



The Sentry-go Monitoring System Monitoring Files & Directories

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
Quick Facts.....	3
Monitoring Access & Changes to Files & Directories	4
Adding a new File or Directory Monitoring Check.....	5
Configuring the File or Directory Monitoring Check.....	9
Specifying Monitoring Criteria.....	13
Excluding Files & Directories	15
Capturing User Access Information.....	17
Scheduling the Check.....	19
Temporarily Ignoring a Configured Check.....	20
Configuring an Automatic Response	20
Recording User Access Information.....	21
What access information is captured by Sentry-go ?	24
Enabling Auditing on Your Server.....	25
Web Reporting with this Monitoring Component	25
The File Access Information Report	26
The Verify File Access Report	27
More Information, Help & Support	28

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

There may be times when you wish to check keep track of changes to files, directories & directory structures as well as the availability of network shares. This may be particularly important if you wish to check for changes, new files being added (e.g. files being uploaded for processing) as well as file counts & sizes to ensure other processes are functioning normally.

In addition, you may also wish to know which users/processes performed actions on those files that triggered the alert or which users/processes are accessing key files or directories. This information can also be logged to a CSV file & accessed as a web report.

With Sentry-go, the monitoring of files & directories is both quick & easy to achieve. The content of files such as log files can also be monitored – for more information, please refer to [Sentry-go - Monitoring Event Logs & Log Files](#).

This component will not only for changes to files/directories etc., but also record who/what applications accessed those files. Two additional monitoring checks are also available for local files/directories - allowing directories accessed & files accessed to be monitored & recorded.

For more information on configuring your environment in order to record file access information, please see [Sentry-go - Monitoring File & Directory Access](#)

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 :	File & Directory Monitor
Aim/Description :	To provide monitoring of files & directories for both local and remote file systems.
Main Monitoring Features :	<ul style="list-style-type: none">• Monitor the file or directory size• Monitor individual file size(s)• Monitor the no. files in the directory• Monitor if the file/mask is updated within a given time• Monitor if the file/mask is not updated within a given time• Monitor if less than X file(s) created within a given time• Monitor if directory or file does not exist ...• Monitor if the directory does not exist, or a subdirectory is added or removed• Monitor if the directory does not exist, or a subdirectory is removed• Monitor if a file is added to a given directory/subdirectory• Monitor if a file is deleted from a given directory/subdirectory• Monitor if a file is updated within a given directory/subdirectory• Monitor if a file is not added to a given directory/subdirectory• Monitor if a file is deleted from a given directory/subdirectory• Monitor access to files or directories• Where applicable, optionally indicate which users, processes & client workstations performed the above actions
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

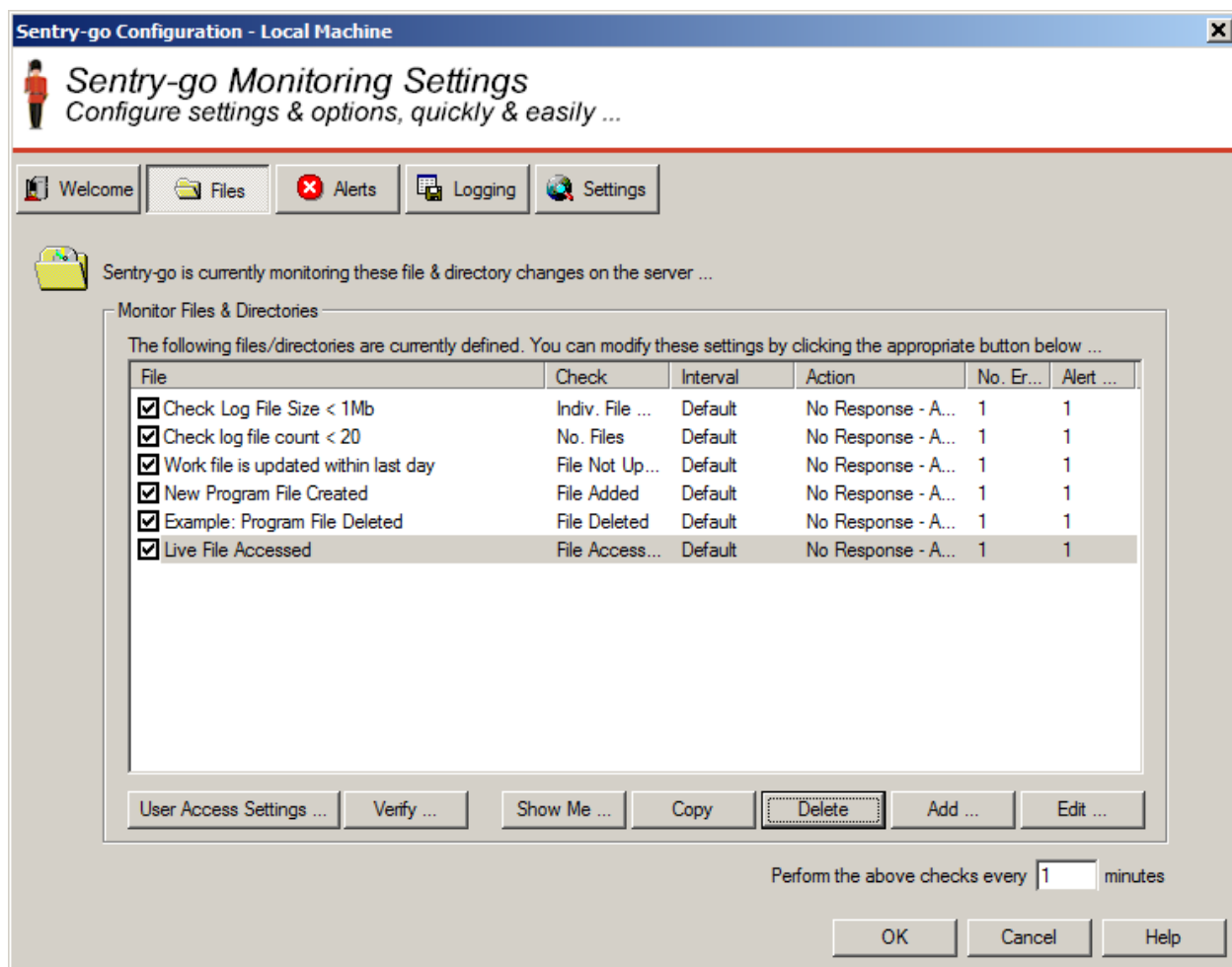
Monitoring Access & Changes to Files & Directories

To monitor files & directories simply select the Sentry-go monitor from the Client 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 "Files" tab. From here, you can configure the following ...

- The monitoring of one or more files or directories.
- What should happen in the check fails.
- How often each check should be run.
- Temporarily disable the monitoring of one, more or all files/directories.

The resulting list will show all the currently defined files & directories 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 includes the application name and a close button. Below the title bar is a header area with the "Sentry-go Monitoring Settings" logo and the tagline "Configure settings & options, quickly & easily ...". A navigation bar contains tabs for "Welcome", "Files", "Alerts", "Logging", and "Settings". The "Files" tab is selected. Below the navigation bar, a message states "Sentry-go is currently monitoring these file & directory changes on the server ...". The main content area is titled "Monitor Files & Directories" and contains a table of monitored items. The table has columns for "File", "Check", "Interval", "Action", "No. Er...", and "Alert ...". Below the table are buttons for "User Access Settings ...", "Verify ...", "Show Me ...", "Copy", "Delete", "Add ...", and "Edit ...". At the bottom, there is a field for "Perform the above checks every" with a value of "1" and the unit "minutes", followed by "OK", "Cancel", and "Help" buttons.

File	Check	Interval	Action	No. Er...	Alert ...
<input checked="" type="checkbox"/> Check Log File Size < 1Mb	Indiv. File ...	Default	No Response - A...	1	1
<input checked="" type="checkbox"/> Check log file count < 20	No. Files	Default	No Response - A...	1	1
<input checked="" type="checkbox"/> Work file is updated within last day	File Not Up...	Default	No Response - A...	1	1
<input checked="" type="checkbox"/> New Program File Created	File Added	Default	No Response - A...	1	1
<input checked="" type="checkbox"/> Example: Program File Deleted	File Deleted	Default	No Response - A...	1	1
<input checked="" type="checkbox"/> Live File Accessed	File Access...	Default	No Response - A...	1	1


In addition to the standard Add, Edit, Delete buttons, the following options are available on this window.

User Access Settings ...

If user access information has been requested as part of any file/directory checks, details can be recorded to a log file for later analysis. Click this button to define or edit settings relating to this log file. See “Recording User Access Information” for more information.


Verify User Access ...

If user access information has been requested as part of a file/directory check, audit information for the appropriate files & directories must be available. To enable or verify that details are available, highlight the appropriate check & click this button.

 This option connects to the monitor's web reporting interface. The monitor must be running and web available for this option to function.

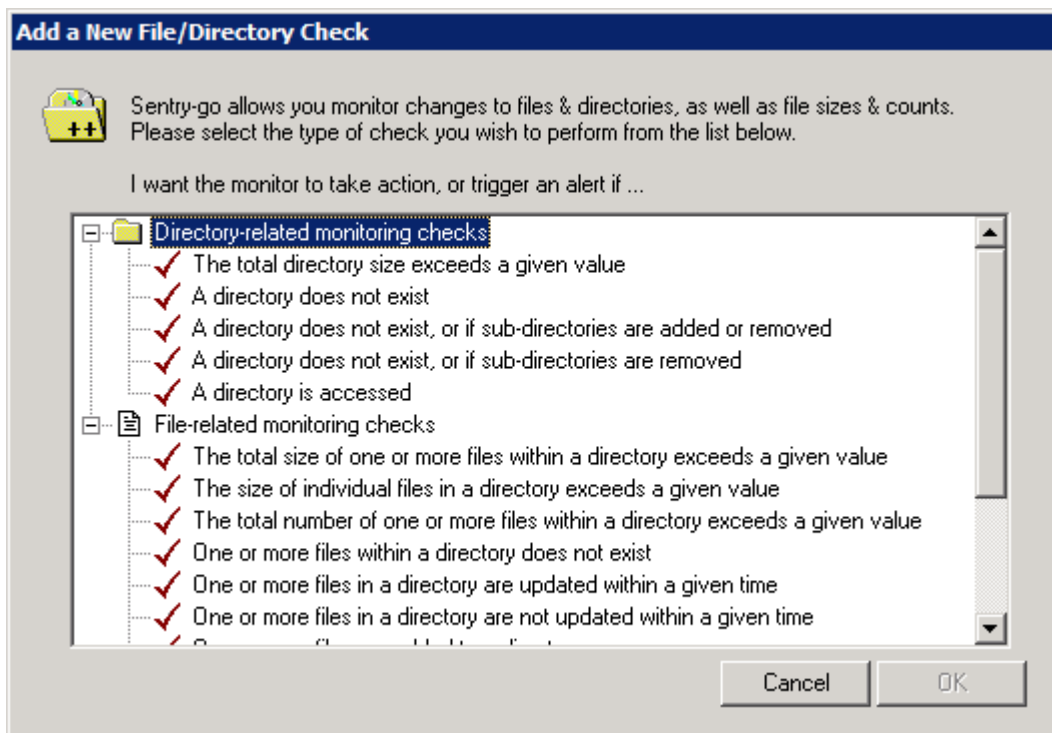
Perform the above checks every (minutes)

This value specifies how often, in minutes, the monitor should check the defined files/directories.

 If the time is overridden for a given check, the value given here is ignored for that check.

Adding a new File or Directory Monitoring Check

To monitor a new file, folder or directory, select the Add option from the main window. The following window will be displayed, allowing you to select the type of monitoring task you wish to perform. Once a selection has been made, individual items can be configured for the monitoring check, as described below.



File Monitoring Checks that can be performed

The total size of one or more files within the directory exceeds a given value

Select this option if you wish to monitor the total size of one or more files or directories.

When selected, simply enter the threshold value, then select the comparison - "equal to", "not equal to", "greater than" or "less than", and the threshold unit (bytes, Kb, Mb etc.)

An alert will be generated if the above condition is met.

- To monitor the size of a file, enter the path & filename – e.g. C:\Directory\File.tmp.
- To monitor the size of all files of a particular type, enter the appropriate the path & file mask - e.g. C:\Directory*.tmp.
- To monitor the size of a directory, enter the appropriate directory name with "*" – e.g. C:\Directory*



Always bear in mind the check being made and use the most appropriate value for the threshold unit.

For example, if you were checking the size of C:\TEMP*.tmp and all sub-directories, the value returned likely to be quite large. Therefore a higher unit such as Mb or Gb should be used to avoid overflow errors from occurring.

The size of one or more individual files in a directory exceeds a given value

Select this option if you wish to monitor the size of individual files within a directory or directories.


When selected, simply enter the threshold value, then select the comparison - "equal to", "not equal to", "greater than" or "less than") and the threshold unit (bytes, Kb, Mb etc.) An alert will be generated if the above condition is met.



This check is identical to the one above, except the size of each individual files is checked and compared with the threshold, as opposed to the cumulative size of all qualifying files.

Always bear in mind the check being made and use the most appropriate value for the threshold unit.

For example, if you were checking the size of C:\WINNT and all sub-directories, the value returned likely to be quite large. Therefore a higher unit such as Mb or Gb should be used to avoid overflow errors from occurring.

The total number of one or more files within a directory in a directory exceeds a given value	Select this option if you wish to monitor the number of files in the specified directory or directories.
	When selected, simply enter the threshold value, then select the comparison - "equal to", "not equal to", "greater than" or "less than".
	An alert will be generated if the above condition is met.
One or more files within a directory does not exist ...	Select this option if you wish to check that the given directory or file exists. If it does not exist, an alert will be triggered.
One or more files within a directory are updated within a given time	Select this option if you wish to monitor the last update time of a file and trigger an alert when it is updated within the given timeframe.
	When selected, simply enter the threshold value and its corresponding unit - "minutes", "hours", "days" or "weeks".
One or more files within a directory are not updated within a given time	Select this option if you wish to monitor the last update time of a file and trigger an alert when it is not updated within the given timeframe.
	When selected, simply enter the threshold value and its corresponding unit - "minutes", "hours", "days" or "weeks".
	 This check is particularly useful if you have an application that updates a log file every X minutes and you wish to check that it's running correctly etc.
One or more files are added to, deleted from or updated within a directory	Select this option if you wish to monitor for files being added, deleted or updated within a given directory.
One or more files are added to a directory	Select this option if you wish to monitor the contents of the given directory and be alerted when a file is added to it.
One or more files are deleted from a directory	Select this option if you wish to monitor the contents of the given directory and be alerted when a file is deleted from it.
One or more files are updated within a directory ...	Select this option if you wish to monitor the contents of the given directory and be alerted when a file is updated within it.
One or more files are not added to a directory within a given timeframe	Select this option if you wish to be alerted if a file or files are not added to a directory within the appropriate timeframe.
	When selected, simply enter the threshold value and its corresponding unit - "minutes", "hours", "days" or "weeks".
One or more files are not deleted from a directory within a given timeframe	Select this option if you wish to be alerted if a file or files are not removed from a directory within the appropriate timeframe.
	When selected, simply enter the threshold value and its corresponding unit - "minutes", "hours", "days" or "weeks".
One or more specific files within a directory is accessed.	Select this option if you wish to be notified if the file, or file mask is accessed.

Directory Monitoring Checks that can be performed

The total directory size exceeds a given value

Select this option if you wish to monitor the total size of all files within the directory or directories.

When selected, simply enter the threshold value, then select the comparison - "equal to", "not equal to", "greater than" or "less than", and the threshold unit (bytes, Kb, Mb etc.)

An alert will be generated if the above condition is met.



Always bear in mind the check being made and use the most appropriate value for the threshold unit.

For example, if you were checking the size of C:\WINNT and all sub-directories, the value returned likely to be quite large. Therefore a higher unit such as Mb or Gb should be used to avoid overflow errors from occurring.

The directory does not exist

Select this option if you wish to check that the given directory exists and be notified if it doesn't or is removed.

The directory does not exist, or if subdirectories are added or removed

Select this option if you wish to check that the given directory exists and be notified if it doesn't, or if the directory structure below it changes – i.e. if a subdirectory within it is either added or removed.

The directory does not exist, or if subdirectories are removed

Select this option if you wish to check that the given directory exists and be notified if it doesn't, or if a subdirectory within it is removed.

A directory is accessed.

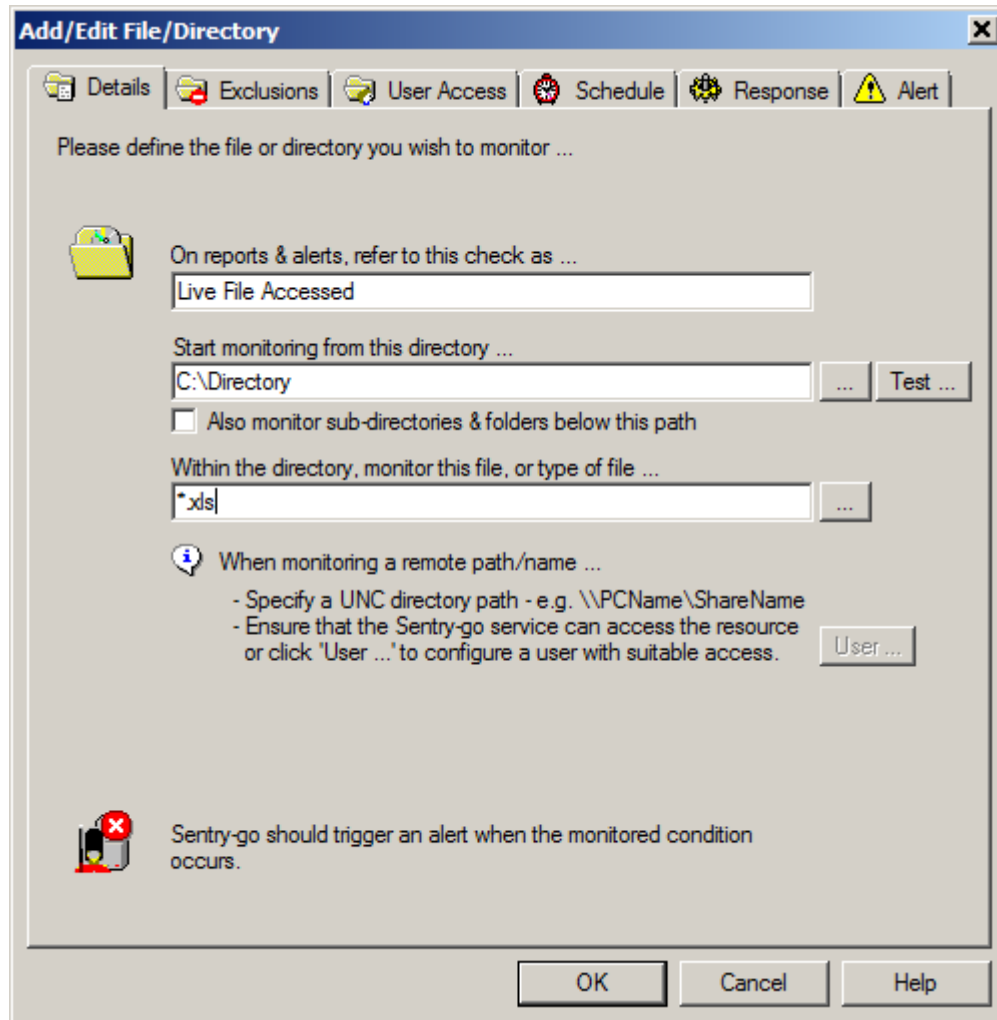
Select this option if you wish to be notified if the directory, or a file within it (and optionally within subdirectories) is accessed.

Once a new check has been defined, properties of the check can be displayed & configured. The same options are available when edit an existing check by select the "Edit" option from the main window.

Configuring the File or Directory Monitoring Check

As shown below, a check is defined by a series of property page tabs, each reflecting a specific area of the check. Depending on the monitoring check being defined, some of these tabs may not be shown.

The first tab allows you to define the file, folder or directory you wish to monitor as well as the criteria against which it will be checked.



The following information is defined here.

On reports & alerts, refer to this 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 and as such it is recommended that a short descriptive name be used for this value.

Start monitoring from this directory

For a directory monitoring check, this is the full path of the directory or folder you wish monitor. If you're monitoring a specific file, or group of files, this is the directory where the files are located or, in if sub-directories are also being monitored, where the scan will be begin.

Click "...” to select the path from Windows.



If the directory is on a remote machine, enter the full path in UNC format – e.g. [\\ServerName\ShareName\FolderName](#) etc.

If a remote location is entered, user access details cannot be captured. Additionally, remote paths cannot be entered when performing "Directory accessed" or "File accessed" monitoring checks.

, the check cannot directory is remote o check that a mask maps to the file(s) you wish to verify works, simply access the command prompt, change to the appropriate directory and type `dir <mask>`.

System environment variables may be used within the file name entered - e.g. `%WINDIR%`. In addition, if the filename contains a date, the following formats may be used ...

- `$$YY` to include the 2 character year
- `$$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.

If date variables are used, Sentry-go will automatically generate the appropriate name before test is performed, thus correcting the date when the time passes midnight etc.

Click "...” to select a file or mask etc. from Windows (see below).

Also monitor subdirectories or folders below this path

Tick this option if you want Sentry-go to continue the scan into all directories below the directory entered above ...

- If this option is not ticked, the monitor will check the contents of the directory entered above, but the contents of sub-directories will be ignored.
- If ticked, any directories found below the path entered will also be scanned - as will their sub-directories respectively until no more are found.

For example, to scan all directories within the "Program Files" folder, enter "C:\Program Files" as the directory, any file names or masks below, and tick this option.



Within the directory monitor this file, or this type of file ...

If you are monitoring a file, a group of files or a specific type of file, enter the filename or mask here.



When selected, simply enter the full name, or mask you wish to monitor, within the directory entered above. This value can be ...

- The complete filename - e.g. MyLog.txt
- A partial filename - e.g. *.txt, My*.log etc.
- An entire mask - e.g. *.* , * etc.

To check that a mask maps to the file(s) you wish to verify works, simply access the command prompt, change to the appropriate directory and type dir <mask>.

System environment variables may be used within the file name entered - e.g. %WINDIR%. In addition, if the filename contains a date, the following formats may be used ...

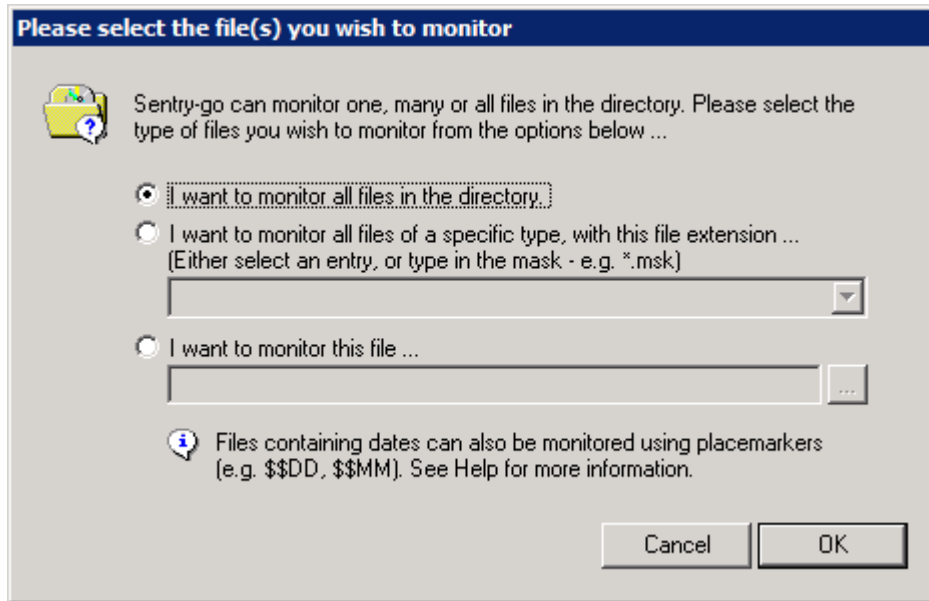
- \$\$YY to include the 2 character year
- \$\$MM to include the 2 character month
- \$\$DD to include the 2 character day
- \$\$DD-n where n is a number greater than 1. Allows you to include a date n-days in the past. The associated month and/or year are automatically adjusted as required.
- \$\$DD+n 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.

If date variables are used, Sentry-go will automatically generate the appropriate name before test is performed, thus correcting the date when the time passes midnight etc.

Click "...” to select a file or mask etc. from Windows (see below).

Selecting file or files ...

When you click "...", the following selection window is displayed, allowing you to more easily determine the name to be entered ...



- **I want to monitor all files in the directory**

Select this option if monitoring should apply to any file in the directory (except those specifically excluded on the "Exclusions" tab).

- **I want to monitor all files of a specific type ...**

Select this option if monitoring should apply to any file with a given file extension in the directory (except those specifically excluded on the "Exclusions" tab).

When selected, you can either choose an extension from the list (e.g. .log files), or enter your own in the field below (e.g. *.tmp, or s*.tmp etc.).

- **I want to monitor this file ...**

Select this option if monitoring should apply to a specific file within the directory specified previously. Simply enter the filename here or click "..." to select it from Windows.

Specifying Monitoring Criteria

Depending on the monitoring type selected when the check was created, the following fields will be available in the lower half of the “Details” tab. These fields allow you to enter the criteria on which the check & alert will be based.

The screenshot shows the 'Add/Edit File/Directory' dialog box with the 'Alert' tab selected. The 'Sentry-go should trigger an alert for this check when ...' section is circled in red. It contains the following fields and options:


- On reports & alerts, refer to this check as ...: Ensure files are updated within the last day
- Start monitoring from this directory ...: C:\Directory
- Also monitor sub-directories & folders below this path
- Within the directory, monitor this file, or type of file ...: *.wrk
- When monitoring a remote path/name ...: - Specify a UNC directory path - e.g. - Ensure that the Sentry-go service can access the resource or click 'User...' to configure a user with suitable access.
- Sentry-go should trigger an alert for this check when ...: File is updated/not updated within the last : 1 days
- Don't trigger an alert if no matching files are found
- Trigger an alert if failures are detected at startup

The no. files in the directory

Enter the number of files you wish to check for when the test is performed. You can trigger an alert if the no. files matches, doesn't match, is greater than or less than the number entered.

The file or directory size

Enter the number of bytes, K/bytes, M/Bytes or G/Bytes you wish to check for. You can trigger an alert if either the total size, or individual file size matches, doesn't match, is greater than or less than the number entered.

 Sizes are rounded to the unit selected. The lower the unit, the more precise the total counted.

File is updated/not updated

Enter the number of minutes, hours, days or weeks within which the associated check should be performed. For example, you can trigger an alert if files are not updated within the last week, or files have been updated within the last hour etc.

Less than X files created within

Enter the number of files you wish to check for when the test is performed. You can trigger an alert if the no. of new files created within the entered minutes, hours, days, weeks etc. is exceeded.

Don't trigger an alert if no matching files found

By default, the above option will trigger an alert if a matching file has not been updated within the given timeframe or no files matching the mask are found. To ignore conditions where no matching files are found, check this option.

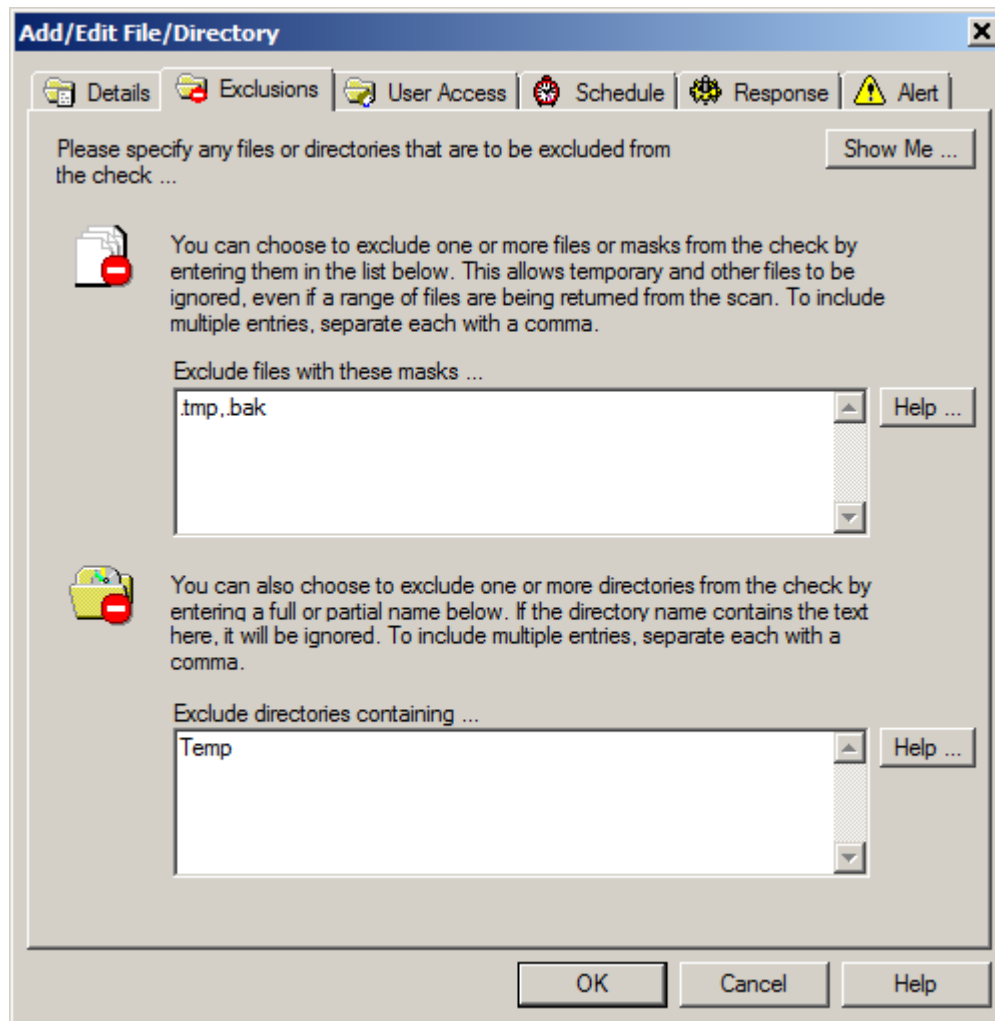
Trigger an alert if failures are detected at startup

By default, the monitor runs checks at startup (and when reconfiguring) in order to initialise its monitoring data. No alerts are triggered at this point – only when the next scan interval or scheduled scan is performed.

Tick this option if you also wish to trigger an alert when these checks are first performed, during this initialisation phase.

Excluding Files & Directories

To further refine the monitoring performed, you can also opt to exclude one or more files, partial files, or one or more sub-directories within the scan. You do this using the “Exclusions” tab.



Exclude Files with these masks ...

The first option allows you to enter one or more filenames or partial filenames separated by commas. If a matched filename equals or contains any of these strings, it will be ignored by the monitor. A wildcard (* character) can be used to indicate how filenames should be matched.



To exclude files ending in a string, start the name with a "*" - e.g. to exclude any file ending in '.bat', enter '*.bat'.

To exclude files beginning with a string, enter the string, followed by "*" - e.g. to exclude all files beginning with "L", enter "L*".

To exclude files containing a given string (anywhere within the name), enter the string with no wildcard character - e.g. to exclude any file containing "test", enter "TEST".

To exclude files beginning with a string and ending with another string, enter a wildcard in the middle of the name - e.g. to exclude any text (.txt) file beginning with the word "TEST", enter "TEST*.txt".

The file is excluded if the name matches any of the checks listed in this field.

Excluded names refer to the name of the file only - directory names are ignored. See also below.

Exclude directories containing ...

The second option allows you to enter one or more directory names or partial directory names separated by commas. If a directory or sub-directory that is being checked contains any of these strings, it will be ignored by the monitor.



For example, if you enter is 'Develop, 2007'.

- The following directories & sub-directories would continue to be scanned ...

C:\Program Files\Production
C:\Program Files\Production\2005


- While these would be ignored ...

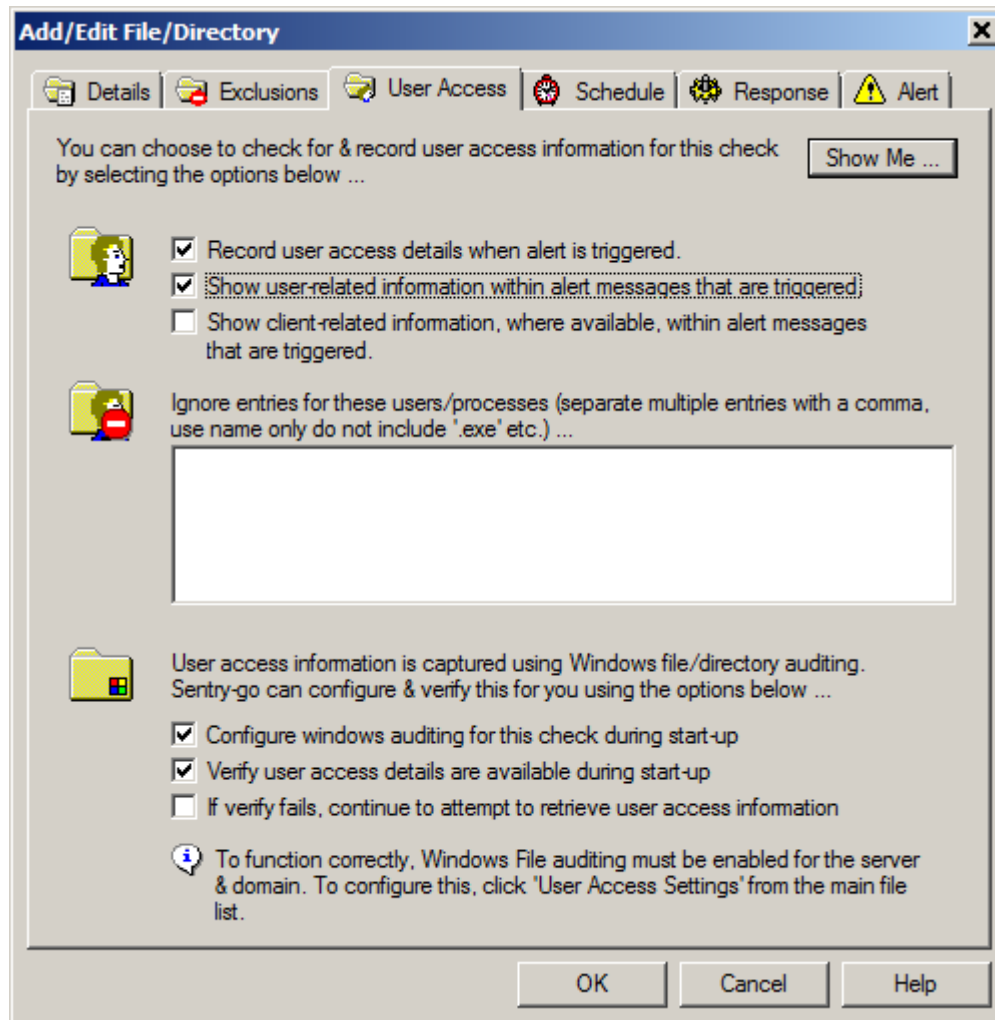
C:\Program Files\Production\2004
C:\Program Files\Development\2005
C:\Program Files\Development\2006

Wildcards should not be used in this field.

Capturing User Access Information

For some checks, you can optionally choose to capture information on the users & processes that accessed the file/directory and therefore may have caused the alert to be triggered. To configure this, select the “User Access” tab.

 Checks accessing remote files cannot be configured to capture user access information.




The options shown here allow you to control how, if at all, this information is to be captured. If you are logging user access information, the captured details will also be recorded to a log (CSV) file. See “Recording User Access Information” for more information.

Record user access details when alert is triggered

Tick this option to capture & record user access details when the alert is triggered. If selected, the monitor automatically attempts to access audit information for the related files/directories at the time the alert is triggered & includes this with the alert information.


Show user-related information within alert messages that are triggered

Tick this option to include user information within the alert message text. If not selected, user information will still be captured to the file (if configured), but not shown alongside the alert message itself.

-  Depending on the number of related file or directory accesses made, selecting this option can cause the alert message text to be a much longer message than it would otherwise be.

Show client-related information, where available, within alert messages that are triggered

Tick this option to include client information within the alert message text. If not selected, client user information will still be captured to the file (if configured), but not shown alongside the alert message itself.

-  Depending on the number of related file or directory accesses made, selecting this option can cause the alert message text to be a much longer message than it would otherwise be.


The availability of client-based information depends on the version of Windows & the type of access made (e.g. local vs. remote).

Ignore entries for these users/processes ...

This option allows you to effectively map-out specific users or processes that may access the monitored file or directory. If any of the values entered here (as a comma-separated list) are found for either the user or process accessing the file, the record will be ignored and no alert triggered.

Configure Windows auditing for this check during start-up

Tick this option (recommended) to indicate that the monitor should attempt to enable auditing on the required files/directories itself, when it is started or reconfigured. If un-ticked, no start-up processing will be performed and you should ensure that auditing information is being recorded, by Windows, for the required files/directories.


-  You can also configure auditing using the option on the main File monitoring list (see below), or manually, using Windows Explorer.

Verify user access details are available during start-up

Tick this option (recommended) to indicate that the monitor should perform a check of audit settings/information availability when it is started or reconfigured. When enabled, the monitor will attempt to verify that audit information is available by ...

- Either writing a test file to the selected directory.
- Or backing up the file and temporarily writing a new line to it, thus altering the file.
- Then verifying that audit information is written to the Event Log.

If access errors are detected, an alert is sent to all users defined as system users.

-  Your Security Policy may also need to be updated to allow object-based auditing to be performed. Contact your System Administrator if you need to do this.

If verify fails, continue to attempt to retrieve user access information

Tick this option if you want the monitor to attempt to retrieve user access information for the check even if the start-up verification fails. This allows the monitor to retrieve details if the server or domain's configuration is corrected without the need to restart it.

Scheduling the Check

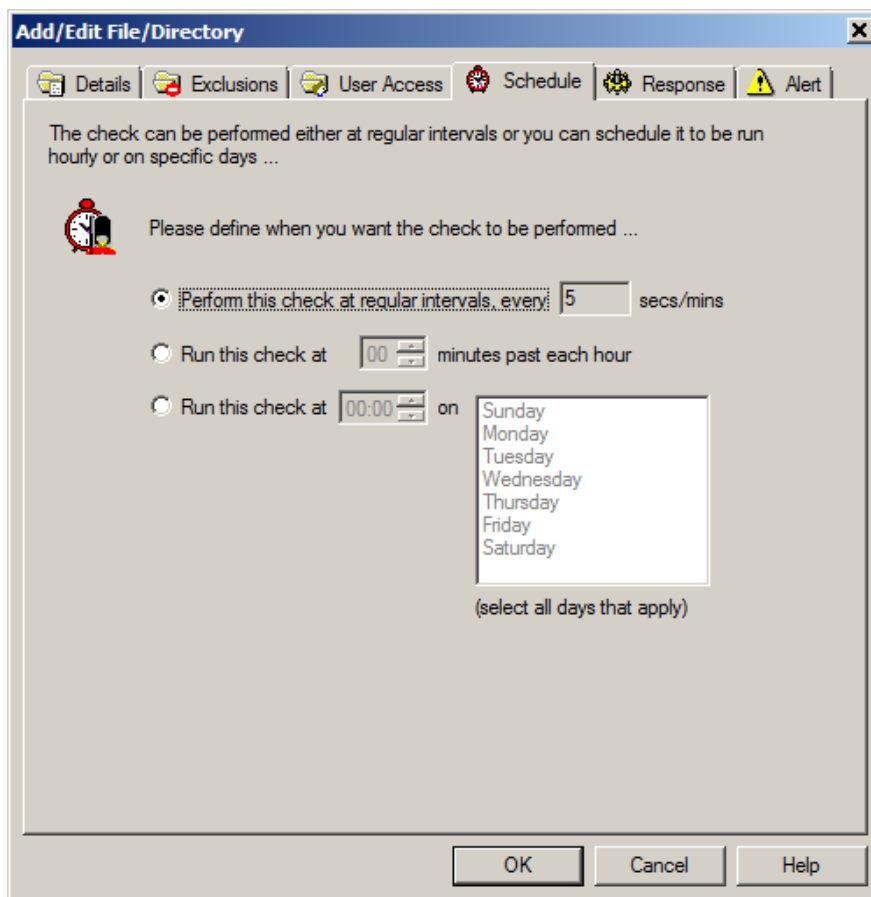
By default, each check is performed periodically at regular intervals throughout the day. The frequency of these checks is determined by the value specified at the bottom of the main list.

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.



It is recommended that checks defined as also capturing user access information are run regularly and at smaller intervals (i.e. more often) as this means that less Event log information needs to be processed by a single check.

For the above reason, when a "directory accessed" or "file accessed" check is defined, the system automatically overrides the default time and sets an interval of 30 seconds. This, however, can be updated below



From here you can define exactly when the check is to be performed.

Perform this check at regular intervals, every (mins)

Select this option to use the default interval specified at the bottom of the on the main list window. In this case the check will be performed every X minutes or seconds, depending on the check.

Run this check at HH:MM and every hour thereafter

Select this option to run the check at the specified time past each hour. In this case, only the minutes (MM) are used to determine when the check is to be performed.

Run this check at HH:MM On [Days]

Select this option to run the check at the specified time on the given days. In this case, the check will be performed at the given time if the associated day has been selected. Select all days that apply.

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.

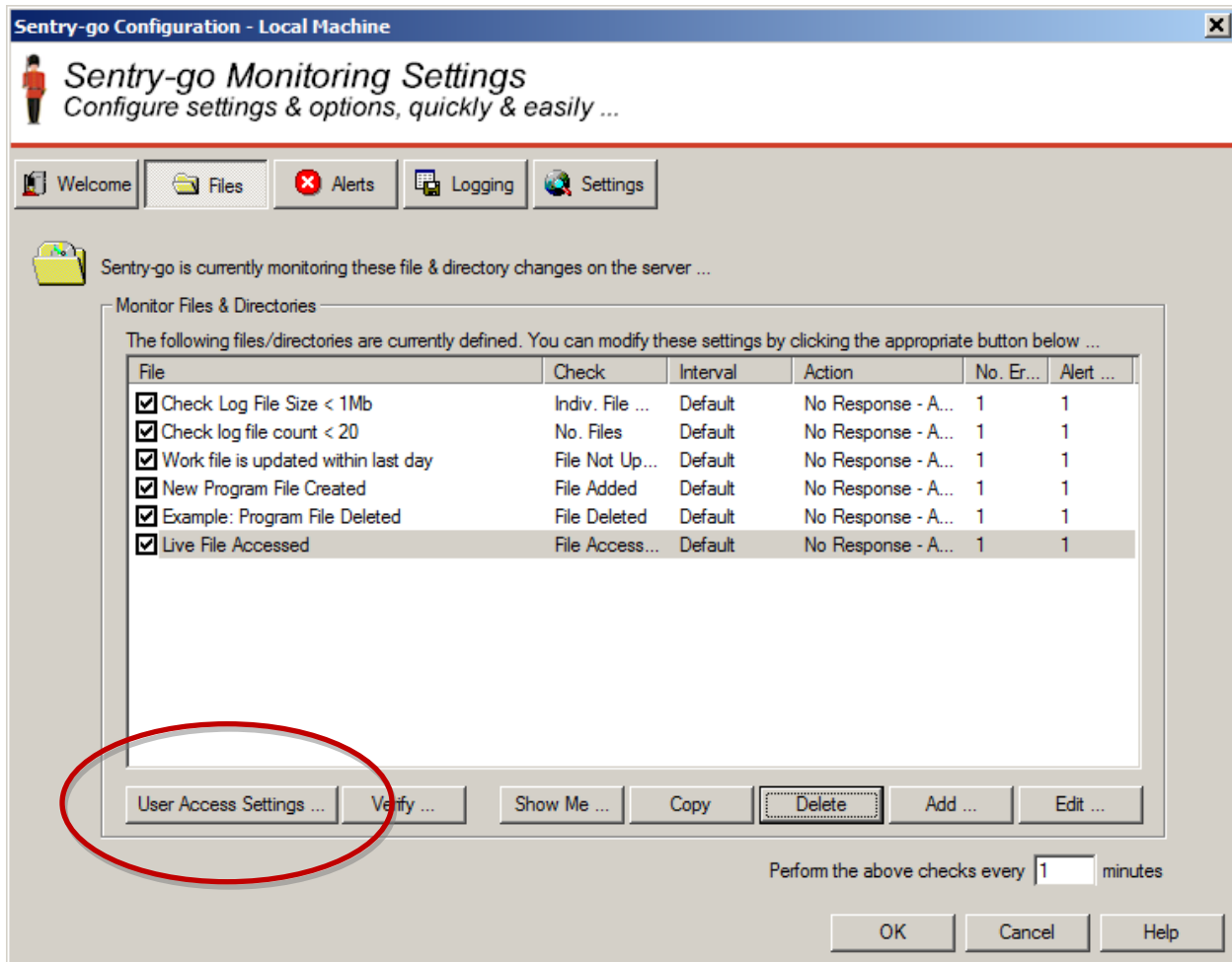


For more information on the options available as well as details on how to configure alerts & responses, see [Sentry-go - Configuring Alert & Automatic Response Options](#).

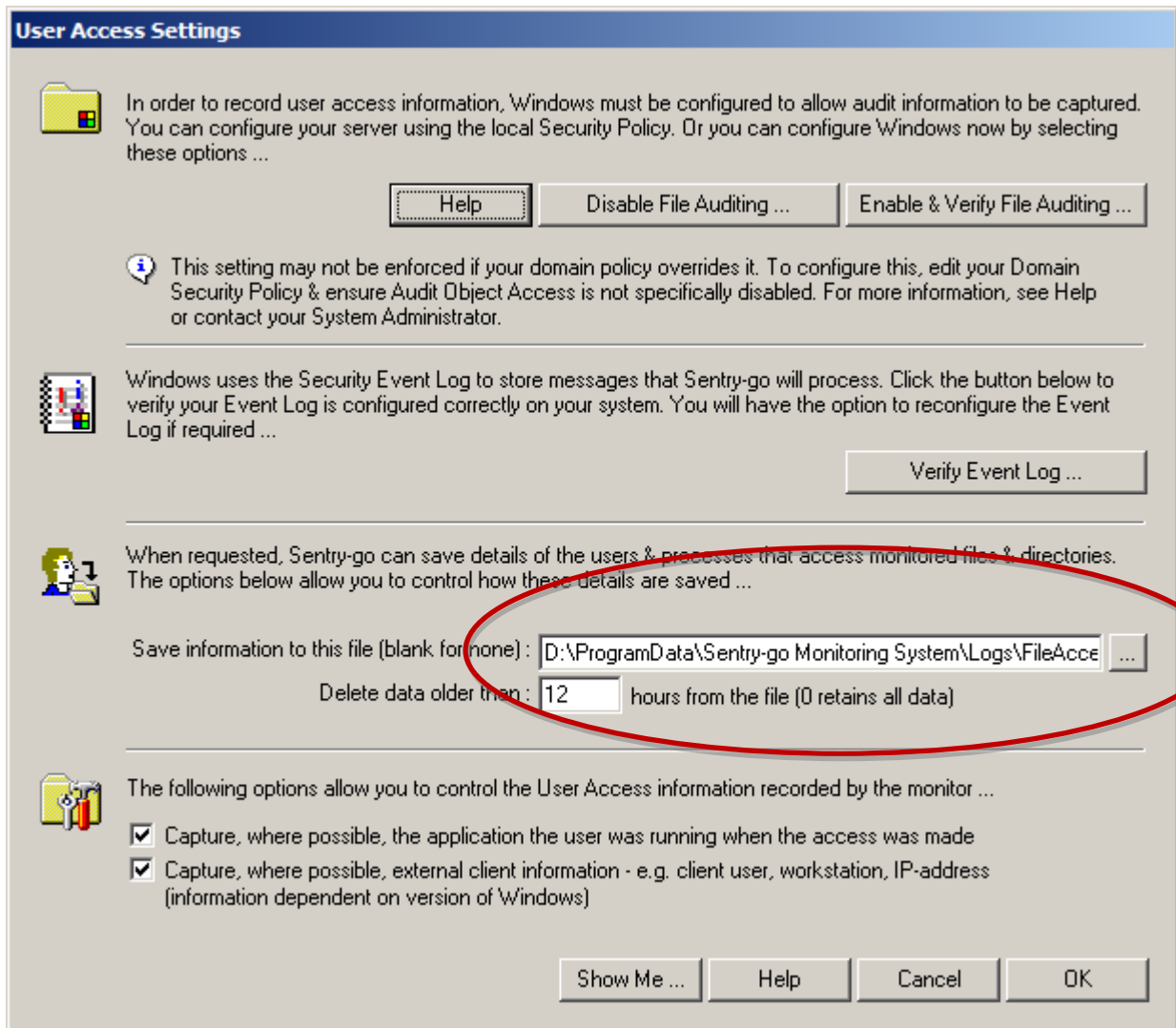
Recording User Access Information

If one or more checks are configured to capture user/process information, the server & domain must also be configured to allow this information to be captured. You also have the option of recording this information to a CSV file for later monitoring & analysis. This file is also used as the feed for the “File Access Information” web report.

To define & configure these options, click the “User Access Settings” button from the main File/Directory monitoring tab.



The following window will be shown ...



The top half of this window allows you to configure the server's file auditing capability & Event Log settings. For more information on configuring your environment, please see [Sentry-go - Monitoring File & Directory Access](#).

The lower half allows you to specify whether user access data is to be saved & control how long the data will be stored for.

Save information to this file

Enter the full path & name of the file in which the data will be saved. Click “...” to choose an existing file from Windows.

Delete data older than

In order to automatically trim the file, this value can be used to remove any data older than the number of hours shown. If set to 0, the file is never cleared down and new values will continue to be appended.



To view (and filter etc.) the contents of this file in a web report, select the “File Access Information” report.

Capture, where available, the application the user was running

By selecting this option, the monitor will additionally attempt to capture information on the process (application) the user was using when the access was made.



Depending on the access made & the version of Windows being run, this information may or may not be available.

Capture, where available, external client information

By selecting this option, the monitor will additionally attempt to capture details of the client that made the associated access request. For example the client user name, workstation & IP-address.



Depending on the access made & the version of Windows being run, this information may or may not be available.

What access information is captured by Sentry-go ?

When user access information is included, the following details can be captured by Sentry-go ...

- **User Name.** The Windows user name (ID) of the user(s) who accessed the file or directory within the scan period.
- **Client User Name.** Where available/applicable, the user name of the connecting client.
- **Client Workstation.** Where available/applicable, the Windows name of the connecting client.
- **Client IP-address.** Where available/applicable, the IP-address of the connecting client.
- **Application/Process Name.** If available, the name of the process accessing the file or directory. For remote accesses, this value will be blank.
- **Date & time.** The date/time of the last access the user/application accessed the file/directory, within the scan period.
- **Accesses.** Depending on the version of Windows, you can optionally record all the accesses that were granted to the user for the file/directory within the scan period.

They can be any combination of the values shown below ...

Access Mask	Meaning/Description
<i>File Read/List Directory</i>	File: Ability to read from the file. Directory: Ability to list the contents of the directory.
<i>File Write/Create File</i>	File: Ability to write data to the file. Directory: Ability to create a file.
<i>Read Extended Attributes</i>	Ability to read extended attributes.
<i>Write Extended Attributes</i>	Ability to write extended attributes.
<i>File Append/Create Subdirectory</i>	File: Ability to append data to the file. create a subdirectory. Directory: Ability to create a subdirectory.
<i>Execute File/Traverse Directory</i>	File: Ability to execute a file. Directory: Ability to traverse the directory.
<i>Delete Directory & All Files</i>	Ability to delete a directory & all files it contains, even if they are read-only.
<i>Read File Attributes</i>	Ability to read file attributes.
<i>Change File Attributes</i>	Ability to change file attributes.
<i>Delete</i>	Ability to delete the file.
<i>Read Security Descriptor & Owner</i>	Ability to read the security descriptor & owner information.
<i>Write DACL</i>	Ability to write DACL (security) information.
<i>Assign Owner</i>	Ability to assign owner.
<i>Synchronize</i>	Synchronizes access.
<i>N/A - <Number></i>	Indicates that the numeric access mask shown could not be translated.



The granting of a given permission indicates that the calling user/application requested it & gives an indication as to how the associated resource may have been used.

For Windows 2003 and earlier, the rights shown indicates that the right was granted; it does not necessarily mean it was actually used by that user or application. By combining this information with other checks made by the monitor, you can help isolate the exact accesses that were made.

For Windows 2008 and later, the rights shown indicates that the right was granted & used by the user or application.

Enabling Auditing on Your Server

In addition to enabling auditing for specific files or directories, Windows auditing must be enabled for the server and/or domain. If it is not, audit information will not be captured, even if configured for the file system itself.

For more information on configuring your environment in order to record file access information, please see [Sentry-go - Monitoring File & Directory Access](#).

Web Reporting with this Monitoring Component

In addition to the [standard Sentry-go web reports](#), this component provides the following additional reports for this component. These can be accessed using a standard URL, or via the monitor's home page.

The File Access Information Report

This report gives details of file accesses logged to the log file for monitoring checks defined as capturing user access information. User access information must be configured to be saved to a log file in order to populate this report. From here you can also filter on specific files, users, servers etc.

URL: <http://<Server Name>:<Port>/SgoMntrFileAccessInfo.sgp>

Recorded information from : D:\ProgramData\Sentry-go Monitoring System\Logs\FileAccess.log

Show details ... for file/directory :
... for server :
... for user :
... for check :
... with attributes containing :
Latest no. recs. to process : (ALL for all records)
Show client access info. :
Show the permissions granted :

Date/Time	Check Name	File Name	Server
07/10/2011 16:43:27 More	Directory was accessed	C:\Data Test\TestFile3.txt	WALTC
07/10/2011 16:43:27 More	File updated within last 10 minutes	C:\Data Test\TestFile.txt	WALTC
07/10/2011 16:43:27 More	File updated within last 10 minutes	C:\Data Test\TestFile2.txt	WALTC
07/10/2011 16:43:27 More	File updated within last 10 minutes	C:\Data Test\TestFile3.txt	WALTC
07/10/2011 16:43:51 More	File updated	C:\Data Test\TestFile.txt	WALTC
07/10/2011 16:43:51 More	File updated	C:\Data Test\TestFile2.txt	WALTC
07/10/2011 16:43:51 More	File updated	C:\Data Test\TestFile3.txt	WALTC
07/10/2011 16:43:51 More	Directory was accessed	C:\Data Test\TestFile.txt	WALTC


The report allows information to be restricted to specific files, checks, users etc. using the entries at the top right of the page. You can also click any link from within the report to restrict details to that information or click "More" to display current information about the file entry logged.

The Verify File Access Report

This report is accessed indirectly from the Console, when you right click over the “File & Directory monitoring” item in the left window and select “Verify User Access ...” from the menu. Alternatively it can be accessed from the monitor’s home page,

Initially a “please wait” message will be displayed while the monitor verifies user access information for the appropriate checks. Once complete, the following report will be displayed.

URL: `http://<Server Name>:<Port>/SgoMntrVerifyAllFileAccessInfo.sgp`


Server : WALTON-64
Licence : Demonstration (Shareware)
Generated on : 4th Nov. 2009 at 16:08:41
System Health :  52% check success ▲ [?] ▲

Sentry-go® Verify File Access Information

The following audit settings are currently defined to Sentry-go Monitoring Service These have been verified & the results are shown below ...

Check Name	File or Path	Result
Live Files Accessed	C:\Directory*.*	File or directory audit enabled. Auditing verified & data retrieved successfully.

Additional Information ...
For additional information, or if errors are reported above, please [click here](#).

Sentry-go


Done Local intranet | Protected Mode: Off 100%

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 information on configuring your environment in order to record file access information, please see [Sentry-go - Monitoring File & Directory Access](#)
- For the very latest information & product updates, please visit <http://www.Sentry-go.com>
- For sales advice, please e-mail Sales@Sentry-go.com
- For technical support, please e-mail Support@Sentry-go.com



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

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

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