



# How to Monitor Event Logs & Log Files with Sentry-go

Last Updated Thursday, 19 April 2012

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

*Be Proactive, Not Reactive!*

Monitoring both the contents of text-based log files as well as Windows own Event Logs is quick & simple with Sentry-go. Once configured, the monitor can automatically check the entries written to these logs & trigger an alert based on their contents, without you having to manually open & verify the data yourself.

## Monitoring an Event Log

To monitor a Windows Event Log on the local server, follow these steps ...

- Start the Easy Access Utility or Client Console, select the monitor & click “Configure”.  
[Click here for more information on configuring Sentry-go.](#)
- Select the “Logs” button to display the primary Logs configuration list.
- Click “Add” to add a new check. The properties window for the check will be displayed.

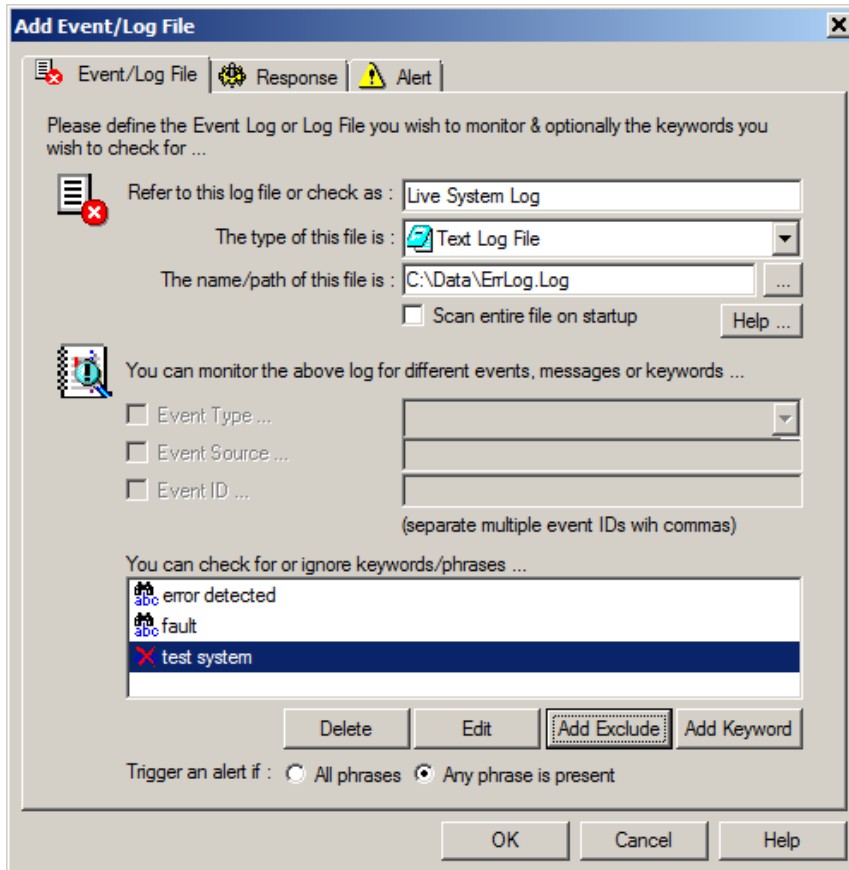
- First enter a suitable name for the check – e.g. Application Event Error.
- Next select the type of file we’re going to monitor – e.g. “Application Event Log”.

- For Event Logs, we can monitor based on items recorded in the record as well as key phrases if required ...
  - To trigger an alert for events of type “error”, select the “Error” event type.
  - To trigger an alert based on a specific event source (the name of the system reporting the error), enter part (or all) of the name in the appropriate field.
  - To trigger an alert based on specific event Ids only, enter each ID separated by a comma in the appropriate field.
  - To trigger an alert when the event message contains one or more phrases, include the keyword(s) or phrase(s) by clicking the “Add Keyword” button.
  - To ignore events where the message text contains one or more phrases, include the keyword(s) or phrase(s) by clicking the “Add Exclude” button.
  - For keyword detection, select the appropriate monitoring options at the bottom of the window.
- Click “Response” to define any automatic action you wish Sentry-go to take in the event the check fails. These settings include ...
  - How many errors should occur in succession before action is taken.
  - The auto-response the monitor should take, if any, if the check fails.
  - [Click here for more information on defining automatic responses.](#)
- Click “Alert” to define the alert that should be triggered in the event the check fails. This includes ...
  - Which group should be notified of the failure.
  - How members of the group should be notified.
  - When notifications should be run etc.
  - [Click here for more information on defining alerts.](#)

## Monitoring a Text Log File

To monitor a text-based log file (e.g. a custom file, SQL Server, IIS, Exchange Log file etc.) follow these steps ...

- Start the Easy Access Utility or Client Console, select the monitor & click “Configure”.  
[Click here for more information on configuring Sentry-go.](#)
- Select the “Logs” button to display the primary Logs configuration list.
- Click “Add” to add a new check. The properties window for the check will be displayed.



- First enter a suitable name for the check – e.g. Live System Log.
  - To monitor a text-based log file, select “Text Log File”.
  - Enter the path/name of the log file ...
    - Remember the file must be accessible from the server running Sentry-go.
    - For remote file use the UNC name (e.g. [\\PCName\Sharename](#) etc.)
    - To include files with dynamic names – e.g. including a date, use place-markers such as `$$DD$$MM$$YY.log` etc.
- [Click here for more information on specifying special filenames.](#)
- For text-based log files, we can monitor based on the text appended to the file. Specifically, we use keyword(s) and/or phrase(s) to indicate which entries we’re interested in and which can be ignored ...
    - To trigger an alert when the entry contains one or more phrases, include the keyword(s) or phrase(s) by clicking the “Add Keyword” button.
    - To ignore entries where the message text contains one or more phrases, include the keyword(s) or phrase(s) by clicking the “Add Exclude” button.
    - Finally select the appropriate monitoring options at the bottom of the window.

- Click “Schedule” to perform the check at specific times (as opposed to the default no. minutes as specified at the bottom of the main list).  
[Click here for more information on Scheduling Sentry-go checks.](#)
- Click “Response” to define any automatic action you wish Sentry-go to take in the event the check fails. These settings include ...
  - How many errors should occur in succession before action is taken.
  - The auto-response the monitor should take, if any, if the check fails.
  - [Click here for more information on defining automatic responses.](#)
- Click “Alert” to define the alert that should be triggered in the event the check fails. This includes ...
  - Which group should be notified of the failure.
  - How members of the group should be notified.
  - When notifications should be run etc.
  - [Click here for more information on defining alerts.](#)

## More Information

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

- See [Monitoring Available Event Logs & Log Files.](#)
- Contact our [Support Team.](#)
- Watch [demonstrations & walkthrough videos on-line.](#)
- Visit <http://www.Sentry-go.com>.

