



Configuring File & Directory Monitoring

With Sentry-go Quick & Plus! monitors

© 3Ds (UK) Limited, November, 2013

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

Be Proactive, Not Reactive!

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 see the “Configuring Event Log & Log File Monitoring guide.

This component will not only monitor 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.

In this guide

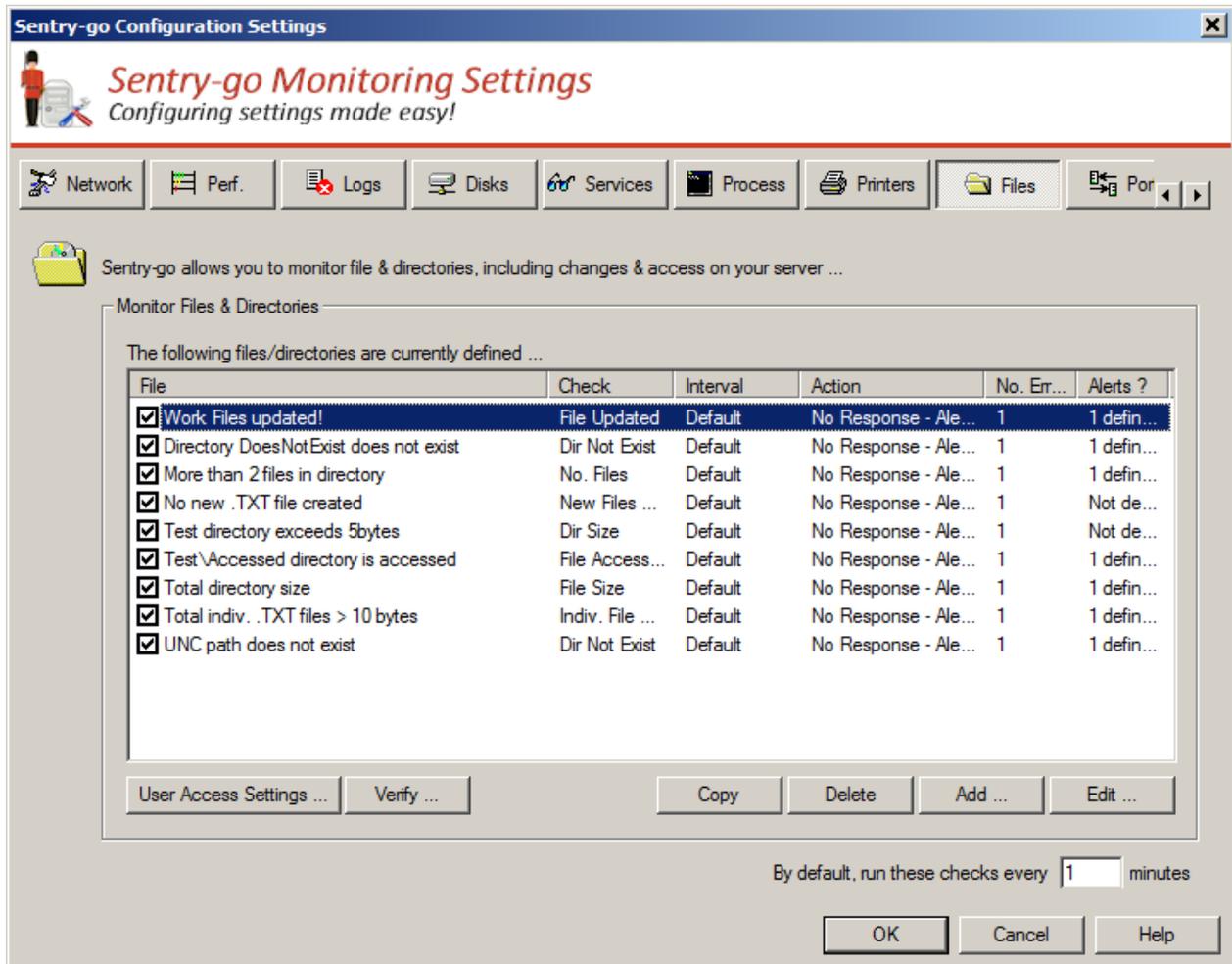
System requirements	3
Monitoring files & directories	3
Adding a new file or directory monitoring check	4
Configuring file monitoring	8
Specifying monitoring criteria	11
Excluding files & directories	13
Capturing user access information	15
Scheduling a check	17
Configuring an automatic response	17
Configuring an alert.....	17
Temporarily ignoring a configured check	17
Web reporting with this monitoring component.....	18
The file access information report.....	18
The verify file access report	19
Recording user access information.....	20
What access information is captured by Sentry-go ?	22
Configuring your system for user access monitoring.....	24
What you need	24
Configuring your domain	25
Configuring your server.....	28
Configuring your event log	34
Configuring the file system.....	37
Disabling or removing auditing on files & directories	44
More Information	45

System requirements

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

Monitoring files & directories

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



By default, run these checks every (minutes)

This value specifies how often, in minutes, Sentry-go should check for available space on the disks listed. For system drives and drives used by the print spooler, it is recommended that a more frequent check be performed - e.g. 5 - 15 minutes.

This interval is only used when the interval is set to “Default”. You can also configure the monitor to check a particular drive at a given time or interval – e.g. hourly, daily etc. To do this, edit the particular disk from the list or configure the interval when the disk is added to the list.

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 ...

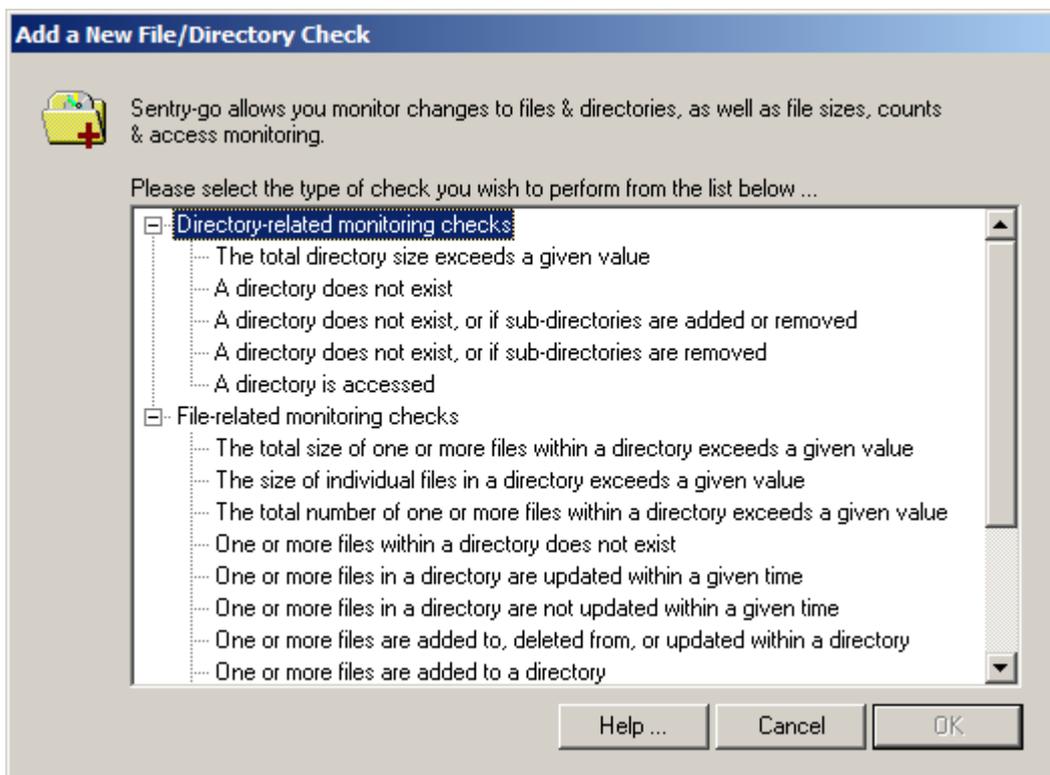
If user access information has been requested as part of a file/directory check, audit information for the appropriate files & directories must be available. To enable or verify that details are available, highlight the appropriate check & click this button.



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

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.

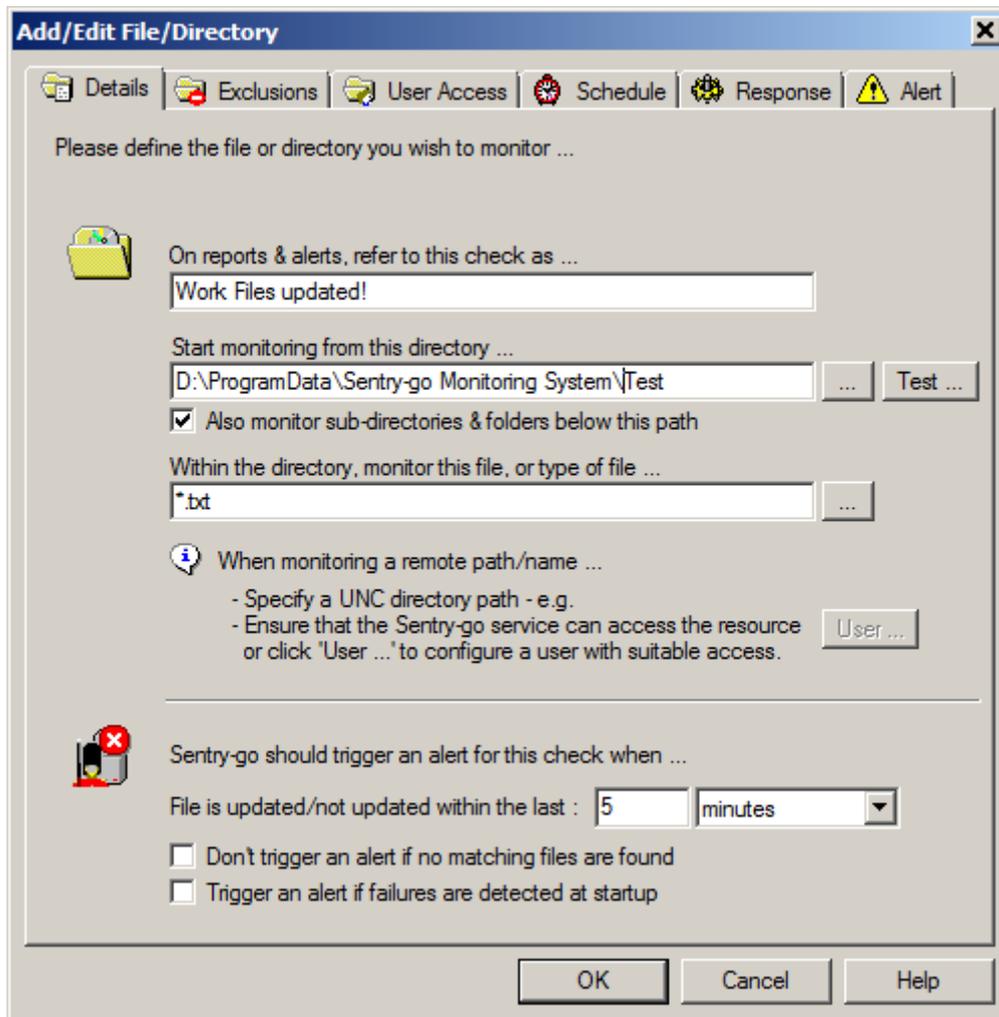
Select this option if you wish to be notified if the directory, or a file within it (and optionally within subdirectories) is accessed.

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 file monitoring

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 ...

Add/Edit File Mask

Sentry-go can monitor one, many or all files in the directory. Please select the type of files you wish to monitor from the options below ...

I want to monitor all files in the directory.

I want to monitor all files of a specific type, with this file extension ...
(Either select an entry, or type in the mask - e.g. *.msk)

I want to monitor this specific file ...

Files containing dates can also be monitored using placemarkers (e.g. \$\$DD, \$\$MM). See Help for more information.

Help ... Cancel OK

From here you can select one of the following ...

- **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).

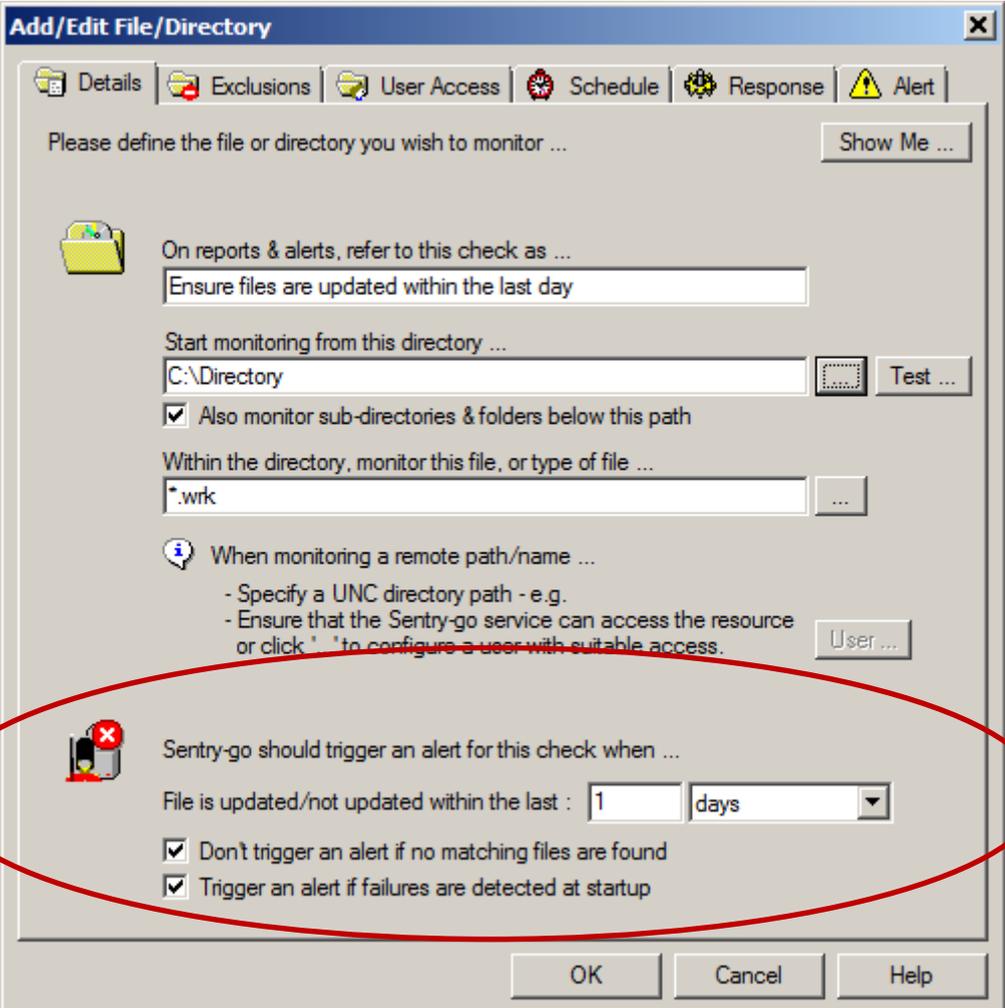
When selected, you can either choose an extension from the list (e.g. .log files), or enter your own in the field below (e.g. *.tmp, or s*.tmp etc.).

- **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 'Details' tab selected. The dialog is titled 'Add/Edit File/Directory' and has a close button (X) in the top right corner. Below the title bar are several tabs: 'Details', 'Exclusions', 'User Access', 'Schedule', 'Response', and 'Alert'. The 'Details' tab is active, and the text 'Please define the file or directory you wish to monitor ...' is displayed above a 'Show Me ...' button. The main area contains several fields and options:

- A folder icon followed by the text 'On reports & alerts, refer to this check as ...' and a text box containing 'Ensure files are updated within the last day'.
- The text 'Start monitoring from this directory ...' followed by a text box containing 'C:\Directory' and a 'Test ...' button.
- A checked checkbox labeled 'Also monitor sub-directories & folders below this path'.
- The text 'Within the directory, monitor this file, or type of file ...' followed by a text box containing '*.wrk' and a '...' button.
- An information icon followed by the text 'When monitoring a remote path/name ...' and two bullet points: '- Specify a UNC directory path - e.g.' and '- Ensure that the Sentry-go service can access the resource or click '...' to configure a user with suitable access.' A 'User ...' button is located to the right.
- A bell icon with a red 'X' followed by the text 'Sentry-go should trigger an alert for this check when ...'. This section is circled in red. It includes a text box 'File is updated/not updated within the last : 1' and a dropdown menu set to 'days'. Below this are two checked checkboxes: 'Don't trigger an alert if no matching files are found' and 'Trigger an alert if failures are detected at startup'.

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

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.

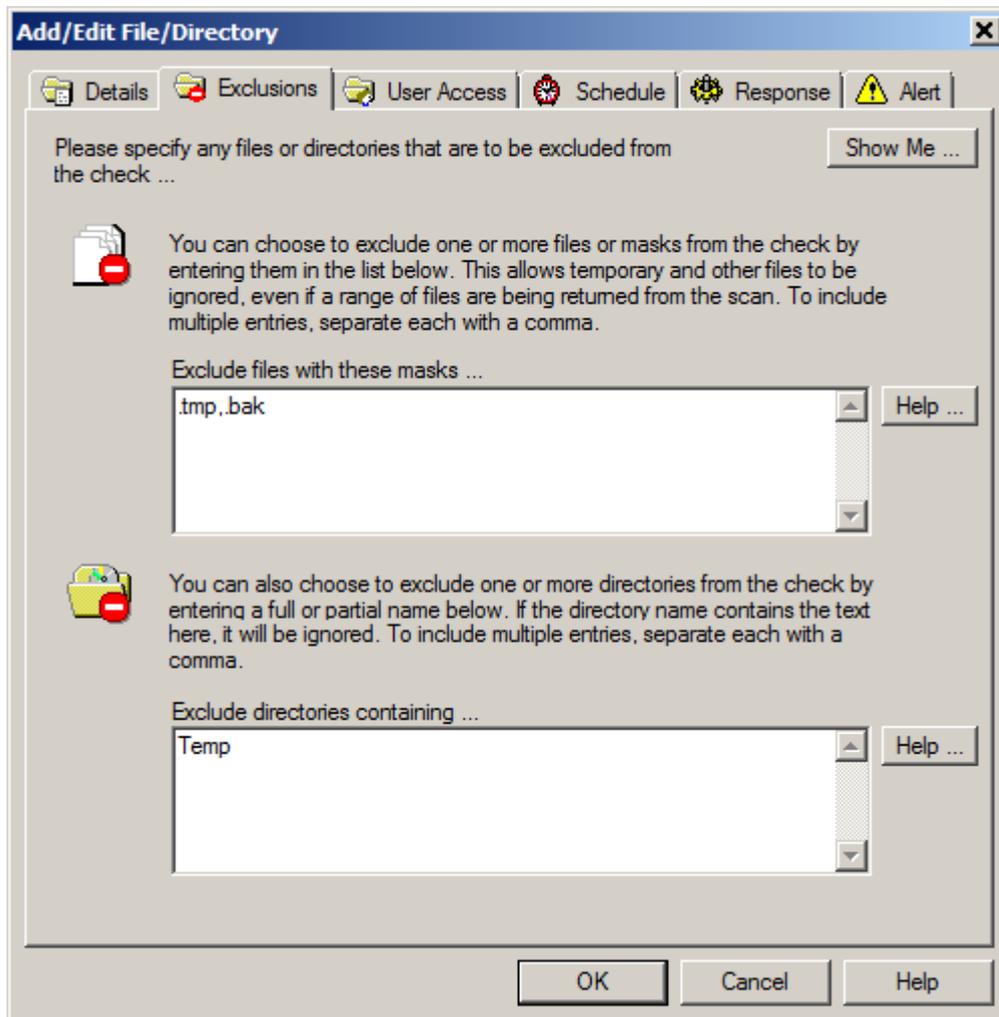
Trigger an alert if failures are detected at startup

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 ...

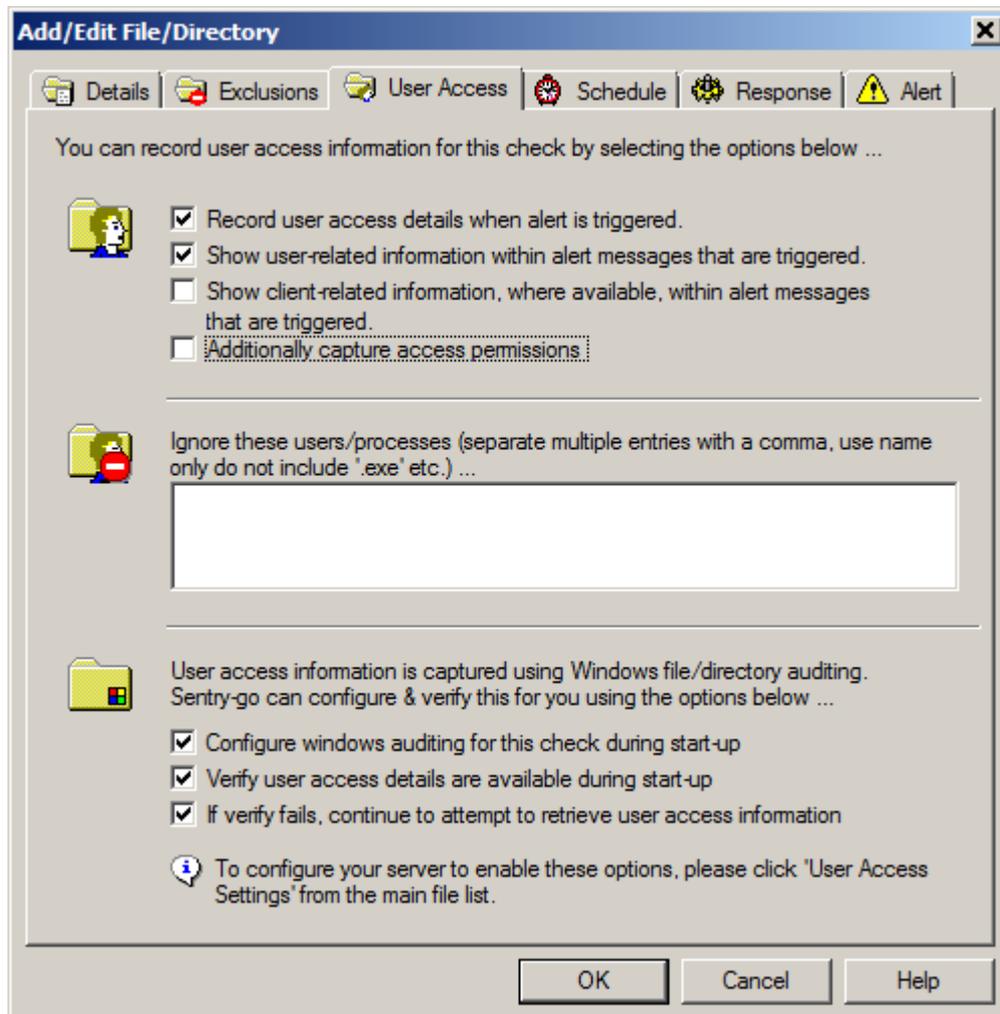
C:\Program Files\Production\2004
C:\Program Files\Development\2005
C:\Program Files\Development\2006

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).

Additionally capture access permissions

Tick this option to collect information about the permissions available to the user when access was made (if available).

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 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.

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

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

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.

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

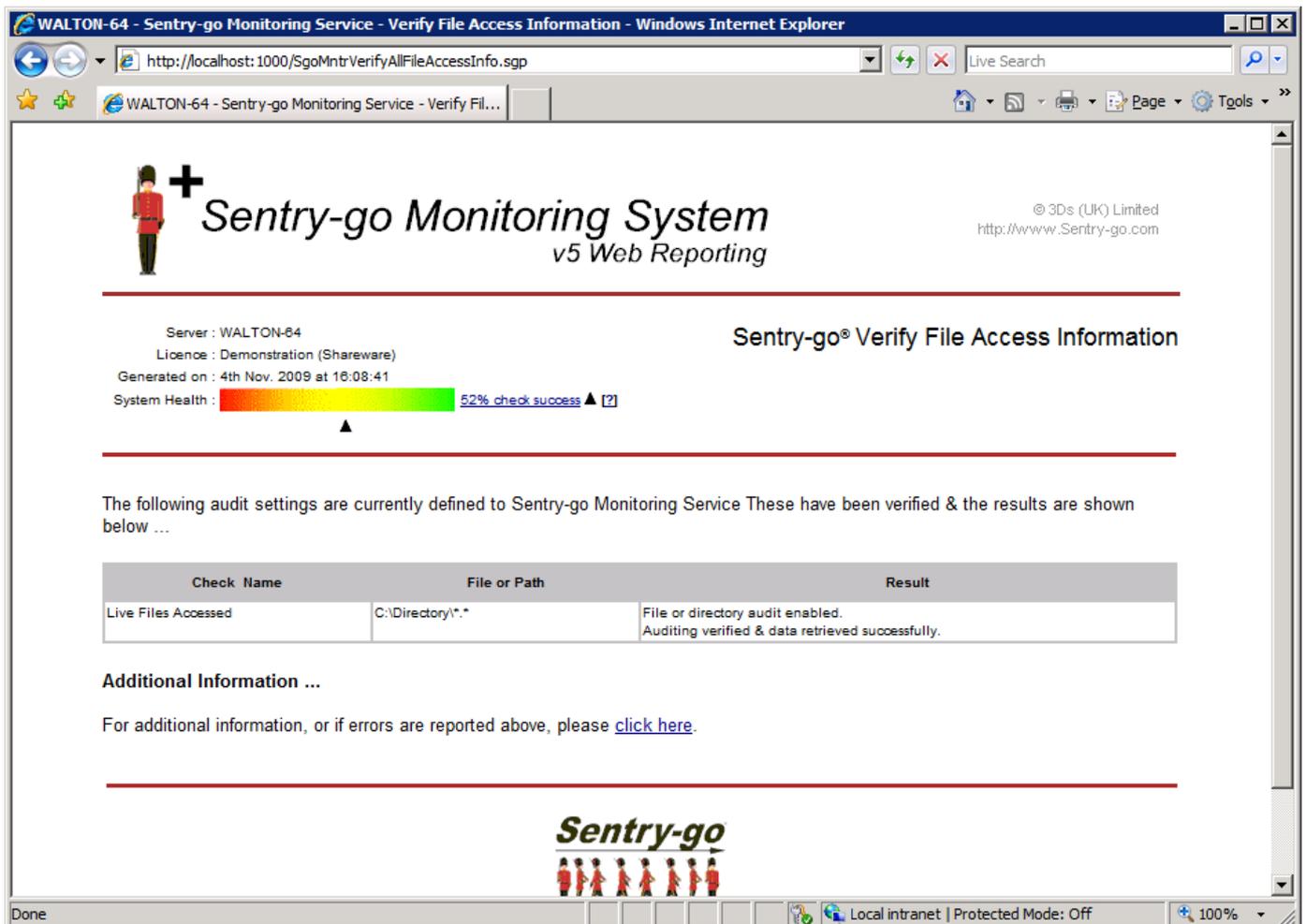
The report allows information to be restricted to specific files, checks, users etc. using the entries at the top right of the page. You can also click any link from within the report to restrict details to that information or click "More" to display current information about the file entry logged.

The verify file access report

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

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.



WALTON-64 - Sentry-go Monitoring Service - Verify File Access Information - Windows Internet Explorer

http://localhost:1000/SgoMntrVerifyAllFileAccessInfo.sgp

WALTON-64 - Sentry-go Monitoring Service - Verify Fil...

 **Sentry-go Monitoring System**
v5 Web Reporting

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

Server : WALTON-64
Licence : Demonstration (Shareware)
Generated on : 4th Nov. 2009 at 18:08:41
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

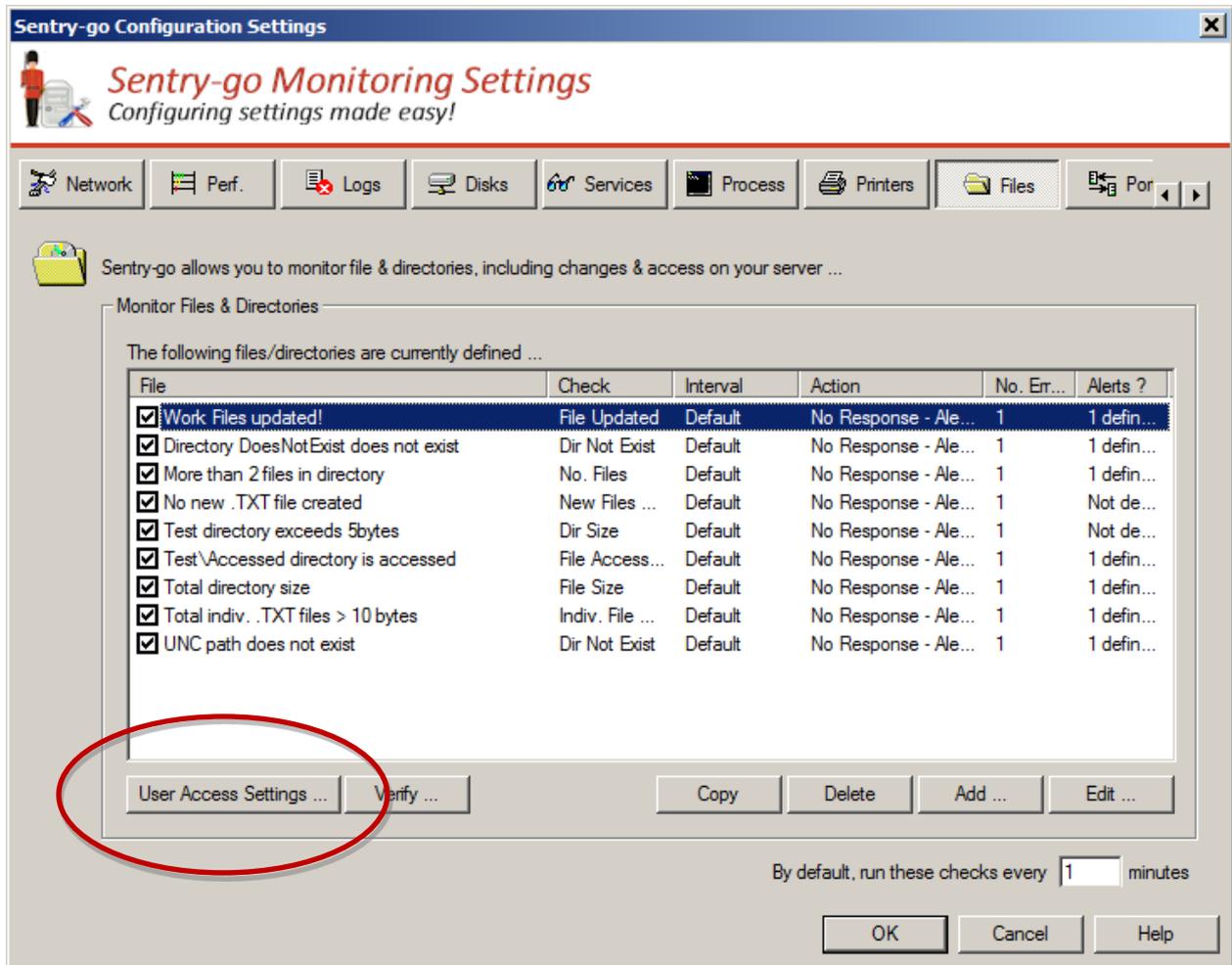
Local intranet | Protected Mode: Off

100%

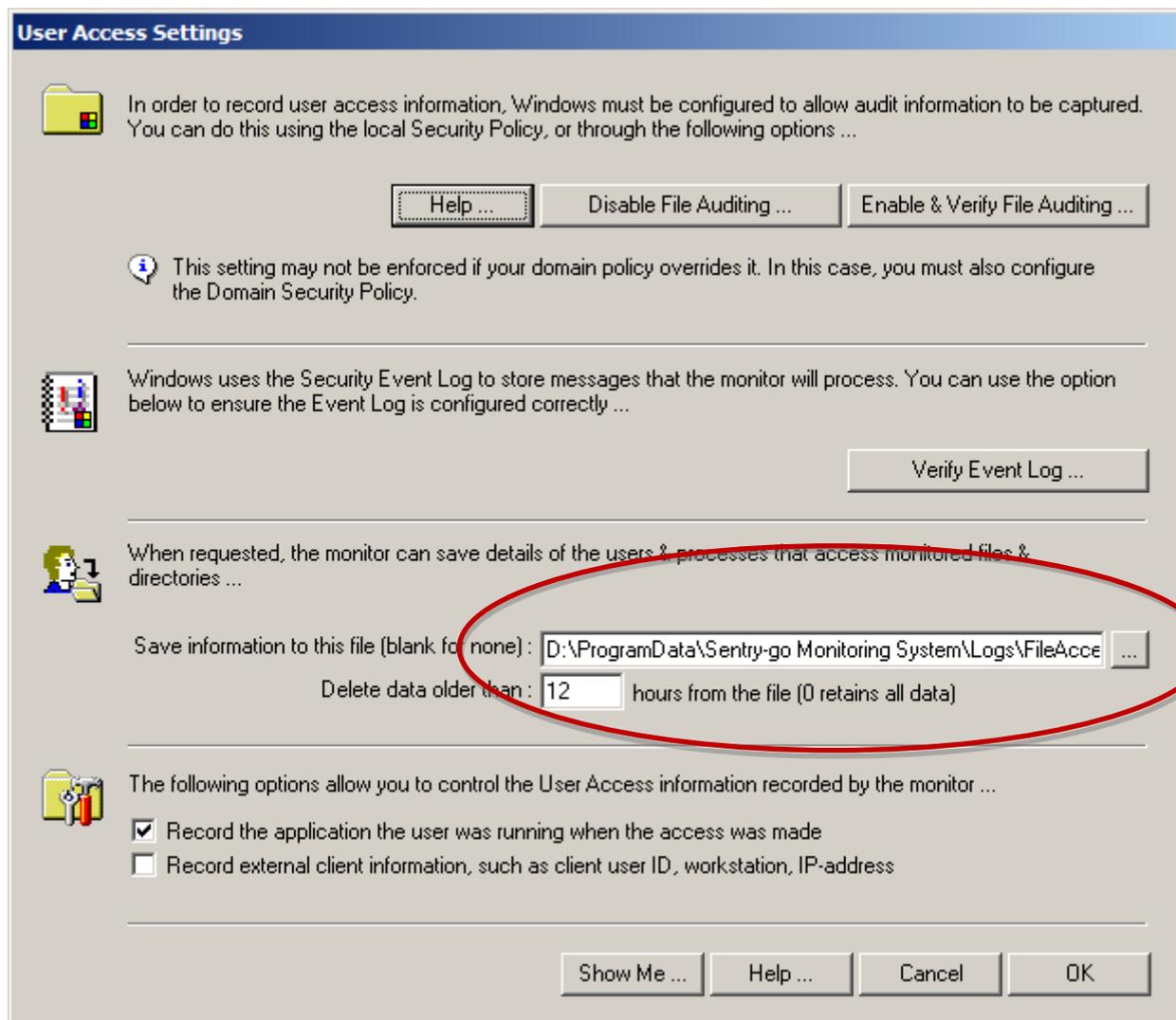
Recording user access information

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, while 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.

Record 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.

Record 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.

Configuring your system for user access monitoring

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.

Specific details, aimed primarily at administrators are shown below.

What you need

By default, Windows doesn't provide tracking information for file or directory accesses. Instead it allows you to generate audit information to the Security Event Log for specific files & directories. The details recorded are dependent on the version of Windows being used and in its raw form can be somewhat cryptic and time-consuming to interpret.

However with Sentry-go, this information is automatically processed & matched to the files/directories being monitored, recording details in a more readable & much more useable & useful format.

To do this, you must ensure the following ...

<i>To ensure this ...</i>	<i>Use either Sentry-go ...</i>	<i>Or Use Windows ...</i>
Your domain must allow the auditing of successful "object access" attempts.	<ul style="list-style-type: none">• Configure the Sentry-go monitor & select the "File" tab.• On this window, click "User Access Settings".• From here you can enable & verify file access auditing on the server.• This will allow you to determine if the domain is configured correctly.• If it isn't, or you wish to review the current settings, edit your domain security policy to ensure the auditing of "object access" is not specifically disabled.• See more information below or contact your System Administrator.	<ul style="list-style-type: none">• Access your Domain Security Policy.• Review & update the settings so that the auditing of "object access" is not specifically disabled.• See more information below or contact your System Administrator.
Your server must be configured to audit successful "object access" attempts.	<ul style="list-style-type: none">• Perform the same test as above.• This will set the appropriate options for the server.• See more information below.	<ul style="list-style-type: none">• Access your Local Security Policy.• Review & update the settings so that the auditing of "object access" – specifically "success" access attempts, are enabled.• See more information below or contact your System Administrator.

To ensure this ...

Your server's Security Event log must be configured to allow audit messages to be captured.

The directories being monitored are configured to generate the appropriate information.

Use either Sentry-go ...

- From here you can verify the Event Log & its settings.
- This will also give you the option of updating the configuration to the recommended settings.
- See more information below or contact your System Administrator.
- Configure the Sentry-go monitor & select the "File" tab.
- On this window, add new (or edit existing) checks and display its properties.
- Select the "User Access" tab & ensure the "Configure windows auditing for this check during start-up" is ticked.
- Other options are also available – see below.

Or Use Windows ...

- Configure the Event Log using Event Viewer and ensure the log file can grow to a sufficient size (at least 20Mb) and is set to overwrite as needed or equivalent (i.e. doesn't ever report full).
- Alternatively, contact your System Administrator.
- Access the directories through Windows Explorer.
- Display security properties & ensure auditing (specifically successful access attempts) for all users is enabled.
- See below for more information.

Configuring your domain



Depending on your current configuration, there may be no changes needed here. However, often your domain settings will override local server options and may prevent the latter from functioning correctly.

For safety & security, domain-level changes must be performed through Windows using a process similar to that outlined here. Checks & verification can, however, be performed through Sentry-go.

If you are in any doubt, or do not have the appropriate domain-level access, please contact your System Administrator.

Remember, changes here can affect all member servers in the domain.

To configure/enable Windows file auditing on a member server, you need to ensure that “object access” auditing is not specifically disabled at the domain level. If it is, any setting made on the member server will have no effect.

! It is important to note the term “not disabled”. It is strongly recommended that you do not specifically enable auditing at the domain level. Instead, you simply don’t prevent member servers from enabling it themselves in their own local policy ...

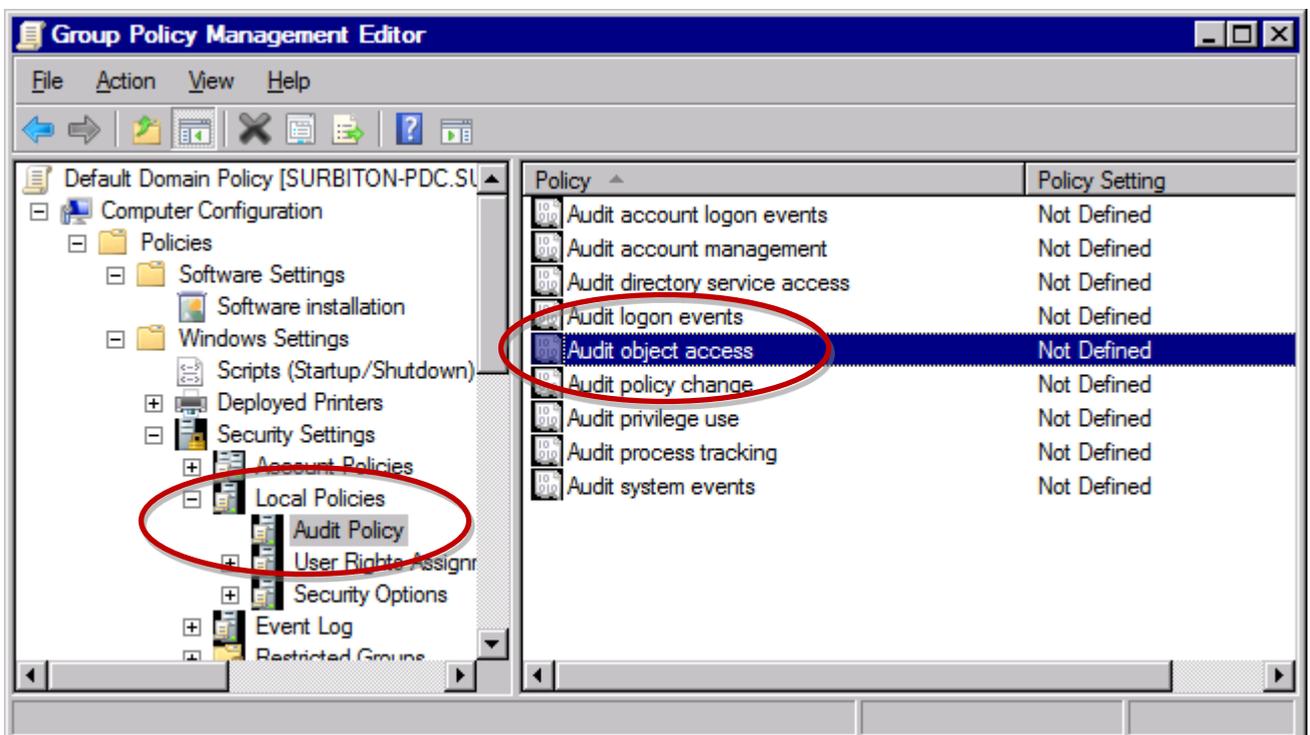
- If you enable object level auditing at the domain level, all member servers will have their auditing enabled by default. This may have an adverse affect on performance and generate a lot of unwanted & unnecessary log entries in their Event Logs.

For this reason, it is generally recommended that you avoid enabling these settings specifically at the domain level, instead, enabling them on the specific servers that require it.

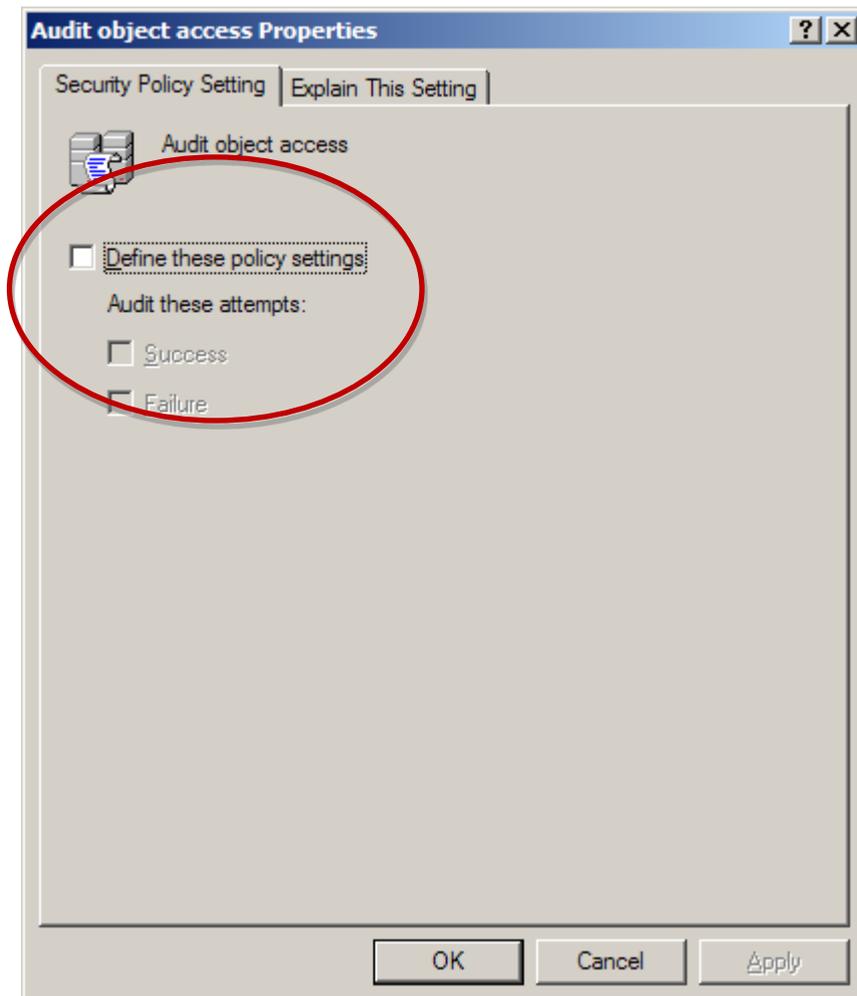
- However, if you specifically disable object level auditing at the domain level, you effectively disallow it for all member servers below it. This in turn overrides any setting specified locally and hence no audit information will be generated & no file access information will be recorded by the monitor.
- The recommended approach is therefore to allow object level auditing at the domain level, but not specifically enable it. You simply don’t disable it in the policy, which in turn allows settings on the individual servers themselves to either enable, or disable auditing.

So, to verify & configure the domain, follow these steps ...

- Logon to the domain controller as an Administrator, or to a server with access to the domain’s group policy.
- From “Administrative Tools”, select “Group Policy Management”
- In the left hand window, expand the GPOs to display the one you wish to edit – for example, the default policy for the domain.
- Right click this entry and select “Edit ...”.
- In the right hand list, double-click ...
 - Computer Configuration
 - Policies
 - Windows Settings
 - Security Settings
 - Local Policies
 - Audit Policy



- The next action depends on the entry against “Audit object access” - files & directories are treated as “object” within auditing ...
 - If it is set to “Not defined”, the policy will not override any local setting which we’ll configure later. No changes are required in this case.
 - If it is set to “Success” or “Success, failure” auditing is already enabled and no further action is required here.
 - If it is set to “No auditing” or “failure” only, you should change the configuration if you want file access information to be generated. Continue to the next step.
- If you need to edit the configuration, select “Audit object access” to display its properties. The resulting window will look something like this ...



- Depending on the existing settings, make one of the following changes. *If you are in any doubt, consult your System Administrator before making any changes ...*
 - If nothing is ticked (including “Define these policy settings”), then no changes are required.
 - If “Define these policy settings” is ticked, but neither “Success” nor “Failure” is checked, then the domain level policy is currently defined to disable object auditing.

With this setting defined, the policy is preventing audit settings on member servers from taking effect and no file access information will be generated. In this case, it is recommended that you simply enable the ability for member servers to audit object access by un-ticking the “Define these policy settings” option - i.e. nothing is ticked on this window.

By doing this, the local policy will have control and you can enable/disable features at the local server level – i.e. on the servers where file access monitoring is required.
 - If “Failure” is already ticked, then this may be because you are monitoring failures domain-wide. *Contact your System Administrator before continuing.*
 - If domain-wide settings are required, you should ensure that the “Success” option is also ticked. If it isn't, local settings will be overridden and no file access information will be generated.
- Once the appropriate change, if any, has been made, click OK to close the window.

Configuring your server

Once the domain configuration has been set to enable auditing on member servers as described above, you can configure the local server to ensure the appropriate audit entries are generated.

You can do this either using Sentry-go configuration options, or through Windows. As with the domain, this should only need to be performed once.

Using Sentry-go

The quickest & easiest way of configuring your server is to use Sentry-go which can verify existing settings & make the necessary local changes as required. To do this, configure the Sentry-go monitor & select the "Files" tab. At the bottom of this window, click the "User Access Settings" button ...

Sentry-go Configuration Settings

Sentry-go Monitoring Settings
Configuring settings made easy!

Network Perf. Logs Disks Services Process Printers Files

Sentry-go allows you to monitor file & directories, including changes & access on your server ...

Monitor Files & Directories

The following files/directories are currently defined ...

File	Check	Interval	Action	No. Err...	Alerts ?
<input checked="" type="checkbox"/> Work Files updated!	File Updated	Default	No Response - Ale...	1	1 defin...
<input checked="" type="checkbox"/> Directory DoesNotExist does not exist	Dir Not Exist	Default	No Response - Ale...	1	1 defin...
<input checked="" type="checkbox"/> More than 2 files in directory	No. Files	Default	No Response - Ale...	1	1 defin...
<input checked="" type="checkbox"/> No new .TXT file created	New Files ...	Default	No Response - Ale...	1	Not de...
<input checked="" type="checkbox"/> Test directory exceeds 5bytes	Dir Size	Default	No Response - Ale...	1	Not de...
<input checked="" type="checkbox"/> Test\Accessed directory is accessed	File Access...	Default	No Response - Ale...	1	1 defin...
<input checked="" type="checkbox"/> Total directory size	File Size	Default	No Response - Ale...	1	1 defin...
<input checked="" type="checkbox"/> Total indiv. .TXT files > 10 bytes	Indiv. File ...	Default	No Response - Ale...	1	1 defin...
<input checked="" type="checkbox"/> UNC path does not exist	Dir Not Exist	Default	No Response - Ale...	1	1 defin...

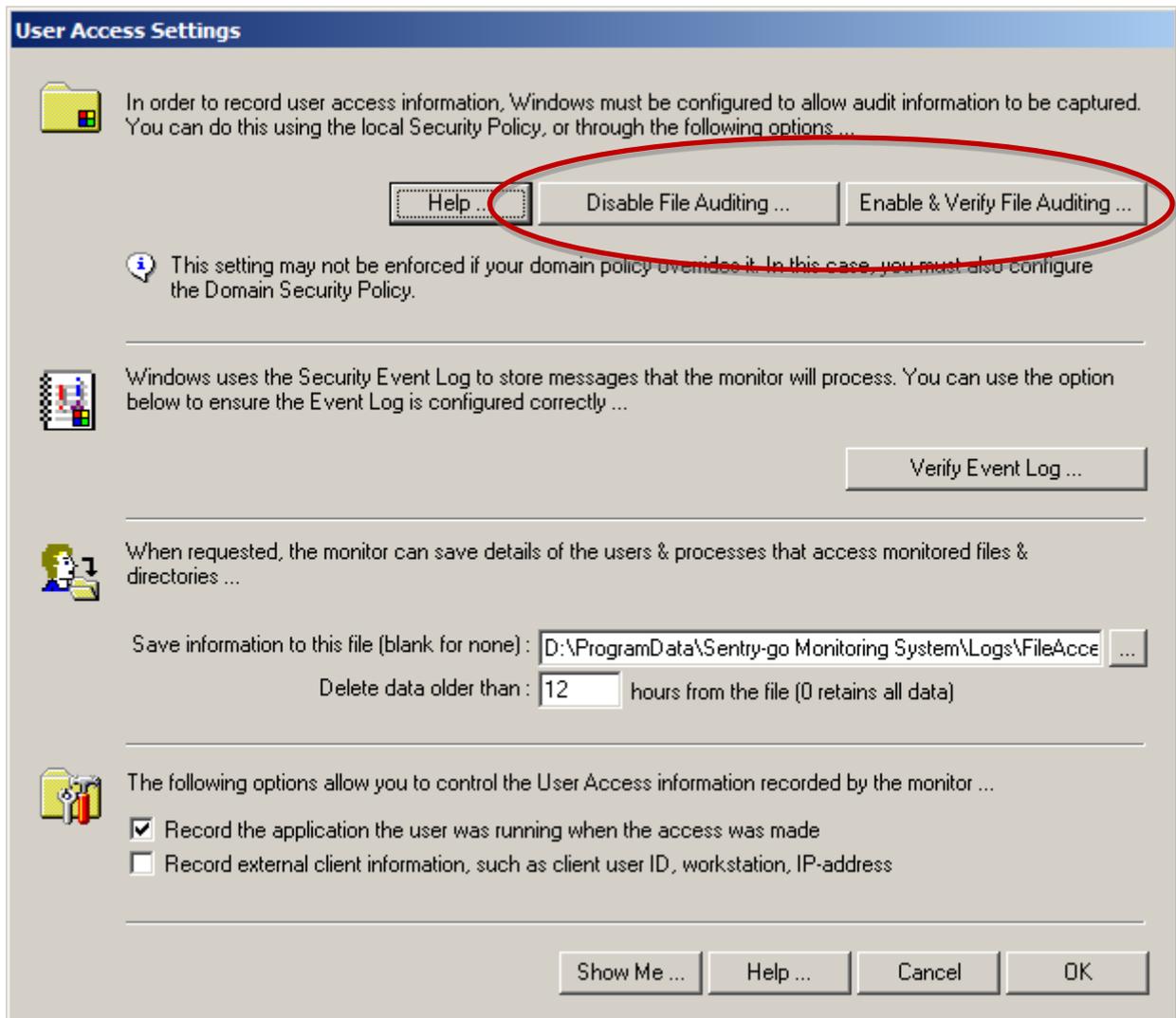
User Access Settings ... Verify ... Copy Delete Add ... Edit ...

By default, run these checks every minutes

OK Cancel Help

The following window will be displayed. To enable auditing on the server, click “Enable File Auditing”. This will also verify that audit information is available or whether your domain settings also need updating.

Likewise, to disable it, choose “Disable File Auditing” ...



 Disabling auditing will mean that no file access information will be available to the monitor.

After selecting either option, the Console will connect the monitor & display a web report. Once complete, the results of the request will be displayed to you. For example ...

WALTON-64 - Sentry-go Monitoring Service - Configure File Auditing - Windows Internet Explorer

http://localhost:1000/SgoMntrEnableFileAudit.sgp

Live Search

WALTON-64 - Sentry-go Mo... WALTON-64 - Sentry-go ... x

Page Tools

 **Sentry-go Monitoring System**
v5 Web Reporting

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

Server : WALTON-64
Licence : Demonstration (Shareware)
Generated on : 4th Nov. 2009 at 15:59:41
System Health :  67% check success [?]

Sentry-go® Configure File Auditing

Sentry-go Monitoring Service will attempt to configure file auditing on the server. The results are shown below ...

Request Summary ...

Request from client : 127.0.0.1
Request : Enable & verify file auditing on this server
Server : WALTON-64

Result : Configuring file access auditing on the server ...
Auditing is already configured on this server ...
Performing tests, please wait ...
Creating temporary file ...
Applying file access settings ...
Verifying file access information is accessible ...
Tests completed successfully. File access information is configured & available on this server.

Done Local intranet | Protected Mode: Off 100%

 Any errors will also be displayed.

If the results indicate that the local server settings were correctly configured but the test for file access failed, it is likely that local options are being overridden by your domain security policy (see above).

In this case, check your domain security policy as described in the previous section or contact your System Administrator.

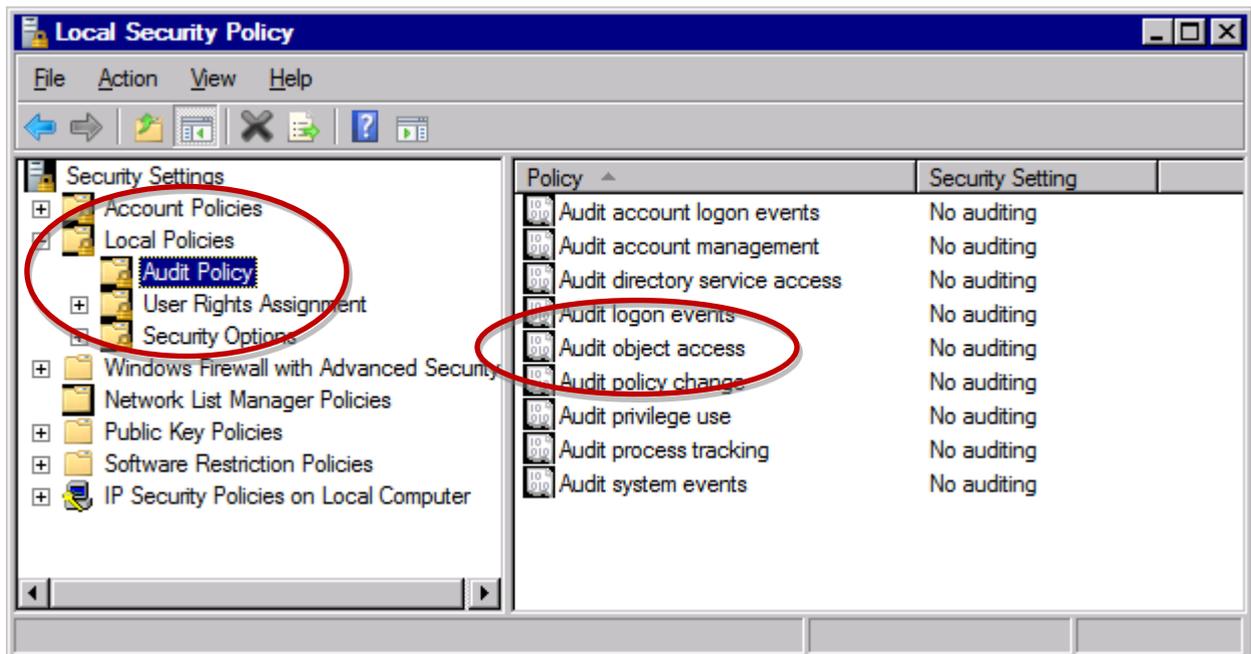
Using Windows

To configure/enable Windows file auditing on your local server, follow the steps outlined below.

-  Settings changed within the local security policy may be overwritten by the next refresh of Group Policy security settings. If this is likely, it is recommended that you change the settings globally within the domain.

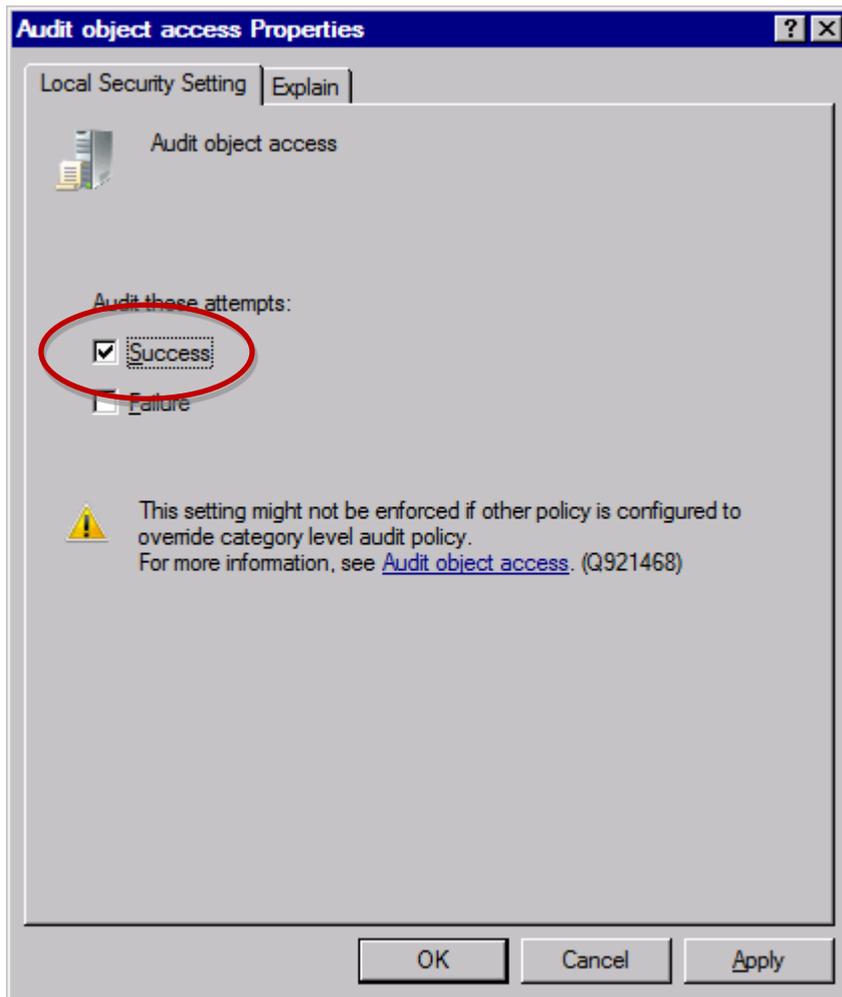
To configure/enable Windows auditing ...

- Logon to the server as an Administrator.
- From Administrative Tools, select “Local Security Policy”
- From the left hand list, expand ...
 - Local Policies
 - Audit Policy



- From the right hand list, select “Audit object access” – files & directories are treated as “object” within auditing.
- If the setting currently includes “Success” then no changes are required.

- If not, display the properties for this setting ...



- Ensure "Success" is ticked. "Failure" audit entries are not required by Sentry-go but may be needed by other software. If "Failure" is already enabled, contact your System Administrator.
- Click "OK" for each window to close & save changes.

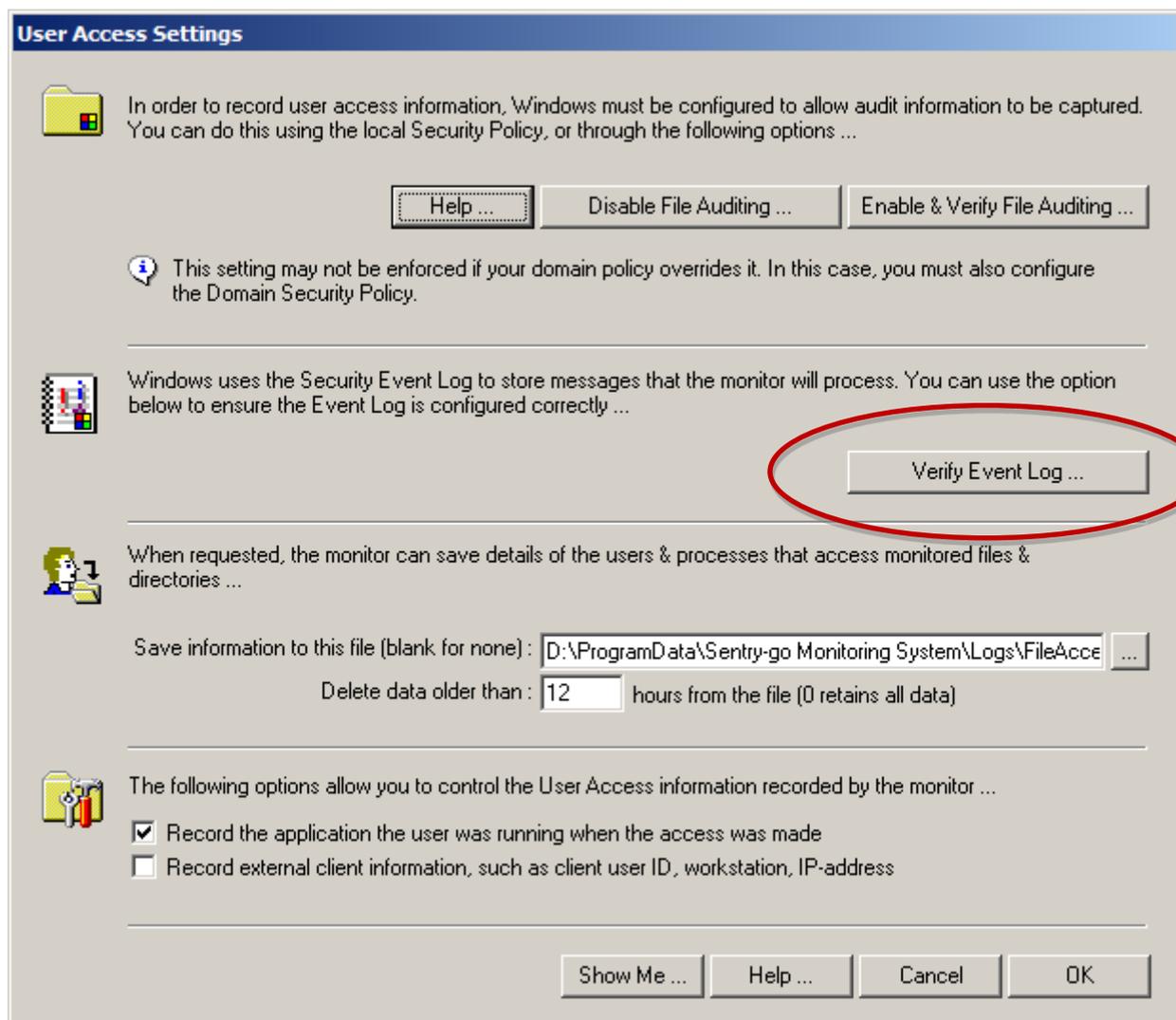
Configuring your event log

Windows auditing writes its messages to the local Security Event Log. With this in mind, you may also wish to review the Security Event Log configuration on the server and if necessary update it. You should only need to do this once.

Again, you can do this through Sentry-go or manually using Windows.

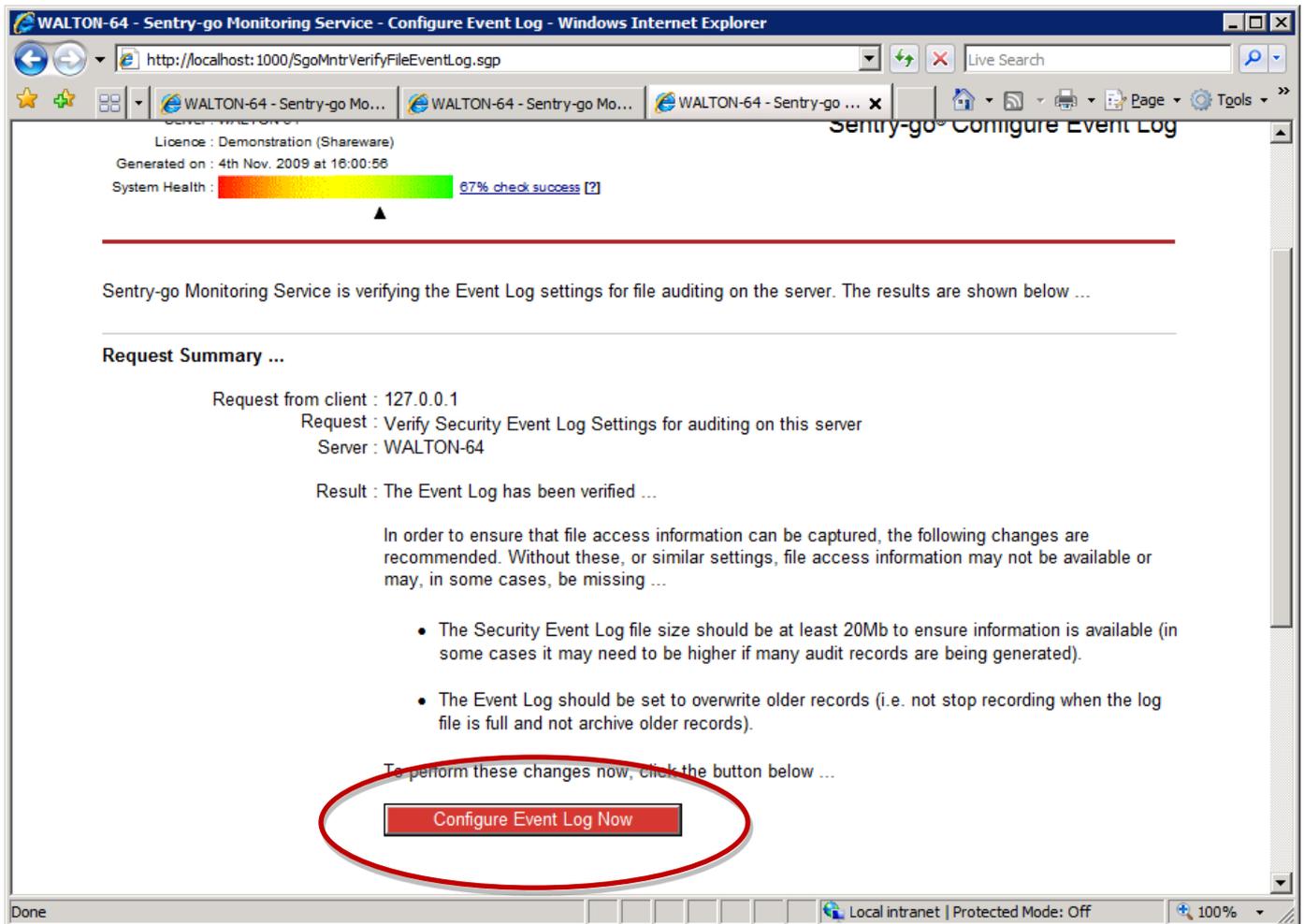
Using Sentry-go

The quickest & easiest way of configuring the server's Security Event Log is by using Sentry-go itself. To do this, configure the Sentry-go monitor using the Client Console & select the "Files" tab. At the bottom of this window, click the "User Access Settings" button to display the following window ...



Now click "Verify Event Log".

After selecting this option, the Console will connect the monitor & display a web report. Once complete, the results of the request will be displayed to you. For example ...



If changes are recommended, this indicates ...

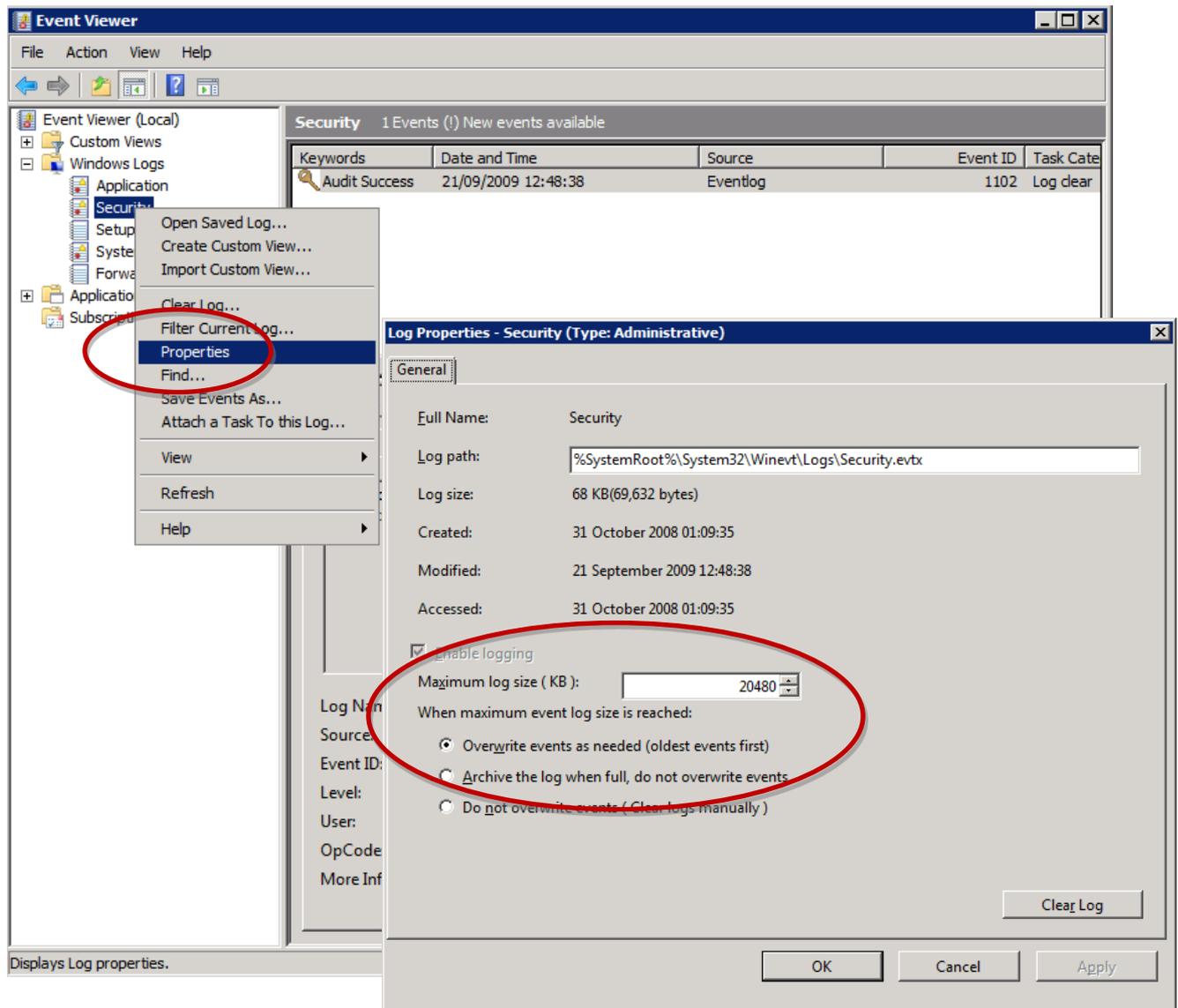
- The size is set below 20Mb (which is the minimum recommended to hold the audit information)
- The audit records are not set to "Overwrite as needed" (or equivalent).

Both of these options may lead to records not being logged and hence file access information being missed. Click the "Configure Event Log Now" button to alter these settings (or see below to set them using Windows instead).

- ⚠ If in doubt, contact your System Administrator before proceeding. Changes here may have an affect on other systems.

Using Windows

To view/configure Event Log settings using Windows on tools, run the Windows Event Viewer (EventVwr.exe) and display properties of the Security Event log ...



For example, the log ...

- Should be set to be large enough to hold the required information for a complete scan cycle (e.g. at least 20480Kb)
- Should be configured so that it will not fill up (e.g. select "Overwrite events as needed").

Configuring the file system

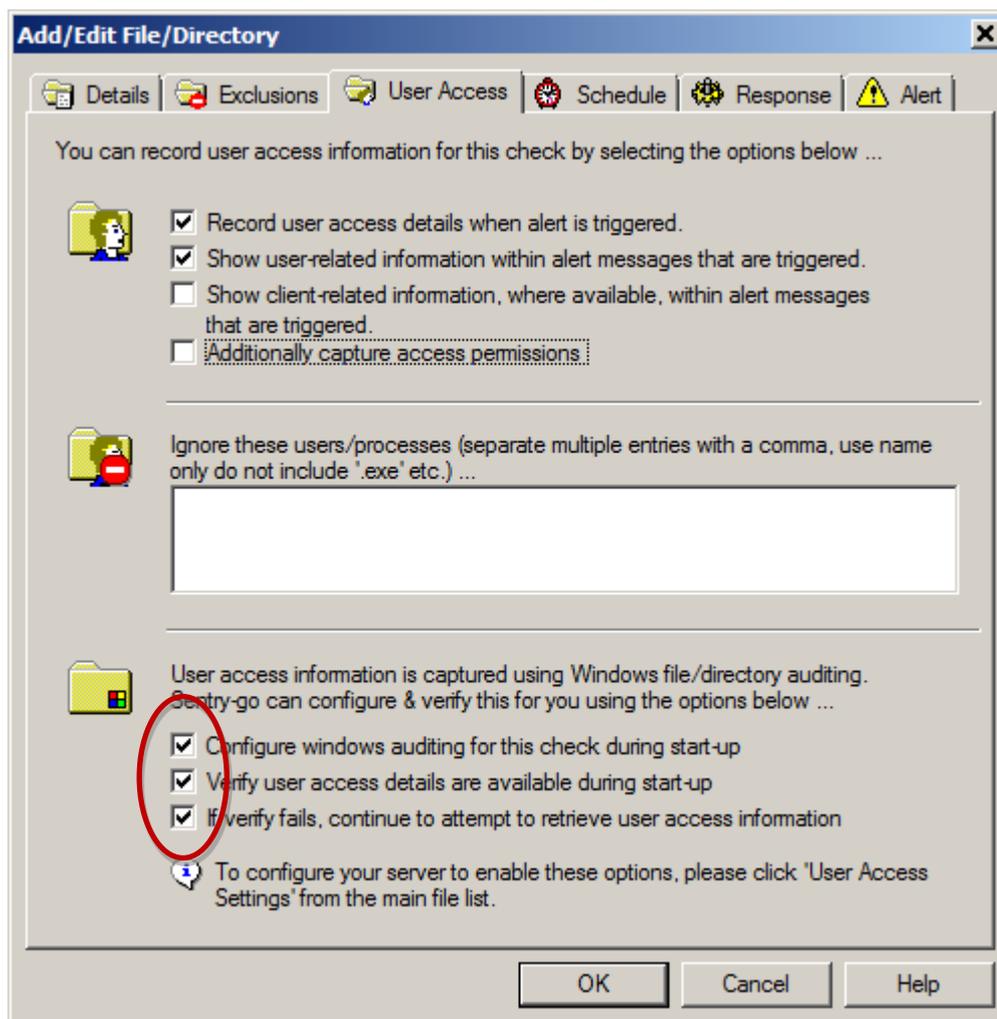
Lastly, to capture user access information, auditing must also be configured for the file/directory being monitored. There are two ways to do this, either automatically using Sentry-go, or manually using Windows Explorer.

Using Sentry-go

In most cases the simplest option is to let the monitor configure access automatically. You can also use options to verify that the settings are correct.

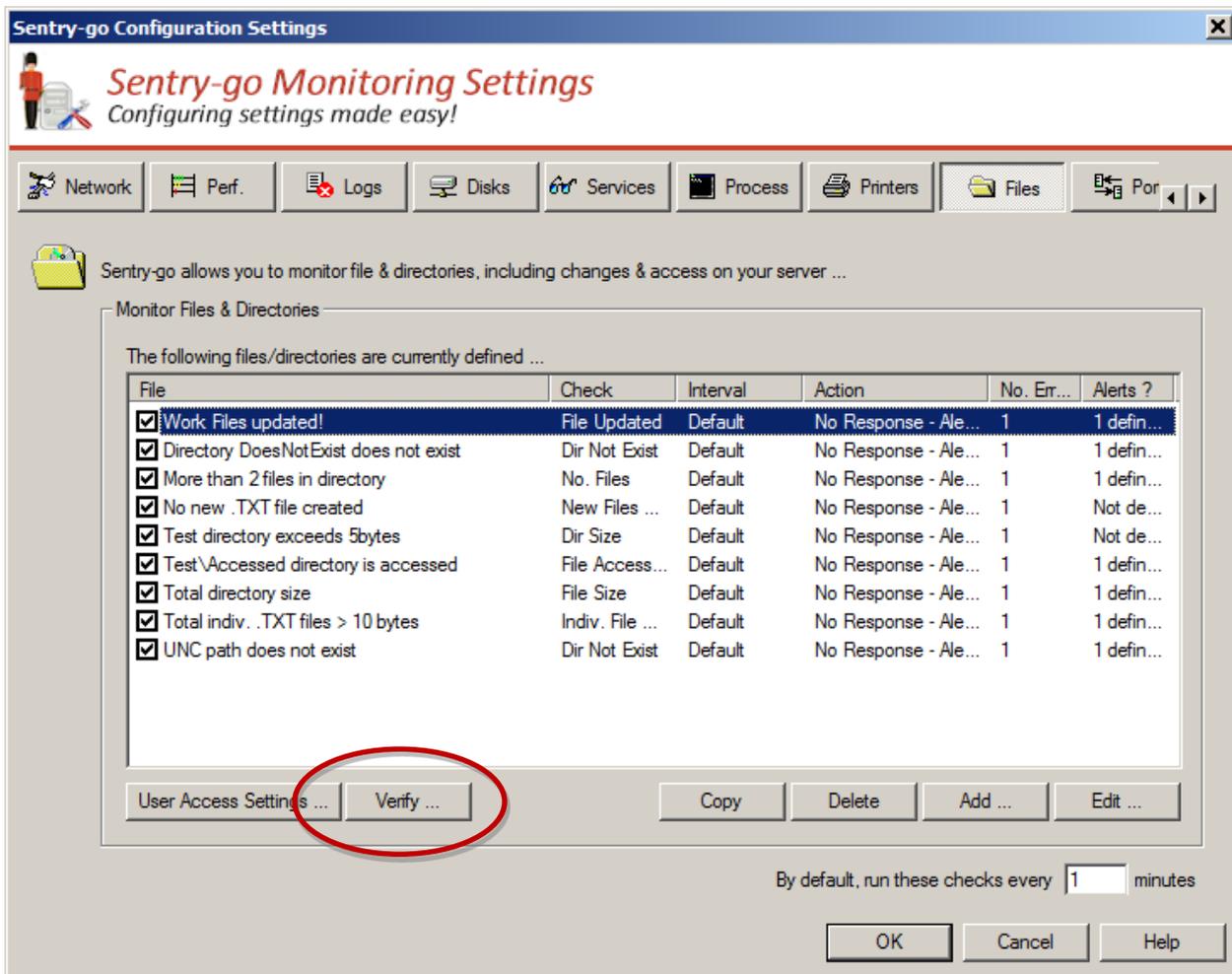
Option 1. When defining or editing the check

When you're defining the check using the Client Console, tick the "Configure Windows auditing for this check during start-up" option. This will configure the monitor to enable/verify auditing during start-up.



After defining a check on the main list

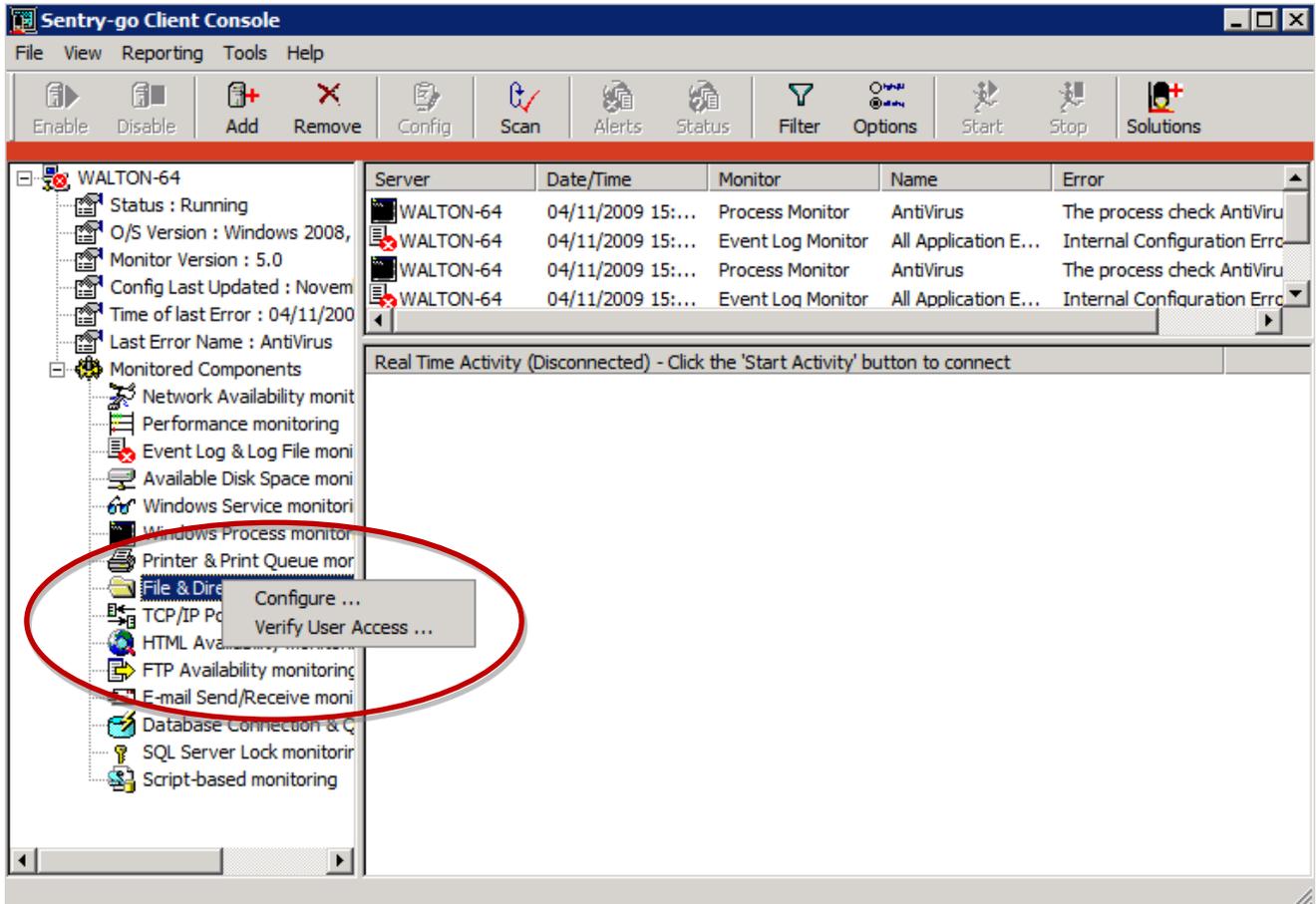
If you've already defined a check and wish to enable auditing or verify user access, highlight it in the list & click "Verify User Access" ...



The monitor's web interface will be accessed and the results displayed on-line.

Verifying All Checks

If you've already defined a number of checks and wish to verify auditing on all that are configured you capture user information, close the configuration window and return to the main Console window.



In the left hand server list, expand the server you wish to verify and display its monitoring components. Right click the "File Monitoring" entry and select "Verify User Access". All checks configured to record user access information will be verified.

Once again, the Console will connect to the monitor's web interface and display a report containing the results of these checks.

Using Windows Explorer

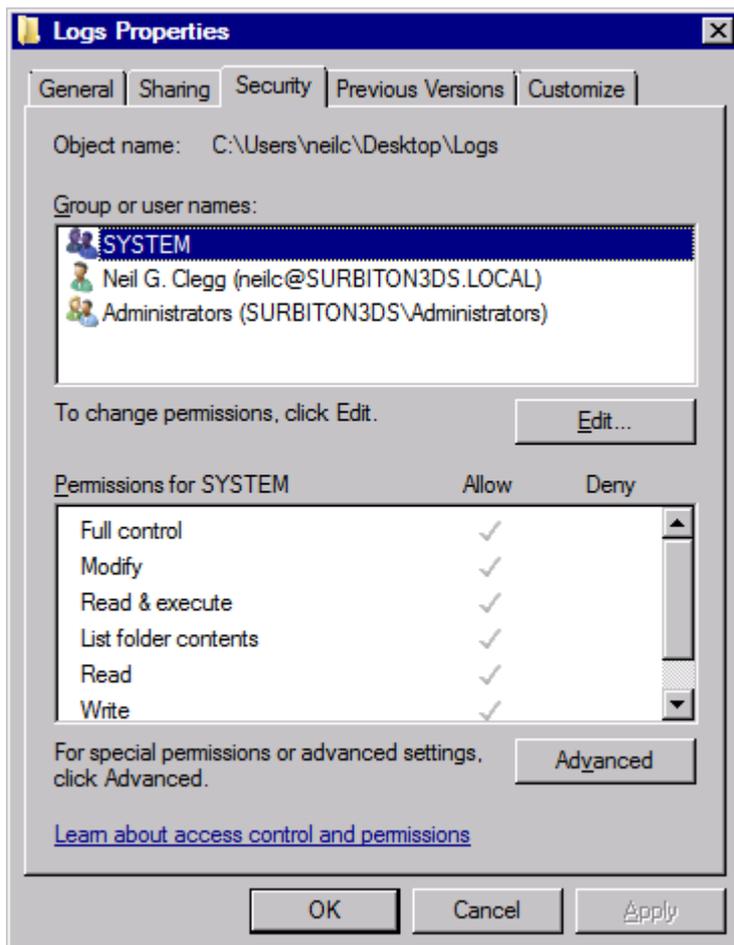
Although it is recommended that you let the monitor configure auditing on files/directories for you, as shown in the previous section, for completeness, we will describe how to do this using Windows Explorer here.

To enable or disable auditing for a file or directory using Windows Explorer ...

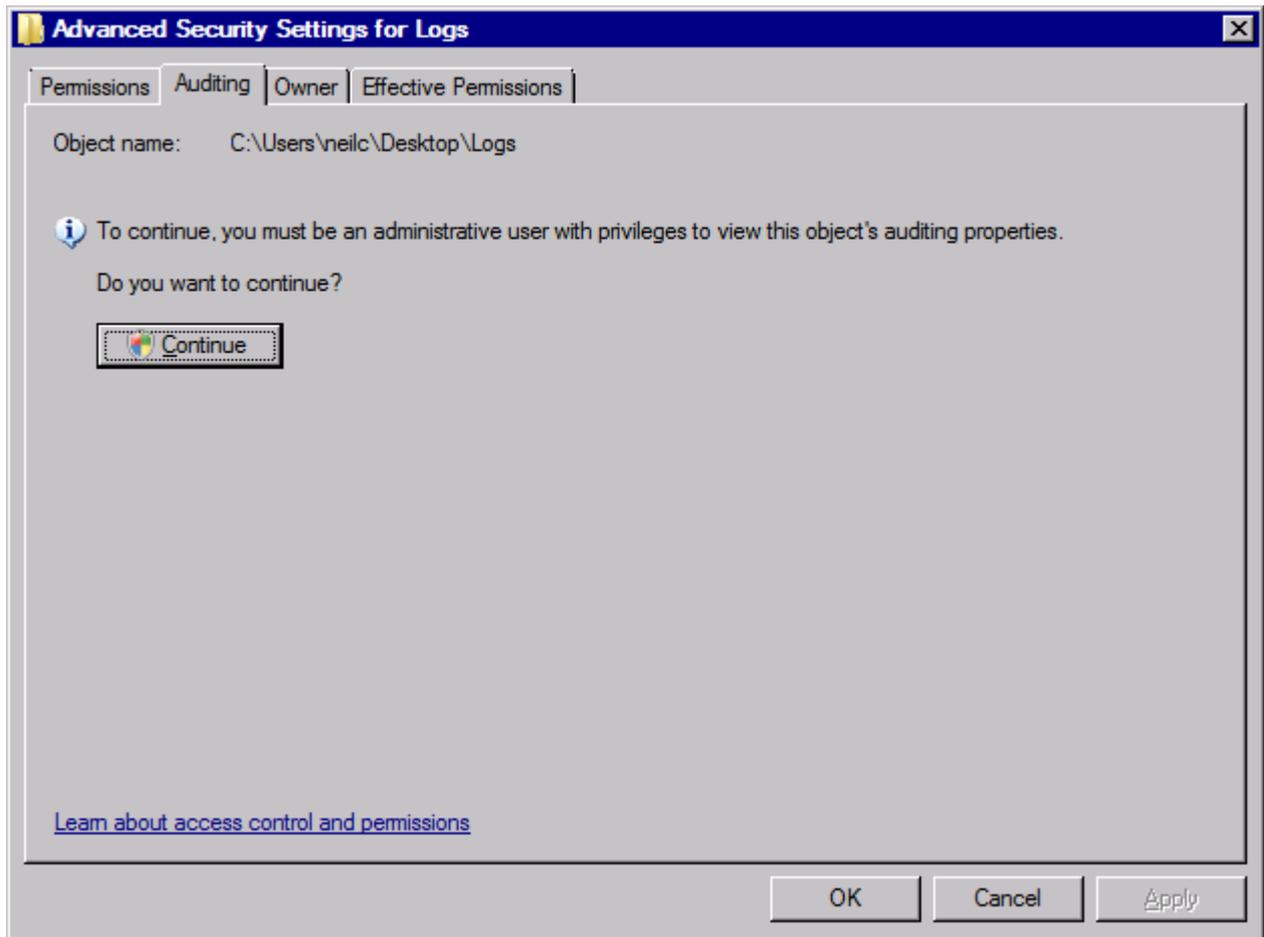
- Logon to the server as an Administrator.
- Access the file or directory using Windows Explorer.

 It is recommended that this is performed locally on the server on which the file/directory resides, even if you are monitoring it remotely.

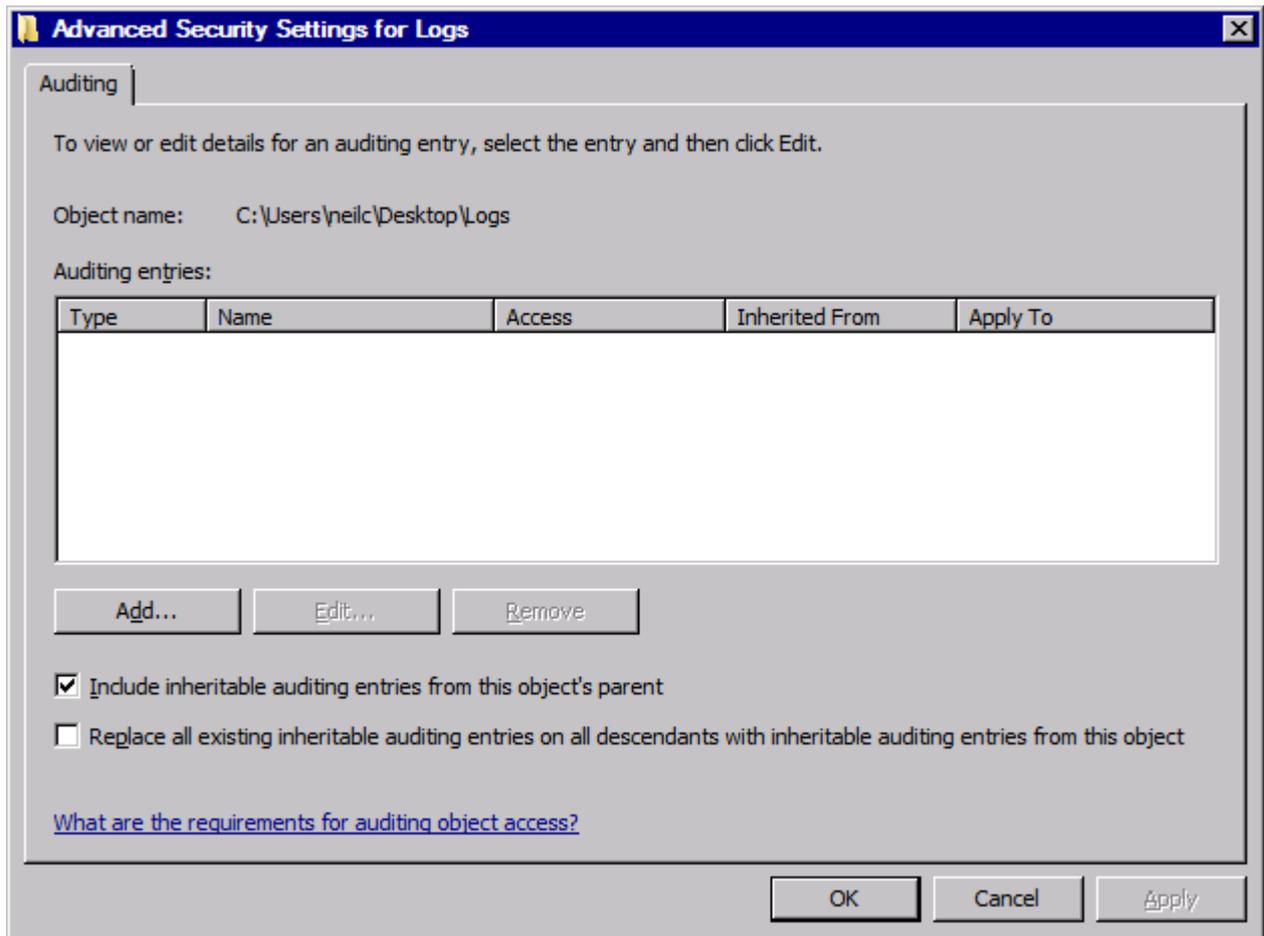
- Right-click over the file or directory & select “Properties” from the menu.
- Click “security” to display the security window.



- Click “Advanced” to display additional settings, then select the “Auditing” tab to display audit details for this file or directory ...

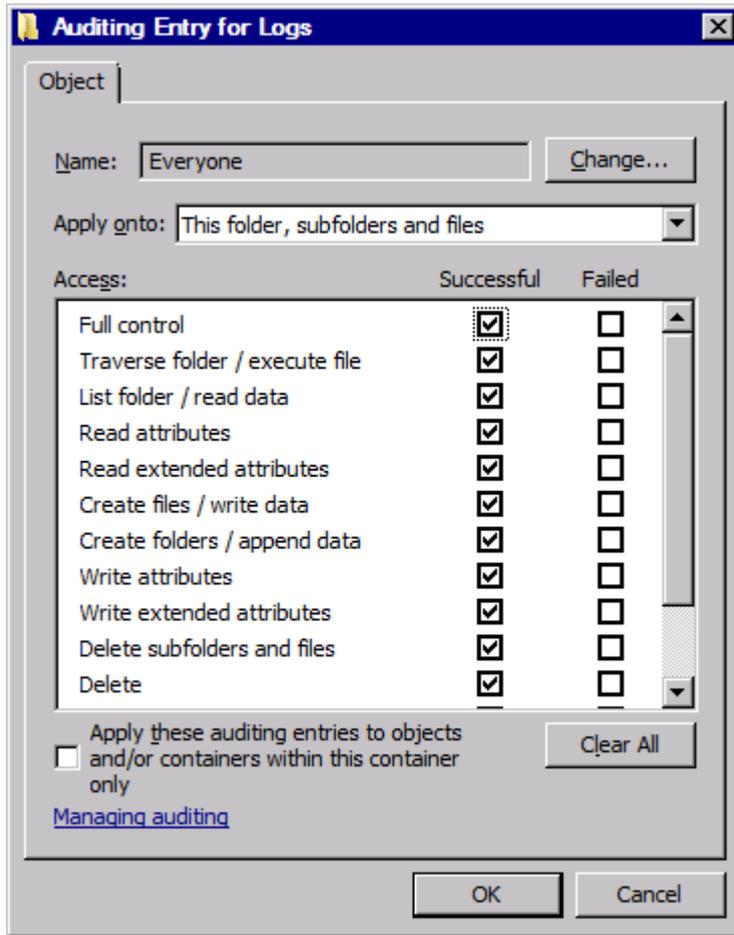


- If you are asked to confirm the request, click “Continue” ...



- Any audit values already configured will be shown.
- To enable monitoring, click “Add”.

- You can choose to enter any valid user or group name, though to ensure all users/processes are recorded, it is recommended you use the “Everyone” group ...



- Tick “Full Control” for “Successful” entries as shown above.

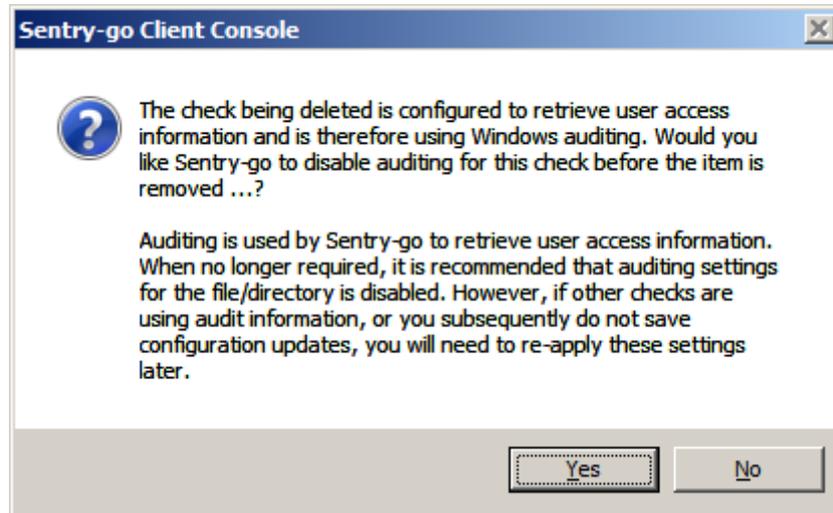
 Failed entries are not used by the monitor.

- Also ensure the “Apply onto” option on this window is set appropriately – e.g. if you are also monitoring sub-directories, ensure this setting includes subfolders etc.
- Click OK for all open windows.

Disabling or removing auditing on files & directories

Using Sentry-go

When a check is removed, Sentry-go automatically checks to see whether auditing was previously enabled for it. If it was, the Console will prompt you as follows ...



Click “Yes” to request that the Sentry-go monitor should reconfigure Windows to disable auditing for the file/directory used by the check.

 If another check monitors the same directory structure or files and user access monitoring is enabled, you should select “No” to this prompt.

If you select “Yes” to the above and subsequently cancel configuration changes – and therefore do not wish to remove the check, you may need to re-instate the audit settings removed here before user access information can be used.

Using Windows Explorer

To disable auditing manually, follow the steps shown in “Using Windows Explorer” above to display audit information, then delete the appropriate entry (e.g. the entry for the “Everyone” group) from the audit 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>*