



How to Monitor Files & Directories with Sentry-go

Last Updated Thursday, 19 April 2012

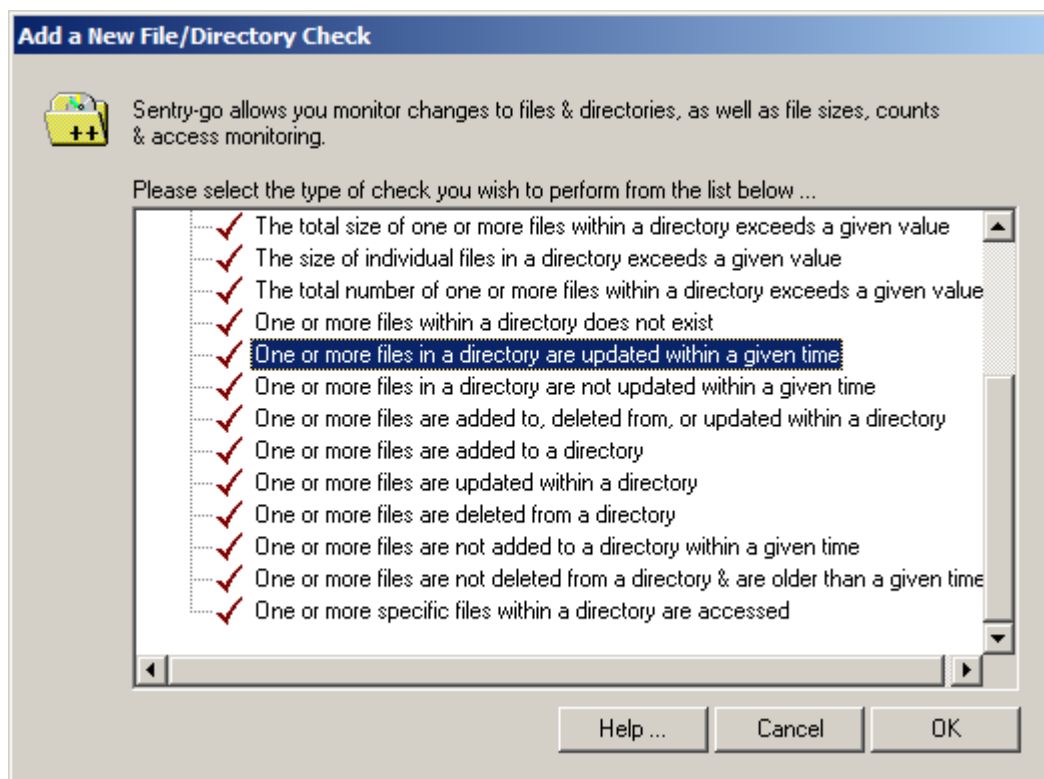
© 3Ds (UK) Limited
<http://www.Sentry-go.com>

Be Proactive, Not Reactive!

Monitoring changes to files, directories & folders, counts & sizes, as well as who is making those changes is quick & simple with Sentry-go. Once configured, the monitor can periodically check your key files & directories, keep a check on changes & log users accessing them. Based on these checks, alerts can be triggered to inform administrators of the changes etc.

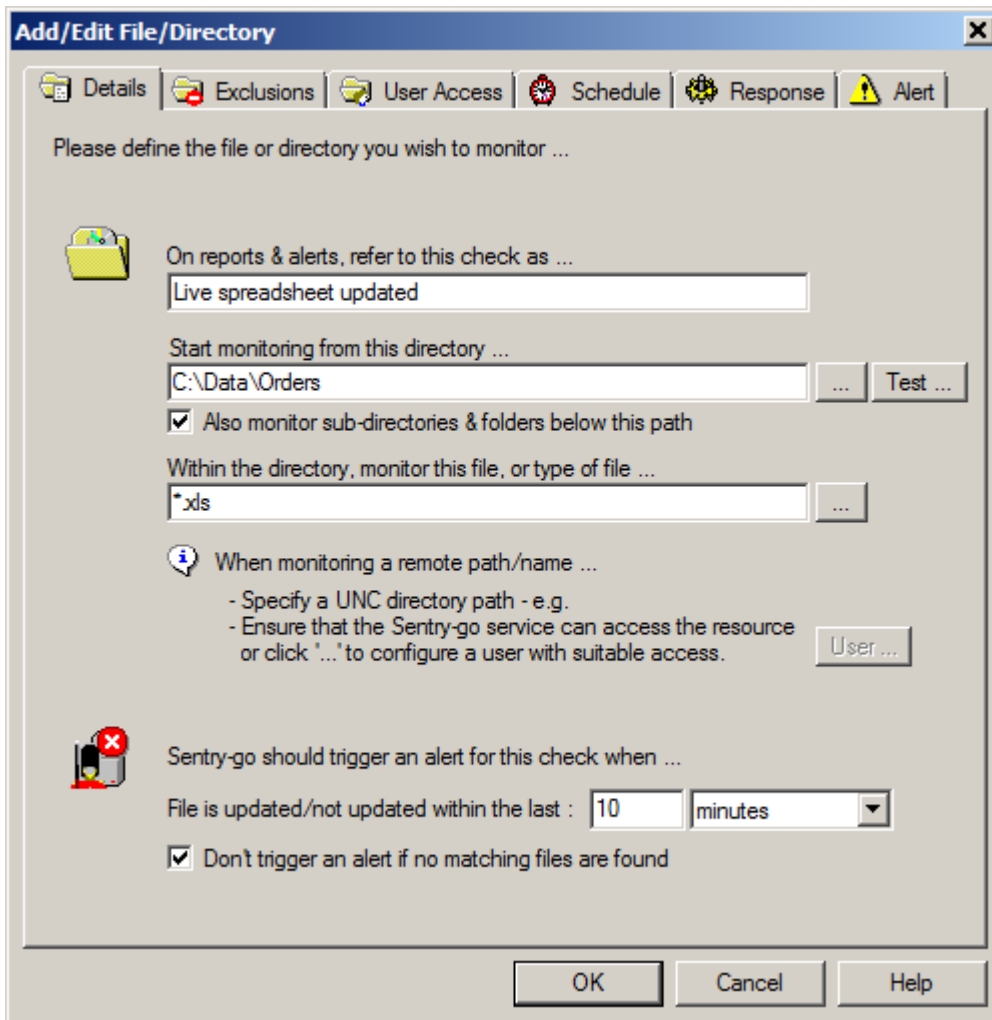
To do this, follow these steps ...

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



- On this window, you can select from a number if directory or file-related monitoring checks. Select the check you wish to define & click OK. For this example we'll select a file-related check.

- The first tab defines the directory &/or file(s) that will be scanned ...



- Enter a suitable name for the check you wish to perform.
- Enter the full path of the directory in which the monitoring scan will start.

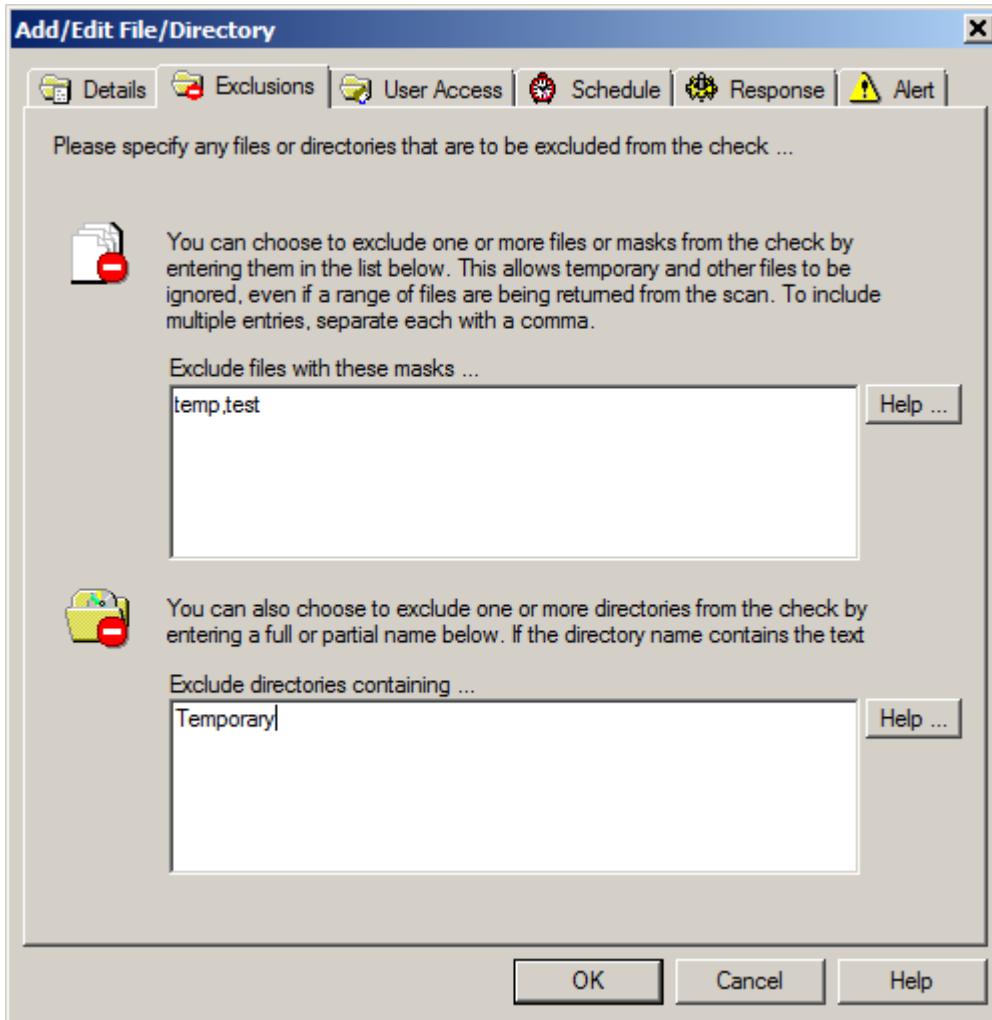
Click the “...” button to select a local directory. *If the path entered is on a remote server, enter its UNC path name – for example \\PCName\ShareName\Directory.*

- To automatically scan any sub-directories below the above path, tick the next option.
- For file-related checks, enter the filename or mask of the file(s) you wish to monitor ...
 - Click the “...” button to select file(s) from the local server.
 - Remember the file must be accessible from the server running Sentry-go.
 - 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.](#)

- Depending on the check being performed, enter the details that indicate when the monitor should trigger an alert. In the example shown, we want to be alerted to any excel spread sheets that have been updated within the last 10 minutes.

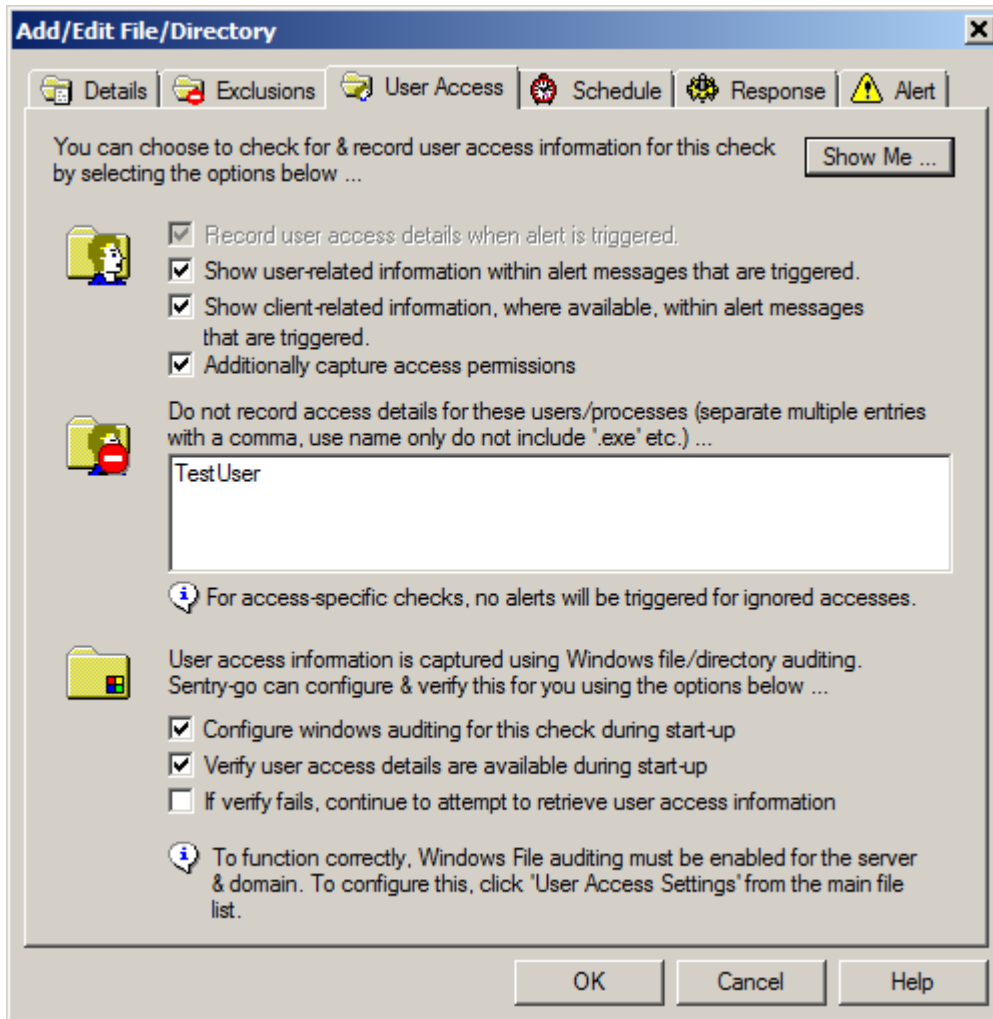
- Click the second tab to exclude one or more directories or files from the scan ...



- The top entry is used to exclude any files we don't wish to be informed about. In our case we've chosen to ignore any files containing "temp" or "test" in its name.
- The lower entry is used to exclude any directories we don't wish to scan. In our case we'll exclude any directory with "temporary" in its name.

- Depending on the check being defined, the “User Access” tab will be available. This is used to record user access information for the file(s) that trigger an alert.

If you do not wish to know who, or what accessed the files, leave these fields un-ticked & move on to the next tab ...



- Tick the first option to automatically record user access information for files that trigger the associated alert.
- To display user access information within alert messages, tick the next option. To record this information but not display it within the alert message text itself, leave this option un-ticked.
- Tick the fourth option if you wish to also show the type of access that was granted to the user.
- If you have user IDs or processes that you do not wish to record information for, enter them here. In our example, we’re ignoring the user “TestUser”.
- The lower options are used to control whether the monitor will configure & verify user access information when it is first started.
- If the latter fails, by default user access information will be disabled for the associated check. However, if you tick the last option, Sentry-go will continue to attempt to retrieve this information and will therefore start recording it if any external configuration fault is subsequently rectified (e.g. if auditing is later enabled etc.)

User access information requires the server to be configured for auditing. Typically this only needs to be performed once on your server & can be configured either manually through Windows or through Sentry-go itself.

[Click here for more information on configuring your server to record User Access information.](#)

- 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 Files & Directories.](#)
- See [Monitoring File & Directory access.](#)
- Contact our [Support Team.](#)
- Watch [demonstrations & walkthrough videos on-line.](#)
- Visit <http://www.Sentry-go.com>.

