

# The Sentry-go Monitoring System

## Monitoring Windows Event Logs & Log Files

Last Updated Wednesday, 04 November 2009

© 3Ds (UK) Limited  
<http://www.Sentry-go.com>

*Be Proactive, Not Reactive!*

---

### Table of Contents

- Symbols .....2
- Background.....2
- Recommended Monitoring Settings .....2
- Quick Facts.....3
- Monitoring Event Logs & Log Files .....3
- Configuring Event Log Monitoring .....5
- Configuring Text File Monitoring.....8
- How to Monitor Log Files ..... 11
- Considerations for Other File Systems .....11
- Temporarily Ignoring a Configured Check.....12
- Configuring an Automatic Response .....12
- More Information, Help & Support .....13



---

## Symbols

Thank you for choosing Sentry-go® as your monitoring solution for Windows. In this guide, the following symbols are used to denote specific items ...



Important information which should be noted – it may affect what you are trying to do.



Additional information relating to the operation being described is shown.

---

## Background

Many server-based applications, as well as Windows itself write their errors to the Windows Event Log. In addition, applications – such as Microsoft Exchange, SQL Server & Internet Information etc. also write messages to their own text-based log files. However, because both of these are typically located on the local machine, proactively monitoring them can be difficult.

With Sentry-go, monitoring messages written to one or more Event Logs, text-based or memory mapped files is both quick & easy to achieve.

---

## Recommended Monitoring Settings

It is recommended that the standard Event logs are monitored for events of type “error”. Optionally you may also wish to check for other event types using the keywords shown below.

Text-based log files are checked via keywords, which should be set based on their content. However, as a guide, the following keywords may be used ...

- error
- denied
- exception
- fail
- fatal
- illegal
- incorrect
- invalid
- not enough
- refused
- unable
- unexpected
- unknown
- violation



The actual keyword list will be dependent on the software writing the log entries and the messages used in those entries.

---

## Quick Facts

Here is a summary of the options available with this component. They are discussed in more detail in the pages that follow ...

Component :	Event Log & Log File Monitor
Aim/Description :	To monitor Event Logs and/or log files for errors based on keywords & phrases, event IDs, source application & event type (dependent on file type)
Main Monitoring Features :	<ul style="list-style-type: none"><li>• Monitor Event Log records for new events based on the above criteria</li><li>• Monitor text-based log files for new entries based on keyword(s) &amp; phrase(s)</li><li>• Scan for &amp; automatically monitor log files.</li></ul>
Periodic Monitoring :	✓
Scheduled Monitoring :	
Local Monitoring :	✓
Dial-up Support :	
Alerting :	All alerting & auto-response options available
Web Reports :	Status report
External software req's :	None

---

## Monitoring Event Logs & Log Files

To monitor Event Logs &/or log files simply select the Sentry-go monitor from the Console with the right mouse button and click "Configure".

A window containing a number of tabs will be displayed. To monitor available disk space, select the "Logs" tab. From here, you can configure the following ...

- The monitoring of one or more Event Logs and/or text-based log files.
- Define each check for keywords and/or events to capture as appropriate
- Temporarily disable the monitoring of one, more or all sites/pages.

The resulting list will show all the currently defined log files and Event Logs being monitored. From here you can add new monitored items, edit existing ones or delete them from the monitor's scan.

The screenshot shows the 'Sentry-go Configuration - Local Machine' window. The title bar reads 'Sentry-go - View & Edit Configuration Settings'. Below the title bar is a navigation menu with buttons for 'Logs', 'Disks', 'Services', 'Process', 'Printers', 'Files', 'Ports', 'HTML', and 'FTP'. The 'Logs' button is selected. Below the navigation menu is a help icon and a text box that says 'This option allows you to monitor Event Logs or text-based log files on the local server ...'. The main area is titled 'Monitor Event Logs & Log Files' and contains a table of currently defined logs. Below the table are 'Delete', 'Add ...', and 'Edit ...' buttons. At the bottom of the window are 'OK', 'Cancel', and 'Help' buttons.

Monitor Event Logs & Log Files

The following logs are currently defined. You can modify these settings by clicking the appropriate button below ...

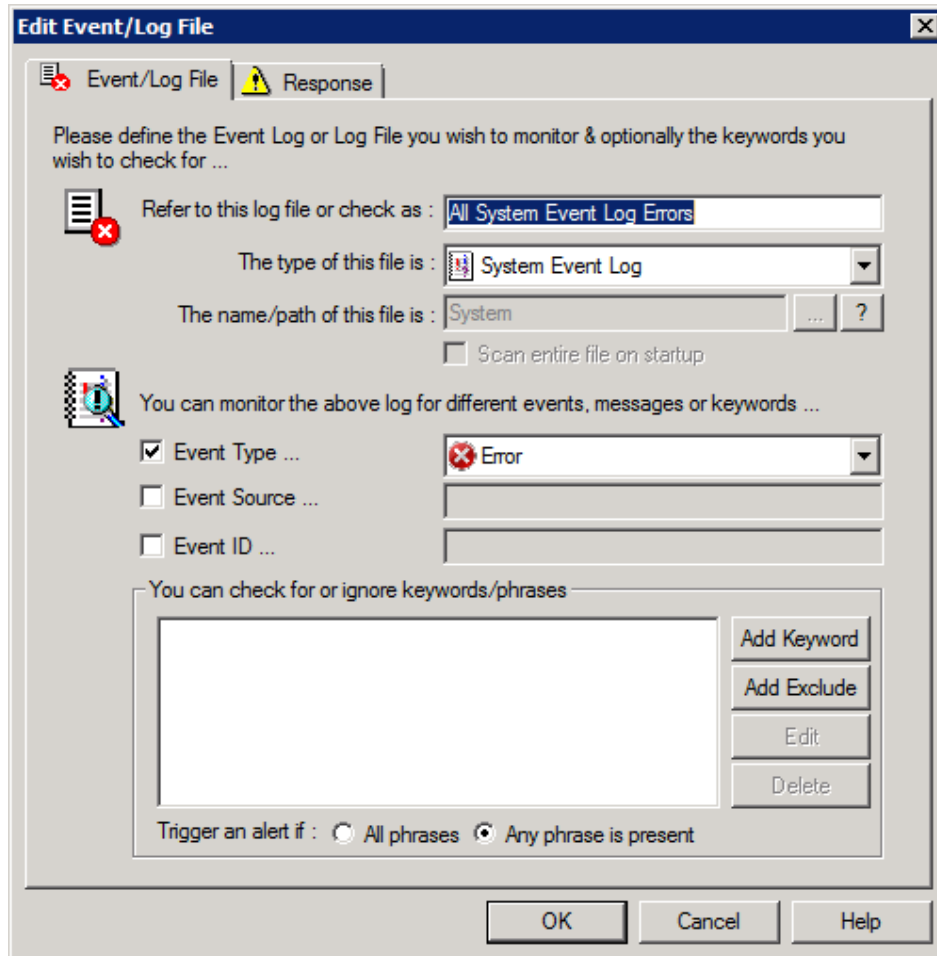
Name	Check Type	Action	Alert Group
<input type="checkbox"/> System Event Log Errors ...	System Event Log	No Response - Alert Only	1
<input type="checkbox"/> Application Event Log Er...	Application Event Log	No Response - Alert Only	1
<input checked="" type="checkbox"/> All Application Event Log...	Application Event Log	No Response - Alert Only	1
<input checked="" type="checkbox"/> All System Event Log Er...	System Event Log	No Response - Alert Only	1
<input checked="" type="checkbox"/> All Failed Audit Errors	Security Event Log	No Response - Alert Only	1
<input type="checkbox"/> Example Log File	Text Log File	No Response - Alert Only	1

Buttons: Delete, Add ..., Edit ...

Buttons: OK, Cancel, Help

## Configuring Event Log Monitoring

To monitor a new Event log or edit an existing one, select the Add or Edit option from the main window.



From here you can define which Event Log you wish to monitor and under which conditions an alert should be triggered.

### Refer to this log file or check as

This is the unique name of the check being made. It is this name that will be displayed on reports and when alerts are generated. It is recommended that a short descriptive name be used for this value.

### The type of this file is ...


Select the type of Event Log you wish to monitor from the list.


### The name/path of this file is

For standard Event Logs this value is read-only and indicates the name of the selected Event Log above. There is no need to enter a path for Event Logs.

For custom Event Logs, this should be the registered name of the Event Log. To find this name ...

- Run Regedit.exe on the machine being monitored to access the local registry. Do not edit the Registry values, we simply want to view them.
- Navigate to the key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog
- Below this key will be a number of sub-keys including Application, System etc. Other registered names will also be listed.
- Enter the appropriate name given here into this field to monitor the custom Event Log.

 Care should be taken when accessing the Registry. Unless you have been advised to do so, or you fully understand your actions, do not change any values in the Registry. Incorrect settings may cause unpredictable results or result in the server failing to boot.

 Do not enter the path of the Event log's ".evt" file in this field. The name entered must be the registered name of the file.

Due to the way the Windows Event Log model works, if an incorrect Event Log name is specified, no error will be returned. Instead, the Application log will be opened and monitored & you will see "false" alerts being reported. See above for information on determining the registered Event Log name.


### Event Type

When checked (ticked), this optional value allows you to select the type of event you wish to filter on -e.g. errors, warnings etc.

 If not entered, all event types are used in the scan.


### Event Source

When checked (ticked), this optional value allows you to define the name of event source (the source name shown in Event Viewer for a particular message - normally the name of the application generating the event) you wish to filter on.

 If not entered, events from all sources are used in the scan.

### Event ID

When checked (ticked), this optional value allows you to enter the ID of the message you wish to check. Each event log message is generated with an ID that uniquely defines it within the context of the source application or system.

 If not entered, all IDs are used in the scan.

To check for more than one ID, enter each, separated with a comma.

## Keywords

The monitor detects errors in Event Logs using Sentry-go's keyword detection technology. Keywords or phrases can be used either to detect an error, or to find errors that you do not wish to monitor. Both are defined at the bottom of this window.

- **Add Keyword.**

Click this button to add a keyword or phrase that you wish to monitor to the list. If the keyword or phrase is found, an alert will be triggered, unless excluded keywords are also found.

- **Add Exclude.**

Click this button to add a keyword or phrase that indicates that the message should be ignored. If an excluded keyword is found, the message is automatically ignored, regardless of other settings.

- **Edit.**

Click Edit to edit an existing keyword or phrase listed.

- **Delete.**

Click Delete to remove an existing keyword or phrase from the list.

- **To Trigger an Alert ... must be present.**

This option determines when an alert should be triggered & keyword detection is defined ...

- **All Phrases.**

Select this option if all keywords listed must be present in the message in order to generate an alert.



Excluded keywords do not count in this check

- **Any Phrase.**

Select this option to trigger an alert if one or more of the keywords listed are found in the message.



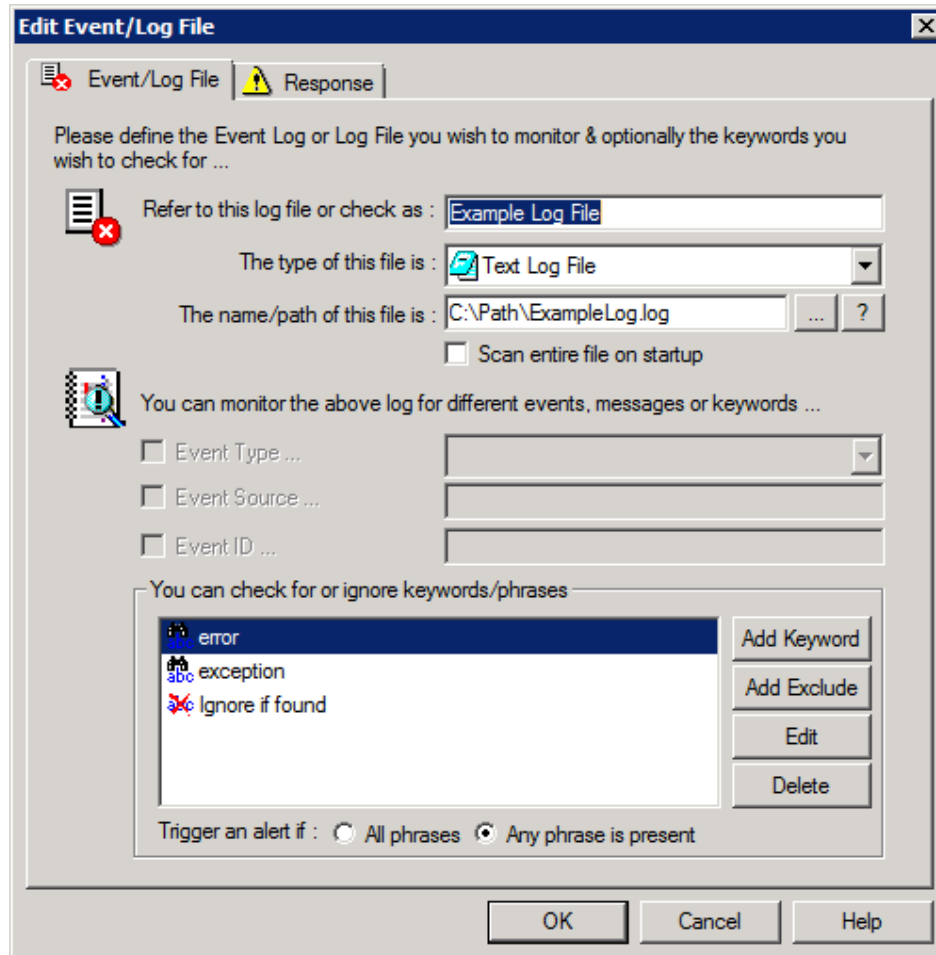
When defining a message, there is no need to add complete error messages to this list - one or more keywords is usually sufficient. By default, standard messages (and all event log errors) are included when Setup installs the monitor.

The keywords used depends on the file being monitored ...

- In most cases, generic keywords can be used such as **"error"**, **"failed"**, **"insufficient"**, **"problem"** etc.
- To be notified of any message that contains the word "error", simply add the word **"error"** to the included list (without quotation marks).
- To be notified of any message that contains the phrase **"this is an error"**, simply add that phrase (without quotes) to the included list.
- To be notified of any message that contains the phrases "this is an error" and "database", use the [And] escape sequence within the included list. In other words, you'd add **"this is an error [And] database"** (without quotation

## Configuring Text File Monitoring

To monitor the contents of records added to a text file simply add the file to the list. You can add a new file or edit an existing one by selecting the Add or Edit option from the main window.



From here you can define which Event Log you wish to monitor and under which conditions an alert should be triggered.

### Refer to this log file or check as

This is the unique name of the check being made. It is this name that will be displayed on reports and when alerts are generated. It is recommended that a short descriptive name be used for this value.

### The type of this file is ...

Select "Test-based log file" from the list of available options.

## The name/path of this file is

This is the fully qualified path of the file you wish to monitor or a fully qualified path & mask of file(s) you wish to monitor



If you enter a fully qualified path & filename, the contents of that file will be monitored.

If you enter a fully qualified path & a mask (e.g. C:\Directory\\*.log), Sentry-go will automatically search for and monitor files of the given mask (e.g. all .log files). Where wildcards (mask) is entered, the monitor will periodically scan the directory for new & deleted files & update the scan accordingly.

When started, the monitor will automatically search for files of the given mask. If found, they will automatically be monitored. However, any existing records will only be scanned if "Scan entire file at startup" is ticked.

The monitor will periodically check for new files. When a new file of the given mask is detected, it will automatically be monitored. It will also be scanned from the beginning of the file regardless of the "Scan entire file at startup" setting.

In addition to a hard-coded path such as "C:\MyLogs\AppLog.log", system environment variables, as well as a number of special place-markers may also be used within this name.

For example ...

- The environment variable %WINDIR% - e.g. %WINDIR%\AppLog.log
- \$\$YY to include the 2 character year
- \$\$MM to include the 2 character month
- \$\$DD to include the 2 character day
- \$\$DD-n where n is a number greater than 1. Allows you to include a date n-days in the past. The associated month and/or year are automatically adjusted as required
- \$\$DD+n where n is a number greater than 1. Allows you to include a date n-days in the future. The associated month and/or year are automatically adjusted as required
- \$\$DD[-n] to include the 2 character day. The -n will not be altered
- \$\$DD[+n] to include the 2 character day. The +n will not be altered

Additionally ...

- If date variables are used, the monitor will automatically reset the date when that date changes - e.g. at midnight and continue monitoring the new file.
- A log file can be defined multiple times if required, in order to specify separate actions and detect different sets of keywords etc.

## Scan Entire File on Startup

By default, Sentry-go will monitor files for new entries added to the file after monitoring has been started. Tick this option if you want Sentry-go to scan & alert on existing entries in the file prior to monitoring for new ones.



Note that each time the monitor is restarted, the file will be scanned. This may take time to complete for large files and, in some cases, may lead to duplicate alerts being generated, especially if the monitor is restarted frequently.

**Event Type**  
**Event Source**  
**Event ID**

These are only appropriate for Event Log monitoring and can be ignored.

## Keywords

The monitor detects errors in Event Logs using Sentry-go's keyword detection technology. Keywords or phrases can be used either to detect an error, or to find errors that you do not wish to monitor. Both are defined at the bottom of this window.

- **Add Keyword.**

Click this button to add a keyword or phrase that you wish to monitor to the list. If the keyword or phrase is found, an alert will be triggered, unless excluded keywords are also found.

- **Add Exclude.**

Click this button to add a keyword or phrase that indicates that the message should be ignored. If an excluded keyword is found, the message is automatically ignored, regardless of other settings.

- **Edit.**

Click Edit to edit an existing keyword or phrase listed.

- **Delete.**

Click Delete to remove an existing keyword or phrase from the list.

- **To Trigger an Alert ... must be present.**

This option determines when an alert should be triggered & keyword detection is defined ...

- **All Phrases.**

Select this option if all keywords listed must be present in the message in order to generate an alert.



Excluded keywords do not count in this check

- **Any Phrase.**

Select this option to trigger an alert if one or more of the keywords listed are found in the message.



When defining a message, there is no need to add complete error messages to this list - one or more keywords is usually sufficient. By default, standard messages (and all event log errors) are included when Setup installs the monitor.

The keywords used depends on the file being monitored ...

- In most cases, generic keywords can be used such as **"error"**, **"failed"**, **"insufficient"**, **"problem"** etc.
- To be notified of any message that contains the word "error", simply add the word **"error"** to the included list (without quotation marks).
- To be notified of any message that contains the phrase **"this is an error"**, simply add that phrase (without quotes) to the included list.
- To be notified of any message that contains the phrases "this is an error" and "database", use the [And] escape sequence within the included list. In other words, you'd add **"this is an error [And] database"** (without quotation

---

## How to Monitor Log Files

When deciding how to monitor your text-based log files, you can select between the following options ...

- Configure the exact path & filename to monitor
- Include environment & date-based variables within the path/filename in order to monitor files that dynamically change name – i.e. based on date.
- Include wildcards – e.g. \*.log within the filename.



In this case, Sentry-go will automatically monitor for new files and monitor them accordingly.

---

## Considerations for Other File Systems

In addition to monitoring changes made to text files on Windows machines, it is also possible to monitor files written to other file systems, if the file is accessible from the machine running Sentry-go. For example, using NFS to map to a Unix directory.

However, in this case, you should be aware of the following ...

- The drive mapping must be available to Sentry-go and cannot simply be mapped by Windows Explorer as this will map the drive after the Sentry-go service has been started.



It is strongly recommended that you define the path/file using its full UNC name as opposed to a mapped drive – e.g. \\MyServer\MyShare\MyFile.txt as opposed to X:\ MyFile.txt where X: is a mapped drive.

The user configured to run the monitoring service must have permission to access the file system or remote share. By default the monitor will run under the local system user account. This will normally be fine for local file access but will not allow the monitor to access remote resources. In this case, run the Sentry-go monitoring service as a domain user.

---

## Temporarily Ignoring a Configured Check

In some cases, you may wish to exclude a check from monitoring without removing it permanently. To do this, simply remove the “tick” or check against the entry you wish to ignore in the main list.

---

## Configuring an Automatic Response

In the event an error is detected, an alert will be triggered. In this case, Sentry-go can be configured to either respond automatically (i.e. take action itself), alert one or more Administrators, or both.

To configure what the monitor should do in the event an error is detected, select the entry from the list and click Edit. On the resulting window, select the Response tab.



For more information on the options available as well as details on how to configure alerts & responses, see [Sentry-go - Configuring Alert & Automatic Response Options](#).

---

## More Information, Help & Support

More information can be found in the guides that accompany the Sentry-go software. You can also access the following resources ...

- For the very latest information & product updates, please visit <http://www.Sentry-go.com>
- For sales advice, please e-mail [Sales@Sentry-go.com](mailto:Sales@Sentry-go.com)
- For technical support, please e-mail [Support@Sentry-go.com](mailto:Support@Sentry-go.com)



**3Ds (UK) Limited**  
*Design, Develop, Deliver Solutions!*

69, Esher Road,  
East Molesey,  
Surrey.  
KT8 0AQ

<http://www.3Ds.co.uk>