tr> <td>11</td> <td>24x7 Event Server has entered active state.</td> </tr> <tr> <td>12</td> <td>24x7 Event Server has left active state</td> </tr> <tr> <td>13</td> <td>Event monitor ## failed and is being restarted.</td> </tr> <tr> <td>14</td> <td>Evaluation period has expired</td> </tr> <tr> <td>15</td> <td>24x7 Event Server configuration file is corrupted or contains invalid entries.</td> </tr> <tr> <td>16</td> <td>24x7 Event Server configuration file can't be opened.</td> </tr> <tr> <td>17</td> <td>Admin action can't be loaded</td> </tr> <tr> <td>18</td> <td>Event ## can't be loaded and will be ignored.</td> </tr> <tr> <td>19</td> <td>24x7 Event Server started.</td> </tr> <tr> <td>20</td> <td>24x7 Event Server stopped.</td> </tr> <tr> <td>21</td> <td>Event ## has been detected.</td> </tr> <tr> <td>22</td> <td>Event monitor ## failed to start.</td> </tr> <tr> <td>23</td> <td>Action for event ## cant' be executed</td> </tr> </tbody> </table> | # | Message | 11 | 24x7 Event Server has entered active state. | 12 | 24x7 Event Server has left active state | 13 | Event monitor ## failed and is being restarted. | 14 | Evaluation period has expired | 15 | 24x7 Event Server configuration file is corrupted or contains invalid entries. | 16 | 24x7 Event Server configuration file can't be opened. | 17 | Admin action can't be loaded | 18 | Event ## can't be loaded and will be ignored. | 19 | 24x7 Event Server started. | 20 | 24x7 Event Server stopped. | 21 | Event ## has been detected. | 22 | Event monitor ## failed to start. | 23 | Action for event ## cant' be executed |
| #              | Message  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 11             | 24x7 Event Server has entered active state.                                    |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 12             | 24x7 Event Server has left active state  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 13             | Event monitor ## failed and is being restarted.                                |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 14             | Evaluation period has expired  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 15             | 24x7 Event Server configuration file is corrupted or contains invalid entries. |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 16             | 24x7 Event Server configuration file can't be opened.                          |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 17             | Admin action can't be loaded   |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 18             | Event ## can't be loaded and will be ignored.                                  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 19             | 24x7 Event Server started.   |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 20             | 24x7 Event Server stopped.   |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 21             | Event ## has been detected.  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 22             | Event monitor ## failed to start.  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 23             | Action for event ## cant' be executed  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| Event Type     | <input type="checkbox"/>   | <input type="checkbox"/> | <p>Event type as it appears in the Windows NT Event Viewer, one of the following:</p> <ul style="list-style-type: none"> <li>• Information</li> <li>• Warning</li> <li>• Error</li> </ul> <p>If not specified, any event type can fire event response actions.</p>   |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| Event Category | <input type="checkbox"/>   | <input type="checkbox"/> | <p>Event category as it appears in the Windows NT Event Viewer, it could be one of the following:</p> <table border="1"> <thead> <tr> <th>#</th> <th>Message</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Admin Alert</td> </tr> <tr> <td>2</td> <td>Application Alert</td> </tr> </tbody> </table>   | # | Message | 1  | Admin Alert                                 | 2  | Application Alert                       |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| #              | Message  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 1              | Admin Alert  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |
| 2              | Application Alert  |                          |  |   |         |    |   |    |   |    |   |    |                               |    |  |    |   |    |                              |    |   |    |                            |    |                            |    |                             |    |                                   |    |                                       |

|                        |                                     |                                     |   |
|------------------------|-------------------------------------|-------------------------------------|---|
| Event Source           | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Event source is always "24x7 Event Server" and it cannot be changed.  |
| Event Computer         | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Event computer is always the name of the computer running 24x7 Event Server and cannot be changed.                            |
| Event Message Contains | <input type="checkbox"/>            | <input type="checkbox"/>            | Text to search in the event message. For complete list of supported messages see description table for the Event ID property. |


## Polled Events

The following event types use event monitors based on periodic polling of event conditions.

### Windows appearance

**Event Type:** WindowEvent

**Event Description:** Appearance of a new graphical window on the screen. The event is detected both when a new window is created and then displayed and when an existing previously hidden window is un-hidden and displayed on the screen.

 **Note:** On Windows NT 4 and Windows 2000 only windows of the local logon session are monitored. On Windows XP and Windows 2003 only windows of first connected user (either local or remote) are monitored.

#### Event Filter Properties:


| Property            | Required?                | Fixed?                   | Description  |
|---------------------|--------------------------|--------------------------|--|
| Process Module Name | <input type="checkbox"/> | <input type="checkbox"/> | The module name of the window owner process (name of the main program file not including path). If not specified, any process can fire event response actions.   |
| Window Class        | <input type="checkbox"/> | <input type="checkbox"/> | The class name of the window. Every window belongs to a certain window class. For example class name of the main Windows Explorer window is "ExploreWClass."<br><br>Window class names are usually defined by programmers who developed the program displaying the window. If you don't have access to the program source code you can use any available debugging tool or Process Spy utility to find out class name of any displayed window. Such Spy utilities are usually provided with C++ compilers and some other development tools.<br><br>If not specified, any window class can fire event response actions. |
| Window Text         | <input type="checkbox"/> | <input type="checkbox"/> | The caption text of the window. If not specified, window with any text event response actions.   |
| Child               | <input type="checkbox"/> | <input type="checkbox"/> | Indicator of the window type: top-level or child. Specify "0" value to monitor top-level windows only; specify "1" to monitor child windows only.  |

|            |                                     |                                     |  |
|------------|-------------------------------------|-------------------------------------|--|
|            |                                     |                                     | If not specified, both top-level and child windows can trigger event response actions. |
| Event Type | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Window event type. This property cannot be modified and is always set to "show"        |

## Windows disappearance

**Event Type:** WindowEvent

**Event Description:** Disappearance of a graphical window from the screen. The event is detected both when a window is closed and destroyed and when a window is hidden (made invisible) from the screen but remains loaded into computer memory. Do not confuse this event with events when a window is overlapped by other windows and because of that is not visible on the screen.

 **Note:** On Windows NT 4 and Windows 2000 only windows of the local logon session are monitored. On Windows XP and Windows 2003 only windows of first connected user (either local or remote) are monitored.

### Event Filter Properties:

| Property            | Required?                           | Fixed?                              | Description  |
|---------------------|-------------------------------------|-------------------------------------|--|
| Process Module Name | <input type="checkbox"/>            | <input type="checkbox"/>            | The module name of the window owner process (name of the main program file not including path). If not specified, any process can fire event response actions.   |
| Window Class        | <input type="checkbox"/>            | <input type="checkbox"/>            | The class name of the window. Every window belongs to a certain window class. For example class name of the main Windows Explorer window is "ExploreWClass."<br><br>Window class names are usually defined by programmers who developed the program displaying the window. If you don't have access to the program source code you can use any available debugging tool or Process Spy utility to find out class name of any displayed window. Such Spy utilities are usually provided with C++ compilers and some other development tools.<br><br>If not specified, any window class can fire event response actions. |
| Window Text         | <input type="checkbox"/>            | <input type="checkbox"/>            | The caption text of the window. If not specified, window with any text event response actions.   |
| Child               | <input type="checkbox"/>            | <input type="checkbox"/>            | Indicator of the window type: top-level or child. Specify "0" value to monitor top-level windows only; specify "1" to monitor child windows only.<br><br>If not specified, both top-level and child windows can trigger event response actions.  |
| Event Type          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Window event type. This property cannot be modified and is always set to "hide"  |

## Screen saver activation

**Event Type:** ScrSaverActive

**Event Description:** Activation of a password-protected screen-saver.

**Event Filter Properties:**

| Property   | Required?                           | Fixed?                              | Description   |
|------------|-------------------------------------|-------------------------------------|---|
| Event Type | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Screen-saver event type. This property cannot be modified and is always set to "active" |

## Screen saver deactivation

**Event Type:** ScrSaverActive

**Event Description:** Deactivation of a password-protected screen-saver.

**Event Filter Properties:**

| Property   | Required?                           | Fixed?                              | Description   |
|------------|-------------------------------------|-------------------------------------|---|
| Event Type | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Screen-saver event type. This property cannot be modified and is always set to "inactive" |

## Service start

**Event Type:** ServiceEvent

**Event Description:** Start of a Windows NT service.

**Event Filter Properties:**

| Property     | Required?                           | Fixed?                              | Description   |
|--------------|-------------------------------------|-------------------------------------|---|
| Service Name | <input type="checkbox"/>            | <input type="checkbox"/>            | The service display name as it appears in the Control Panel's Service applet. If not specified, start of any service can fire event response actions. |
| Event Type   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Service event type. This property cannot be modified and is always set to "start"   |



**Tip:** [WMI Event](#) type can be also used to monitor for service state changes.

## Service stop

**Event Type:** ServiceEvent

**Event Description:** Stop of a Windows NT service.

**Event Filter Properties:**

| Property     | Required?                           | Fixed?                              | Description  |
|--------------|-------------------------------------|-------------------------------------|--|
| Service Name | <input type="checkbox"/>            | <input type="checkbox"/>            | The service display name as it appears in the Control Panel's Service applet. If not specified, stopping of any service can fire event response actions. |
| Event Type   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Service event type. This property cannot be modified and is always set to "stop"   |



**Tip:** [WMI Event](#) type can be also used to monitor for service state changes.

## Process hung

**Event Type:** WindowHung

**Event Description:** Hanging of a Windows process. Hanging is often called freezing. In Windows Task Manager hung processes are displayed with *[Process not responding]* note.



**Note:** Only graphical processes, i.e. applications that have graphical user interface (GUI) windows can be processed. A GUI window is considered hung if it doesn't respond to system messages during the specified time period.

**Event Filter Properties:**

| Property            | Required?                           | Fixed?                   | Description  |
|---------------------|-------------------------------------|--------------------------|--|
| Process Module Name | <input type="checkbox"/>            | <input type="checkbox"/> | The module name of the hung process (name of the main program file not including path). If not specified, all hung processes fire event response actions.  |
| Timeout             | <input checked="" type="checkbox"/> | <input type="checkbox"/> | This parameter controls how long 24x7 Event Server waits for the process to begin responding to the system events before it is considered as hung.<br><br>Enter this parameter in seconds.<br><br>If not specified, 60 seconds timeout is used by default. |

## Process crash

This event is monitored using [Dr.Watson error](#) event. See Dr.Watson event for details.

## Dr. Watson error

**Event Type:** DrWatsonError

**Event Description:** Crashing of a process generating a Dr. Watson error message. You can use this event type to monitor and intercept process crashes.



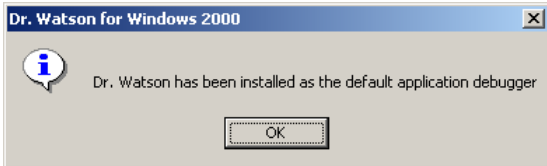
**Note:** This event type is implemented by monitoring an appearance of Dr. Watson Error Message on the on the screen. For Windows NT 4 and Windows 2000 it is "process=csrss.exe;child=0;wnd\_class=#32770"; for for Windows XP and later it is "process=dwwin.exe;child=0;wnd\_class=#32770;". If you have system debuggers or other

development tools and debugging utilities such as Microsoft Development Studio, Lotus Notes' Quincy utility and other that take place of the Dr.Watson, you will not be able to use this event.

To restore Dr. Watson as the default Windows debugger go to a command prompt, type the following command then press the Enter key:

`drwtsn32 -i`

In response you should receive the following message



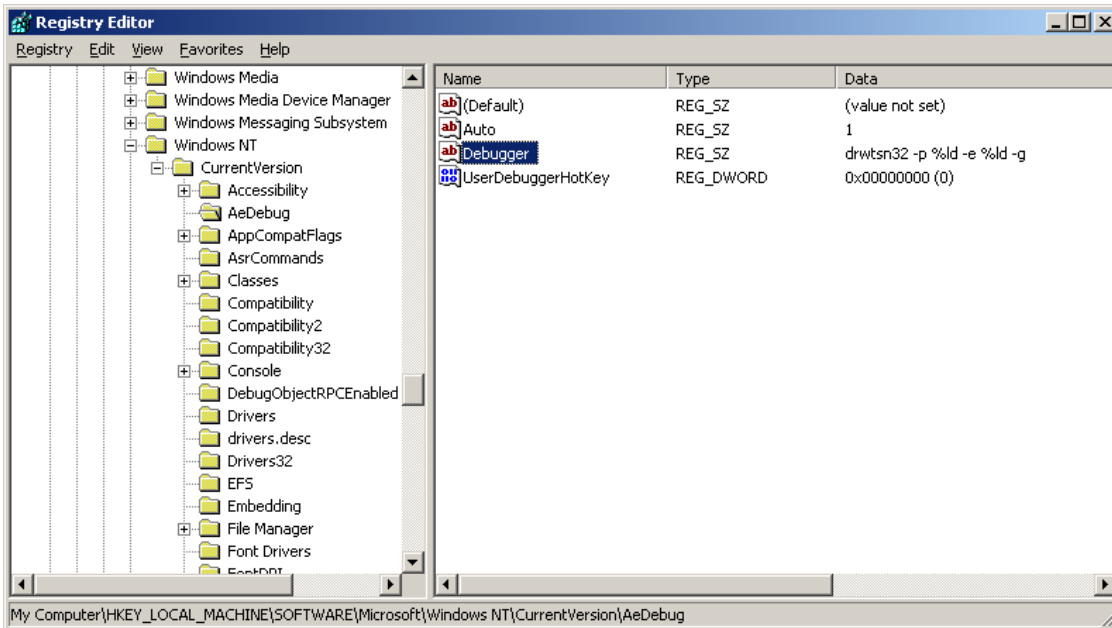
To tell if Dr. Watson is installed as the default debugger check the following key in the Windows registry:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\Debugger`

If Dr. Watson is installed as the default debugger, the registry entry line should have a path entered similar to the following for the *Debugger* Key:

`"drwtsn32 -p %ld -e %ld -g"`

Sample Registry Editor screenshot



**Event Filter Properties:**

| Property   | Required?                | Fixed?                   | Description   |
|------------|--------------------------|--------------------------|---|
| Title Text | <input type="checkbox"/> | <input type="checkbox"/> | Title text of the Dr. Watson window. This text normally contains name of the crashed process. |

 **Tips:**

- When Dr. Watson encounters an error the error is logged under the file "drwtsn32.log" or "user.dmp" in the Windows home folder. Actual file name depends on the operation system and the new information is appended to that file. You can also use File Change Event to monitor Dr Watson log file and this way detect process crashes.



- If your computer is encountering errors often, load Dr. Watson into the Windows Startup folder to load the debugger each time the computer boots.

## New NT Event Log record

**Event Type:** NewEventLog

**Event Description:** New record added to one of the Windows NT (NT/2000/XP/2003) Event Log files.

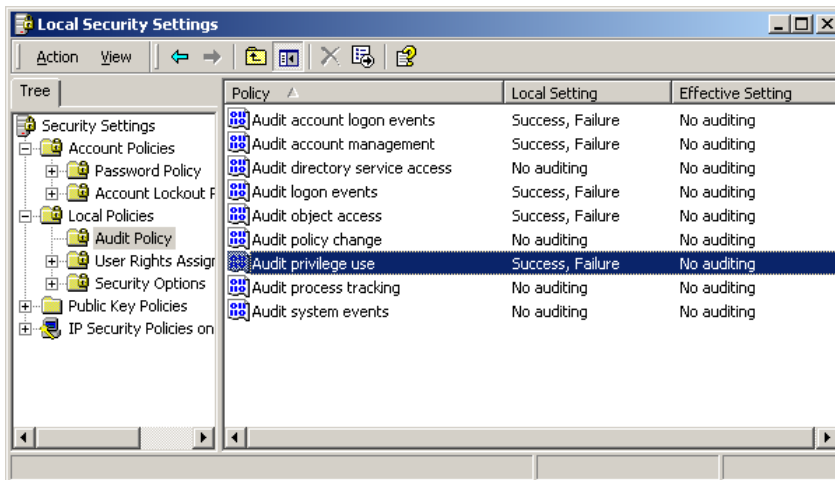
**Event Filter Properties:**

| Property               | Required?                           | Fixed?                   | Description   |
|------------------------|-------------------------------------|--------------------------|---|
| Event Log Name         | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Name of the Windows NT Event Log to monitor, one of the following: <ul style="list-style-type: none"> <li>• Application</li> <li>• System</li> <li>• Audit</li> </ul>   |
| Event ID               | <input type="checkbox"/>            | <input type="checkbox"/> | Event number as it appears in the Windows NT Event Viewer. Event ID is specific to the application that generated this event. If not specified, any event ID can fire event response actions.   |
| Event Type             | <input type="checkbox"/>            | <input type="checkbox"/> | Event type as it appears in the Windows NT Event Viewer, one of the following: <ul style="list-style-type: none"> <li>• Information</li> <li>• Warning</li> <li>• Error</li> </ul> If not specified, any event type can fire event response actions.        |
| Event Category         | <input type="checkbox"/>            | <input type="checkbox"/> | Event category as it appears in the Windows NT Event Viewer. Event category is specific to the application that generated this event. If not specified, any event type can fire event response actions.   |
| Event Source           | <input type="checkbox"/>            | <input type="checkbox"/> | Event source as it appears in the Windows NT Event Viewer. Event category is specific to the application that generated this event and usually is the same as name of that application. If not specified, any event source can fire event response actions. |
| Event Computer         | <input type="checkbox"/>            | <input type="checkbox"/> | Event computer that generated this event. If not specified, any event computer can fire event response actions.   |
| Event Message Contains | <input type="checkbox"/>            | <input type="checkbox"/> | Text to search in the event message. If not specified, any event can fire event response actions.   |



**Tip:**

- You should enable system auditing if you want to monitor failed logons, object access and other resource usage. To enable system auditing open Windows Control Panel; double-click Administrative Tools icon, then double-click Local Security Policy icon. The **Local Security Settings** window will open. Expand **Local Policies** folder and customize individual policies. To modify a particular setting double-click on that setting name and then choose which events you want to audit.



Note that if domain-level settings are defined after a successful login to the network they override local policy settings!

- [WMI Event](#) type can be also used to monitor for event log changes.

## New text log file record

**Event Type:** NewTextLog

**Event Description:** Addition of a new record to the specified text-based log file.



**Notes:**

- Text lines within the monitored log file must terminate either with LF (line-feed) or CR/LF pair of characters (carriage-return and line-feed together). Only correctly terminated lines are processed.
- This event monitor is primarily based on the text file size polling method. If the file is truncated before a new record is added causing the file size to remain constant or shrink the event is not detected.
- If multiple messages (text lines) are added between checks the event action is fired once for every new message. The text filter is applied each new message separately.
- Only flat ASCII text files are supported.

**Event Filter Properties:**

| Property             | Required?                           | Fixed?                   | Description  |
|----------------------|-------------------------------------|--------------------------|--|
| File Mask            | <input type="checkbox"/>            | <input type="checkbox"/> | Name of the file to monitor. You can use standard wildcards to specify file mask for multiple files. If not specified, any file can trigger event response action.   |
| Base Folder          | <input checked="" type="checkbox"/> | <input type="checkbox"/> | File path to the base folder   |
| New Message Contains | <input type="checkbox"/>            | <input type="checkbox"/> | This is the substring that you want to search in the message text. Leave this blank to trigger event action for any new text. If used as macro-parameter in the event response action, it returns the complete message text. |



**Tips:**

- Both already existing local folders and network folders can be monitored.

- For the event to be detected, the log file's size must increase.
- Usually, the last line in a file isn't correctly terminated. For such lines, the program will wait for the next file size increase and rescan the file starting from the last processed terminator.

## Server downtime

**Event Type:** ServerDown

**Event Description:** Server computer or net service is not available. A server (or net service) is considered as not available if it doesn't respond to a PING request during the specified timeout period.

**Event Filter Properties:**

| Property         | Required?                           | Fixed?                              | Description  |
|------------------|-------------------------------------|-------------------------------------|--|
| Host Computer    | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | The IP address or DNS name (computer or service name). If not specified, <i>LocalHost</i> is monitored by default. |
| Response Timeout | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | The timeout period in seconds. If not specified, 1 second is used by default.                                      |
| Event Type       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Service event type. This property cannot be modified and is always set to "down"                                   |



### Tips:

- The monitoring method is based on periodic "pinging" of the specified computer (in other words, periodically sending ICMP echo-requests and analyzing remote computer response).
- Performance and detection of "Server downtime" event may be affected by your firewall software settings. To avoid false event detections make sure you keep your firewall software updated and configure it not to block ICMP protocol and to allow 24x7 Event Server monitors to pass through.

## TCP service downtime (FTP, HTTP, SMTP, etc...)

**Event Type:** TCPServiceDown

**Event Description:** TCP/IP-based service is not available. A service is considered as not available if it's impossible to establish a TCP/IP connection with it during the specified timeout period. Any TCP-based service can be monitored.

**Event Filter Properties:**

| Property      | Required?                           | Fixed?                   | Description  |         |    |         |    |            |           |               |           |             |           |            |           |        |    |
|---------------|-------------------------------------|--------------------------|--|---------|----|---------|----|------------|-----------|---------------|-----------|-------------|-----------|------------|-----------|--------|----|
| Host Computer | <input checked="" type="checkbox"/> | <input type="checkbox"/> | The IP address or DNS name (computer or service name). If not specified, <i>LocalHost</i> is monitored by default.   |         |    |         |    |            |           |               |           |             |           |            |           |        |    |
| Service       | <input checked="" type="checkbox"/> | <input type="checkbox"/> | The service port number. If not specified, HTTP service on port 80 is monitored by default.<br><br>Common services and their port numbers: <table border="1" data-bbox="883 1692 1084 1885"> <tbody> <tr><td>daytime</td><td>13</td></tr> <tr><td>netstat</td><td>15</td></tr> <tr><td><b>FTP</b></td><td><b>21</b></td></tr> <tr><td><b>telnet</b></td><td><b>23</b></td></tr> <tr><td><b>SMTP</b></td><td><b>25</b></td></tr> <tr><td><b>DNS</b></td><td><b>53</b></td></tr> <tr><td>finger</td><td>79</td></tr> </tbody> </table> | daytime | 13 | netstat | 15 | <b>FTP</b> | <b>21</b> | <b>telnet</b> | <b>23</b> | <b>SMTP</b> | <b>25</b> | <b>DNS</b> | <b>53</b> | finger | 79 |
| daytime       | 13                                  |                          |  |         |    |         |    |            |           |               |           |             |           |            |           |        |    |
| netstat       | 15                                  |                          |  |         |    |         |    |            |           |               |           |             |           |            |           |        |    |
| <b>FTP</b>    | <b>21</b>                           |                          |  |         |    |         |    |            |           |               |           |             |           |            |           |        |    |
| <b>telnet</b> | <b>23</b>                           |                          |  |         |    |         |    |            |           |               |           |             |           |            |           |        |    |
| <b>SMTP</b>   | <b>25</b>                           |                          |  |         |    |         |    |            |           |               |           |             |           |            |           |        |    |
| <b>DNS</b>    | <b>53</b>                           |                          |  |         |    |         |    |            |           |               |           |             |           |            |           |        |    |
| finger        | 79                                  |                          |  |         |    |         |    |            |           |               |           |             |           |            |           |        |    |

|                  |                                     |                                     |  |             |           |        |     |     |     |      |     |        |     |       |     |        |     |
|------------------|-------------------------------------|-------------------------------------|--|-------------|-----------|--------|-----|-----|-----|------|-----|--------|-----|-------|-----|--------|-----|
|                  |                                     |                                     | <table border="1"> <tr> <td><b>HTTP</b></td> <td><b>80</b></td> </tr> <tr> <td>rlogin</td> <td>513</td> </tr> <tr> <td>rsh</td> <td>514</td> </tr> <tr> <td>UUCP</td> <td>540</td> </tr> <tr> <td>klogin</td> <td>543</td> </tr> <tr> <td>krcmd</td> <td>544</td> </tr> <tr> <td>kshell</td> <td>544</td> </tr> </table> | <b>HTTP</b> | <b>80</b> | rlogin | 513 | rsh | 514 | UUCP | 540 | klogin | 543 | krcmd | 544 | kshell | 544 |
| <b>HTTP</b>      | <b>80</b>                           |                                     |  |             |           |        |     |     |     |      |     |        |     |       |     |        |     |
| rlogin           | 513                                 |                                     |  |             |           |        |     |     |     |      |     |        |     |       |     |        |     |
| rsh              | 514                                 |                                     |  |             |           |        |     |     |     |      |     |        |     |       |     |        |     |
| UUCP             | 540                                 |                                     |  |             |           |        |     |     |     |      |     |        |     |       |     |        |     |
| klogin           | 543                                 |                                     |  |             |           |        |     |     |     |      |     |        |     |       |     |        |     |
| krcmd            | 544                                 |                                     |  |             |           |        |     |     |     |      |     |        |     |       |     |        |     |
| kshell           | 544                                 |                                     |  |             |           |        |     |     |     |      |     |        |     |       |     |        |     |
| Response Timeout | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | The timeout period in seconds. If not specified, 1 second is used by default.  |             |           |        |     |     |     |      |     |        |     |       |     |        |     |
| Event Type       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Service event type. This property cannot be modified and is always set to "down"   |             |           |        |     |     |     |      |     |        |     |       |     |        |     |



**Tips:**

- The monitoring method is based on periodically opening and closing socket connections to the specified service/host. This method is different from the "Server downtime" event, which is based on sending ICMP echo-requests.
- Performance and detection of "TCP service downtime" event may be affected by your proxy and firewall settings. To avoid false event detections make sure you keep your proxy and firewall software updated and configure it to allow 24x7 Event Server monitors to pass through selected service ports.

### Web server slow response

**Event Type:** WebServerSlowResp

**Event Description:** Unavailability or unacceptable performance of the specified resource on the specified HTTP-server.



**Notes:**

- The resource is considered unavailable if the Web server doesn't send a complete response to HTTP GET request during the specified timeout period.
- 24x7 Event Server doesn't try to download the resource. It only checks the reply to the GET request.

**Event Filter Properties:**

| Property                            | Required?                           | Fixed?                              | Description  |
|-------------------------------------|-------------------------------------|-------------------------------------|--|
| Web Server Name or IP               | <input type="checkbox"/>            | <input type="checkbox"/>            | The IP address or DNS name (for example, <a href="http://www.microsoft.com">www.microsoft.com</a> ). If not specified, <i>LocalHost</i> is monitored by default. |
| HTTP port number                    | <input type="checkbox"/>            | <input type="checkbox"/>            | The service port number. If not specified, HTTP service on port 80 is monitored by default.  |
| Resource                            | <input type="checkbox"/>            | <input type="checkbox"/>            | The name of the resource or page in standard Internet URL format. If not specified, default page (/ resource) is monitored by default.                           |
| Server Response Threshold (Timeout) | <input type="checkbox"/>            | <input type="checkbox"/>            | The timeout period in seconds. If not specified, 5 seconds timeout is used by default.   |
| Event Type                          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Service event type. This property cannot be modified and is always set to "down"   |



**Tips:**

- The timing may be affected by your proxy and firewall settings. If you use proxy and/or firewall software take into account cache setting on the proxy server and authentication settings on the firewall when choosing right timeout value for this event type.

- The monitoring method for this event is based on sending HTTP GET requests and measuring web server response times. This is different from the “TCP service downtime” event, which is based on pinging specific TCP service such as HTTP and getting a response from the server without measuring response time and checking response completion.
- No locally cached information is used.
- Your web server may require different time to return complete response for different web pages. The response time also depends on the size of monitored pages and many other factors, for example timing of the internal database query used on the server to obtain dynamic page contents. Therefore, for reliable results you should only monitor pages that have static contents and don't change often.

## New file

**Event Type:** DirChange

**Event Description:** Appearance of a new file in the monitored folder. By "new file" we mean any file that is written, copied, FTP-ed or created/transferred any other way to the monitored file folder. Both local and network folders can be monitored.

**Event Filter Properties:**

| Property    | Required?                           | Fixed?                              | Description  |
|-------------|-------------------------------------|-------------------------------------|--|
| File Mask   | <input type="checkbox"/>            | <input type="checkbox"/>            | Name of the file to monitor. You can use standard wildcards to specify file mask for multiple files. If not specified, any new file can trigger event response action. |
| Base Folder | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | File path to the base folder   |
| Event Type  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | File event type. This property cannot be modified and is always set to “created”   |



**Tip:** "New File" event is a simplified version of "Folder changes" generic event. Use the generic event if you need to monitor multiple events (file creation, depletion, change) in the same folder and you can reuse the same event response action for file event types.

## File deletion

**Event Type:** DirChange

**Event Description:** Disappearance of a file in the monitored folder. By "file deletion" we mean any file that is deleted, renamed or moved out of the monitored file folder. Both local and network folders can be monitored.

**Event Filter Properties:**

| Property    | Required?                           | Fixed?                              | Description  |
|-------------|-------------------------------------|-------------------------------------|--|
| File Mask   | <input type="checkbox"/>            | <input type="checkbox"/>            | Name of the file to monitor. You can use standard wildcards to specify file mask for multiple files. If not specified, any deleted file can trigger event response action. |
| Base Folder | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | File path to the base folder   |
| Event Type  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | File event type. This property cannot be modified and is always set to “deleted”   |



**Tip:** "File deletion" event is a simplified version of "Folder changes" generic event. Use the generic event if you need to monitor multiple events (file creation, depletion, change) in the same folder and you can reuse the same event response action for file event types.

## File change (size or time)

**Event Type:** DirChange

**Event Description:** Change of a file in the monitored folder. This monitor detects both situations:

1. File size changes (and optionally file modification time)
2. Only file modification time changes while file size remains the same

Both local and network folders can be monitored.

**Event Filter Properties:**

| Property    | Required?                           | Fixed?                              | Description  |
|-------------|-------------------------------------|-------------------------------------|--|
| File Mask   | <input type="checkbox"/>            | <input type="checkbox"/>            | Name of the file to monitor. You can use standard wildcards to specify file mask for multiple files. If not specified, any deleted file can trigger event response action. |
| Base Folder | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | File path to the base folder   |
| Event Type  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | File event type. This property cannot be modified and is always set to "changed"   |



**Tip:** "File deletion" event is a simplified version of "Folder changes" generic event. Use the generic event if you need to monitor multiple events (file creation, depletion, change) in the same folder and you can reuse the same event response action for file event types.

## Folder changes (generic event)

**Event Type:** DirChange

**Event Description:** Creation, deletion, or change of a file contents or file attributes in the monitored folder. Both local and network folders can be monitored.

**Event Filter Properties:**

| Property    | Required?                           | Fixed?                   | Description  |
|-------------|-------------------------------------|--------------------------|--|
| File Mask   | <input type="checkbox"/>            | <input type="checkbox"/> | Name of the file to monitor. You can use standard wildcards to specify file mask for multiple files. If not specified, any file can trigger event response action.   |
| Base Folder | <input checked="" type="checkbox"/> | <input type="checkbox"/> | File path to the base folder   |
| Event Type  | <input type="checkbox"/>            | <input type="checkbox"/> | File event type. Any of the following: <ul style="list-style-type: none"> <li>• "created" – a new file is created</li> <li>• "deleted" – a file is deleted or renamed</li> <li>• "changed" – a file is changed (a change could be of any type – size, modification time, creation time, attributes, including archive bit)</li> <li>• "changed:size_increase" – a file has its size increased</li> </ul> |

|  |  |  |  |
|--|--|--|--|
|  |  |  | <ul style="list-style-type: none"> <li>• “changed:size_decrease” – a file has its size decreased</li> <li>• “changed:date” – a file has its last modification date/time changed</li> <li>• “changed:attrs” – a file has its attributes (such as read/write, hidden, archived) changed or a file creation date/time value is changed.</li> </ul> <p>If this property is not specified any file event type can trigger event response actions.</p> |
|--|--|--|--|

**Tips:**

- Both already existing folders and non-existing folders can be processed.
- Event is not generated if the target folder itself is created or deleted. But if the target folder was deleted and there were some files in it, the “delete” event will be generated for each of these files.
- It’s impossible to distinguish what happened to the target folder, after it was renamed or deleted. Both cases are handled in the same way, i.e. as if the target folder was deleted.
- [WMI Event](#) type can be also used to monitor for folder changes.

## File size threshold

**Event Type:** FileSizeThreshold

**Event Description:** The current size of the specified file reaches or exceeds certain values. This event type can be used to monitor both file size increases and decreases.

**Event Filter Properties:**

| Property       | Required?                           | Fixed?                   | Description  |
|----------------|-------------------------------------|--------------------------|--|
| File Name      | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Full file name including path.   |
| Size Threshold | <input checked="" type="checkbox"/> | <input type="checkbox"/> | File size threshold, in bytes.   |
| Threshold Type | <input type="checkbox"/>            | <input type="checkbox"/> | Threshold type such as less (<) or greater (>). If this property is not specified “greater (>)” threshold size is used by default. |

## NT Event Log size threshold


**Event Type:** EventLogSizeThreshold

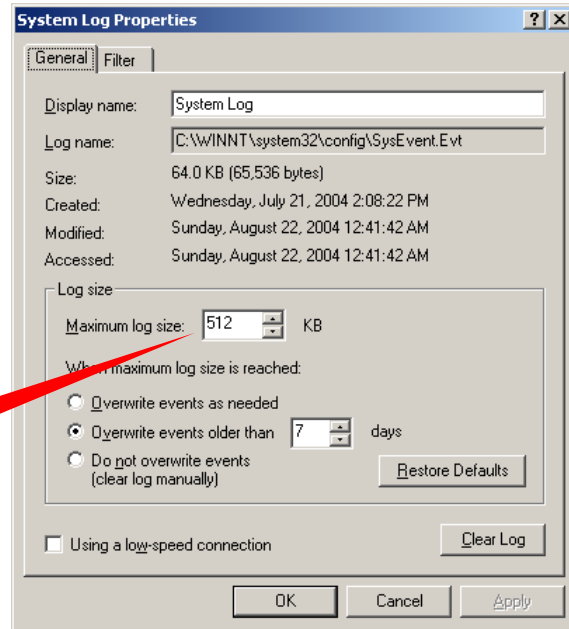
**Event Description:** The current size of the specified Windows NT Event Log file reaches certain value. This event type can be used to monitor size of Windows NT Event Logs and backup or archive log files before they reach their maximum allowed size and start overwriting old event log records.

**Event Filter Properties:**

| Property       | Required?                | Fixed?                   | Description  |
|----------------|--------------------------|--------------------------|--|
| Event Log Name | <input type="checkbox"/> | <input type="checkbox"/> | The name of the NT Event Log, one of the following: <ul style="list-style-type: none"> <li>• Application</li> <li>• Security</li> <li>• System</li> <li>• Name of custom log file</li> </ul> |

|                |                                     |                          |   |
|----------------|-------------------------------------|--------------------------|---|
|                |                                     |                          | If this property is not specified <b>Application Event Log</b> is monitored by default. |
| Size Threshold | <input checked="" type="checkbox"/> | <input type="checkbox"/> | File size threshold, in bytes.  |

 **Tip:** This event type can be used to monitor size of Windows NT Event Logs and backup or archive log files before they reach their maximum allowed size and start overwriting old event log records. To find out and optionally change maximum sizes of your Windows Event Log file open that file in the Windows Event Viewer utility, which is normally can be found in Control Panel's Administrative Tools; right-click on the specific log and then select **Properties** from the popup menu. The **Log Properties** dialog will appear (see sample screenshot on the right). **Maximum log size** property controls how big the log file can grow before the system begins overwriting old event log records.



Maximum log size

### New e-mail message




**Event Type:** EmailMessage

**Event Description:** Appearance of a new email message in the specified mailbox.

**Event Filter Properties:**

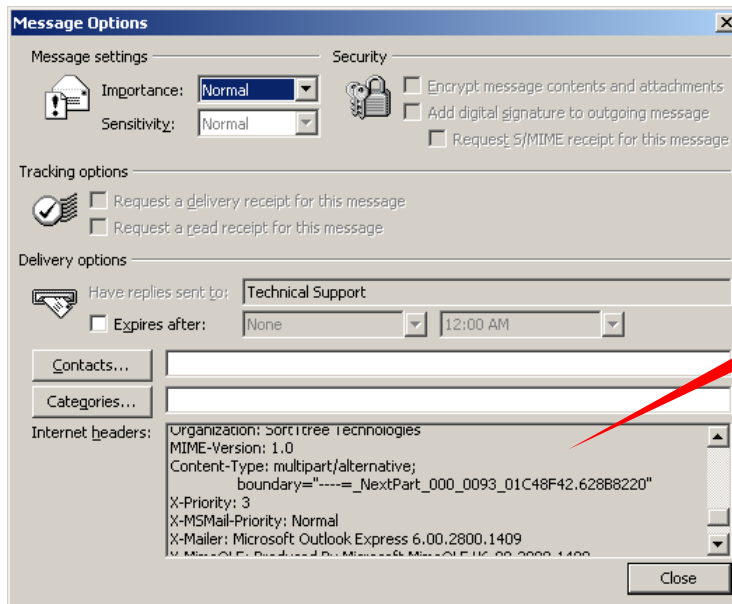
| Property          | Required?                           | Fixed?                   | Description   |
|-------------------|-------------------------------------|--------------------------|---|
| Mailbox Address   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | POP3 email mailbox to watch on. The mailbox must be specified in the following format<br><br><b>&lt;user&gt;[:&lt;password&gt;]@&lt;server&gt;[:&lt;port&gt;]</b><br><br>Password and port values are optional. Example:<br><b>smith:password@pop3.server</b> |
| Subject Contains  | <input type="checkbox"/>            | <input type="checkbox"/> | Text to search in the message subject. If not specified, any new email can fire event response actions.   |
| Message Contains  | <input type="checkbox"/>            | <input type="checkbox"/> | Text to search in the message body. If not specified, any new email can fire event response actions.  |
| Message Sender    | <input type="checkbox"/>            | <input type="checkbox"/> | Text to search in the email sender address. If not specified, email from any sender can fire event response actions.  |
| Message Recipient | <input type="checkbox"/>            | <input type="checkbox"/> | Text to search in the email recipient address. If not specified, email with any recipient address can fire event response actions.  |
| Email Program     | <input type="checkbox"/>            | <input type="checkbox"/> | Name of a sender's email program. This information is extracted from email headers. If not specified, email send from any email program can fire event  |



|                  |                          |                          |   |
|------------------|--------------------------|--------------------------|---|
|                  |                          |                          | <p>response actions.</p> <p> <b>Note:</b> Not all email systems support this email parameter. See the following Tips section for instructions on how to determine if your messages contain this parameter.</p>   |
| Message Priority | <input type="checkbox"/> | <input type="checkbox"/> | <p>Email message priority. This information is extracted from email headers. If not specified, email with any priority can fire event response actions.</p> <p> <b>Note:</b> Not all email systems support this email parameter. Different email programs also use different methods and values to indicate message priorities. The value 3 is most commonly used as "Normal" priority, 1 as "High" and 2 as "Low." See the following Tips section for instructions on how to determine if your messages contain this parameter.</p> |
| Content Type     | <input type="checkbox"/> | <input type="checkbox"/> | <p>Message content type such as "multipart/alternative", "text/plain", "text/html" and other. If not specified, email with any content can fire event response actions.</p>   |
| Sender's IP      | <input type="checkbox"/> | <input type="checkbox"/> | <p>This is network IP address or computer name of the message sender. This information is extracted from email headers. If not specified, email sent from any computer can fire event response actions.</p> <p> <b>Note:</b> Not all email systems support this email parameter. See the following Tips section for instructions on how to determine if your messages contain this parameter.</p>  |
| Has Attachments  | <input type="checkbox"/> | <input type="checkbox"/> | <p>This filter parameter controls whether to monitor only messages that contain email attachments. If not specified, any email message with and without attachments) can fire event response actions.</p>   |

 **Tips:**

- Multiple mailboxes on the same or different servers can be monitored simultaneously.
- "Email Program" filter uses optional "X-Mailer" line from the email message header. The event is ignored if this line is not available and the "Email Program" filter is set to some value.
- "Message Priority" filter uses optional "X-Priority" line from the email message header. The event is ignored if this line is not available and the "Message Priority" filter is set to some value.
- "Sender's IP" filter uses optional " X-Originating-IP" line from the email message header. The event is ignored if this line is not available and the "Message Priority" filter is set to some value.
- To find out which optional lines are available in the email message you want to monitor, open that message in your email program and then open message properties and click "View Source" or "View Internet Headers" menu or button. Different email programs use different menus for displaying message properties and headers. For example, in Microsoft Outlook you can open a message and then in the message window click **View/Options** menu. This will open the **Message Options** dialog. Message headers will displayed on the bottom of the screen in the scrollable **Internet Headers** box.



## New fax received

**Event Type:** NewFaxRec

**Event Description:** A new fax message is received through the local Windows Fax Server.

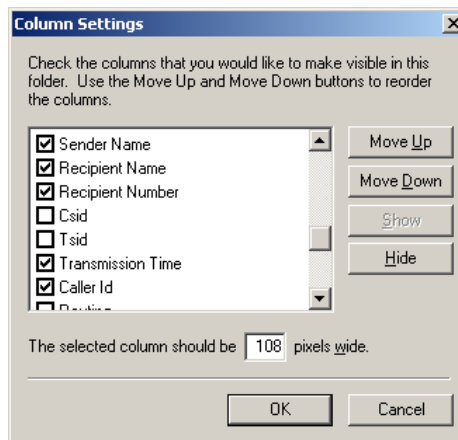
 **Note:** Fax messages can be routed to any recipient/computer on the network but they must be received using the Windows Fax Server running on the computer hosting 24x7 Event Server

### Event Filter Properties:

| Property  | Required?                | Fixed?                   | Description   |
|-----------|--------------------------|--------------------------|---|
| Fax From  | <input type="checkbox"/> | <input type="checkbox"/> | Fax sender number or name as it appears in the Received Faxes folder (usually C:\Documents and Settings\All Users\Documents\My Faxes\Received Faxes). See Tips section below for more details.<br><br>If not specified, fax from any sender can trigger event response actions. |
| Caller ID | <input type="checkbox"/> | <input type="checkbox"/> | Fax calling station identifier. This is usually includes sender's fax number. See Tips section below for more details.<br><br>If not specified, fax from any sender can trigger event response actions.   |
| Fax To    | <input type="checkbox"/> | <input type="checkbox"/> | Fax recipient number. If not specified, fax to any number including routed faxes can trigger event response actions.  |

 **Tips:**

- To view "Sender", "Recipient", "Caller ID" and other fax related columns in the Sent/Received Faxes folder click Windows **Start** button and then click **Programs** menu, click **Accessories** menu, click **Communications** menu then **Fax** menu and then **My Faxes** menu. This will open **My Faxes** folder in the Windows Explorer. Navigate to the **Sent** and/or **Received Faxes** folder and then click **View/Details** menu. After that click **View/Choose Columns...** menu. The Column Settings dialog will appear. Select all relevant columns and click the **OK** button.



Lookup the displayed values and enter them into event filter properties exactly.

- This event monitors appearances of fax notification records in the Windows NT Application Event Log having the following parameters:  
 source -- "Fax Service"  
 category -- "Inbound"  
 event ID -- 8202

## New fax sent

**Event Type:** NewFaxSent

**Event Description:** A new fax message is sent through the local Windows Fax Server.

**Note:** Fax messages can be created and sent from any computer on the network but they must be transmitted using the Windows Fax Server running on the computer hosting 24x7 Event Server.

**Event Filter Properties:**

| Property            | Required?                | Fixed?                   | Description  |
|---------------------|--------------------------|--------------------------|--|
| Sender Name         | <input type="checkbox"/> | <input type="checkbox"/> | Name of the fax sender as specified on the fax cover page. This name is not available if the fax is sent without cover page.<br><br>If not specified, fax from any sender can trigger event response actions.                |
| Sender Company Name | <input type="checkbox"/> | <input type="checkbox"/> | Name of the fax sender company as specified on the fax cover page. This name is not available if the fax is sent without cover page.<br><br>If not specified, fax from any company can trigger event response actions.       |
| Sender Department   | <input type="checkbox"/> | <input type="checkbox"/> | Name of the fax sender department as specified on the fax cover page. This name is not available if the fax is sent without cover page.<br><br>If not specified, fax from any department can trigger event response actions. |
| Fax Billing Code    | <input type="checkbox"/> | <input type="checkbox"/> | The billing code associated with the message's sender as specified on the fax cover page. This name is not available if the fax is sent without cover page.<br><br>If not specified, fax with any billing code can trigger   |

|                  |                          |                          |   |
|------------------|--------------------------|--------------------------|---|
|                  |                          |                          | event response actions.   |
| Recipient Name   | <input type="checkbox"/> | <input type="checkbox"/> | Name of the fax recipient as specified on the fax cover page. This name is not available if the fax is sent without cover page.<br><br>If not specified, fax to any recipient can trigger event response actions. |
| Recipient Number | <input type="checkbox"/> | <input type="checkbox"/> | Recipient fax number.<br><br>If not specified, fax to any recipient can trigger event response actions.   |



**Tips:**

- This event monitors appearances of fax notification records in the Windows NT Application Event Log having the following parameters:  
source -- "Fax Service"  
category -- "Outbound"  
event ID -- 8204

## User logon

**Event Type:** UserProfile

**Event Description:** A user's logon to the local computer.



**Note:** This event monitor can only detect logons that cause user profile to be loaded. This normally happens during interactive user logons only. The User Logon event monitor is unable to detect auxiliary logons such as these created by the system when running batch processes using other user's account.

**Event Filter Properties:**

| Property     | Required?                           | Fixed?                              | Description  |
|--------------|-------------------------------------|-------------------------------------|--|
| Account Name | <input type="checkbox"/>            | <input type="checkbox"/>            | Name of the user account.<br><br>If not specified, any account can trigger event response actions. |
| Event type   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Event type. This property cannot be modified and is always set to "logon"                          |

## User logoff

**Event Type:** UserProfile

**Event Description:** A user's logoff from the local computer.



**Note:** This event monitor can only detect logoff that cause user profile to be unloaded. This normally happens during system shutdowns and restarts and during interactive user logoffs only. The User Logon event monitor is unable to detect auxiliary logoffs such as these created by the system after running batch processes using other user's account.

**Event Filter Properties:**


| Property     | Required?                | Fixed?                   | Description               |
|--------------|--------------------------|--------------------------|---------------------------|
| Account Name | <input type="checkbox"/> | <input type="checkbox"/> | Name of the user account. |

|            |                                     |                                     |  |
|------------|-------------------------------------|-------------------------------------|--|
|            |                                     |                                     | If not specified, any account can trigger event response actions.          |
| Event type | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Event type. This property cannot be modified and is always set to "logoff" |

## Database downtime

**Event Type:** DBState

**Event Description:** The specified database becomes not available (i.e. database connection fails or cannot be established during the specified timeout period)

 **Note:** ODBC version 3.x and any required database client software must be installed on the system running 24x7 Event Server.


**Event Filter Properties:**

| Property      | Required?                           | Fixed?                              | Description   |
|---------------|-------------------------------------|-------------------------------------|---|
| ODBC Profile  | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Name of the ODBC profile for this database connection.  |
| Database User | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Name of the database user for this database connection.   |
| Password      | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Password for this database connection.  |
| Timeout       | <input type="checkbox"/>            | <input type="checkbox"/>            | Connection timeout. The connection is considered as not available if it cannot be established during the specified timeout.<br><br>5 seconds is used by default if no value is entered for the timeout parameter. |
| Event type    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Event type. This property cannot be modified and is always set to "down"  |

## Database startup

**Event Type:** DBState

**Event Description:** The specified database becomes available (i.e. database connection stops failing and can be now established during the specified timeout period).

 **Note:** ODBC version 3.x and any required database client software must be installed on the system running 24x7 Event Server.

**Event Filter Properties:**


| Property      | Required?                           | Fixed?                   | Description   |
|---------------|-------------------------------------|--------------------------|---|
| ODBC Profile  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Name of the ODBC profile for this database connection.  |
| Database User | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Name of the database user for this database connection. |
| Password      | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Password for this database connection.                  |

|            |                                     |                                     |   |
|------------|-------------------------------------|-------------------------------------|---|
| Timeout    | <input type="checkbox"/>            | <input type="checkbox"/>            | Connection timeout. The connection is considered as not available if it cannot be established during the specified timeout.<br><br>5 seconds is used by default if no value is entered for the timeout parameter. |
| Event type | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Event type. This property cannot be modified and is always set to "down"  |

## Database data change

**Event Type:** DBData

**Event Description:** The result-set of a user supplied SQL query changes from the previous run.

 **Note:** ODBC version 3.x and any required database client software must be installed on the system running 24x7 Event Server.

**Event Filter Properties:**

| Property      | Required?                           | Fixed?                   | Description  |
|---------------|-------------------------------------|--------------------------|--|
| ODBC Profile  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Name of the ODBC profile for this database connection.   |
| Database User | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Name of the database user for this database connection.  |
| Password      | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Password for this database connection.   |
| Query         | <input checked="" type="checkbox"/> | <input type="checkbox"/> | SQL query to be run by the event monitor. Must be a valid SQL SELECT query returning only single value of numeric or string data type.   |
| Query Timeout | <input type="checkbox"/>            | <input type="checkbox"/> | Query timeout. If a timeout occurs before any results are returned from the database 24x7 Events Server writes an error to the log and optionally alerts system administrators as specified in the 24x7 Event Server global error handling properties. |


 **Tips:**

- To call stored procedures and other non-SELECT type SQL commands create user-defined database functions and call them using a SELECT type query.
- If the returned result-set is empty or contains more than 1 column it is considered as an error condition and in turn it causes 24x7 Events Server to write an error to the log and optionally alert system administrators as specified in the 24x7 Event Server global error handling properties.

## Database performance threshold

**Event Type:** DBData

**Event Description:** Database performance metric reaches certain threshold. This event monitor periodically runs a user-supplied SQL query returning value of the desired database performance metric.

 **Note:** ODBC version 3.x and any required database client software must be installed on the system running 24x7 Event Server.

**Event Filter Properties:**

| Property        | Required?                           | Fixed?                   | Description  |
|-----------------|-------------------------------------|--------------------------|--|
| ODBC Profile    | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Name of the ODBC profile for this database connection.   |
| Database User   | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Name of the database user for this database connection.  |
| Password        | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Password for this database connection.   |
| Query           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | SQL query to be run by the event monitor. Must be a valid SQL SELECT query returning only single value of numeric data type.   |
| Query Timeout   | <input type="checkbox"/>            | <input type="checkbox"/> | Query timeout. If a timeout occurs before any results are returned from the database 24x7 Events Server writes an error to the log and optionally alerts system administrators as specified in the 24x7 Event Server global error handling properties.   |
| Threshold Value | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <p>The event is triggered when the specified threshold value is reached during specified period of time. Threshold values can be singular and dual. Dual values can be entered as two space-separated numbers for specifying value ranges (minimum and maximum values).</p> <p>Examples:</p> <p>1) To define a maximum value for the number of concurrent sessions in a Oracle database not exceeding 100 enter "100" for the threshold value, enter "&gt;" for the threshold type and enter "SELECT count(*) FROM v\$session" for the query.</p> <p>2) To define a minimum number for Cache Hit Rate for a Oracle database not falling below 95% enter "100" for the threshold value, enter "&lt;" for the threshold type and enter "SELECT 100*(1-sum(getmisses)/sum(gets)) FROM v\$rowcache" for the query.</p> <p>3) To define a range of valid values for the number of concurrent tasks stored in an imaginary tblProjectTasks table in Microsoft Access database that could run at any given point in time and must fall into 5 to 10 range, enter "5 10" for the threshold value, enter "between" for the threshold type and enter "SELECT * FROM tblProjectTasks WHERE project_id = 1" for the query.</p> |
| Threshold Type  | <input type="checkbox"/>            | <input type="checkbox"/> | <p>Threshold value comparison type such as less (&lt;), greater (&gt;), less or equal (&lt;=), greater or equal (&gt;=), equal (=), not equal (&lt;&gt;), between and not between. The threshold value must be entered as two comma-separated numbers if between or not between is specified for the comparison type.</p> <p>If threshold type is not specified the greater or equal (&gt;=) value is used by default.</p>   |
| Event Duration  | <input type="checkbox"/>            | <input type="checkbox"/> | The time interval in seconds during which the threshold value must be reached. If duration is not specified or 0, the event is triggered as soon as the specified counter reaches its threshold value.   |



**Tips:**

- To call stored procedures and other non-SELECT type SQL commands create user-defined database functions and call them using a SELECT type query.
- If the returned result-set is empty or contains more than 1 column it is considered as an error condition and in turn it causes 24x7 Events Server to write an error to the log and optionally alert system administrators as specified in the 24x7 Event Server global error handling properties.
- By default brief changes crossing the threshold value but then returning back don't trigger "Database performance threshold" event. This is done on purpose to avoid false alarms. To trigger the event immediately enter 0 for the "event duration" parameter.

## System performance threshold

**Event Type:** PerfCount

**Event Description:** The event is triggered when the current value of a specified Windows Performance Counter (such as CPU usage, disk I/O, ASP errors, etc...) crosses user specified threshold value and constantly remains below or above that value during user specified time interval.

**Event Filter Properties:**

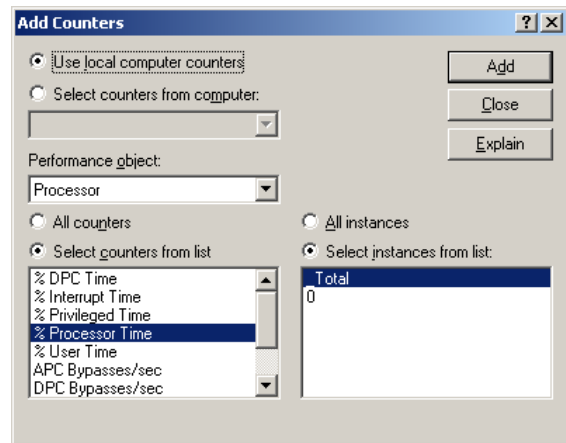
| Property        | Required?                           | Fixed?                   | Description   |
|-----------------|-------------------------------------|--------------------------|---|
| Counter Name    | <input checked="" type="checkbox"/> | <input type="checkbox"/> | The Performance Counter name as it appears in the Windows Performance Monitor. You can either select one of the default names or type in any other valid counter name. See the following Tips section for instructions on name formats and where to find available counter names.   |
| Threshold Value | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <p>The event is triggered when the specified threshold value is reached during specified period of time. Threshold values can be singular and dual. Dual values can be entered as two space-separated numbers for specifying value ranges (minimum and maximum values).</p> <p>Examples:</p> <p>1) To define a maximum value for overall CPU usage (\Processor(_Total)\% Processor Time counter) not exceeding 80% enter "80" for the threshold value and enter "&gt;" for the threshold type.</p> <p>2) To define a minimum number for Cache Hit Rate for Internet Information Server (\Active Server Pages\Cache Hit Rate counter) not falling below 100 enter "100" for the threshold value and enter "&lt;" for the threshold type.</p> <p>3) To define a range of valid values for the number of instances of a process MYPROCESS.EXE that could run at any given point in time (\Process(MYPROCESS)\ID Process counter) between 5 and 10 enter "5 10" for the threshold value and enter "between" for the threshold type.</p> |
| Threshold Type  | <input type="checkbox"/>            | <input type="checkbox"/> | Threshold value comparison type such as less (<), greater (>), less or equal (<=), greater or equal (>=), equal (=), not equal (<>), between and not between. The threshold value must be entered as two comma-separated numbers if between or not  |

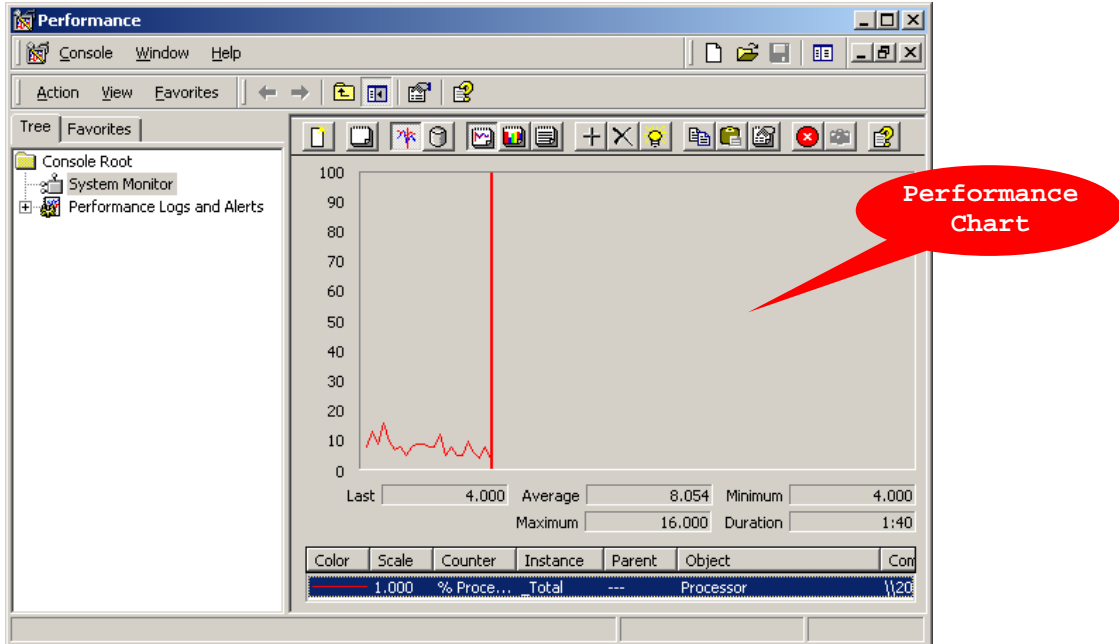


|                |                          |                          |  |
|----------------|--------------------------|--------------------------|--|
|                |                          |                          | between is specified for the comparison type.<br>If threshold type is not specified the greater or equal (>=) value is used by default.  |
| Event Duration | <input type="checkbox"/> | <input type="checkbox"/> | The time interval in seconds during which the threshold value must be reached. If duration is not specified or 0, the event is triggered as soon as the specified counter reaches its threshold value. |

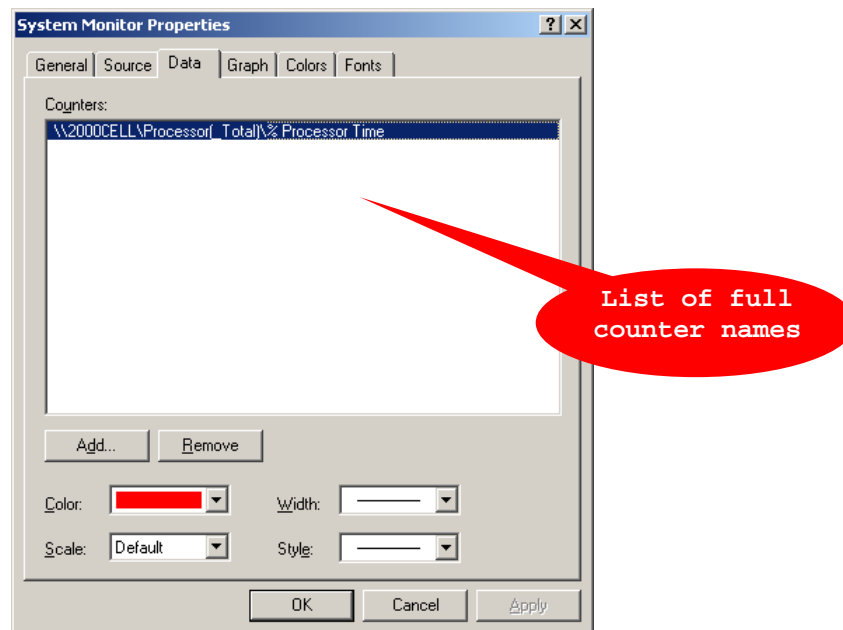
 **Tips:**

- By default brief changes crossing the threshold value but then returning back don't trigger "System performance threshold" event. This is done on purpose to avoid false alarms. To trigger the event immediately enter 0 for the "event duration" parameter.
- [WMI Event](#) type can be also used to monitor performance counters.
- To find out available performance counters and their names
  1. Open **Administrative Tools** folder in the Windows Control Panel.
  2. Double-click the **Performance** icon. This will start the Windows Performance Monitor utility.
  3. On the left side of the Windows Performance Monitor select **System Monitor** option.
  4. Right-click on the Performance Chart and select **Add Counters...** item from the popup menu. This will display **Add Counters** dialog (see example screen on the right side).
  5. Use **Performance object** drop-down list and **Select counters from list** list box to browse available counter names. To see the description of the selected counter click the **Explain** button.
  6. Click the **Add** button to add selected counter to the Performance Chart and then click the **Close** button to close **Add Counters** dialog.
  7. Right-click on the Performance Chart again (see example screen below) and then select **Properties...** item from the popup menu.





8. The **System Monitor Properties** dialog will be displayed. Activate **Data** tab page. There you can see all selected counters and their names.




9. The computer name part is optional and can be skipped when monitoring local computers. Normally the counter name entered into event filter properties should be in the following format: **\\CounterName(InstanceName)\CounterType**

## Disk free space threshold

**Event Type:** DiskFreeSpace

**Event Description:** The event is triggered when the amount of free space on the monitored disk drops below user specified threshold value and constantly remains below that value during at least 10 seconds.

**Event Filter Properties:**

| Property       | Required?                           | Fixed?                              | Description  |
|----------------|-------------------------------------|-------------------------------------|--|
| Disk Name      | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Drive letter followed by a colon, for example C:, D:, E:<br><br>The disk name can refer to any disk including local disks, removable disks, and mapped network shares.<br><br> <b>Note:</b> User space quotas are not taken into account. 24x7 Event Server always evaluates the complete disk space. |
| Size Threshold | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | The threshold value in Mbytes for the minimum amount of available free space. The event is triggered when the free space on the disk falls below this threshold value and remains below during at least 10 seconds.  |
| Threshold Type | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Threshold type. This property cannot be modified and is always set to "le_eq"  |
| Event Duration | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | The time interval in seconds during which the size threshold value must be reached. This property cannot be modified and is always set to 10 seconds.  |



**Tip:**

- Brief free space changes crossing the threshold value but then returning back don't trigger "Disk free space threshold" event. This is done on purpose to avoid false alarms.
- [WMI Event](#) type can be also used to monitor for disk space.


## Registry change

**Event Type:** RegChange

**Event Description:** Changes in the system registry. This event uses an incremental query comparing all registry values within a specific registry key changed since the last execution.

**Event Filter Properties:**

| Property          | Required?                           | Fixed?                   | Description   |
|-------------------|-------------------------------------|--------------------------|---|
| Registry Root     | <input checked="" type="checkbox"/> | <input type="checkbox"/> | The path to the root of the monitored registry key. The following mnemonic names are available for use for root keys: <ul style="list-style-type: none"> <li>• HKCR – HKEY_CLASSES_ROOT</li> <li>• HKCC – HKEY_CURRENT_CONFIG</li> <li>• HKLM – HKEY_LOCAL_MACHINE</li> <li>• HKUSR – HKEY_USERS</li> <li>• HKCU – HKEY_CURRENT_USER</li> </ul> |
| Registry Key Name | <input type="checkbox"/>            | <input type="checkbox"/> | Full name of the registry key not including root. For example, name of the registry key for Internet  |

|            |                          |                          |   |
|------------|--------------------------|--------------------------|---|
|            |                          |                          | <p>Explorer browser containing initial start page should be entered as the following:</p> <p>Software\Microsoft\Internet Explorer\Main</p> <p> <b>Note:</b> If Registry Key Name is not specified 24x7 Event Server monitors values entered directly under in the specified registry root.</p> |
| Value Name | <input type="checkbox"/> | <input type="checkbox"/> | <p>Name of the registry value to monitor. If value name is not specified then any change in the specified registry key can trigger event response actions.</p> <p>Leave Value Name parameter blank if you want to monitor creation of new registry values.</p>  |
| Event Type | <input type="checkbox"/> | <input type="checkbox"/> | <p>Type of changes to monitor, one of the following:</p> <ul style="list-style-type: none"> <li>• created</li> <li>• deleted</li> <li>• changed</li> </ul> <p>If Event Type is not specified then any changes trigger event response actions.</p>   |

 **Notes:**

- Both already existing and non-existing keys and values can be monitored.
- If the specified registry key is deleted the “delete” event will be generated for each of value that previous found under that key. The event is ignored if the Event Type is set to "created" or "changed."
- It is impossible to distinguish what happens to the registry key when it is renamed or deleted. Both cases are handled in the same way as if the specified key is deleted.



**Tip:** In case if you intent to use registry monitor to fix certain registry values ,in other words restore them whenever they are changed you can use the following method:

1. Start Registry Editor
2. Navigate to the registry key of interest.
3. Use **Registry/Export Registry File...** menu in the Registry Editor to export registry key to an editor.
4. Open the exported file in the Notepad and delete from the file all lines referring to values for which you don't care if they change or not.
5. For the event monitor select "change" event type and for then event action select "Run Command"
6. For the command line specify **regedit /s [name of the registry file]**. Replace **[name of the registry file]** with the full name of the exported registry file. When executed, this command will import previously exported values back to the registry.
7. [WMI Event](#) type can be also used to monitor for registry changes.

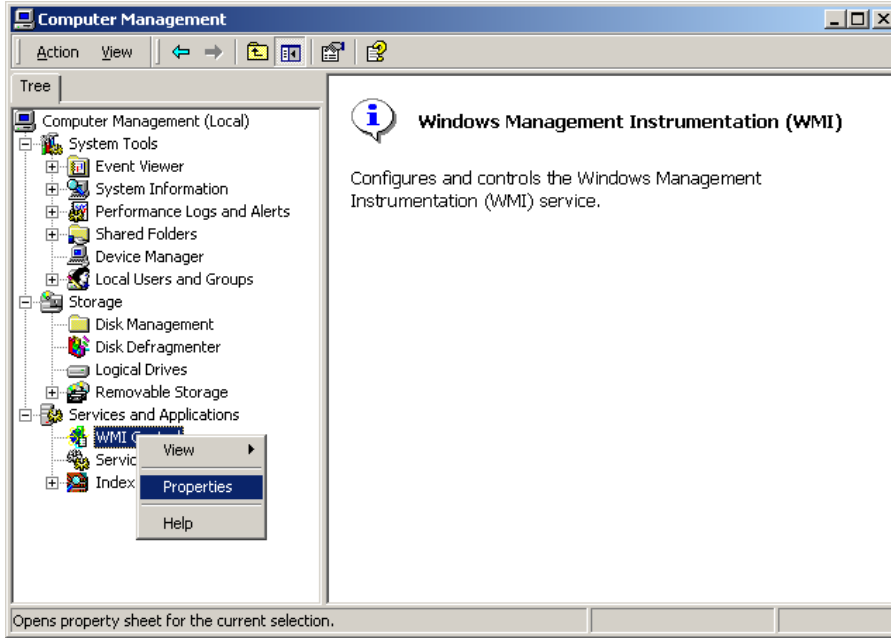
## WMI event

**Event Type:** WMIEvent

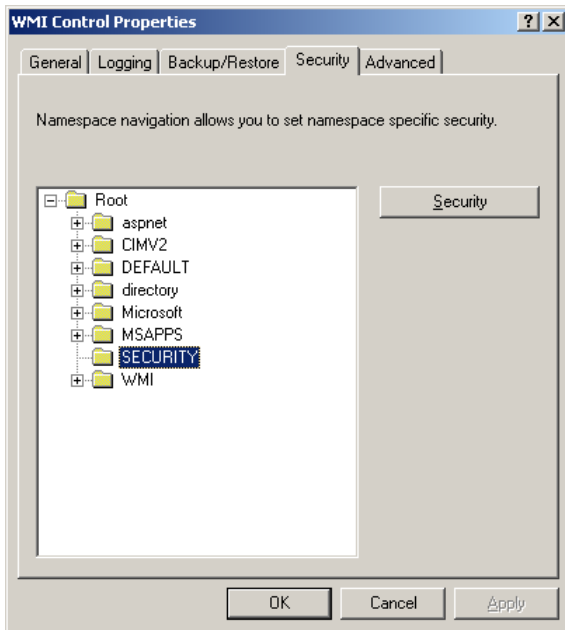
**Event Description:** The result-set of a user supplied WMI SQL query changes from the previous run.



**Note:** WMI must be installed and enabled on the system running the 24x7 Event Server service and also on the system where the query is run. Before using WMI events ensure that WMI permissions have been set. It is recommended that the account used for running WMI queries has full permissions for the Root WMI namespace. To check this, view the properties for WMI via the Computer Management console:



Right-click on the **WMI Control** item and then select **Properties** menu. In response you should receive the following dialog.



Use the **Securities** tab and button to configure WMI access.

**Event Filter Properties:**

| Property  | Required?                           | Fixed?                   | Description   |
|-----------|-------------------------------------|--------------------------|---|
| Namespace | <input checked="" type="checkbox"/> | <input type="checkbox"/> | WMI-namespace to connect to.  |
| SQL Query | <input checked="" type="checkbox"/> | <input type="checkbox"/> | SQL query to be run by the event monitor. Must be a valid WMI SQL SELECT query. |

|                  |                          |                          |   |
|------------------|--------------------------|--------------------------|---|
| User Credentials | <input type="checkbox"/> | <input type="checkbox"/> | <p>Domain user and password for running WMI query on a remote computer using specific user account.. Either of the following formats can be used for specifying User Credentials</p> <ul style="list-style-type: none"> <li>• <b>ntlm</b>domain:&lt;domain&gt;:&lt;user_name&gt;:&lt;password&gt;</li> <li>• <b>Kerberos</b>:&lt;principal_name&gt;:&lt;user_name&gt;:&lt;password&gt;</li> <li>• <b>domain-based</b>: [&lt;domain&gt;]&lt;user_name&gt;:&lt;password&gt;</li> </ul> <p>If not specified, account running 24x7 Event Server is used to run the query. Do not use 'User Credentials' with local queries.</p> |
|------------------|--------------------------|--------------------------|---|

**Note:**

- Values returned by WMI Query can be of simple data types only.
- Date/time values are reported using reported in UTC format. UTC (Coordinated Universal Time) is also popularly known as GMT (Greenwich Mean Time), or Zulu time. Local time differs from UTC by the number of hours of your time zone.
- WMI "Reference" data-types aren't supported.
- WMI multi-value (array) data-types aren't supported.
- Do not use 'User Credentials' with local queries.
- In case if WMI query returns multiple rows the 24x7 Event Server fires assigned event response actions for each row as if a separate event is detected for each row.
- Every returned value can be used and referenced by name in the assigned event actions just like any other predefined event property.

**Tips:**

- You can use "WITHIN [duration]" clause with the query to indicate how often you want the query to poll for events. For example, the following query will poll for process namespace changes every 5 seconds

```
SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_Process'
```

The duration parameter can be specified as a decimal number meaning fractions of a second. For example, 0.05 means 50 milliseconds.

- Namespace can point to a remote computer. For example, to setup an event monitoring start of batch processes on computer REMOTE\_SERVER use the following namespace and query:  

```
\\REMOTE_SERVER\\ROOT\\CIMV2
SELECT * FROM __InstanceCreationEvent WITHIN 0.05 WHERE TargetInstance ISA 'Win32_Process'
AND Name=cmd.*
```
- WMI events can be used to monitor nearly all major server type applications and services. Here are some examples:

(1) The following query can be used to detect when number of connections to Microsoft Exchange server reaches 100 or greater value:

```
SELECT * FROM Win32_PerfRawData_MSExchangeIS_MSExchangeIS WHERE ActiveConnectionCount > 100
```

(2) The following query can be used to detect when lots of messages are sent/received by Microsoft Exchange server indicating unusual level of activity:

```
SELECT * FROM Win32_PerfRawData_MSExchangeIS_MSExchangeIS WHERE
MessagesDeliveredPermin > 1000 OR MessagesSubmittedPermin > 1000
```

(3) To check for a particular file creation in a particular folder, use the following:

```
SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA
'CIM_DirectoryContainsFile' AND TargetInstance.GroupComponent = 'Win32_Directory.Name="c:\\Data"
```

(4) To check for new event log records, use the following:

```
SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_NTLogEvent'
AND TargetInstance.Logfile = "System"
```

(5) To check for insertion of a disk into the CD-ROM drive use the following:

```
SELECT * FROM __InstanceModificationEvent WITHIN 10 WHERE TargetInstance ISA
'Win32_CDROMDrive' AND TargetInstance.MediaLoaded = TRUE AND PreviousInstance.MediaLoaded =
FALSE
```

(6) To check for registry changes use the following:

```
SELECT * FROM RegistryValueChangeEvent WHERE hive='HKEY_LOCAL_MACHINE' AND
KeyPath='Software\\SomeCompany\\SomeSoftwareName' AND ValueName='SomeValue'
```

(7) To check for service state changes, use the following

```
SELECT * FROM __InstanceModificationEvent WITHIN 10 WHERE TargetInstance ISA 'Win32_Service'
AND TargetInstance.Name = 'alerter'
```


- The complete description of WMI SQL dialect is available here [http://msdn.microsoft.com/library/en-us/wmisdk/wmi/wql\\_sql\\_for\\_wmi.asp](http://msdn.microsoft.com/library/en-us/wmisdk/wmi/wql_sql_for_wmi.asp)

## User-defined Events

**Event Type:** ProcessResult

**Event Description:** The event is triggered when user-specified process completes with a specific exit code.

**Event Filter Properties:**

| Property            | Required?                           | Fixed?                   | Description   |
|---------------------|-------------------------------------|--------------------------|---|
| Command Line        | <input checked="" type="checkbox"/> | <input type="checkbox"/> | The command to run, in other words, name of an executable file, batch file or script file to run following by optional command line parameters.   |
| Timeout             | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Process execution timeout. Process is automatically killed if it takes longer to run and the event is ignored.<br><br> <b>Note:</b> The timeout value must be less than the event monitor frequency interval. Failure to set correct timeout value can lead to multiple concurrent run-away processes with a new process added on every new event monitor recursion run, which will cause the entire system at some point to become very slow, stop responding and even crash. |
| Exit Code           | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Process exit code. The following parameter ("Exit Code Condition") determines how the returned exit code value is treated.  |
| Exit Code Condition | <input type="checkbox"/>            | <input type="checkbox"/> | Process exit code condition such as less (<), greater (>), less or equal (<=), greater or equal (>=), equal   |

|  |  |  |  |
|--|--|--|--|
|  |  |  | <p>(=), not equal (&lt;&gt;), between and not between. The condition value must be entered as two comma-separated numbers if between or not between is specified for the comparison type.</p> <p>If Exit Code Condition is not specified the equal (=) value is used by default.</p> <p>This Exit Code Condition defines how to evaluate process exit code and which exit codes indicate event occurrence. In case if the specified process completes with an exit code not satisfying the Exit Code Condition then it is considered as an event, otherwise if the Exit Code Condition is satisfied it is considered as a non-event.</p> |
|--|--|--|--|

 **Tips:**

- Every system process in DOS and Windows returns an exit code to the calling process. Some processes always return the same exit code; other can return different exit codes indicating different process completion statuses. Most DOS commands return 0 to indicate successfully completion and a non-zero number to indicate errors. To find out list of exit codes that can be returned by a command or program you intent to run check your program documentation or contact your program vendor in case if this information is not available in the documentation.
- To test which exit codes are returned in different situations create a simple batch file containing 2 lines: the first line containing full command line for your program including program path and command line parameters (if any) and the second line containing **echo %ERRORLEVEL%** to print the returned exit code to the screen. Run this batch file from the DOS command prompt and test it in different conditions to find out how your program responds to these conditions.

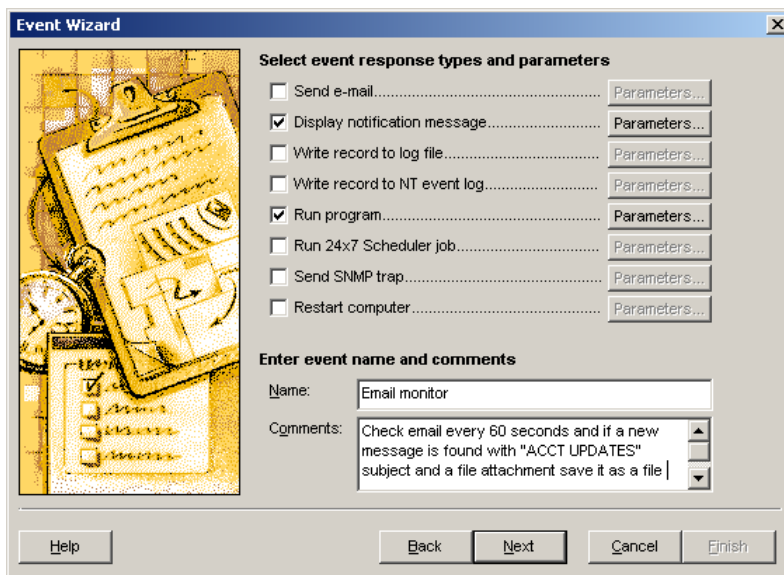


## CHAPTER 5: Event Actions


### Automating Event Responses


24x7 Event Server supports rich set of methods that can be used to automate virtually any type of event response. These response methods are called *event response actions* or simply *event actions*. Most commonly event actions are used for various automated event notifications and corrective actions. 24x7 Event Server enables you to customize event action to suit your organizational needs. You can have different event actions selected for different events, as well as multiple actions selected for a single event. For example, you could have email type action selected for notifying system administrators about occurrence of an important system event (such as critical system service failure), and another batch type action selected for automatically running "fix-it" job (such as restarting the failed service).


Using Event Wizard you can select which event actions you want to link to a particular event and then customize action parameters to suite your needs. The following image shows sample event with 2 actions selected.



To customize action properties click the **Parameters** button displayed on the same line with the action type name. This will open Action Properties & Parameters dialog for the selected action.

 **Tip:** Different action types have different set of properties, which are specific to that type only. For example, **Send e-mail** action type features "Recipient", "Subject" and "Message Text" properties while **Run Program** action type features "Command Line" and "Standard Input" properties. For detailed descriptions of action properties see the next topic.

 **Tip:** Multiple actions associated with a single event are executed sequentially one after another. Although 24x7 Event Server can execute event actions in any order the Event Wizard always saves them in the order they are listed on the screen. Because of the predetermined action execution order you can link different actions and thus create complex event responses, for example you can use **Write record to log file** action to save certain event information in a text file then this information can be passed to a VB script file executed using **Run Program** action. In addition you can use the **Delay** property to control event response timing.

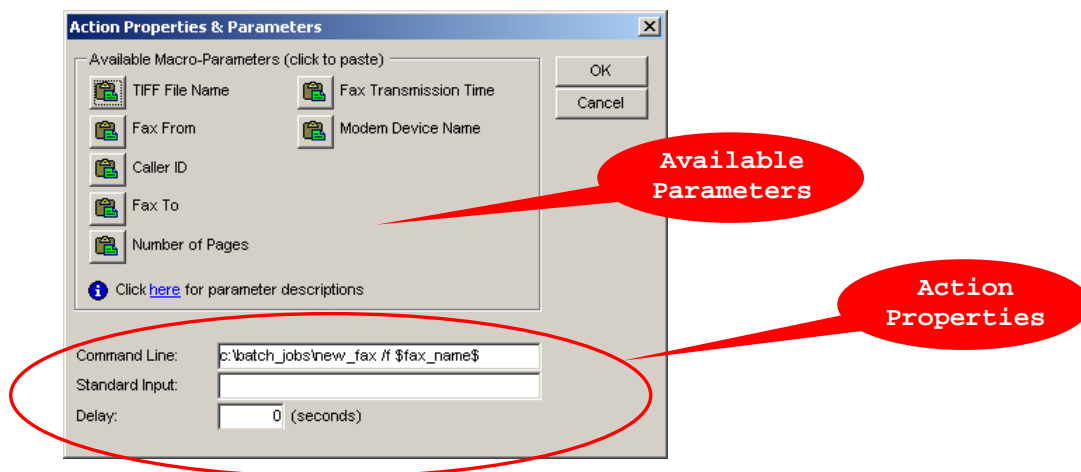
 **Tip:** 24x7 Event Server is capable to execute virtually unlimited number of actions associated with a single event. To simplify event management and setup the Event Wizard's graphical interface allows choosing multiple actions with different types only.



**Tip:** Multiple event actions for different events are executed simultaneously. For example, if events A, B and C occur at the same time or almost at the same time 24x7 Event Server will execute any associated actions for all 3 events simultaneously. **Keep in mind when configuring event actions that incorrect settings can lead to various side effects such as file sharing violations, database locks and so on.** For example, if all 3 events A, B and C are configured to write to the same text log file and all 3 events will occur at the same time then only one of them will be able to write to the log file. Other 2 events will have their actions fail because the target log file will be used at that time by the first event

## Action Properties and Parameters

You can use the **Action Properties & Parameters** dialog screen to customize selected event actions. Sample dialog is shown below. See the previous topic for details on how to display this dialog.



Each action type has its own set of action-specific properties. For descriptions of supported actions and action properties see [CHAPTER 5, Supported Actions](#) topic.

The only common part for all actions is the **Delay** property. This property controls how long 24x7 Event Server waits since the event occurrence before executing the action. You can use this property to setup delayed event response actions. For example, if an event is created for monitoring new files and an action is setup to run a batch file for processing new files, the delay property can be used to delay the batch run by 10 seconds. This time should be sufficient for the process creating new files to complete its file writing operations. Action delay must be specified in seconds. Default zero value indicates the action must be run immediately.

All available action properties appear on the bottom of the **Action Properties & Parameters** dialog screen. Values for action parameters can contain both static text and dynamic macro-parameters, which are substituted in the action run-time with event-specific data values. To indicate a macro-parameter enclose macro-parameter name in \$ signs. Multiple macro-parameters can be used within the same action property.

Example command line for Run Program action type:

```
c:\batch_jobs\new_fax.exe /f $fax_name$
```

This command will start **new\_fax.exe** program and on the command line it will pass name of the TIFF file for the newly received fax.

Each event type has its own set of event-specific macro-parameters. In addition to event specific macro-parameters you can also global system macro-parameters which are available for all actions and event. For more information on supported macro parameters see [Event-specific Parameters](#) and [System Parameters](#) topics later in this CHAPTER.

If you remember parameter names you can type them in the properties value or you can use parameter buttons displayed in the top part of the dialog to paste them. To paste the parameter first click on the event property field where you want to insert the parameter then click the desired parameter button.

In addition to regular text you can use several special symbols such as carriage-return, tab, end of line or other that cannot be normally entered into the property field. See [Special Symbols](#) topic later in this CHAPTER for description of supported special symbols.

Special symbols can be used for formatting event properties and controlling action behavior. Here are a couple of examples demonstrating how to use special symbols.

For example, you want to send an email containing 3 lines of text. The following action property for **Message text** demonstrate how this can be done

Line 1\nLine 2\nLine3

For example, you want to send a user name following by the "Enter" key then following by password and another "Enter key" to DOS program standard input when launching this program using Run Program action type. The following action property for **Standard input** demonstrate how this can be done

My name\rMy password\r

## Event-specific Parameters

Virtually all event parameters available for use in event filters can be used in event action properties as macro-parameters. Each event type supports its own set of event-specific macro-parameters. Certain event types support additional macro-parameters for returning real-time actual values. These parameters are available in event actions only. For example, "Free Disk Space" event type can be used to monitor free disk space. This event supports disk name and threshold free space parameters in events filters. In addition to these two you can use **\$value\$** macro-parameter to obtain the actual amount of free space at the time the event action is fired.



**Tip:** If you know macro-parameter name you can type it directly in the action properties or you can use the **Action Properties & Parameters** dialog screen to copy and paste macro-parameter names. For a list of supported macro-parameter names and their descriptions see [Event Log Tables and Event Data](#) topic in the User-Defined Reports section in CHAPTER 3.

Example command line for "Run Program" action type:

```
c:\batch_jobs\new_fax.exe /f $fax_name$
```

## System Parameters

All event actions support a number of system-level macro-parameters, which are not event type specific. These macro-parameters can be used just as other event specific macro-parameters described in a previous topic. The following table describes available system macro-parameters.

| Macro-parameter | Description   |
|-----------------|---|
| \$systime\$     | System time in hh:mm:ss format expressed as local time.   |
| \$systime_uct\$ | System time in hh:mm:ss format expressed as Coordinated Universal Time (also called Greenwich Mean Time). |
| \$sysdate\$     | System date in mm/dd/yyyy format.   |
| \$sysdate2\$    | System date in dd/mm/yyyy format.   |
| \$systempfile\$ | Unique name of a temporary file created in the user's default temporary folder                            |

|             |  |
|-------------|--|
|             | whose location is specified in the %TEMP% environment variable. To ensure that file name remains unique and not used by other processes 24x7 creates an empty file in the user's default temporary folder. |
| \$sysname\$ | Event name as entered in the event properties.   |
| \$systype\$ | Event type name.   |
| \$sysuser\$ | Name of the currently logged in user (or name of the user whose account is used to run the Event Server service).  |
| \$syshost\$ | Host computer name (network computer name).  |

## Special Symbols

The following table describes special symbols that can be used in event action properties.

| Symbol | Description                               |
|--------|---|
| \n     | New-line character (ASCII code 10)        |
| \r     | Carriage-return character (ASCII code 13) |
| \t     | Tab character (ASCII code 9)              |
| \\     | Back-slash character                      |
| \;     | Semicolon character                       |
| \=     | Equal sign character                      |

## Supported Actions

### Write to text log file

**Action Type:** WriteTextLogFile

**Action Description:** Appends text to a text file. If the destination file does not exist a new file is created automatically.

**Action Properties:** Action properties can contain [macro-parameters](#).

| Property  | Description   |
|-----------|---|
| File Name | Full name of the target log file including file path. |
| Message   | Text to write to this                                 |

### Write to Windows Event Log

**Action Type:** WriteNTEventLog

**Action Description:** Writes new record to Windows Event Log.

**Action Properties:** Action properties can contain [macro-parameters](#).

| Property  | Description   |
|-----------|---|
| File Name | Full name of the target log file including file path.   |
| Log Name  | Windows Event Log name. This parameter must be set to one of following: <ul style="list-style-type: none"> <li>• Application</li> <li>• System</li> <li>• Security</li> </ul> |

| Event Source | Name for the event source. This could be any text up to 255 characters long, for example, "My application."  |   |                  |   |       |   |         |   |             |   |               |    |               |
|--------------|--|---|------------------|---|-------|---|---------|---|-------------|---|---------------|----|---------------|
| Event ID     | Event number. This could be any number. Use different numbers for different events specific to the Event Source.   |   |                  |   |       |   |         |   |             |   |               |    |               |
| Event Type   | One of the following numbers: <table border="1" data-bbox="518 380 1062 648"> <thead> <tr> <th>#</th> <th>Type Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Error</td> </tr> <tr> <td>2</td> <td>Warning</td> </tr> <tr> <td>4</td> <td>Information</td> </tr> <tr> <td>8</td> <td>Audit Success</td> </tr> <tr> <td>16</td> <td>Audit Failure</td> </tr> </tbody> </table> | # | Type Description | 1 | Error | 2 | Warning | 4 | Information | 8 | Audit Success | 16 | Audit Failure |
| #            | Type Description   |   |                  |   |       |   |         |   |             |   |               |    |               |
| 1            | Error  |   |                  |   |       |   |         |   |             |   |               |    |               |
| 2            | Warning  |   |                  |   |       |   |         |   |             |   |               |    |               |
| 4            | Information  |   |                  |   |       |   |         |   |             |   |               |    |               |
| 8            | Audit Success  |   |                  |   |       |   |         |   |             |   |               |    |               |
| 16           | Audit Failure  |   |                  |   |       |   |         |   |             |   |               |    |               |
| Message      | Text message to write to event log.  |   |                  |   |       |   |         |   |             |   |               |    |               |

## Display non-blocking GUI window

**Action Type:** GUIMessage

**Action Description:** Displays a non-blocking message box window.

**Action Properties:** Action properties can contain [macro-parameters](#).

| Property | Description                         |
|----------|-------------------------------------|
| Title    | Text to use for window caption.     |
| Message  | Text to display in the message box. |



**Notes:**

- Multiple messages boxes can be displayed simultaneously.
- Use this action type for event testing only. Do not use it on productions systems running unattended because every message box allocates a bit of system resources until it is closed by an operator.

## Send e-mail

**Action Type:** SendMailMsg

**Action Description:** Sends an email message.

**Action Properties:** Action properties can contain [macro-parameters](#).

| Property | Description                      |
|----------|----------------------------------|
| To       | Email message recipient address. |
| Subject  | Email message subject            |
| Message  | Email message text.              |



**Notes:**

- To send message to multiple recipients use email distribution groups. Such groups can be setup on your email server. See your email server manual for details.

- You must configure email settings (server and sender names) in the system options before you can use this action type.

## Send SNMP trap

**Action Type:** SendSnmpTrap

**Action Description:** Generates a SNMP trap

**Action Properties:** Action properties can contain [macro-parameters](#).

| Property       | Description  |
|----------------|--|
| Enterprise OID | The OID of the enterprise that generated the SNMP trap.  |
| ID             | Any number. It is recommended that you use different numbers for different events. Trap Id is sent as a trap variable. |
| Message        | User-supplied message. Trap message is sent as a trap variable.  |



### Notes:

- Windows NT SNMP service must be running at the time when the trap is sent.
- To configure trap destinations, SNMP communities, security and other options go to SNMP service properties, which are accessible through Control Panel's Services applet.

## Run Program

**Action Type:** RunProcess

**Action Description:** Runs an external process specified by the standard command-line expression.

**Action Properties:** Action properties can contain [macro-parameters](#).

| Property             | Description  |
|----------------------|--|
| Command Line         | The command line to execute. This command line can contain any valid parameters. If program name or parameter values contain spaces enclose them in double quotes. |
| Standard Input       | (Optional) The path to a text file that you want to send to the process standard input. This file can contain references to <a href="#">macro-parameters</a> .     |
| Bind to User Desktop | This parameter tells the 24x7 Event Server to bind the process to default user Desktop   |



### Notes:

- Any process that can be started from the Windows Start menu (Run option) can be started from event response action. Use Run option in the Windows Start menu to verify the command line is correct.
- By default Windows runs all child processes on the virtual desktop bound to the parent process. Because 24x7 Event Server runs as a system service all started processes by default run on the invisible services desktop. In case if you need to see or interact with the started process use "Bind to User Desktop" property to change the process desktop to the default visible user desktop.

## Run 24x7 Scheduler job

**Action Type:** RunProcess

**Action Description:** Runs 24x7 Scheduler job.

**Action Properties:** Action properties can contain [macro-parameters](#).

| Property           | Description  |
|--------------------|--|
| Job ID or Job Name | The id or name of the job as it appears in the 24x7 Scheduler. |



**Notes:**

- By default Windows runs all child processes on the virtual desktop bound to the parent process. Because 24x7 Event Server runs as a system service all started processes by default run on the invisible services desktop. In case if the 24x7 Scheduler job starts another process and you need to see or interact with that process use "Bind to User Desktop" property to change the job desktop to the default visible user desktop.

## Restart system

**Action Type:** SysRestart

**Action Description:** Restarts the local system

**Action Properties:** None

## CHAPTER 6: Optional Event Management Packs

Specialized Event Management Packs (EMP) are available for the most popular applications. Event Management Packs are shipped separately from 24x7 Event Server. They can be purchased and installed on as needed bases.

Each pack contains a set of pre-configured event monitors for a specific application. See [Adding/Removing Event Management Packs](#) topic in CHAPTER 3 for information on how to install new Event Management Packs.

The following Event Management Packs are currently available or will be available in a near future.

- Exchange Server
- Microsoft SQL Server
- Oracle
- Internet Information Services (IIS)
- Terminal Services
- Server Performance Pack
- Security Monitoring and Auditing

Additional Event Management Packs may be developed and shipped later.



## CHAPTER 7: Examples

### Overview

This chapter presents seven step-by-step examples for creating event monitors and automating event response actions. They are intended for people who want to learn 24x7 Event Server by example and get started quickly.

The following examples are available:

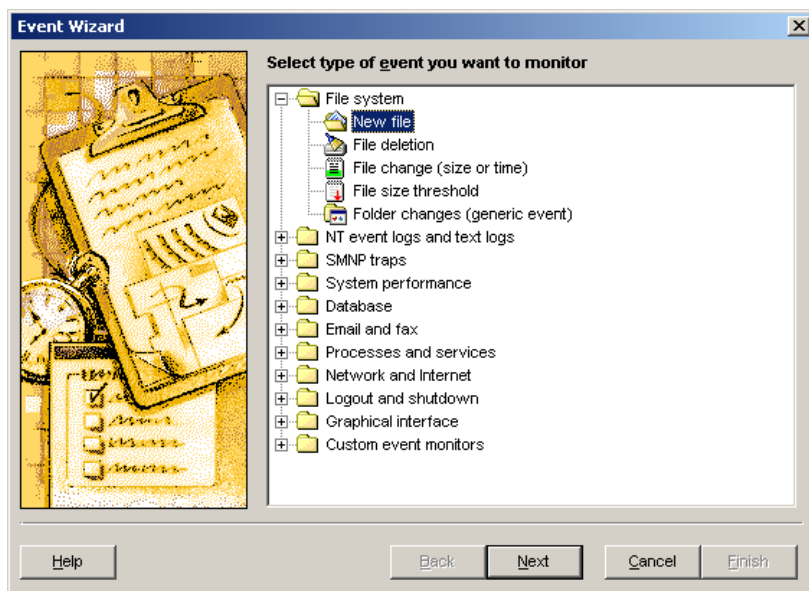
- Example 1 – "New file" monitoring and automation
- Example 2 – Windows NT Event Log monitoring and converting recorded error messages to SNMP traps
- Example 3 – Database data change monitoring and notification
- Example 4 – Hung application monitoring and correction
- Example 5 – Low disk space monitoring and alerting
- Example 6 – Text log file monitoring and alerting
- Example 7 – Incoming email monitoring and loading email attachments into a database.

### Example 1 – "New file" monitoring and automation

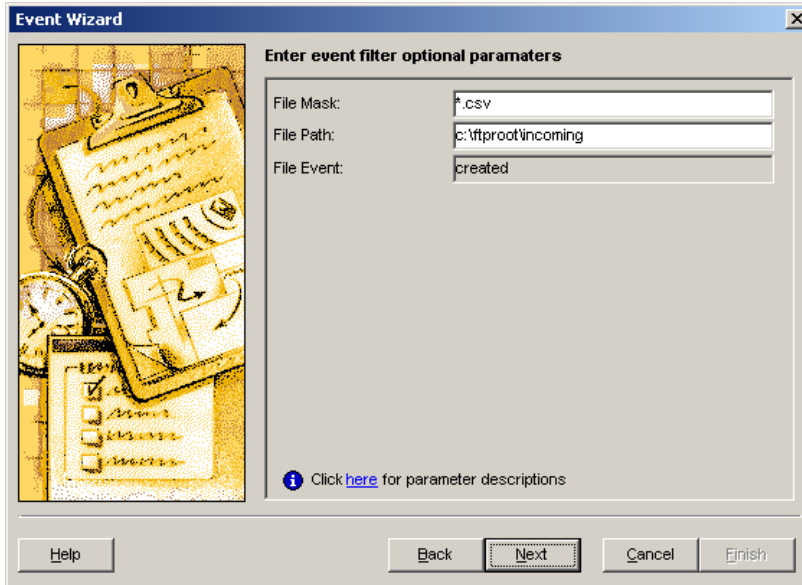
**Task:** Monitor appearance of new files with extension `.CSV` in `c:\ftproot\incoming` directory and once new files are found start file processing application `CSVLOADER.EXE` for each new file passing full file name as command line parameter.

#### Steps:

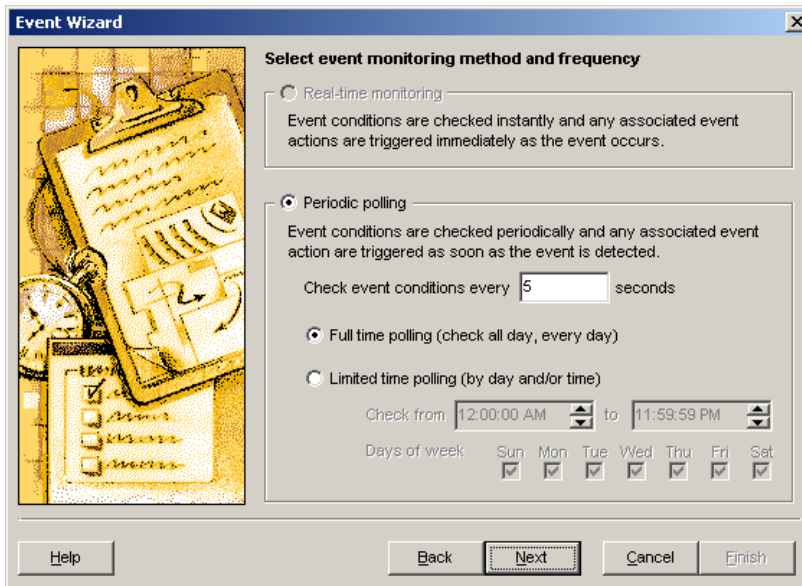
1. Start 24x7 Event Server Management Console and then click **File/New Event** menu to add a new event. The Event Wizard will appear.
2. Expand **File system** folder and then within the expanded folder select **New file** item. Click the **Next** button.



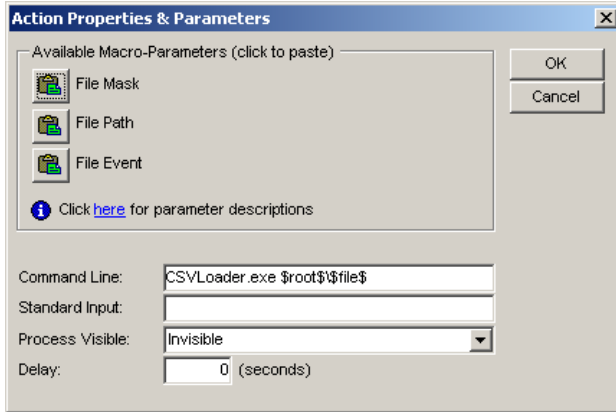
3. Enter `*.scv` into the **File Mask** field; enter `c:\ftproot\incoming` into the **File Path** field. Click the **Next** button.



4. Customize event monitor schedule as needed. Click the **Next** button again if it's ok to check for files 24 hours a days, 7 days a week, every 5 seconds, otherwise select a different schedule and then click the **Next** button.



5. Check **Run program** option. This will make the corresponding **Parameters** button enabled and then click the enabled **Parameters** button. The **Actions Properties and Parameters** dialog will appear.



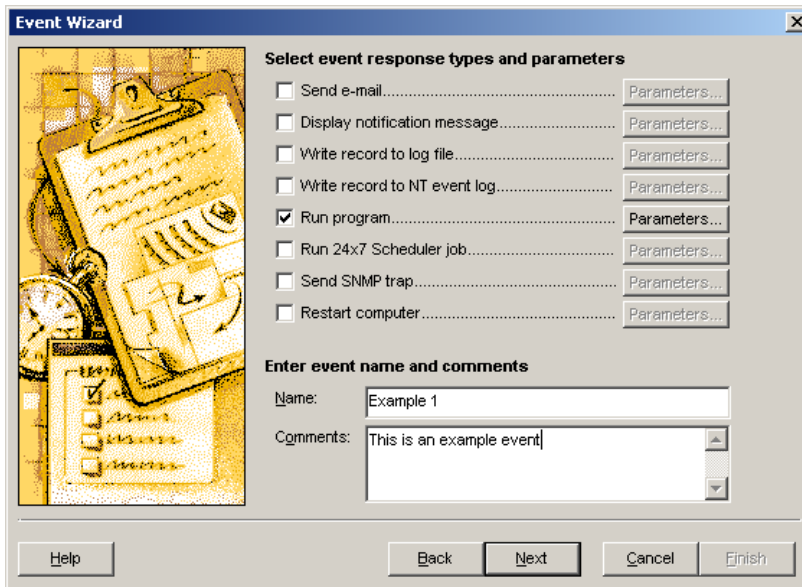
In the **Command line** field type [CSVLoader.exe](#) then type 1 space. Click the **Paste File Path** button, type 1 backslash and then click the **Paste File Mask** button. The resulting text should look as below

[CSVLoader.exe \\$root\\$\\\$file\\$](#)

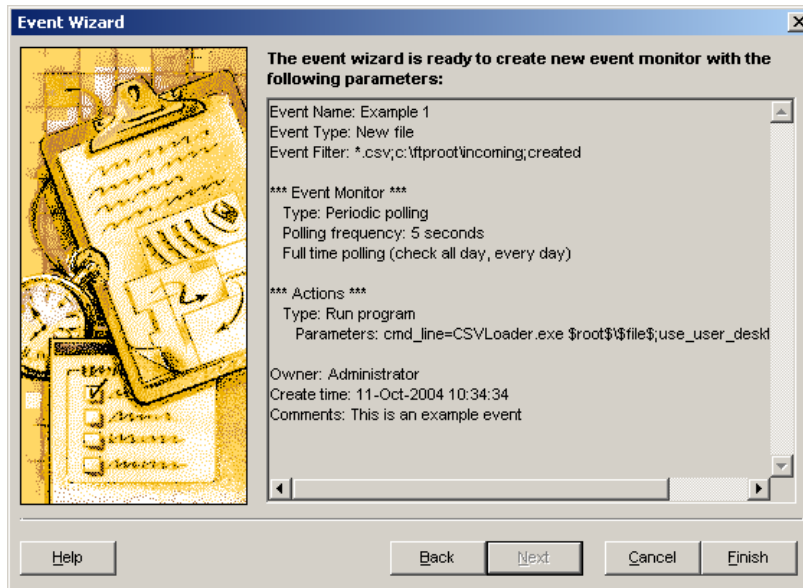
Please note that when the event response action will be fired the [\\$root\\$](#) and [\\$file\\$](#) macro-parameters will be replaced with the actual directory and file names so that the resulting command line parameter for CSVLOADER.EXE program will contain the complete file name of the new file.

Click the **OK** button to close the **Actions Properties and Parameters** dialog.

- Enter event name [Example 1](#) into the **Name** field and then enter optional comments into the **Comments** field. Click the **Next** button when ready.



- This is the last step. Click the **Finish** button and then click **File/Save** menu to save the new event.

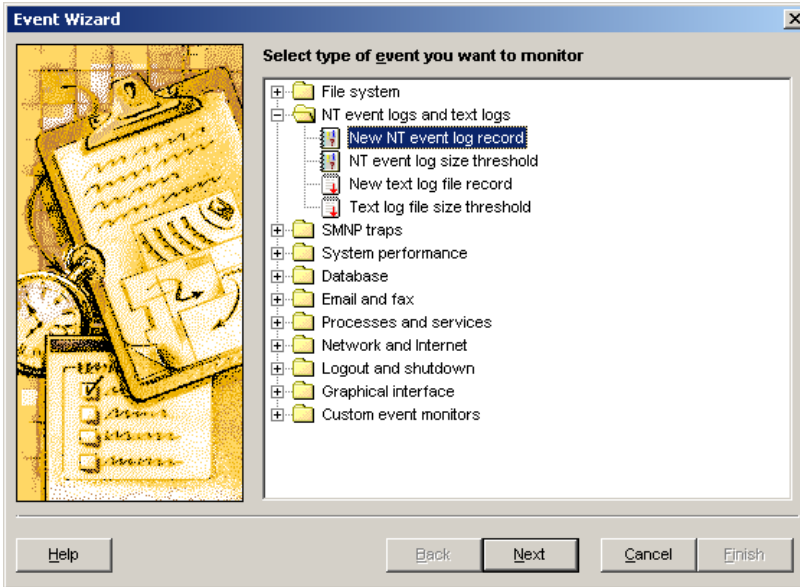


## Example 2 – Windows NT Event Log monitoring and converting error messages to SNMP traps

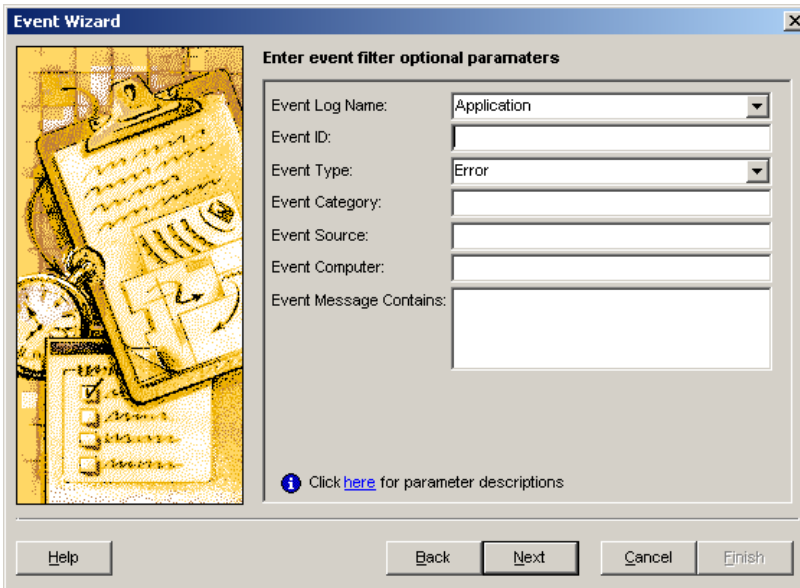
**Task:** Monitor Windows NT System and Application event logs and generate SNMP traps for records having ERROR type. Send generated traps to a central enterprise management console, such as Microsoft Operations Manager, IBM Tivoli, HP OpenView or other.

### Steps:

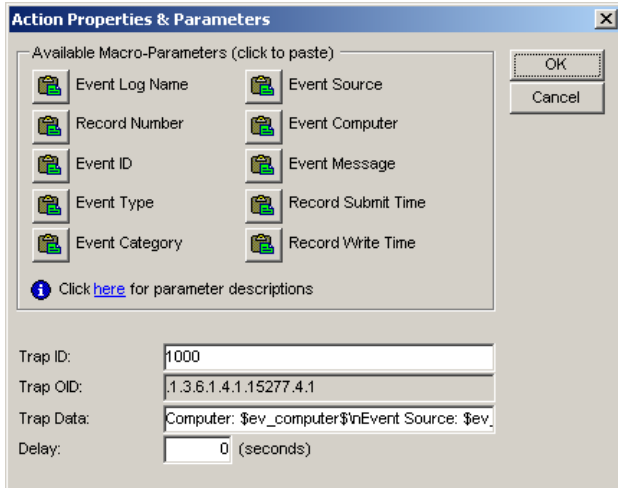
1. Start 24x7 Event Server Management Console and then click **File/New Event** menu to add a new event. The Event Wizard will appear.
2. Expand **NT event logs and text logs** folder and then within the expanded folder select **New NT event log record**. Click the **Next** button.



3. Select **Application** from the drop-down list in the **Event Log Names** field; select **Error** from the drop-down list in **Event Type** field. Click the **Next** button.



4. Skip the event monitor schedule step leaving the default schedule as is. Click the **Next** button again.
5. Check **Send SNMP trap** option. This will make the corresponding **Parameters** button enabled and then click the enabled **Parameters** button. The **Actions Properties and Parameters** dialog will appear.



In the **Trap ID** field type **1000** or any other ID you use for application traps. You normally should use your SNMP Enterprise Management Console to select IDs and enter descriptions for user-defined traps and also configure it to display complete trap data.

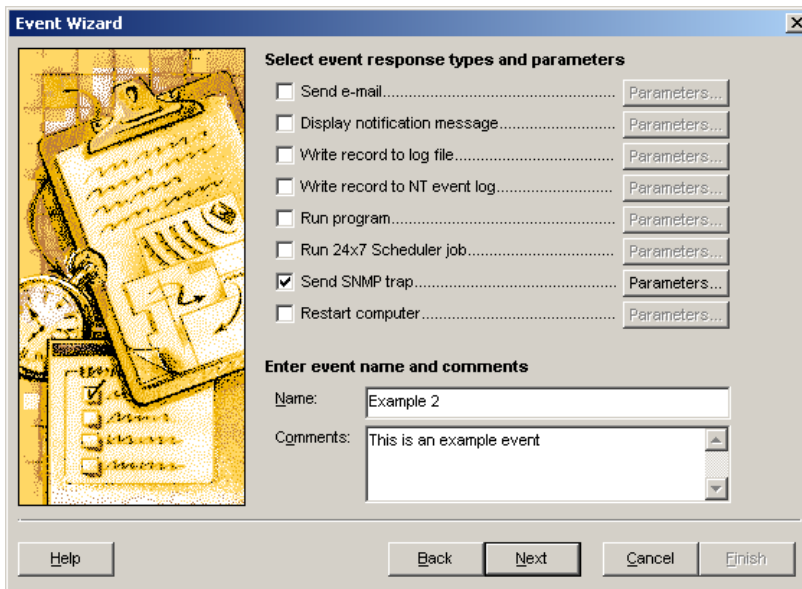
In the trap data type **Computer:** then click the **Paste Event Computer** button, type **\n** to insert the "new line" symbol, type **Event Source:** and then click the **Paste Event Source** button, type **\n** to insert the "new line" symbol, type **Event ID:** and then click the **Paste Event ID** button, type **\n** to insert the "new line" symbol, type **Error Message:** and then click the **Paste Event Message** button... The resulting text should look as below

**Computer: \$ev\_computer\$ Event Source: \$ev\_source\$ Event ID: \$ev\_id\$ Error Message: \$ev\_desc\$**

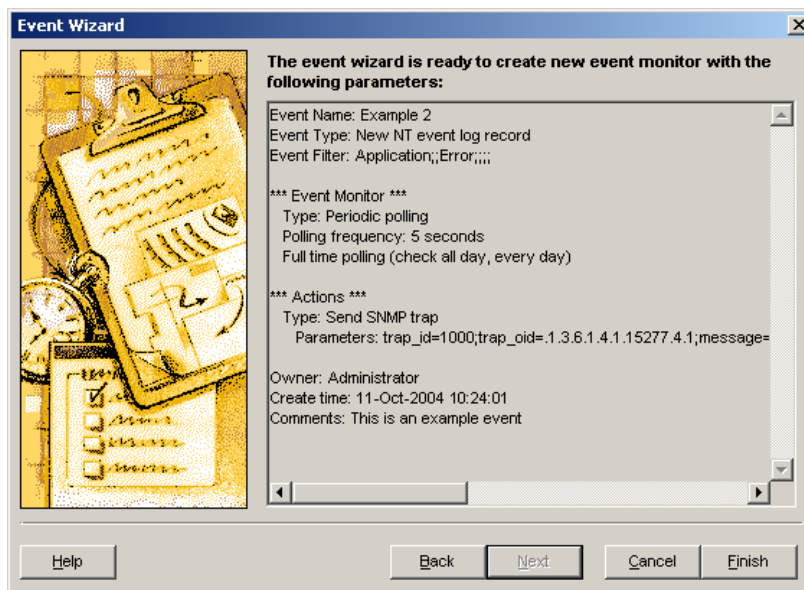
Please note that when the event response action will be fired the **\$ev\_computer\$, \$ev\_source\$, \$ev\_id\$** and **\$ev\_desc\$** macro-parameters will be replaced with the actual values from the new record in the Application event log.

Click the **OK** button to close the **Actions Properties and Parameters** dialog.

6. Enter event name **Example 2** into the **Name** field and then enter optional comments into the **Comments** field. Click the **Next** button when ready.



7. Click the **Finish** button to close the Event Wizard



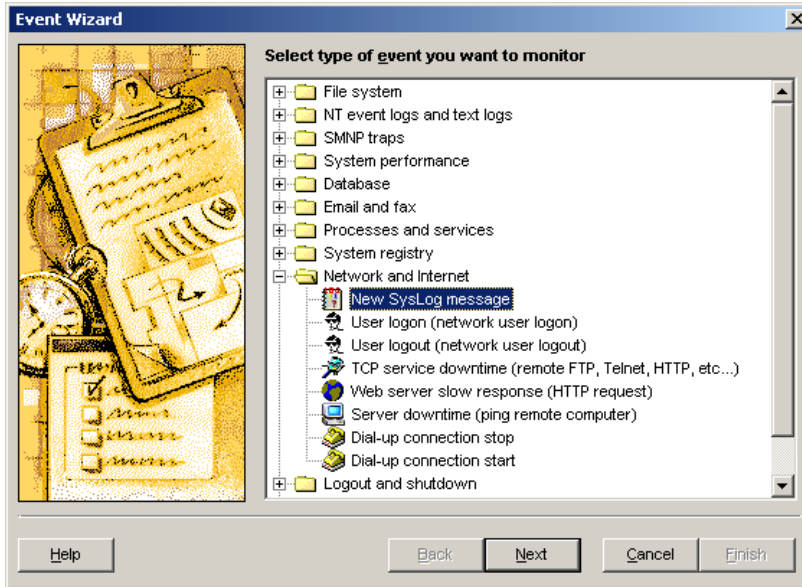
8. Repeat steps 1 to 7 except that in step 3 select "System" event log name instead of "Application." When done click **File/Save** menu to save the new events.

## Example 3 – SysLog monitoring and converting Alert messages to SNMP traps

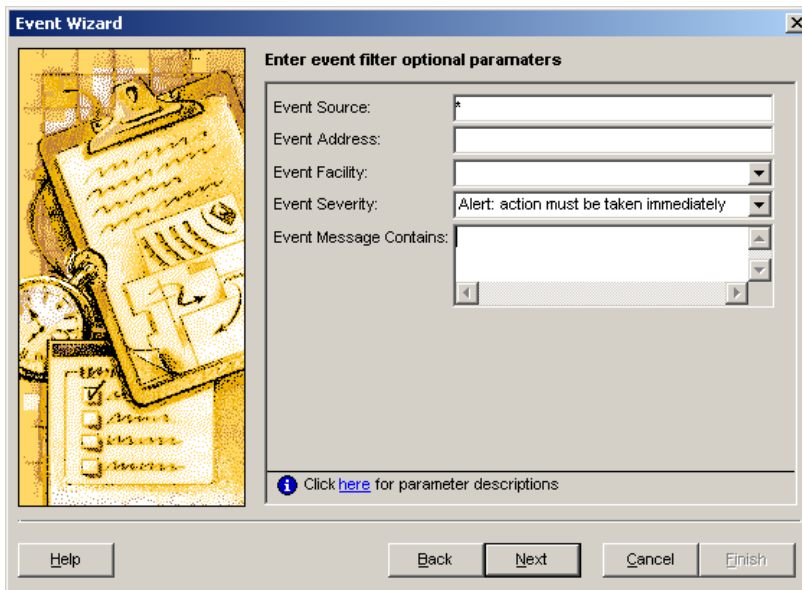
**Task:** Monitor SysLog messages generate SNMP traps for records having ALERT severity. Send generated traps to a central enterprise management console, such as Microsoft Operations Manager, IBM Tivoli, HP OpenView or other.

### Steps:

1. Start 24x7 Event Server Management Console and then click **File/New Event** menu to add a new event. The Event Wizard will appear.
2. Expand **Network and Internet** folder and then within the expanded folder select **New SysLog message**. Click the **Next** button.

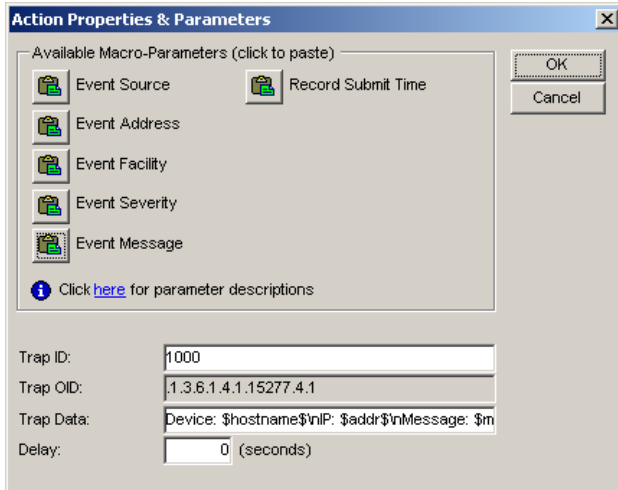


3. Select **Alert: action must be taken immediately** from the drop-down list in the **Event Severity** field, Click the **Next** button.



4. Skip the event monitor schedule. Click the **Next** button again.
5. Check **Send SNMP trap** option. This will make the corresponding **Parameters** button enabled and then click the enabled **Parameters** button. The **Actions Properties and Parameters** dialog will appear.





In the **Trap ID** field type **1000** or any other ID you use for system traps. You normally should use your SNMP Enterprise Management Console to select IDs and enter descriptions for user-defined traps and also configure it to display complete trap data.

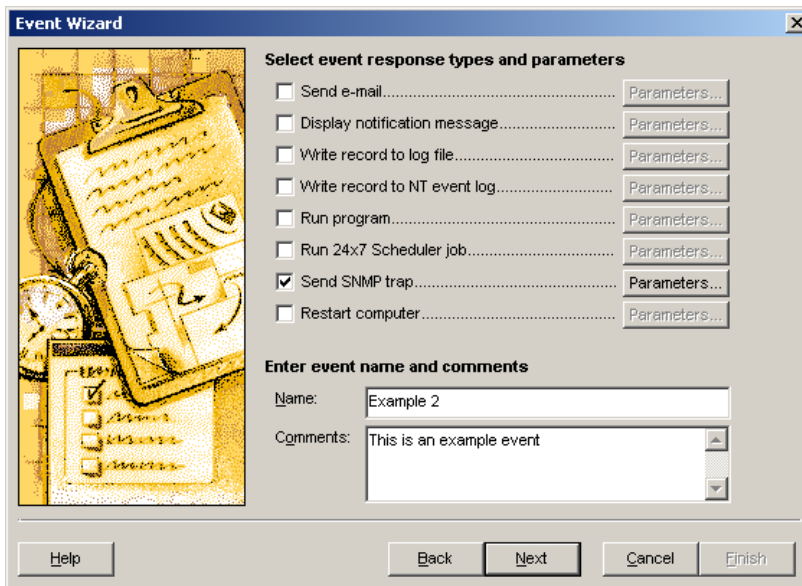
In the trap data type **Device:** then click the **Paste Event Source** button, type **\n** to insert the "new line" symbol, type **IP:** and then click the **Paste Event Address** button, type **\n** to insert the "new line" symbol, type **Message:** and then click the **Paste Event Message** button... The resulting text should look as below

**Device: \$hostname\$ \n IP: \$addr\$ \n Message: \$msg\$**

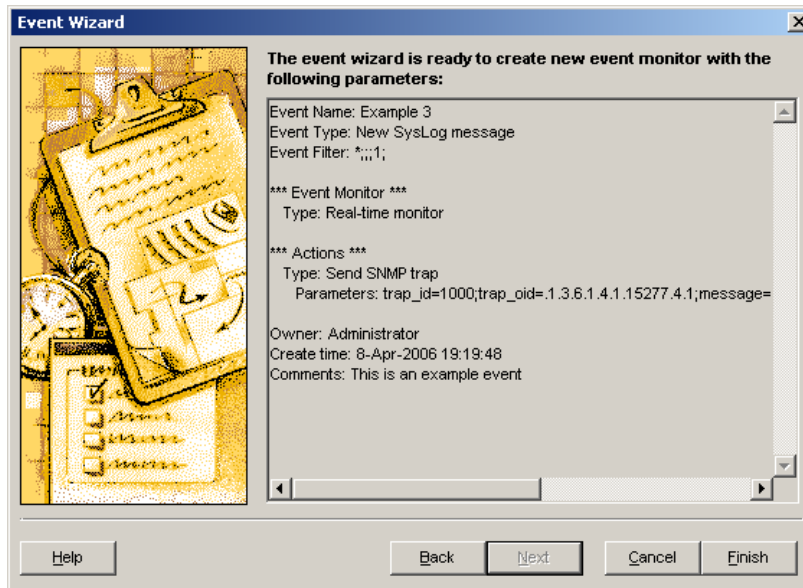
Please note that when the event response action will be fired the **\$hostname\$**, **\$addr\$**, and **\$msg\$** macro-parameters will be replaced with the actual values from the new syslog message.

Click the **OK** button to close the **Actions Properties and Parameters** dialog.

6. Enter event name **Example 3** into the **Name** field and then enter optional comments into the **Comments** field. Click the **Next** button when ready.



7. Click the **Finish** button to close the Event Wizard



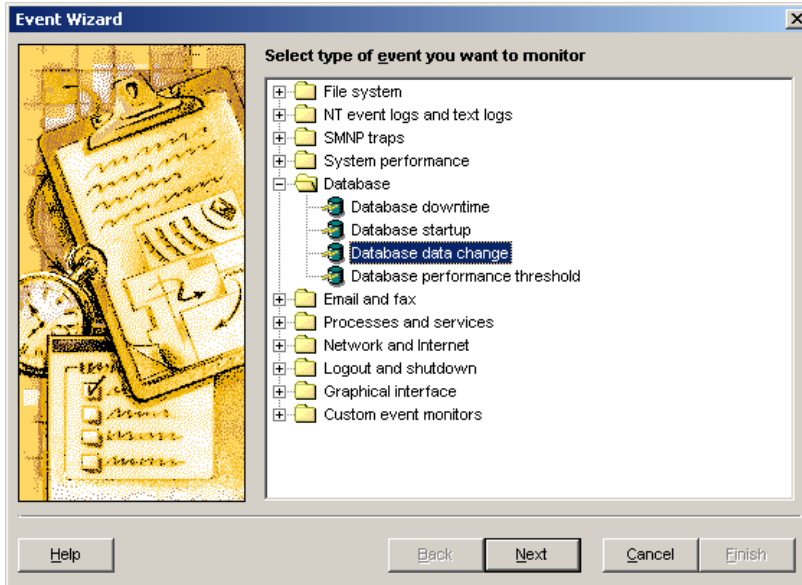
8. Repeat steps 1 to 7 except that in step 3 select "Emergency" event severity instead of "Alert." When done click **File/Save** menu to save the new events.
9. Repeat steps 1 to 7 except that in step 3 select "Critical" event severity instead of "Alert." When done click **File/Save** menu to save the new events.

## Example 4 – Database data change monitoring and notification

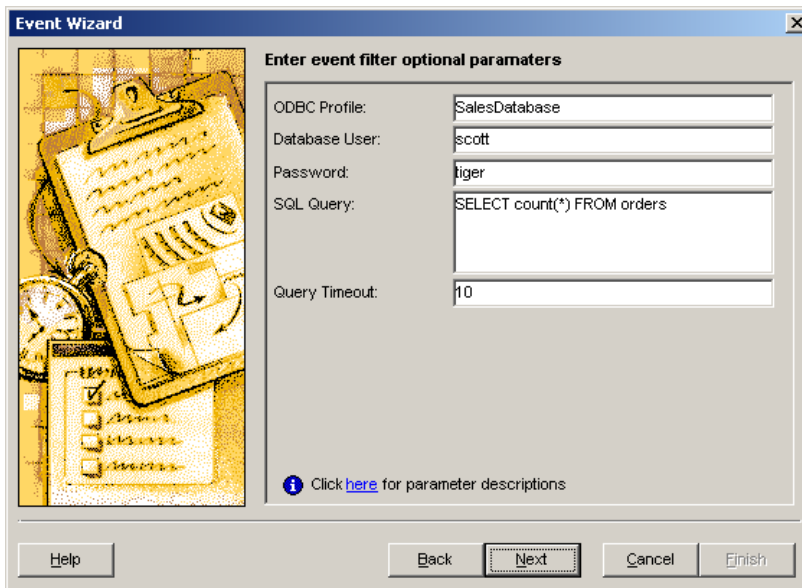
**Task:** Monitor records in ORDERS table and whenever a new record is added send email notification to the sales department.

**Steps:**

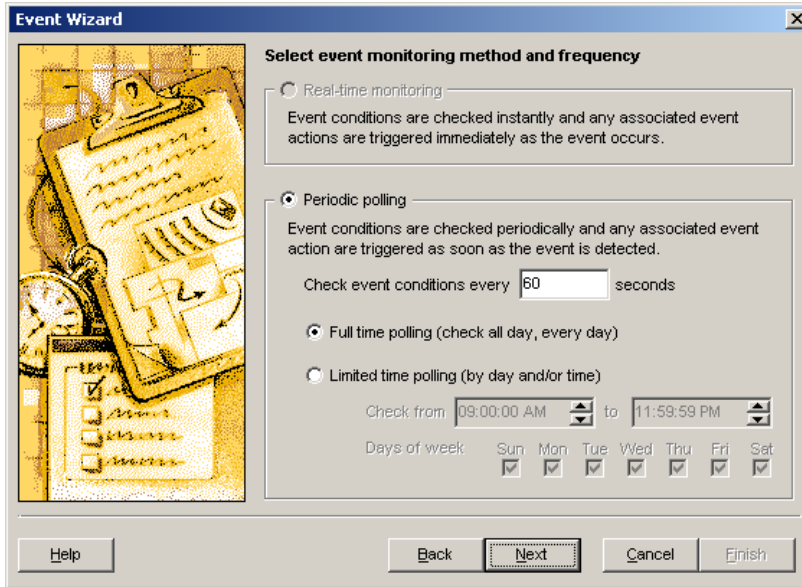
1. Start 24x7 Event Server Management Console and then click **File/New Event** menu to add a new event. The Event Wizard will appear.
2. Expand **Database** folder and then within the expanded folder select **Database data change** item. Click the **Next** button.



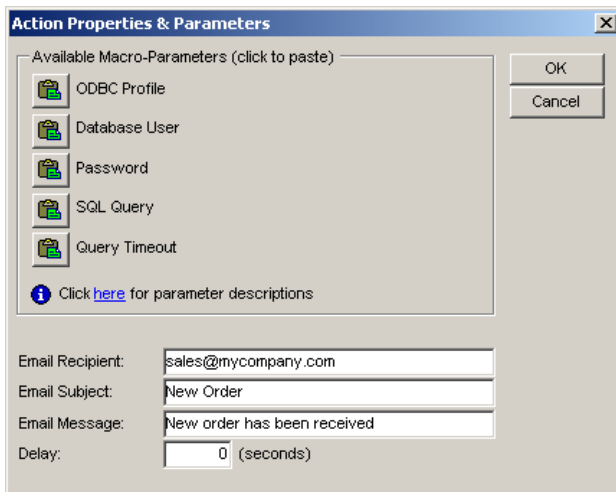
3. Enter **SalesDatabase** into the **ODBC Profile** field; enter **scott** into the **Database User** field; enter **tiger** into the **Password** field; enter **SELECT \* FROM orders.** Into the **SQL Query** field. Click the **Next** button.



4. Customize event monitor schedule as needed. For example enter 60 to check for new orders every 60 seconds. Click the **Next** button.

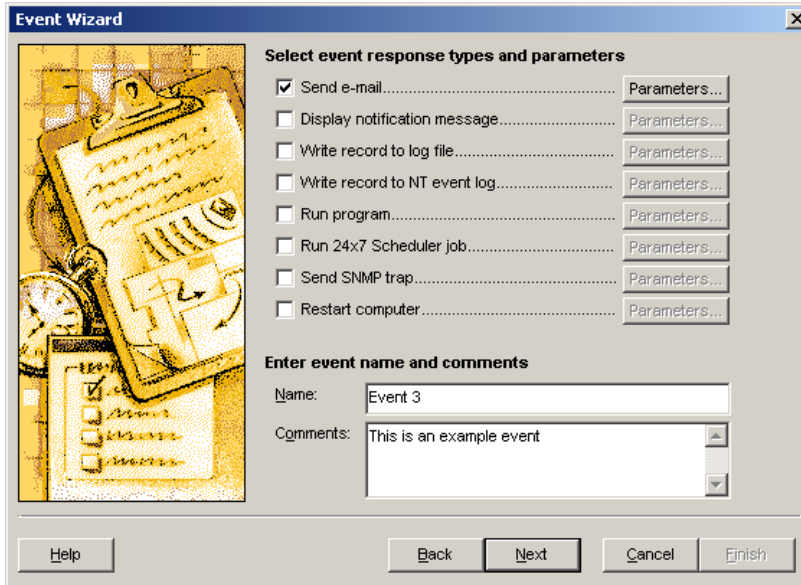


5. Check **Send email** option. This will make the corresponding **Parameters** button enabled and then click the enabled **Parameters** button. The **Actions Properties and Parameters** dialog will appear.

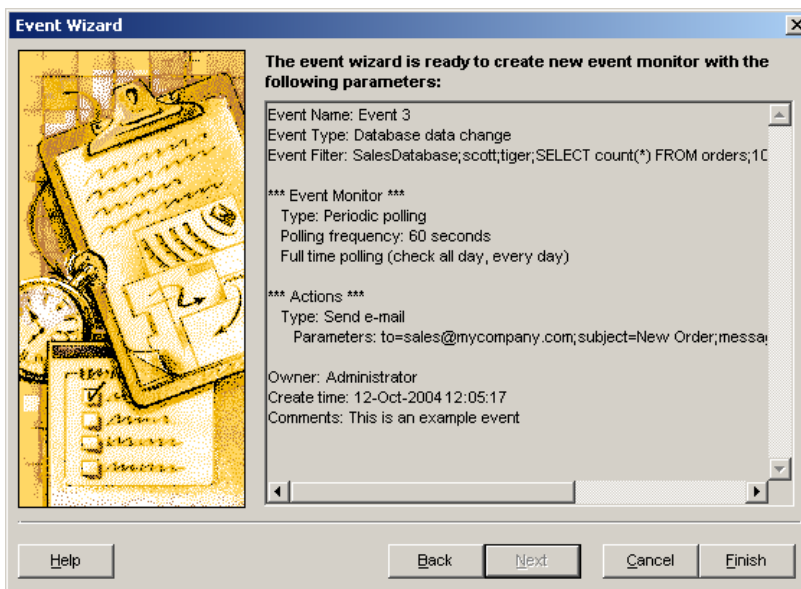


In the **Email recipient** field type your sales department general email address, for example [sales@mycompany.com](mailto:sales@mycompany.com). In the **Email Subject** field type [New Order](#). In the Email Message field type [New order has been received](#). Click the **OK** button to close the **Actions Properties and Parameters** dialog.

6. Enter event name [Example 3](#) into the **Name** field and then enter optional comments into the **Comments** field. Click the **Next** button when ready.



7. This is the last step. Click the **Finish** button and then click **File/Save** menu to save the new event.



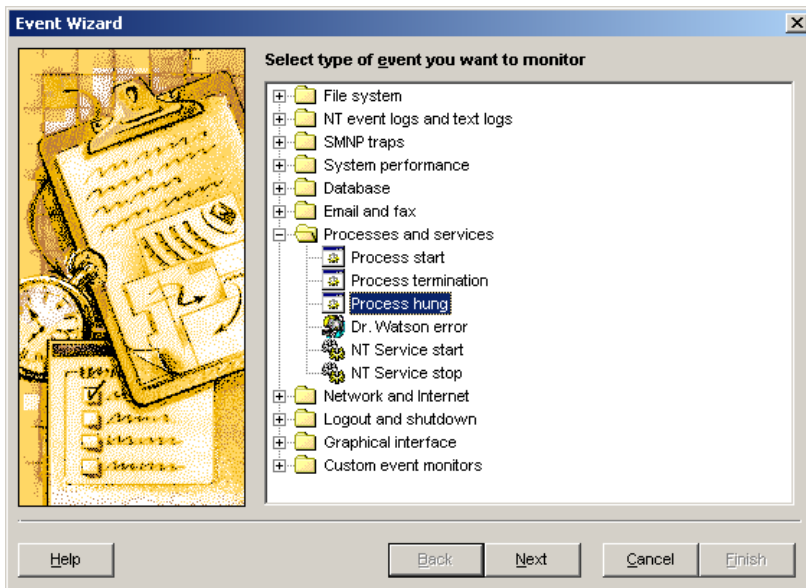
## Example 5 – Hung application monitoring and restarting

**Task:** Monitor hung applications and automatically restart them. In order to do that you will need KillProcess or a similar utility. KillProcess utility is now part of 24x7 Automation Suite software. This utility can be downloaded freely from <http://www.softretech.com/24x7/archive/49.htm>. You will also need to create a batch file called RESTART.BAT this file should have the following contents:

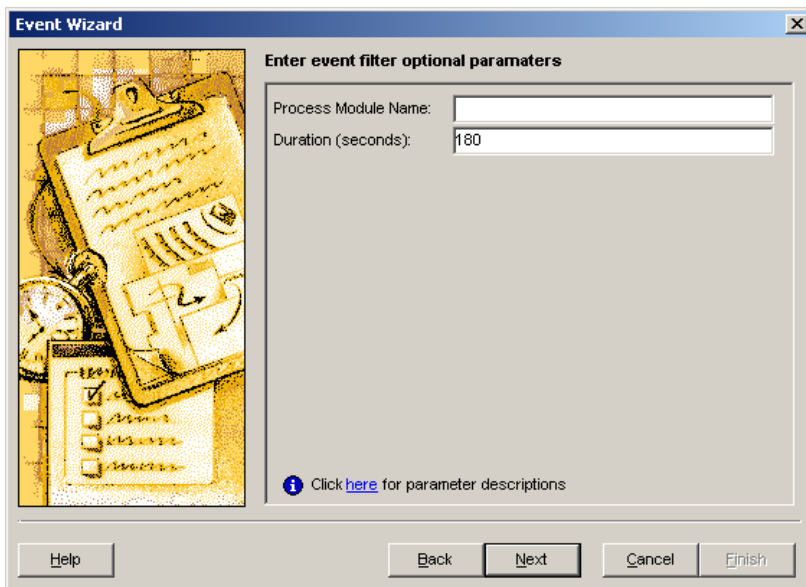
```
KillProcess %1
%1
```

**Steps:**

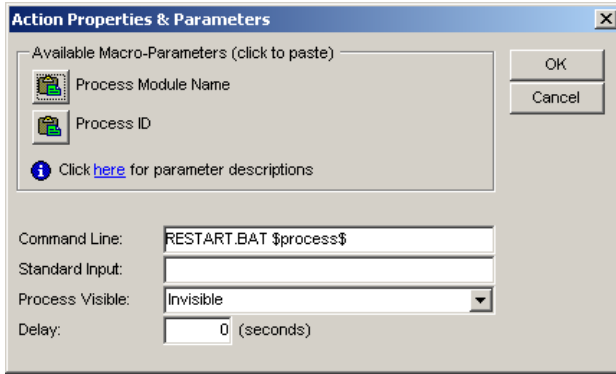
1. Start 24x7 Event Server Management Console and then click **File/New Event** menu to add a new event. The Event Wizard will appear.
2. Expand **Processes and services** folder and then within the expanded folder select **Process hung** item. Click the **Next** button.



3. To monitor a specific application enter name of the main executable file (as it appears in the Task Manager when the application is running) into the **Process Module Name** field. To monitor all applications leave this field blank. Click the **Next** button.

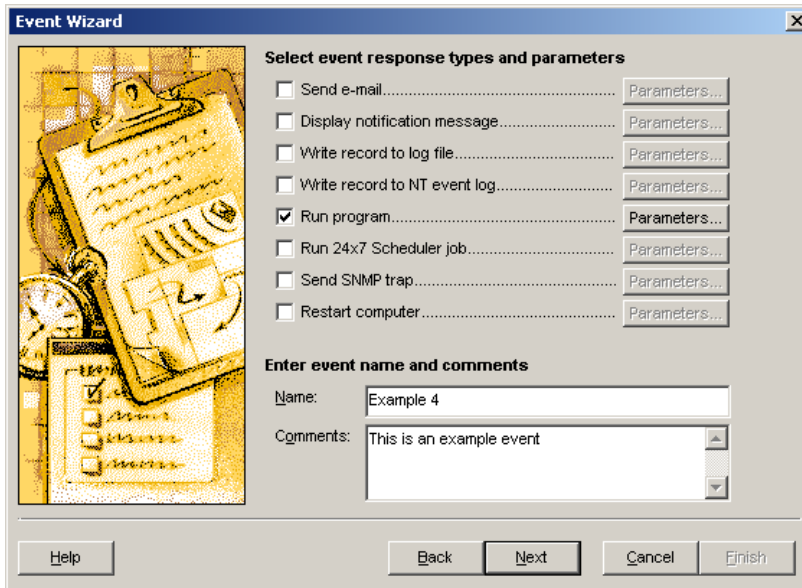


4. Skip the event monitor schedule step leaving the default schedule as is. Click the **Next** button again.
5. Check **Run program** option. This will make the corresponding **Parameters** button enabled and then click the enabled **Parameters** button. The **Actions Properties and Parameters** dialog will appear.

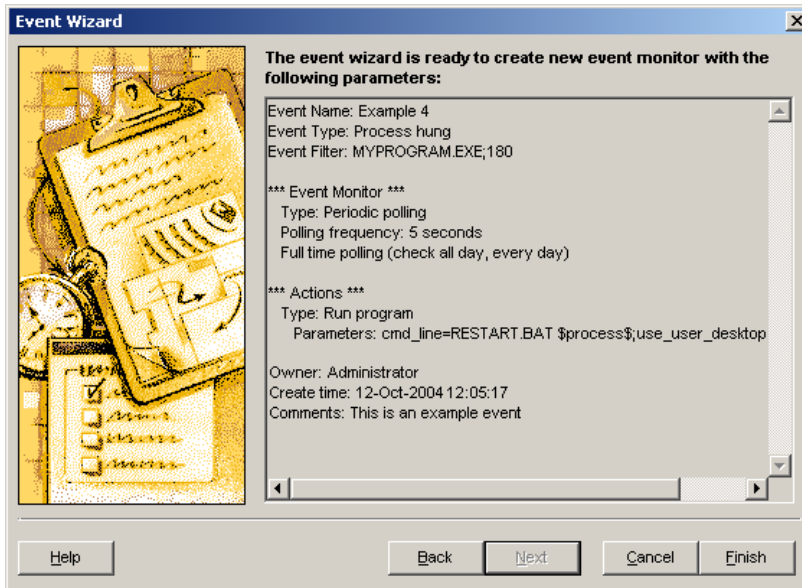


In the **Command line** field type **RESTART.BAT** then type 1 space and then click the **Paste Process Module Name** button. Click the **OK** button to close the **Actions Properties and Parameters** dialog.

6. Enter event name **Example 4** into the **Name** field and then enter optional comments into the **Comments** field. Click the **Next** button when ready.



7. This is the last step. Click the **Finish** button and then click **File/Save** menu to save the new event.

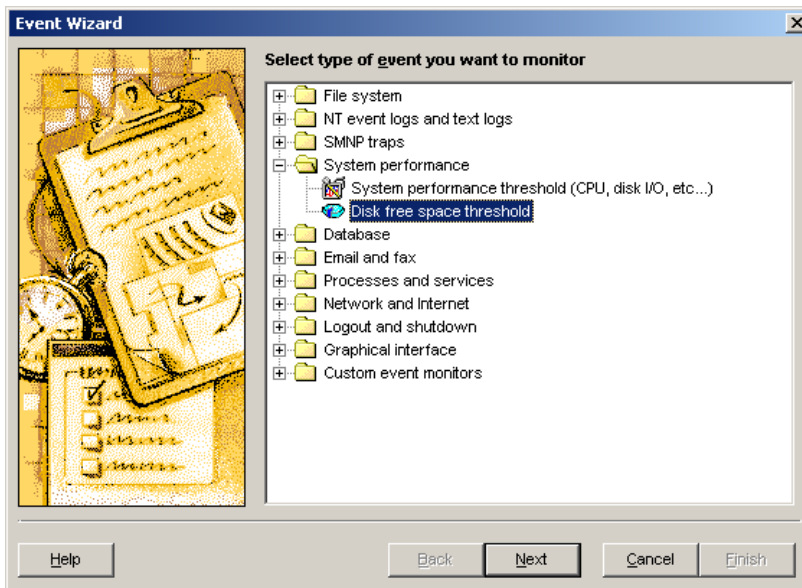


## Example 6 – Low disk space monitoring and alerting

**Task:** Monitor amount of free disk space on drive C: and write a log record to the Windows NT System Event Log whenever amount of free space falls below 200 Mbytes. In addition, send an email alert to IT personnel.

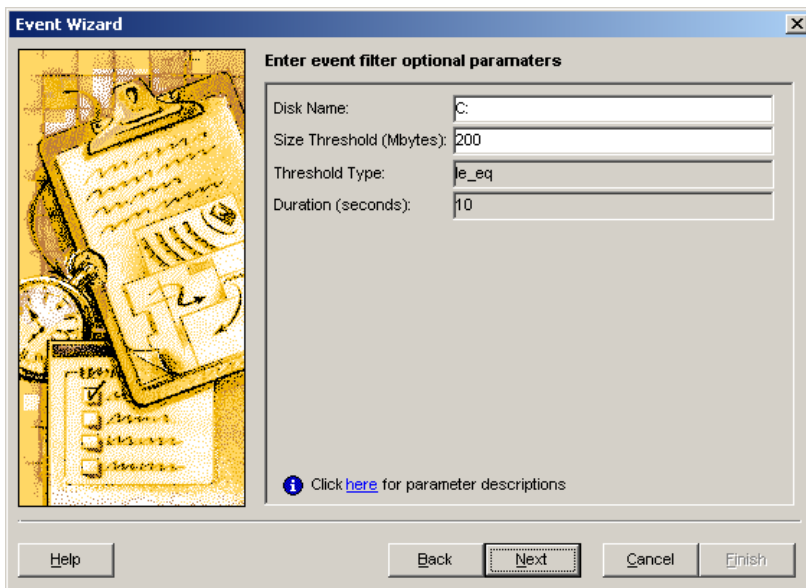
### Steps:

1. Start 24x7 Event Server Management Console and then click **File/New Event** menu to add a new event. The Event Wizard will appear.
2. Expand **System Performance** folder and then within the expanded folder select **Disk free space threshold** item. Click the **Next** button.

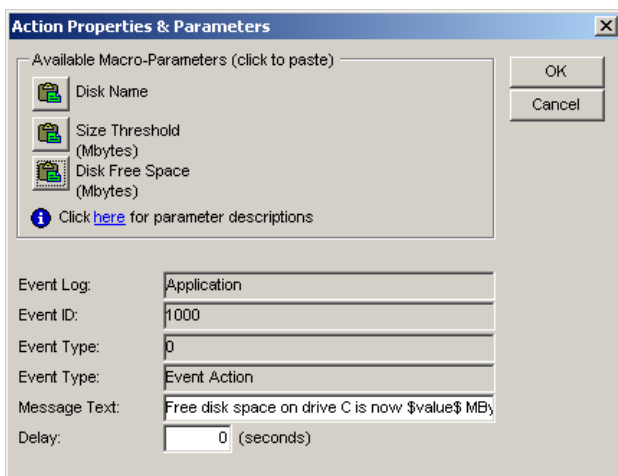


3. Enter **C:** into **Disk Name** field. Enter **200** into **Size Threshold (Mbytes)** field. Click the **Next** button.





4. Skip the event monitor schedule step leaving the default schedule as is. Click the **Next** button again.
5. Check **Write record to NT event log** option. This will make the corresponding **Parameters** button enabled and then click the enabled **Parameters** button. The **Actions Properties and Parameters** dialog will appear.

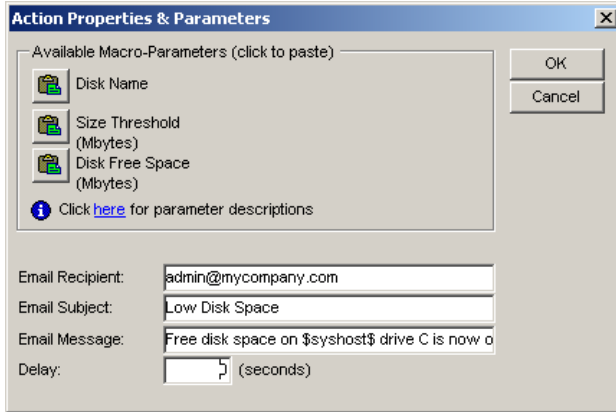


In the **Message Text** field type [Free disk space on drive C is now \\$value\\$ MBytes](#).

Please note that when the event response action will be fired the [\\$value\\$](#) macro-parameter will be replaced with the amount of actual free disk space on the drive C.

Click the **OK** button to close the **Actions Properties and Parameters** dialog.

6. Check **Send email** option. This will make the corresponding **Parameters** button enabled and then click the enabled **Parameters** button. The **Actions Properties and Parameters** dialog will appear.

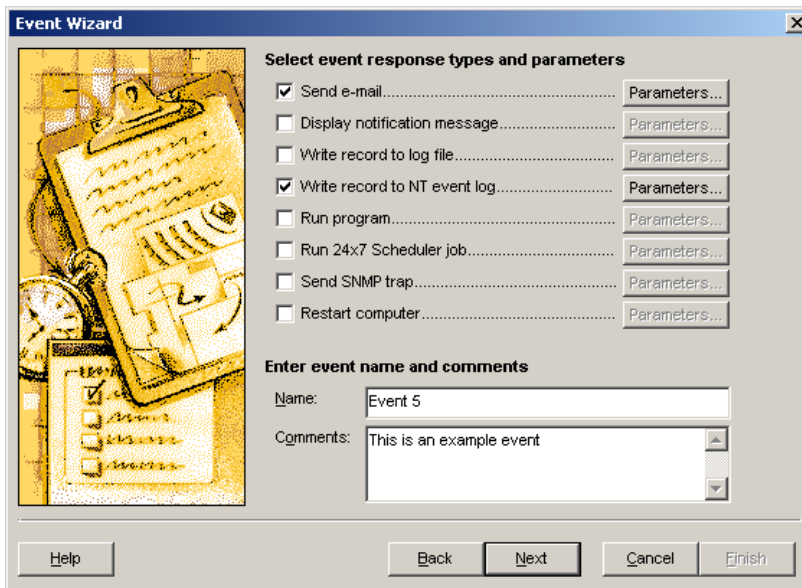


In the **Email recipient** field type your email address, for example [admin@mycompany.com](mailto:admin@mycompany.com). In the **Email Subject** field type [Low Disk Space](#). In the Email Message field type [Free disk space on \\$syshost\\$ drive C is now only \\$value\\$ MBytes](#).

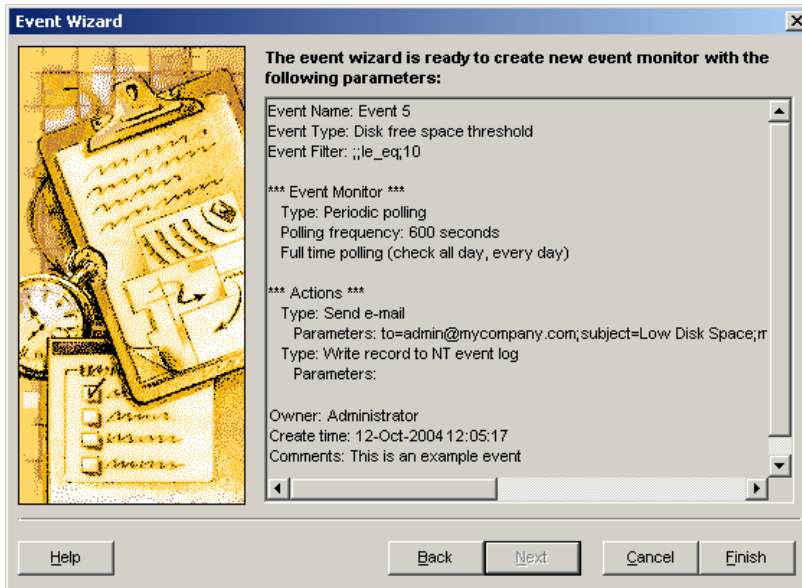
Please note that when the event response action will be fired the [\\$syshost\\$](#) macro-parameter will be replaced with the computer name and the [\\$value\\$](#) macro-parameter will be replaced with the amount of actual free disk space on the drive C.

Click the **OK** button to close the **Actions Properties and Parameters** dialog.

7. Enter event name [Example 5](#) into the **Name** field and then enter optional comments into the **Comments** field. Click the **Next** button when ready.



8. This is the last step. Click the **Finish** button and then click **File/Save** menu to save the new event.

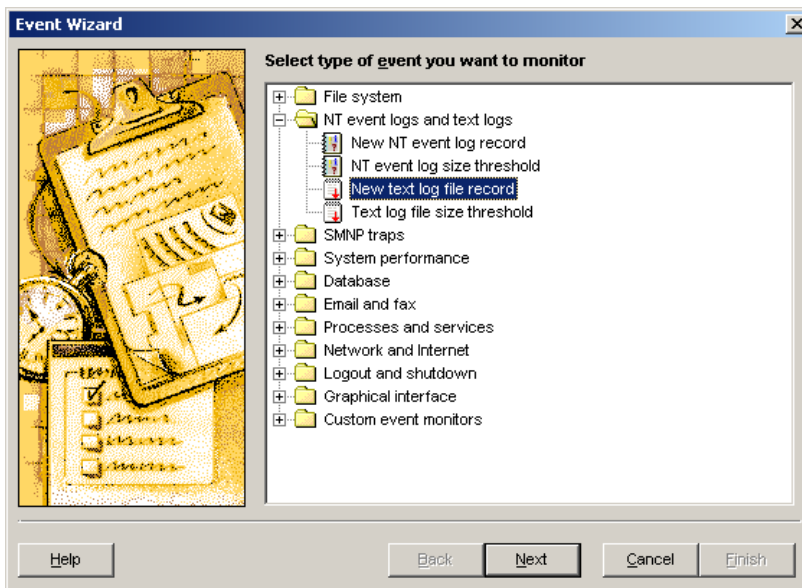


## Example 7 – Text log file monitoring and alerting

**Task:** Monitor records added to log file MYLOG.LOG in C:\LOGS folder and send an email alert to IT personnel whenever a newly added record contains word ERROR. The email alert will contain the complete record text.

### Steps:

1. Start 24x7 Event Server Management Console and then click **File/New Event** menu to add a new event. The Event Wizard will appear.
2. Expand **NT event logs and text files** folder and then within the expanded folder select **New text log file record** item. Click the **Next** button.



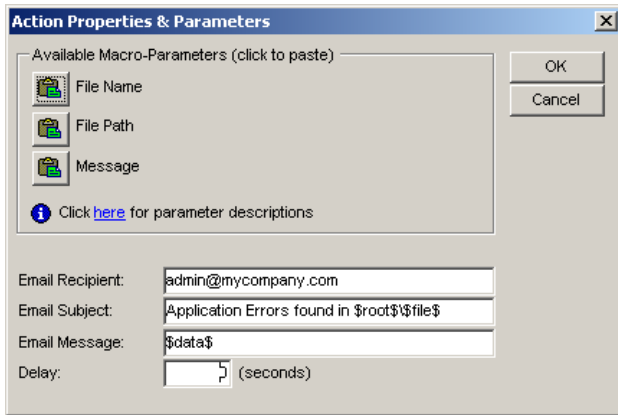
- Enter `mylog.log` into the **File Name** field; enter word `error` into **Message Contains** field; enter `c:\logs` into the **File Path** field. Click the **Next** button.

The screenshot shows the 'Event Wizard' dialog box with the title 'Enter event filter optional parameters'. On the left is a decorative image of a clipboard with a checklist. The main area contains three text input fields: 'File Name' with 'mylog.log', 'Message Contains' with 'error', and 'File Path' with 'c:\logs'. Below these fields is a link: 'Click [here](#) for parameter descriptions'. At the bottom are buttons for 'Help', 'Back', 'Next', 'Cancel', and 'Finish'.

- Customize event monitor schedule as needed. Click the **Next** button again if it's ok to check for log changes files 24 hours a days, 7 days a week, every 5 seconds, otherwise select a different schedule and then click the **Next** button.

The screenshot shows the 'Event Wizard' dialog box with the title 'Select event monitoring method and frequency'. On the left is the same decorative image of a clipboard. The main area has three radio button options: 'Real-time monitoring', 'Periodic polling', and 'Limited time polling (by day and/or time)'. The 'Periodic polling' option is selected. Below it, there is a text field 'Check event conditions every' with the value '5' and the unit 'seconds'. Underneath are three more radio button options: 'Full time polling (check all day, every day)' (which is selected), and 'Limited time polling (by day and/or time)'. The 'Limited time polling' option has two time pickers: 'Check from' set to '12:00:00 AM' and 'to' set to '11:59:59 PM'. Below these are checkboxes for 'Days of week' for Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are checked. At the bottom are buttons for 'Help', 'Back', 'Next', 'Cancel', and 'Finish'.

- Check **Send email** option. This will make the corresponding **Parameters** button enabled and then click the enabled **Parameters** button. The **Actions Properties and Parameters** dialog will appear.



In the **Email recipient** field type your email address, for example [admin@mycompany.com](mailto:admin@mycompany.com). In the **Email Subject** field type [Application Errors found in](#) then type 1 space and then click **Paste File Path** button, type 1 backslash and then click the **Paste File Name** button. The resulting text should look as below

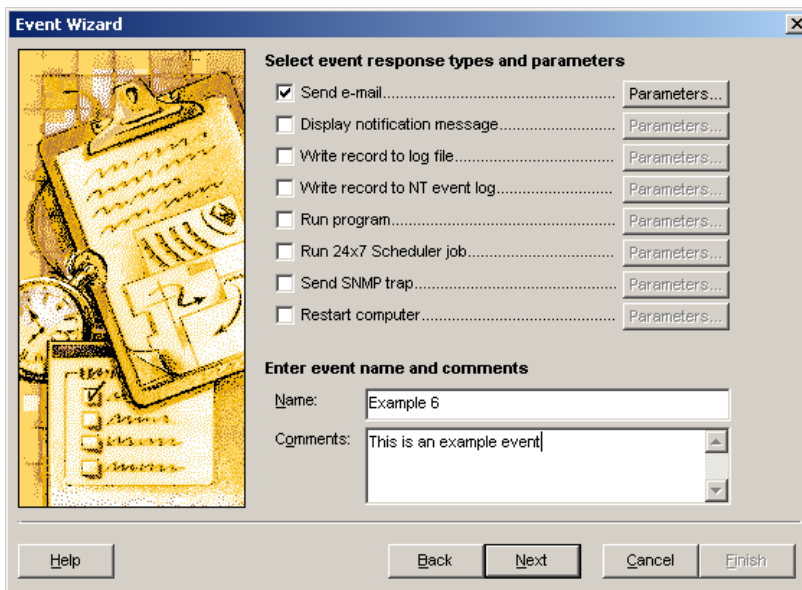
[Application Errors found in \\$root\\$\file\\$](#)

Activate the Email Message field and then click the **Paste Message** button.

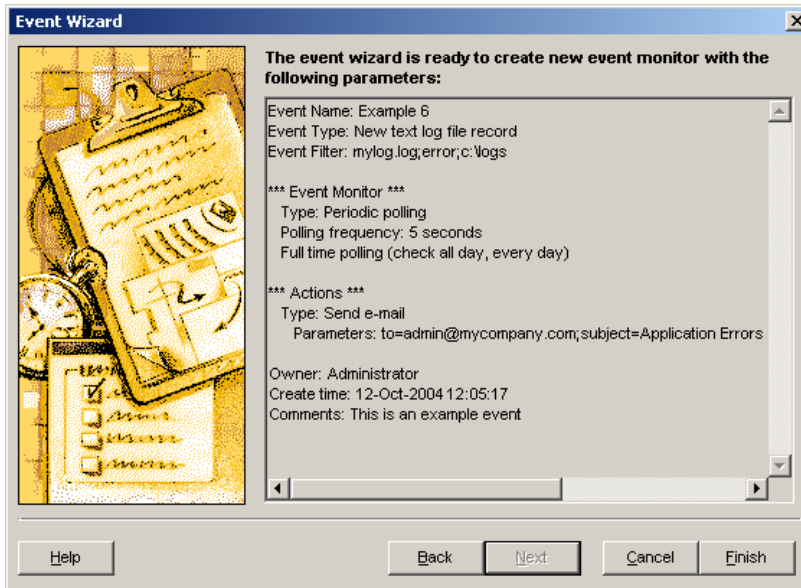
Please note that when the event response action will be fired the [\\$root\\$](#) and [\\$file\\$](#) macro-parameters will be replaced with the actual directory and file name of the log file so that the resulting text will contain the complete file name of the new file. The email message will contain the complete record from MYLOG.LOG file as specified by [\\$data\\$](#) macro-parameter.

Click the **OK** button to close the **Actions Properties and Parameters** dialog.

6. Enter event name [Example 6](#) into the **Name** field and then enter optional comments into the **Comments** field. Click the **Next** button when ready.



This is the last step. Click the **Finish** button and then click **File/Save** menu to save the new event.

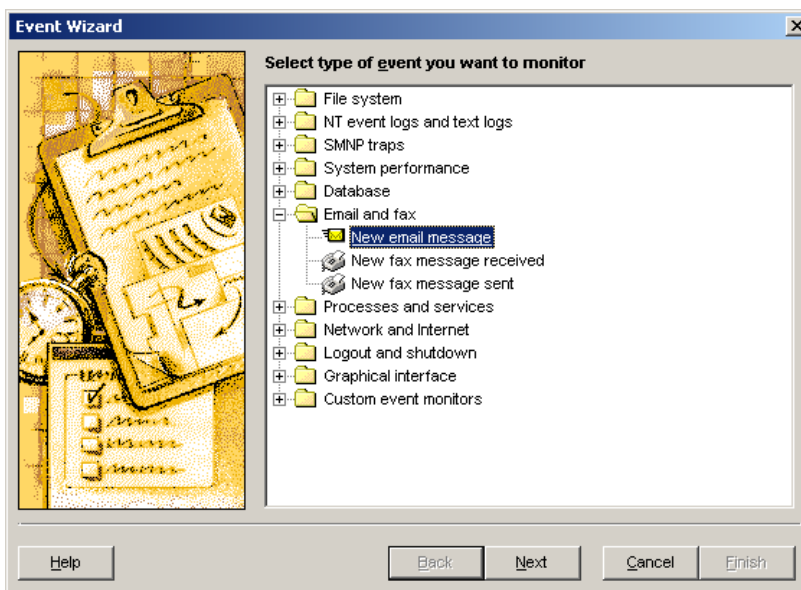


## Example 8 – Incoming email monitoring and loading email attachments into a database

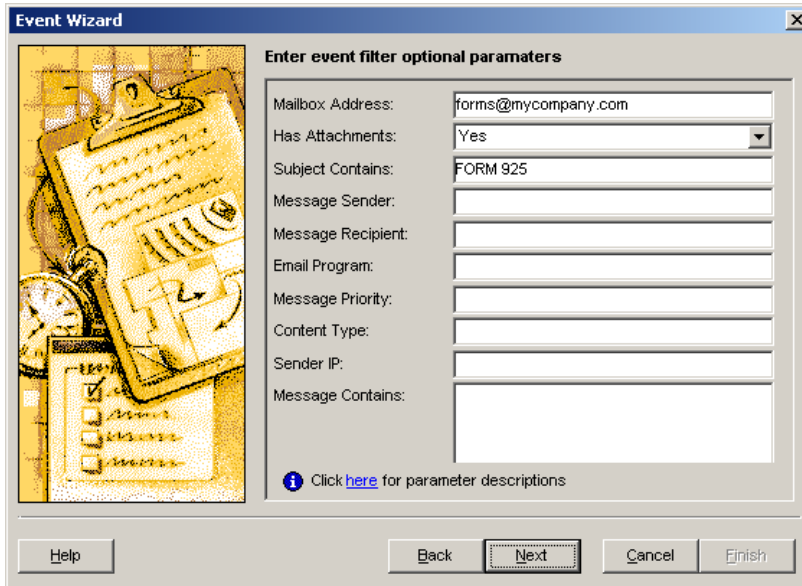
**Task:** Monitor new emails in POP3 mailbox FORMS@MYCOMPANY.COM, If email subject contains words FORM 925, save attached files in the default temporary folder and then run a 24x7 Scheduler job #118 that loads files into the forms processing database.

### Steps:

1. Start 24x7 Event Server Management Console and then click **File/New Event** menu to add a new event. The Event Wizard will appear.
2. Expand **Email and fax** folder and then within the expanded folder select **New email message** item. Click the **Next** button.

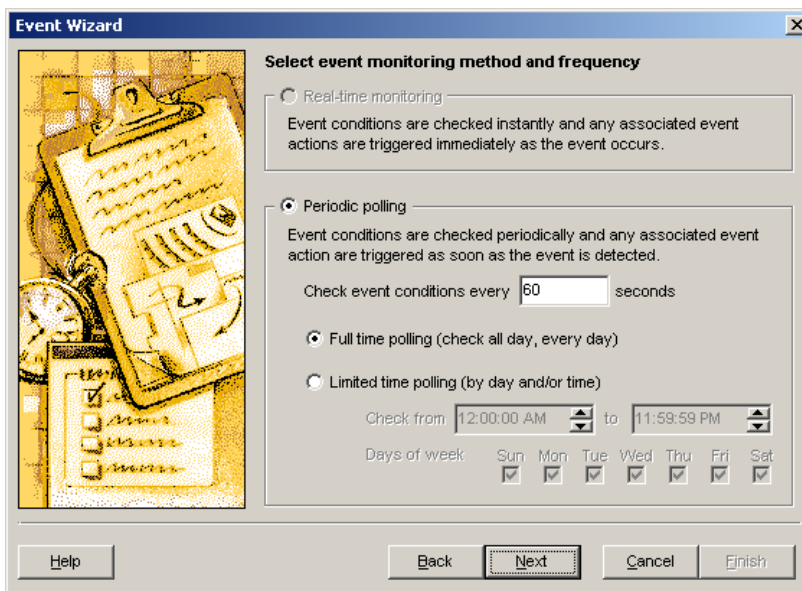


3. Enter `forms:mypassword@mycompany.com` into the **Mailbox Address** field (here we use `forms` as `mypassword` as a password for the mailbox). Enter `FORM 925` into the **Subject Contains** field. Click the **Next** button.



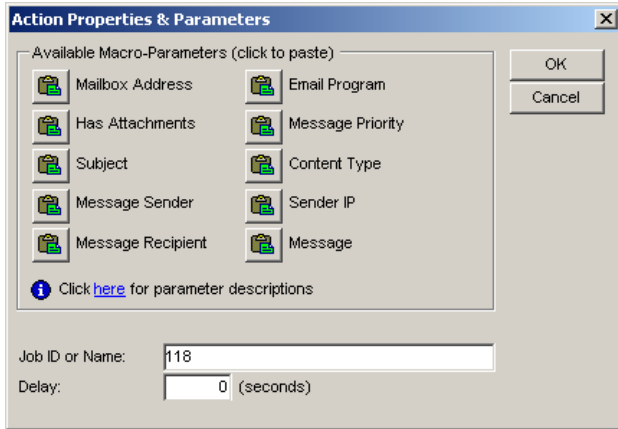
The screenshot shows the 'Event Wizard' dialog box with the title 'Enter event filter optional parameters'. On the left is a decorative image of a clipboard with a checklist. The main area contains several input fields: 'Mailbox Address' (text box with 'forms@mycompany.com'), 'Has Attachments' (dropdown menu with 'Yes'), 'Subject Contains' (text box with 'FORM 925'), and empty text boxes for 'Message Sender', 'Message Recipient', 'Email Program', 'Message Priority', 'Content Type', and 'Sender IP'. A larger text area for 'Message Contains' is at the bottom. A link 'Click here for parameter descriptions' is visible. At the bottom are buttons for 'Help', 'Back', 'Next', 'Cancel', and 'Finish'.

4. Customize event monitor schedule as needed. Click the **Next** button again if it's ok to check for new email 24 hours a days, 7 days a week, every minute, otherwise select a different schedule and then click the **Next** button.



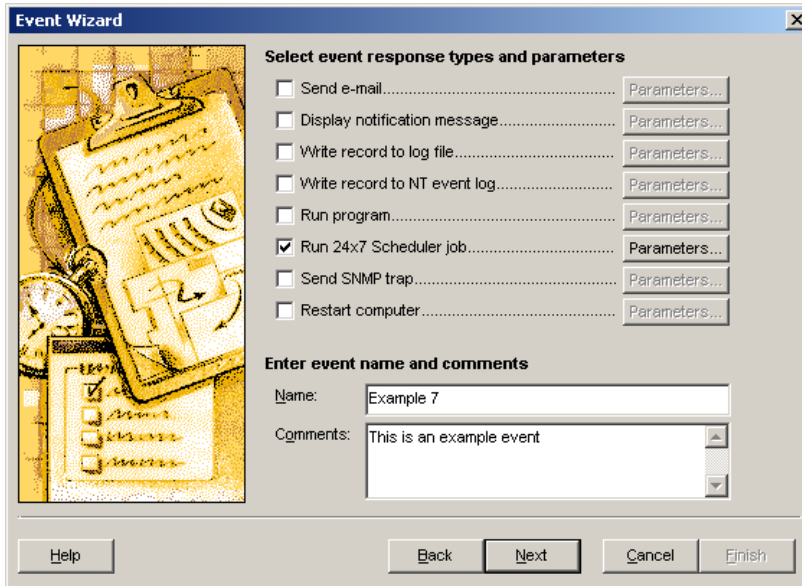
The screenshot shows the 'Event Wizard' dialog box with the title 'Select event monitoring method and frequency'. On the left is the same decorative image of a clipboard. The main area has three radio button options: 'Real-time monitoring' (unselected), 'Periodic polling' (selected), and 'Limited time polling (by day and/or time)' (unselected). Below 'Periodic polling' is a text box for 'Check event conditions every' with the value '60' and the unit 'seconds'. Below 'Limited time polling' are two time pickers: 'Check from' (12:00:00 AM) and 'to' (11:59:59 PM). Below these are checkboxes for 'Days of week' (Sun, Mon, Tue, Wed, Thu, Fri, Sat), all of which are checked. At the bottom are buttons for 'Help', 'Back', 'Next', 'Cancel', and 'Finish'.

5. Check **Run 24x7 Scheduler job** option. This will make the corresponding **Parameters** button enabled and then click the enabled **Parameters** button. The **Actions Properties and Parameters** dialog will appear.



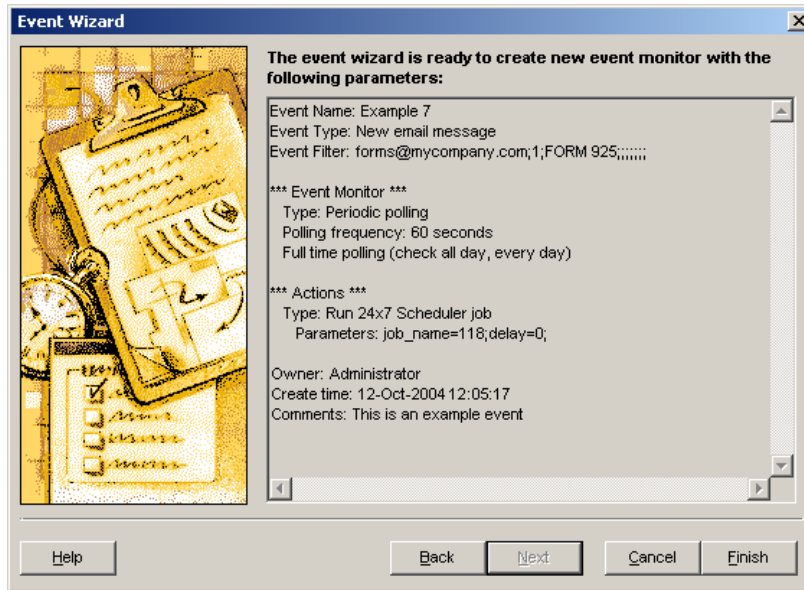
In the **Job ID or Name** field type **118**. Click the **OK** button to close the **Actions Properties and Parameters** dialog.

6. Enter event name **Example 7** into the **Name** field and then enter optional comments into the **Comments** field. Click the **Next** button when ready.



7. This is the last step. Click the **Finish** button and then click **File/Save** menu to save the new event.





## Appendix 1: Technical Support

Your questions, comments, and suggestions are welcome.

For technical support, e-mail to [support@softtreetech.com](mailto:support@softtreetech.com) or use the on-line support form at <http://www.softtreetech.com/Support.htm>.

When reporting problems, please provide as much information as possible about your problem. Be sure to include the following information:

- 1 Is the problem reproducible? If so, how?
- 2 What version of Windows are you running? For example, Windows NT 4.0, Windows 2000, etc.
- 3 What version of the 24x7 Event Server are you running?
- 4 If a dialog box with an error message was displayed, please include the full text of the dialog box, including the text in the title bar.
- 5 If the problem involves an external program, provide as much information as possible about this program.
- 6 Make sure you include the serial number for your copy of 24x7 Event Server. Use the **Help/About** menu to look up the correct numbers. Registered users have priority support.

For registration information, purchasing or other sales information, please contact our sales department: [sales@softtreetech.com](mailto:sales@softtreetech.com).

For general information, software updates, the latest information on known problems and answers to frequently asked questions, visit the 24x7 Event Server home page on the Web: <http://www.softtreetech.com/24x7/>.

We are happy to help in any way we can, but if you are having problems, please check the troubleshooting section first to see if your question is answered there.

## Appendix 2: Licensing

You must obtain 24x7 Automation Suite site license or a separate 24x7 Event Server license before you can install 24x7 Event Server on your system.

Redistribution: You must obtain redistribution license before you can redistribute it with your program.

=====

### 24x7 Event Server Software License

The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is licensed, not sold.

**CAUTION:** Loading this software onto a computer indicates your acceptance of the following terms. Please read them carefully.

**GRANT OF LICENSE:** SoftTree Technologies, Inc. ("SoftTree Technologies") grants you a license to use the software ("Software"). You may install the Software on no more than one machine per valid license or as defined by purchased licenses. You may make other copies of the Software for backup and archival purposes only.

You may permanently transfer all of your rights under this Software LICENSE only in conjunction with a permanent transfer of your validly licensed copy of the product(s).

**LICENSE TYPES:** The Software and associated add-in components are licensed on a RUN-TIME basis, which means, that for each computer on which the Software is installed, a valid run-time license must exist.

#### Single License

Allows installation and execution of the Software on a single computer (a stand-alone computer or a single workstation in a network or a single network server) per license.

#### Site License

Allows installation and execution of the Software on multiple computers within a single physical location (i.e. an office or data center location at a single physical address).

#### Enterprise License

Allows installation and execution of the Software on multiple computers in multiple locations throughout the licensed company's facilities.

**RESTRICTIONS:** Unregistered versions (shareware licensed copies) of the Software may be used for a period of not more than 30 days. After 30 days, you must either stop using the Software, or purchase a validly licensed copy.

You must maintain all copyright notices on all copies of the Software. You may not sell copies of the Software to third parties without express written consent of SoftTree Technologies and under SoftTree Technologies' instruction.

EVALUATION copies may be distributed freely without charge so long as the Software remains whole including but not limited to existing copyright notices, installation and setup utilities, help files, licensing agreement, In executing such an act as distributing without the similar copyright or license violation, to the maximum extent permitted by applicable law you may be held liable for loss of revenue to SoftTree Technologies or SoftTree Technologies' representatives due to loss of sales or devaluation of the Software or both.

You must comply with all applicable laws regarding the use of the Software.

**COPYRIGHT:** The Software is the proprietary product of SoftTree Technologies and is protected by copyright law. You acquire only the right to use the Software and do not acquire any rights of ownership. You agree not to remove any product identification, copyright notices, or other notices or proprietary restrictions from the Software. You agree not to cause or permit the reverse engineering, disassembly, or decompilation of the Software.

**DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS:** You may not rent, lease or transfer the Software except as outlined under GRANT OF LICENSE - use and copy.

Without prejudice to any other rights, SoftTree may terminate this Software LICENSE if you fail to comply with the terms and conditions of this Software LICENSE. In such event, you must destroy all copies of the Software and all of its component parts.

**WARRANTY DISCLAIMER:** SoftTree Technologies is providing this license on an "as is" basis without warranty of any kind; SoftTree Technologies disclaims all express and implied warranties, including the implied warranties of merchantability or fitness for a particular purpose.

**LIMITATION OF LIABILITY:** SoftTree Technologies shall not be liable for any damages, including direct, indirect, incidental, special or consequential damages, or damages for loss of profits, revenue, data or data use, incurred by you or any third party, whether in an action in contract or tort, even if you or any other person has been advised of the possibility of such damages.

SoftTree Technologies, Inc.  
62 Ilyse Ct  
Staten Island NY, 10306  
USA

Copyright (c) SoftTree Technologies, Inc. 2004-2006 All Rights Reserved