



Configuring Event Log Monitoring

With Sentry-go Quick & Plus! monitors

© 3Ds (UK) Limited, November, 2013

<http://www.Sentry-go.com>

Be Proactive, Not Reactive!

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.

In this guide

System requirements	2
Recommended settings	2
Monitoring event logs & log files	2
Event logs & log file settings	3
Configuring event log monitoring	4
Configuring text file monitoring.....	7
How to monitor log files	11
Considerations for file types.....	11
Considerations for other file systems.....	11
Scheduling a check	12
Configuring an automatic response	12
Configuring an alert.....	12
Temporarily ignoring a configured check	12
More Information	13

System requirements

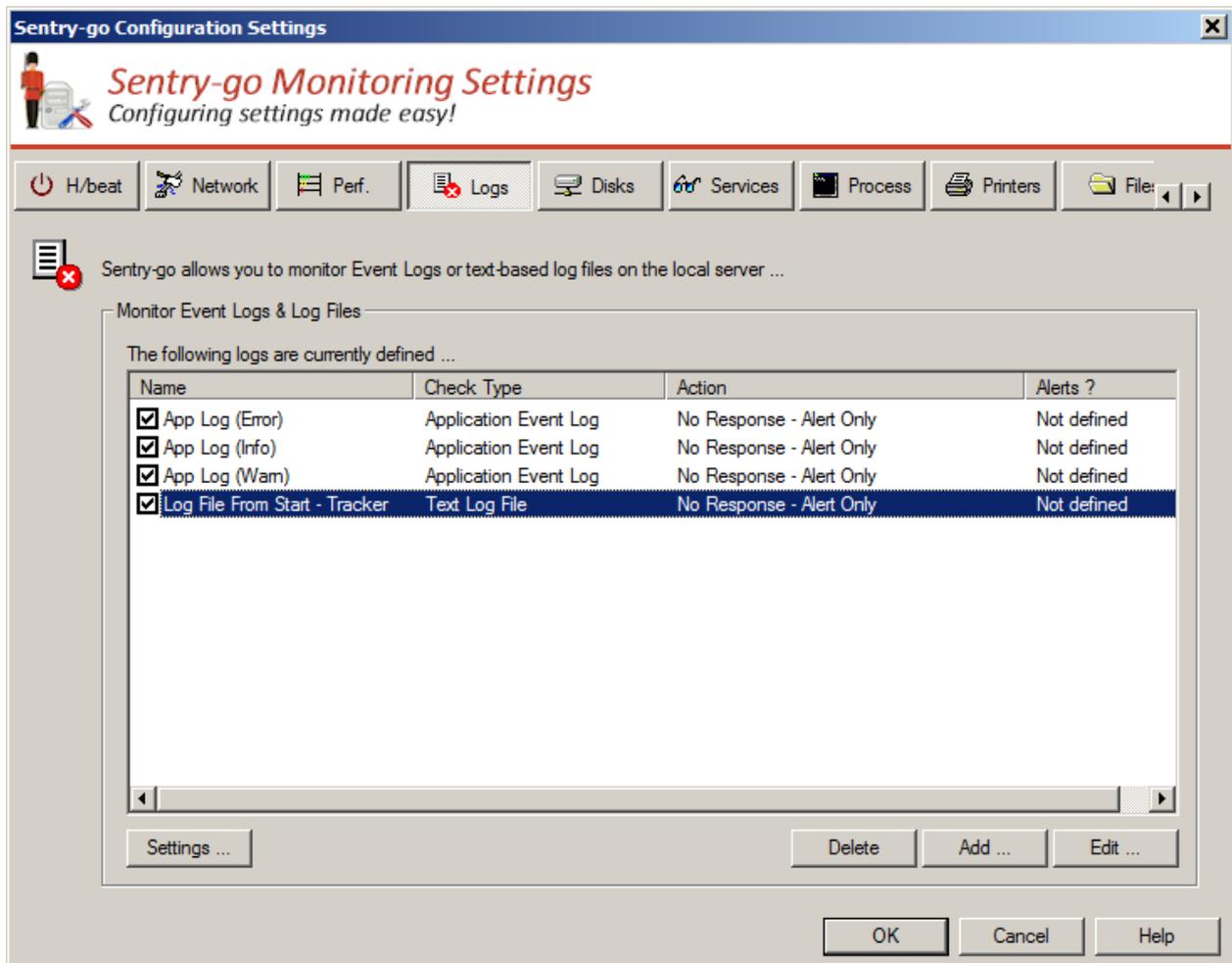
This component is fully compatible with both Sentry-go Quick Monitors v6 and above, and Sentry-go Plus! v6 monitors and above.

Recommended settings

It is recommended that the System & Application Event Logs are monitored for errors being recorded. Other requirements are dependent on the software installed.

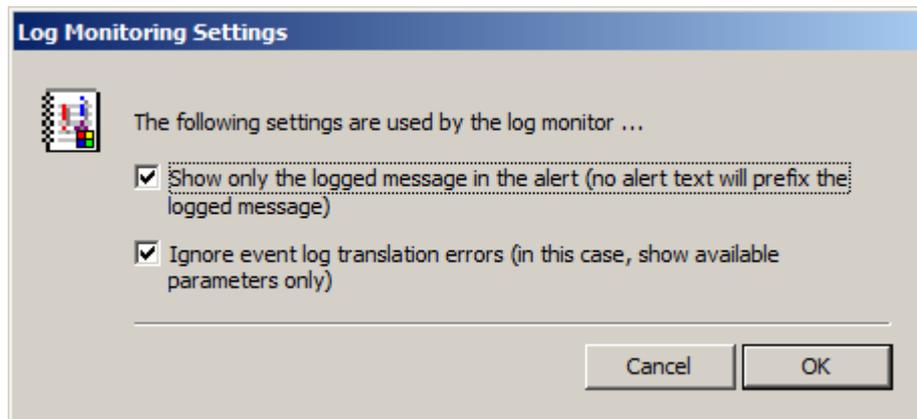
Monitoring event logs & log files

To set up monitoring, configure the appropriate monitor and select the “Logs” tab.



Event logs & log file settings

To view or edit global settings for the log monitor, click the “Settings” button to display the following window or edit global settings for the log monitor, click the “Settings” button to display the following window ...



Show only the logged message in the alert

By default, the captured message text from the log file or event log will be displayed within information relating to the alert – e.g. “The following message was detected” etc. This makes the alert message more readable when sent by e-mail or to Consoles.

Tick this option to only log the message text, with no additional alert-related information shown before it.

 In earlier versions of Sentry-go this was the default behaviour.

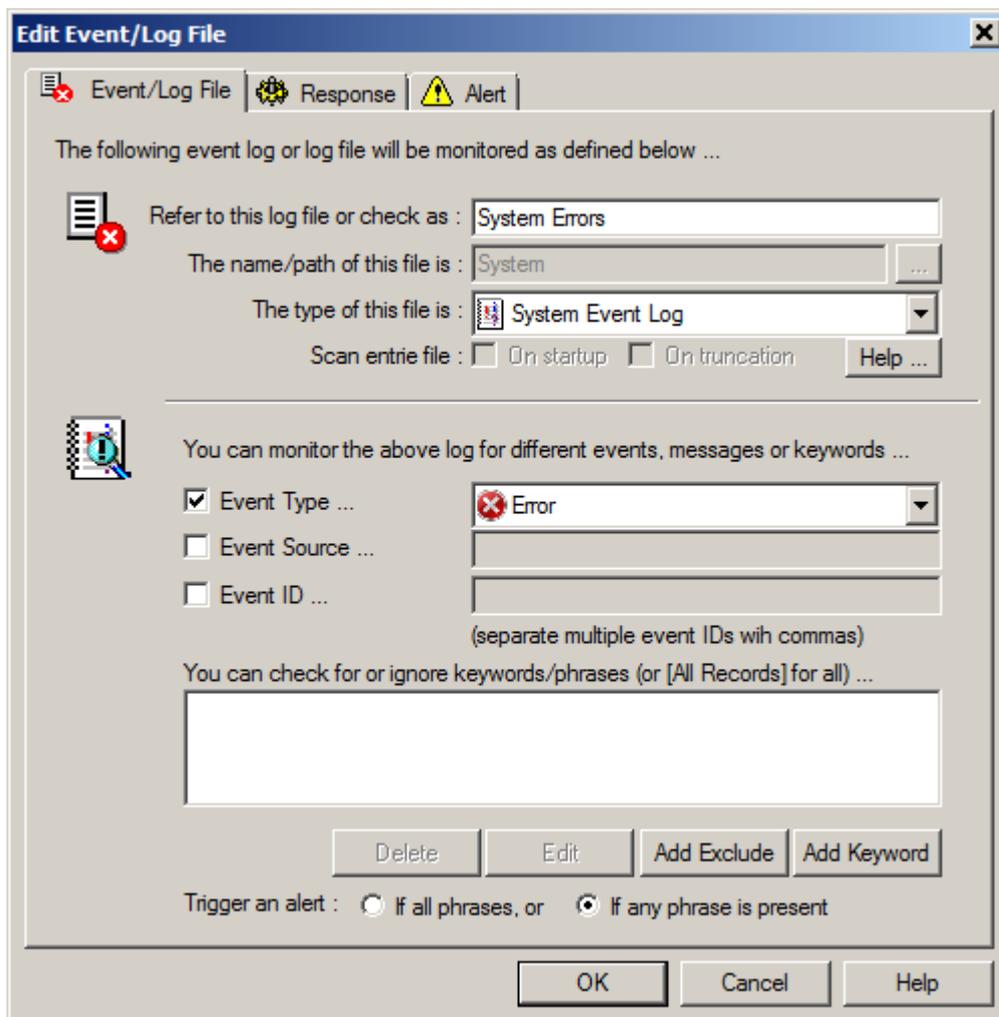
Ignore event log translation errors

When an event log message cannot be translated (e.g. the required DLLs are not installed on the server, the message is corrupt etc.), Sentry-go will, by default, substitute an error message followed by any variables that were supplied.

Tick this option to replace the error message with a default text “Event log message: “ followed by the variables that would have been displayed (or the raw XML for later versions of Windows).

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 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.

The type of this file is ...

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

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.

 To record all events, enter [All Records] as your phrase.

- **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.

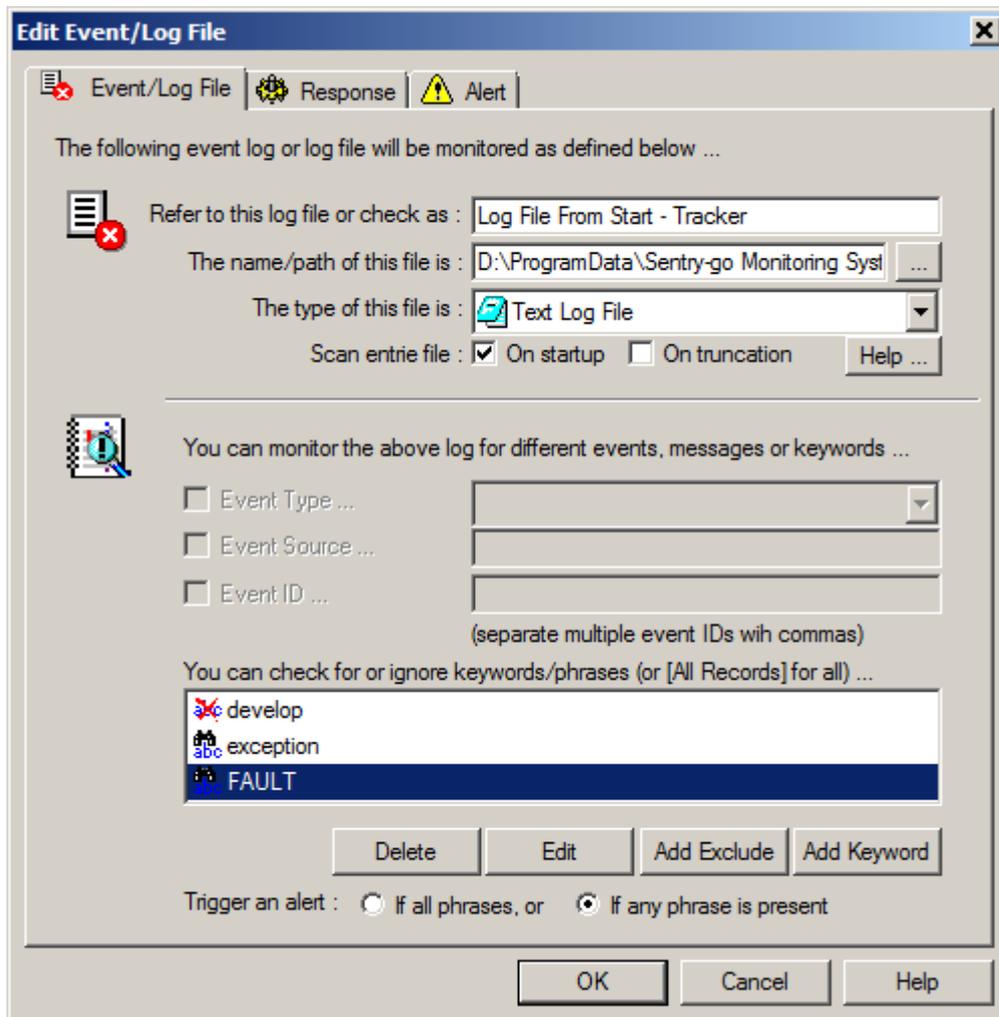
 When defining a message, there is no need to add complete error messages to this list - one or more keywords is usually sufficient. By default, standard messages (and all event log errors) are included when Setup installs the monitor.

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 log file 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 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.

The type of this file is ...

Select either “Text-based log file” or “Text-based (Unicode) log file” from the list of available options.



On later versions of Windows, text files may be saved in UNICODE format instead of the older ANSI standard. An example of this is the SQL Server error log.

If you are unsure which version your log file is ...

- Open it using Notepad
- Click File/Save As
- Note the encoding being suggested in the 'Save As' window.

If it is not ANSI, then select “Text-based (Unicode) log file” here.

If “Text-based log file” is selected for a UNICODE file, you may find alerts are not triggered as expected.

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.

Scan Entire File on Truncation

Sentry-go will monitor files to see whether they are truncated (shortened). This can happen, for example, if the file is replaced with a new one or older records are removed by the application writing to it. By default if this happens, the monitor searches for the new end of file and continues monitoring.

For systems where files can roll-over (be replaced by new ones – e.g. SQL Server), there may be times when the truncated file should be treated as an entirely new file and **all records** therefore scanned. To do this, tick the “Scan Entire File on Truncation” option.

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.

 To record all events, enter [All Records] as your phrase.

- **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 file types

Most log files are text based. However, on newer versions of Windows you may find the file is actually stored in UNICODE format, as opposed to the older ANSI standard. An example of this is the SQL Server error log file. Although both types will display perfectly well in Notepad, they are in fact stored differently on disk and must be accessed in the appropriate fashion. When monitoring a text-based log file, you can check the format required by ...

- Open the log file using Notepad
- Once loaded, click “File/Save As” from the menu
- Note the encoding being suggested within the 'Save As' window. If it shows “ANSI”, then you should select the log type as “Text-based log file”. If not (e.g. it reports “UNICODE”, select “Text-based (Unicode) log file” from the dropdown list.



If you notice alerts are not being triggered when you expect them, verify the type of file being configured as described above.

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.



Always 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.

Scheduling a check

By default, each check is performed periodically at regular intervals throughout the day. The frequency of these checks is determined by the value specified at the bottom of the main list.

However, there may be times when you wish to perform the check at a different time, maybe at a set time each day, or on certain days etc. To do this, select the “Schedule” tab.

For more information, please see the “Sentry-go Monitoring Schedule” guide.

Configuring an automatic response

In the event an error is detected, Sentry-go can be configured to optionally respond automatically - i.e. to take action itself.

To configure this, select 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 automatic responses, please see the “Configuring Automatic Responses” guide.

Configuring an alert

In the event an error is detected and either no automatic response is defined or the response doesn't resolve the fault, an alert will be triggered. Depending on the monitor's general settings, you can either notify one or more contacts individually, or specify the alert group you wish to inform.

To configure these options, select the entry from the list and click Edit. On the resulting window, select the “Alert” tab.



For more information, please see the “Configuring Sentry-go Alerts” guide.

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.

More Information

If you need more help or information on this topic ...

- Read all [papers/documents on-line](#).
- Watch [demonstrations & walkthrough videos on-line](#).
- Visit <http://www.Sentry-go.com>.
- Contact our [Support Team](#).



*Sentry-go, © 3Ds (UK) Limited, 2000-2013
East Molesey, Surrey. United Kingdom
T. 0208 144 4141
W. <http://www.Sentry-go.com>*