



# The Sentry-go Monitoring System

## Running the Log Monitor Wizard

Last Updated Thursday, 19 April 2012

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

*Be Proactive, Not Reactive!*

---



## Table of Contents

|  |    |
|--|----|
| Symbols .....                          | 2  |
| Background.....                        | 2  |
| Running the Wizard .....               | 2  |
| Selecting the Type of Monitoring ..... | 3  |
| Event Log Monitoring .....             | 4  |
| Log File Monitoring .....              | 5  |
| Specifying Keywords.....               | 7  |
| Results.....                           | 8  |
| Next Steps .....                       | 9  |
| More Information, Help & Support ..... | 10 |

---

## 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

This guide gives full details of how you can use the Log Monitor Wizard to quickly & easily configure Sentry-go's Event Log & Log File monitoring on your local or remote server.

---

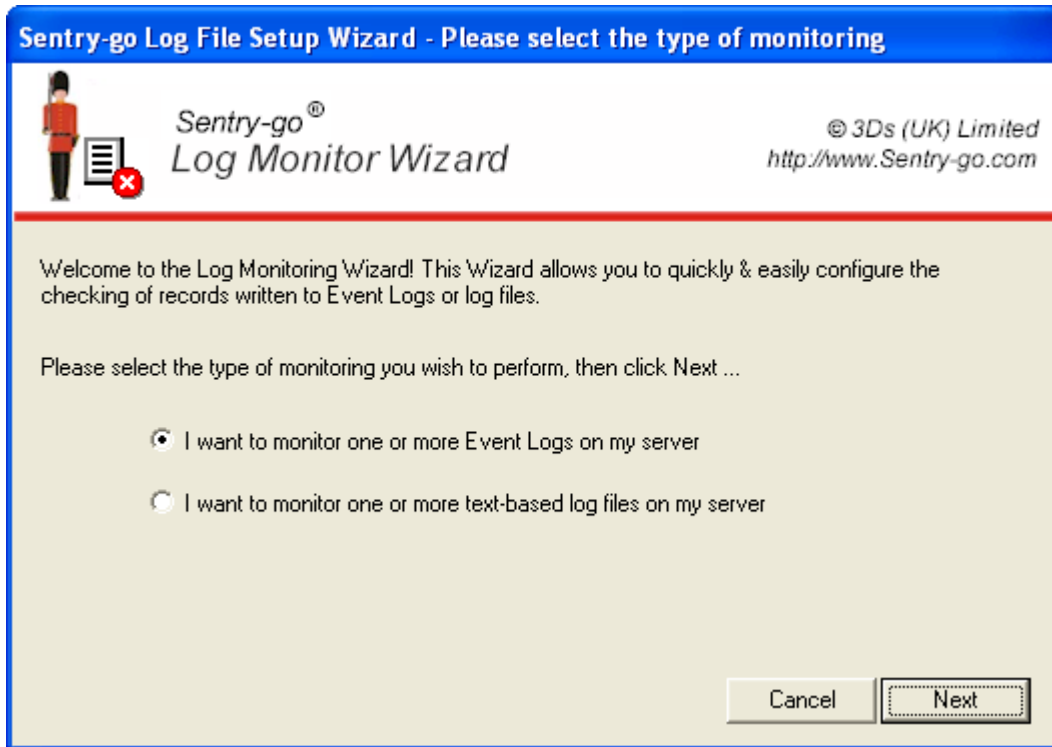
## Running the Wizard

You can access the Wizard either directly from Windows Explorer or when prompted by Setup.

---

## Selecting the Type of Monitoring

The Wizard's first screen allows you to determine whether you wish to configure the monitoring of one or more Event Logs or text-based log files on the server being configured.



### **I want to monitor one or more Event Logs on my server**

Select this option if you wish to configure the monitoring of one or more Windows Event Logs.

### **I want to monitor one or more text-based log files on my server**

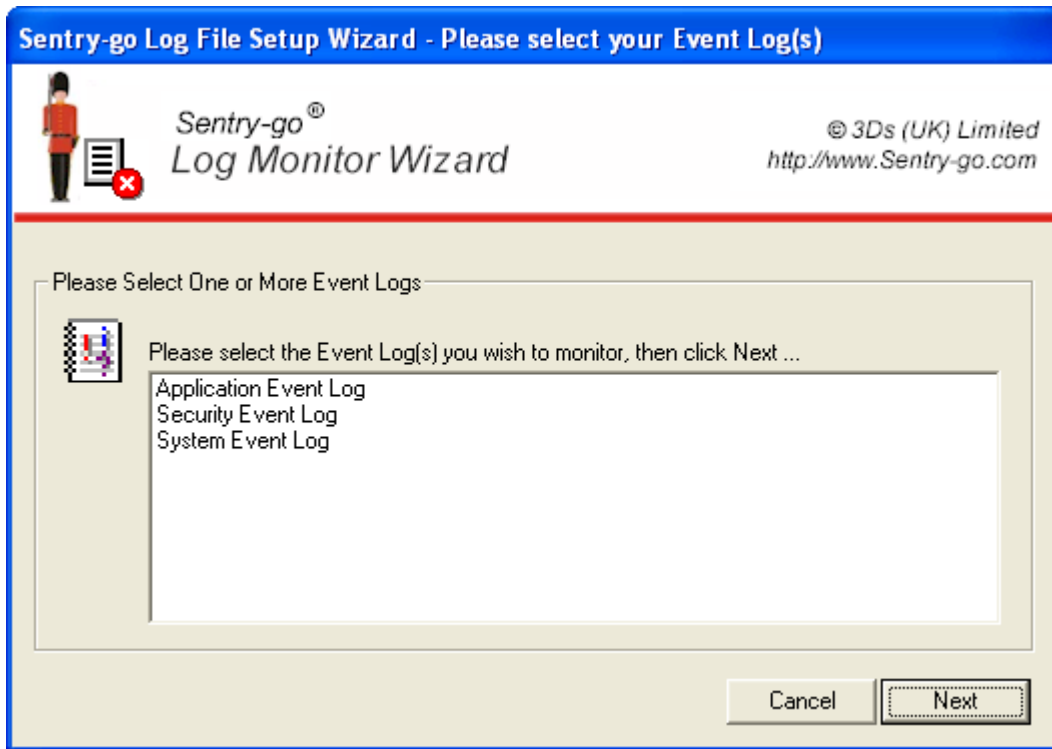
Select this option if you wish to monitor the contents of other log files on the server, such as those written by applications such as IIS, SQL Server or 3<sup>rd</sup> party systems.

Click Next to Continue.

---

## Event Log Monitoring

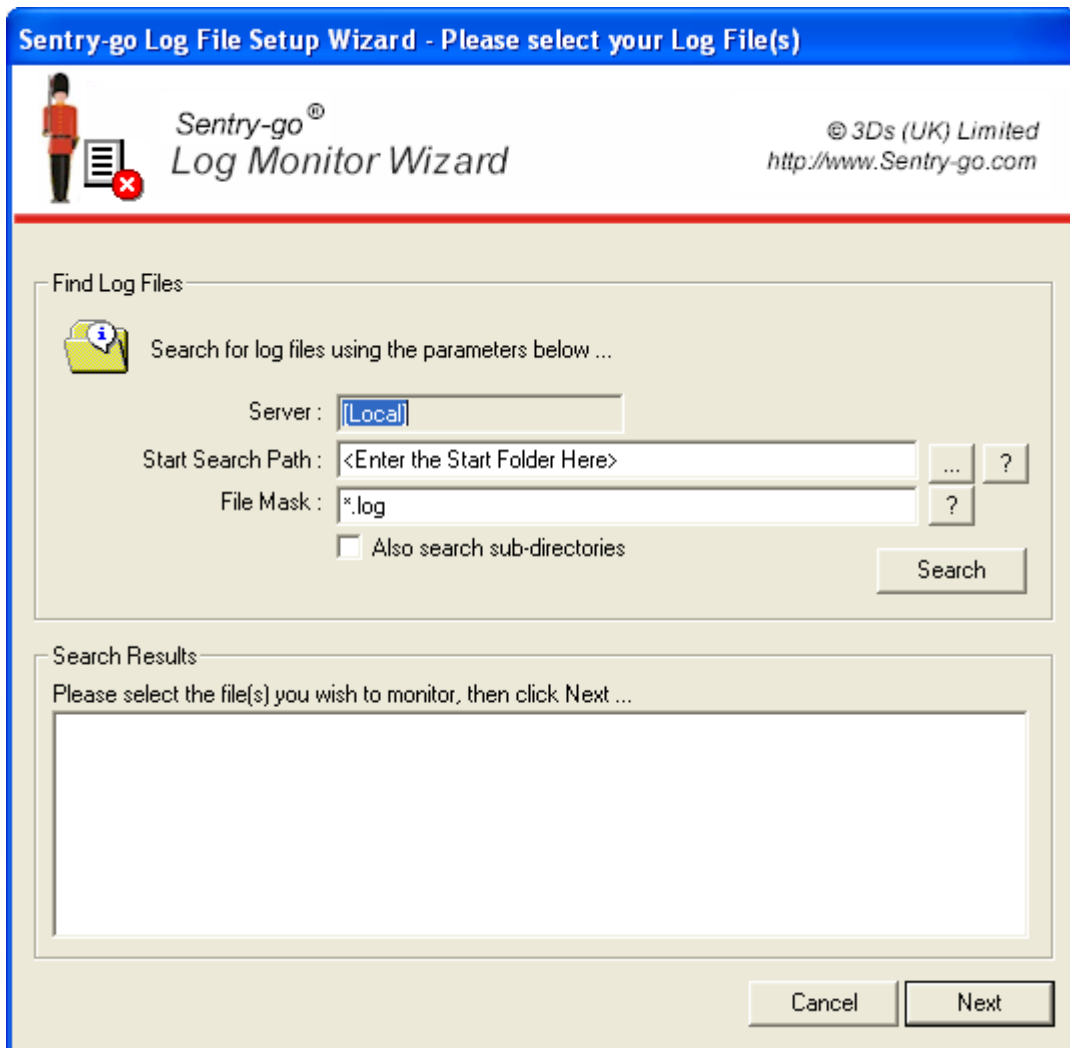
If you chose to configure Event Log monitoring, the following window will be displayed.



The Wizard will search for Event logs on the appropriate computer & list them here. Simply select the Event Logs you wish and click Next.

## Log File Monitoring

If you chose to configure Log File monitoring, the following window will be displayed allowing you to search for & select the files you wish to monitor.



The screenshot shows the 'Sentry-go Log File Setup Wizard - Please select your Log File(s)' window. The title bar is blue with white text. The window has a light beige background. At the top left is a small icon of a person in a red uniform next to a document with a red 'X'. To the right of this is the text 'Sentry-go® Log Monitor Wizard'. Further right is the copyright information: '© 3Ds (UK) Limited http://www.Sentry-go.com'. Below this is a red horizontal line. The main area is divided into two sections. The top section is titled 'Find Log Files' and contains a folder icon with an 'i' and the text 'Search for log files using the parameters below ...'. Below this are four input fields: 'Server:' with a dropdown menu showing '[Local]', 'Start Search Path:' with a text box containing '<Enter the Start Folder Here>' and a browse button (...), 'File Mask:' with a text box containing '\*.log' and a help button (?), and a checkbox labeled 'Also search sub-directories' which is currently unchecked. A 'Search' button is located to the right of these fields. The bottom section is titled 'Search Results' and contains the text 'Please select the file(s) you wish to monitor, then click Next ...' above a large empty rectangular box. At the bottom of the window are 'Cancel' and 'Next' buttons.

### Server

This read-only field shows the name of the server on which the search will be performed. If the local server or PC is being configured, "[Local]" will be displayed.

### **Start Search Path**

Enter the path of the files that you wish to search for and display, or click “...” to select the appropriate folder ...

- For local drives, the path should be in the format similar to C:\Path
- For remote drives, the path should be in UNC format – e.g. ShareName or \ShareName\Folder

### **File Mask**

Enter the mask of the file(s) you wish to search for. For example ...

- \*.log
- \*.txt
- \*.\*

### **Also search sub-directories**

Tick this option if you want the Wizard to not only search for the entered mask in the directory entered,. But also in any sub-directories below it.

### **Search**

Click the “Search” button to search for and display a list of available files matching the mask entered.

### **Selection**

Once displayed, select one or more files that you wish to monitor from the list.

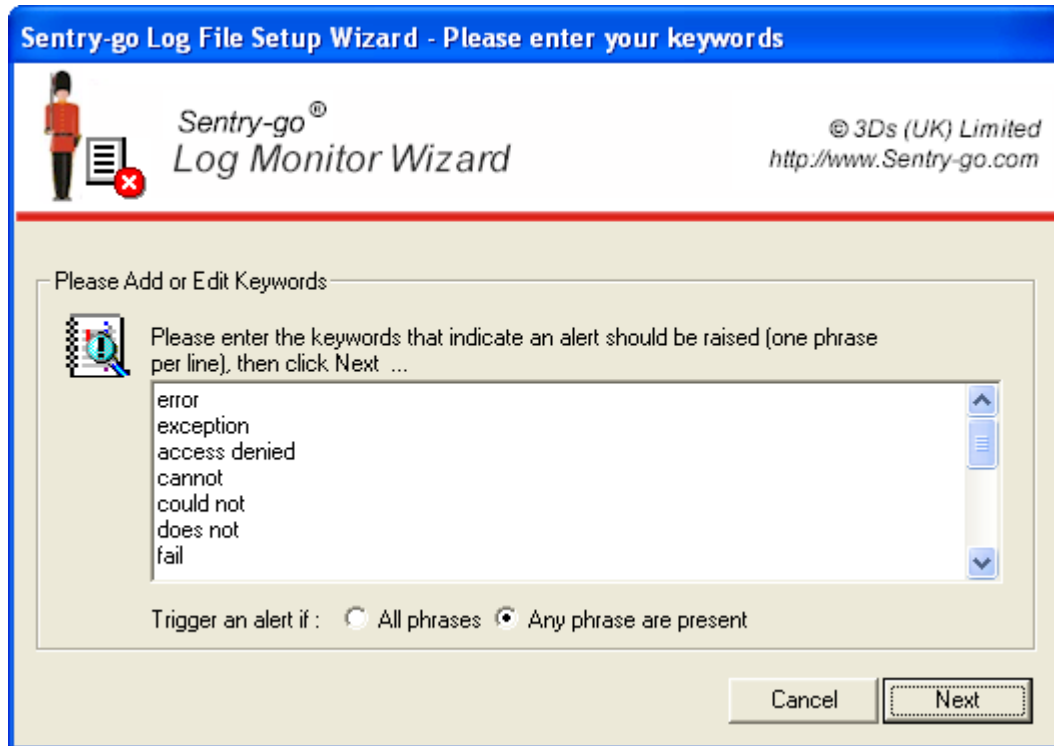
Click Next to continue.



---

## Specifying Keywords

The keywords window allows you to view and edit the keywords & phrases that will be used to monitor records written to either the selected Event Logs or log files.



### Keywords

The keywords/phrases entered will be used by the monitor to determine if an alert should be triggered when a record is written to the file. Default keywords will be shown automatically but you can update these or add new ones to list as required. Add each new keywords or phrase on a new line.

### Trigger an alert if all phrases are present

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

### Trigger an alert if any phrase is present

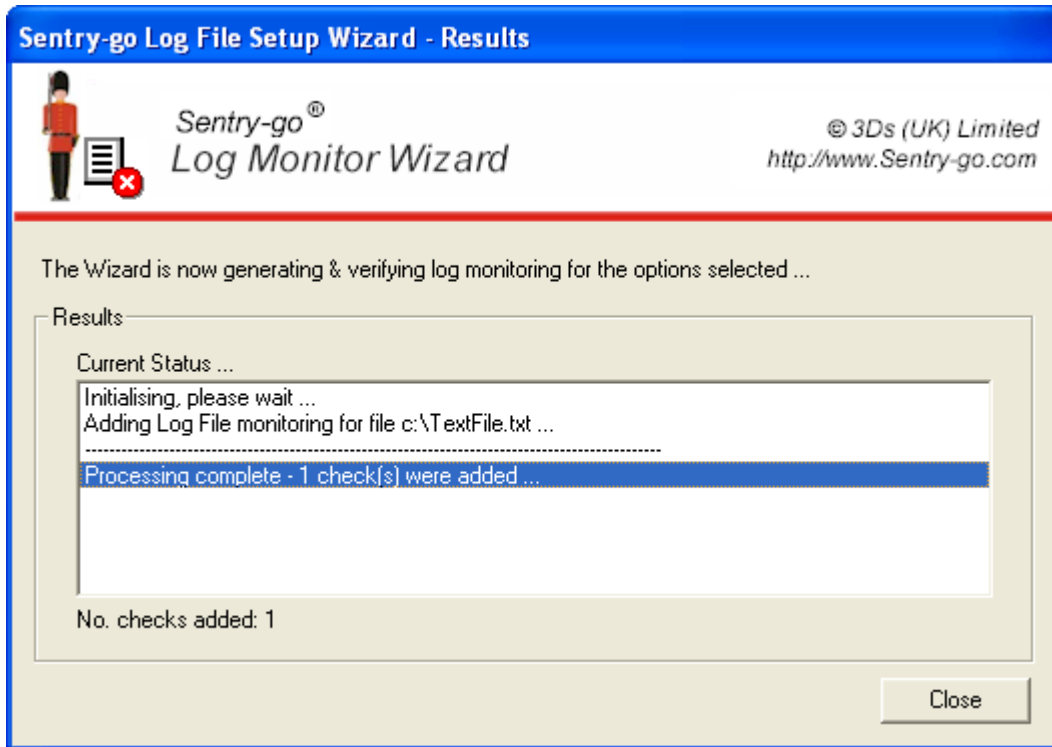
Select this option to trigger an alert if one or more of the keywords or phrases listed are found in the message/record. This is the most common option for general monitoring.

Click Next to continue.

---

## Results

The Wizard will now configure the appropriate values, updating its current status as the process continues. Once complete, a message will indicate how many checks were added.



Click Close to close the Wizard and return to the Configuration window.

---

## Next Steps

The Wizard will automatically generate the appropriate checks as outlined above. It will also ...

- Set default values for alerts
- Enable/disable checks as appropriate

Once complete, it is recommended that you review the new checks within the Client Console and further refine alerts, actions and thresholds as appropriate.

- For Event Logs, you may also wish to add the checking of event types – e.g. all errors, specific events and sources as opposed to purely keyword verification.

For Log files, if the file(s) being monitored contain place markers such as dates, you may also wish to update the filename to include generic values. For example ...

| <b>Place marker</b>       | <b>Description</b>   |
|---------------------------|--|
|                           |  |
| %EnvironmentVariableName% | To include the value of the named environment variable   |
| \$\$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)<br><br>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)<br><br>Allows you to include a date n-days in the future. The associated month and/or year are automatically adjusted as required |
| \$\$DD[-n]                | (Where n is a number greater than 1)<br><br>Allows you to include a date n-days in the future. The associated month and/or year are automatically adjusted as required |
| \$\$DD+n                  | (Where n is a number greater than 1)<br><br>Allows you to include a date n-days in the future. The associated month and/or year are automatically adjusted as required |

---

## 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>