



FILE SYSTEM AUDITOR[®]

VERSION 2

ScriptLogic[®] **File System Auditor** **Report Configuration** **User Guide**



A QUEST SOFTWARE COMPANY

© 2011 by ScriptLogic Corporation
All rights reserved.

This publication is protected by copyright and all rights are reserved by ScriptLogic Corporation. It may not, in whole or part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from ScriptLogic Corporation. This publication supports File Service Auditor 2.x. It is possible that it may contain technical or typographical errors. ScriptLogic Corporation provides this publication “as is,” without warranty of any kind, either expressed or implied.

ScriptLogic Corporation
6000 Broken Sound Parkway NW
Boca Raton, Florida 33487-2742

1.561.886.2400

www.scriptlogic.com

Trademark Acknowledgements:

File System Auditor and ScriptLogic are registered trademarks of ScriptLogic Corporation in the United States and/or other countries.

The names of other companies and products mentioned herein may be the trademarks of their respective owners.

DOCUMENTATION CONVENTIONS

Typeface Conventions

Bold Indicates a button, menu selection, tab, dialog box title, text to type, selections from drop-down lists, or prompts on a dialog box.

CONTACTING SCRIPTLOGIC

ScriptLogic may be contacted about any questions, problems or concerns you might have at:



ScriptLogic Corporation
6000 Broken Sound Parkway NW
Boca Raton, Florida 33487-2742



561.886.2400 Sales and General Inquiries
561.886.2450 Technical Support



561.886.2499 Fax



www.scriptlogic.com

SCRIPTLOGIC ON THE WEB

ScriptLogic can be found on the web at www.scriptlogic.com. Our web site offers customers a variety of information:

- Download product updates, patches and/or evaluation products.
- Locate product information and technical details.
- Find out about Product Pricing.
- Search the Knowledge Base for Technical Notes containing an extensive collection of technical articles, troubleshooting tips and white papers.
- Search Frequently Asked Questions, for the answers to the most common non-technical issues.
- Participate in Discussion Forums to discuss problems or ideas with other users and ScriptLogic representatives.

Contents

WHAT IS FILE SYSTEM AUDITOR?	1
REPORTING EVENTS	2
STARTING THE REPORT CONFIGURATION CONSOLE	2
EXAMINING THE REPORT CONFIGURATION CONSOLE START PAGE	2
CREATING A REPORT	5
CHANGING AUTHENTICATION MODE	7
SETTING FILTERS	8
<i>Setting the Date/Time Range Filter</i>	8
<i>Setting the Users Filter</i>	9
<i>Setting the Events Filter</i>	12
<i>Setting the Paths Filter</i>	13
<i>Setting the Processes Filter</i>	15
<i>Setting the Servers Filter</i>	16
<i>Setting the Workstations Filter</i>	17
VIEWING AND SORTING RESULTS	17
<i>Navigating Through the Database</i>	17
<i>Viewing Results</i>	18
<i>Sorting Results</i>	18
EXPORTING REPORT DATA	18
PRINTING A REPORT	19
EXPORTING A REPORT	20
SCHEDULING A REPORT	23
SETTING TIME ZONES AND REGIONAL SETTINGS	25
SETTING THE EMAIL ACCOUNT	26
TROUBLESHOOTING	27
UNINSTALLING FILE SYSTEM AUDITOR	28
AUDIT DATABASE SCHEMA	29
INDEX	30

What is File System Auditor?

The ScriptLogic File System Auditor, a unique solution for recording Windows file server activity, allows administrators to audit file access, generate easy-to-understand reports, and create alerts tied to file system events. Ideal for protecting confidential or sensitive data, File System Auditor assists in compliance reporting by creating an audit trail of file activity on patient records, financial reports, or other sensitive information.

File System Auditor assists in security management by sending email alerts or saving the report to a file share whenever specific file system events occur, such as failed access attempts, or modifications of a particular set of files and folders.

The screenshot displays the ScriptLogic File System Auditor [Report Configuration Console] interface. The main window is divided into several sections:

- Database Connection:**
 - SQL Server Instance: QATEST2K-2K3R2
 - Database Name: SLFileAuditor
 - Authentication Mode: Windows
- Selected Report Filter:**
 - Date/Time Range: The past 1 hour from Tuesday, September 15, 2009
 - Users: [All Users]
 - Events: [All Events]
 - Paths: [All Paths]
 - Processes: [All Processes]
 - Servers: [All Servers]
 - Workstations: [All Workstations]
- Report Preview (Maximum of 1000 Events):**

Report Not Scheduled

Server Name	Time Generated	Account	Event
QATEST2K-2K3R2 (ACME)	9/15/2009 1:16:05 PM	Administrator (ACME\Administrator)	Folder - Renamed
QATEST2K-2K3R2 (ACME)	9/15/2009 1:15:57 PM	Administrator (ACME\Administrator)	Folder - Created
QATEST2K-2K3R2 (ACME)	9/15/2009 1:04:06 PM	Administrator (ACME\Administrator)	Folder - Created
- File System Auditor Report Viewer:**

Summary: 11 Events
Date Range: The past 1 hour from Tuesday, September 15, 2009 4:09 PM
Events: [All Events]
Paths: [All Paths]
Users: [All Users]
Processes: [All Processes]
Servers: [All Servers]
Workstations: [All Workstations]

ScriptLogic Corporation - File System Auditor

Tuesday, September 15, 2009

Date:	Time:	User:	Event:
9/15/2009	3:12:13 PM	Administrator (ACME\Administrator)	Folder - Created
Server: QATEST2K-2K3R2 (ACME)			
Process: FSAReportingConsole.exe			
Workstation: qatest2k-2k3r2.ACME.com (197.168.0.1)			
Path: C:\Documents and Settings\Administrator.QATEST2K-2K3R2.000\Local Settings\Application Data\ScriptLogic_Corporation			
9/15/2009	3:12:13 PM	Administrator (ACME\Administrator)	Folder - Created
Server: QATEST2K-2K3R2 (ACME)			
Process: FSAReportingConsole.exe			
Workstation: qatest2k-2k3r2.ACME.com (197.168.0.1)			
Path: C:\Documents and Settings\Administrator.QATEST2K-2K3R2.000\Local Settings\Application Data\ScriptLogic_Corporation\FSAReportingConsole.exe_url_jnxsdl2pqvrvvaatyk21ybm5hawtdo			
9/15/2009	3:12:13 PM	Administrator (ACME\Administrator)	Folder - Created
Server: QATEST2K-2K3R2 (ACME)			

Reporting Events

Once File System Auditor is configured, use the File System Auditing Console to filter the auditing database for reporting purposes. You can specify the date and time during which to collect data, and the users, events, paths, processes, and servers to collect. By default all are collected.

Note: Only the data that resides in the auditing database is available for reporting. The data that is captured in the auditing database is determined by the filters defined in the **File System Auditor Configuration Console**. See the *Getting Started Guide* for information on configuring File System Auditor.

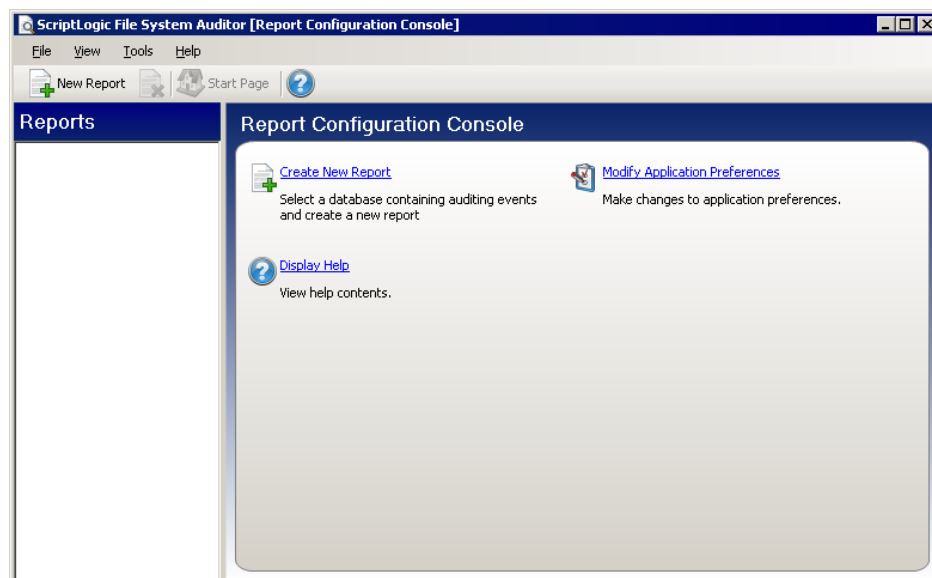
STARTING THE REPORT CONFIGURATION CONSOLE

- ▶ Click **Start**, point to **Programs** > **ScriptLogic Corporation** > **File System Auditor 2**, and then select **Report Configuration Console**.

Each time you run the program you will be greeted by the splash screen, which displays the version of the application.

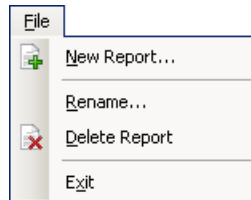
EXAMINING THE REPORT CONFIGURATION CONSOLE START PAGE



The **File System Auditor Report Configuration Console** displays the **Start Page**, which upon installation, may be blank. If you are upgrading to the current version of File System Auditor, your existing reports are listed.



Option	Description
Create New Report	Create a new report. See <i>Creating a Report</i> .
Modify Application Preferences	Configure general options and set up email. See <i>Setting Time Zones and Regional Settings</i> and <i>Setting the Email Account</i> .
Display Help	Display online help.

File Menu and Toolbar Buttons



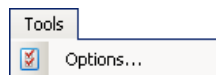
Button	Menu Option	Description
	New Report	Create a new report. See <i>Creating a Report</i> .
	Rename	Rename a selected report.
	Delete Report	Delete a selected report.
	Exit	Exit Reporting Console.

View Menu and Toolbar Button



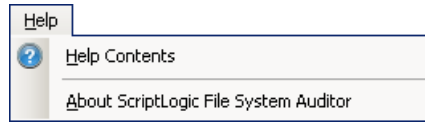
Button	Menu Option	Description
	Start Page	Display the Start Page.


Tools Menu




Menu Option	Description
Options	Configure general preferences and set up email. See <i>Setting Time Zones and Regional Settings</i> and <i>Setting the Email Account</i> .

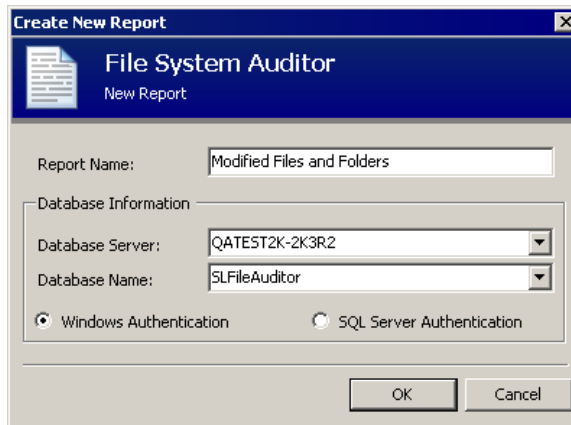
Help Menu and Toolbar Button



Button	Menu Option	Description
	Help Contents	Access online help
	About ScriptLogic File System Auditor	View information about the version of File System Auditor installed on your computer and the End User License Agreement (EULA).

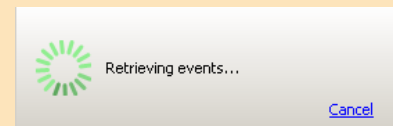
CREATING A REPORT

1. Click . Alternatively, choose **New Report** from the **File** menu or click [Create New Report](#) on the **Report Configuration Console Start Page**. The **Create New Report** box displays the default database server and database name.
2. In the **Report Name** box, type a name to identify the report.
3. From the **Database Server** list, choose a database server hosting the database containing the data you want to report upon.
4. From the **Database Name** list, choose the database.

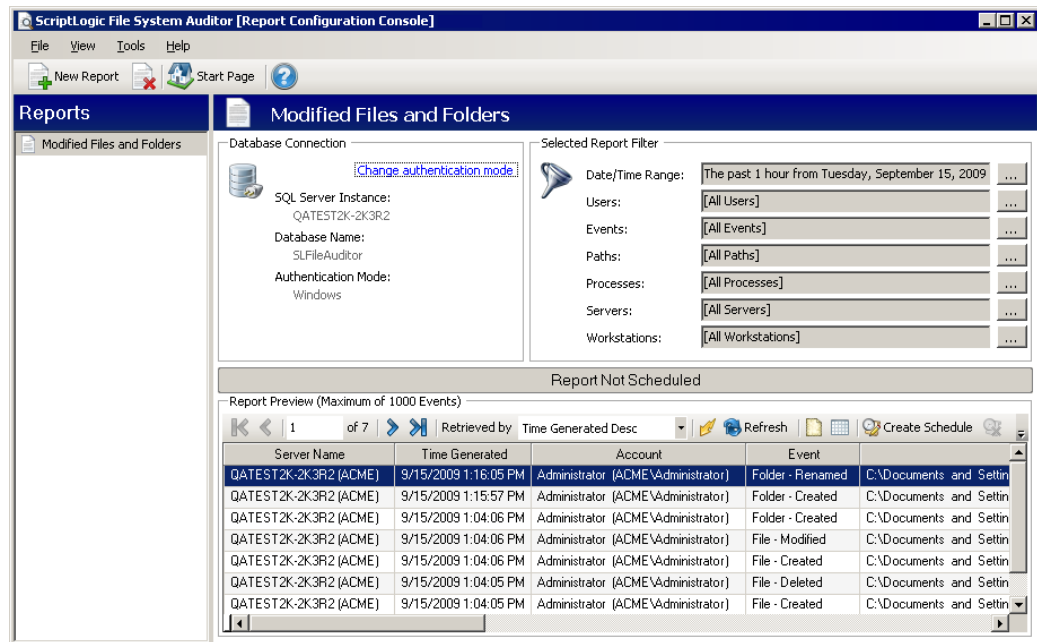


5. Click **OK**. The report name is listed in the **Reports** area and displays as the header to indicate the **Database Connection**, **Selected Report Filter**, and **Report Filter Results** areas are connected to that report.






Note: As data is being retrieved from the database, you see a progress message. If the retrieval is taking too long and you want to cancel the process, click [Cancel](#).



By default, the first 1,000 results in the selected database instance collected over the past hour display in the **Report Preview** area. By default, results are listed in ascending order by time of generation.



Toolbar	Description
	Change method for connecting to the database. See <i>Changing Authentication Mode</i> .
	Set a filter. See <i>Setting Filters</i> .
	Move to the first event in the database.
	Move to the previous event in the database.
	The number of the highlighted event and the number of total events. You can type a new value in the box to move to a specific event in the database. For example, since only the first 1,000 events display, you could type in 2000 to view the next group of events in the database.
	Move to the next event in the database.
	Move to the last event in the database.
	By default, results are listed in ascending order by time of generation. You can sort the list by selecting to sort by account or time generated in either ascending or descending order. See <i>Viewing and Sorting Results</i> .
	When selected, the Report Preview area is refreshed automatically whenever a change is made to the filters. The Auto Refresh button remains selected until you click to release it.
	Refresh the Report Preview area.
	Generate a report.

Toolbar	Description
	Export report data to a .csv file. See <i>Exporting Report Data</i> .
 Create Schedule	Schedule the report to run at a specific date and time. You can send the report results to a specified email address. See <i>Scheduling a Report</i> .
 Edit Schedule	Edit a scheduled report.
	Delete a report's schedule.
 Group By	Display results in groups. See <i>Viewing and Sorting Results</i> .

CHANGING AUTHENTICATION MODE

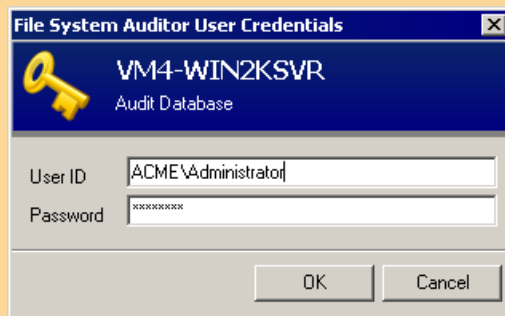
The data displayed in the **Report Preview** area is pulled from the database displayed in the **Database Connection** area. You can change the authentication of the database.

1. Click [Change authentication mode](#). The **Database Settings** box displays the report name, database server, and database name.



2. Choose whether the database server uses **Windows Authentication** or **SQL Server Authentication**.

If you chose to change to SQL Server Authentication, the **User Credentials** box appears. Enter the **User ID** and **Password**, and then click **OK**.




3. Click **OK**.

SETTING FILTERS

You can set filters to include or exclude specific data when the report is generated. The actual data in the database is not affected.

Selected Report Filter

 Date/Time Range: The past 1 hour from Tuesday, September 15, 2009 ...

Users: [All Users] ...


Events: [All Events] ...

Paths: [All Paths] ...

Processes: [All Processes] ...


Servers: [All Servers] ...

Workstations: [All Workstations] ...

Note: If you want the results in the **Report Preview** area to update whenever you change a filter, click . The button remains selected until you click to release the button.

Setting the Date/Time Range Filter

By default, the report data displays for the previous hour on the current date. You can pull data for a specified number of hours or days.

1. Click  next to the **Date/Time Range** filter setting in the **Selected Report Filter** area. The **Date Time Filter** box opens.

Edit Audit Reporting Filter

Date Time Filter

Report file system events for the following number of hours:

Hours:

Report file system events between the following times

Date / Time From:

February, 2007						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	1	2	3
4	5	6	7	8	9	10
Today: 2/20/2007						

12:00 AM

Date / Time To:

February, 2007						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	1	2	3
4	5	6	7	8	9	10
Today: 2/20/2007						

10:31 AM

OK Cancel

Report File System Events to the following number of hours

Select to include events in the report for the number of hours as indicated in the **Hours** box. By default, reports include file system events for one hour.

Report File System Events between the following times

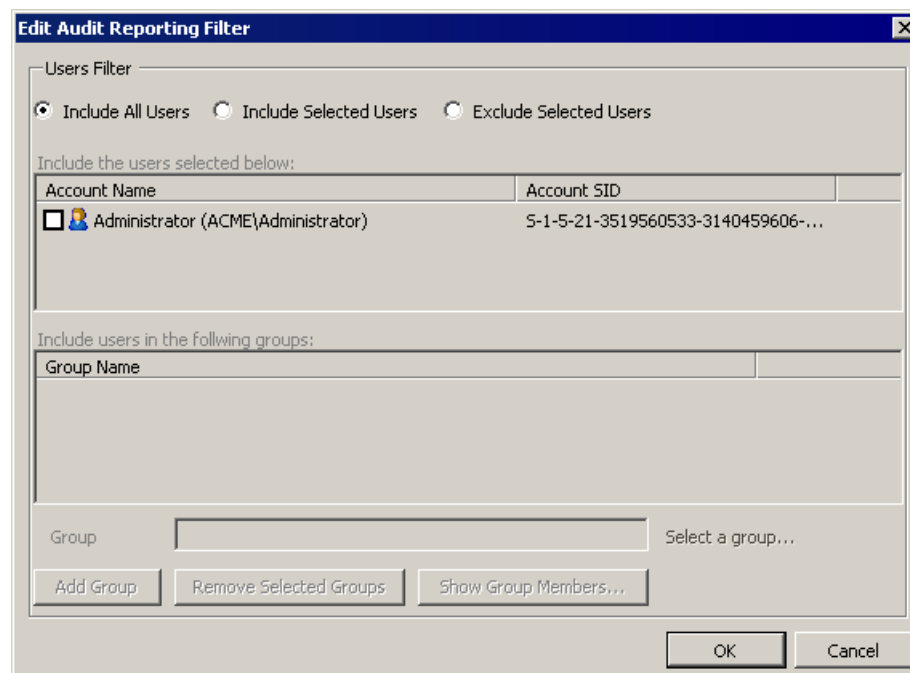
Select to specify a specific date and time within which to report file system events. To select a date range, select the start and end day on the calendars. To select a time range, select the hour, minute, or seconds, and then use the up and down arrows to change the setting.

2. Click **OK**. The specified date and time display in the **Date/Time Range** box.

Setting the Users Filter

By default, all users who are currently signed on to the system are included in the report. You can filter the results by including or excluding specific users and groups.

1. Click **...** next to the **Users** filter setting in the **Selected Report Filter** area. The **Users Filter** box displays the users who are currently signed on to the system.



Include All Users

By default, all users who are currently signed on to the system are included in the report.

Include Selected Users

Select to specify specific users and/or groups to include in the report.

Exclude Selected Users

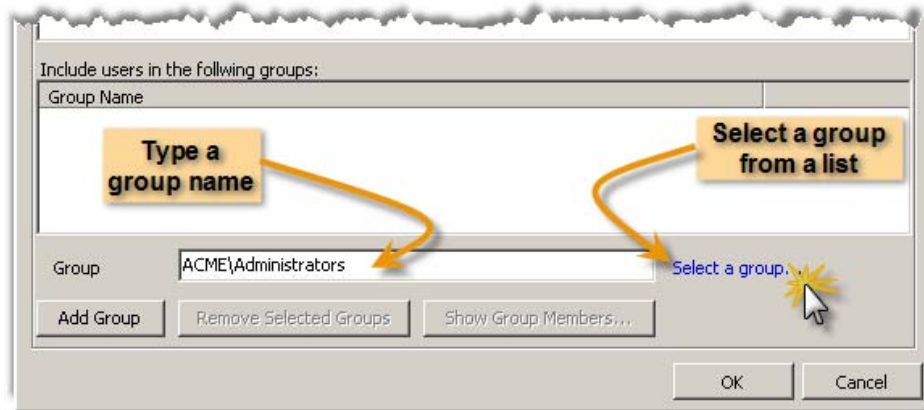
Select to specify specific users and/or groups to exclude from the report.

Button	Description
Select a group...	Select a group from a list. See Adding Groups.
Add Group	Add groups to the list. See Adding Groups.
Remove Selected Groups	Remove selected groups from the list. See Adding Groups.
Show Group Members...	Display members of the selected group. See Adding Groups.

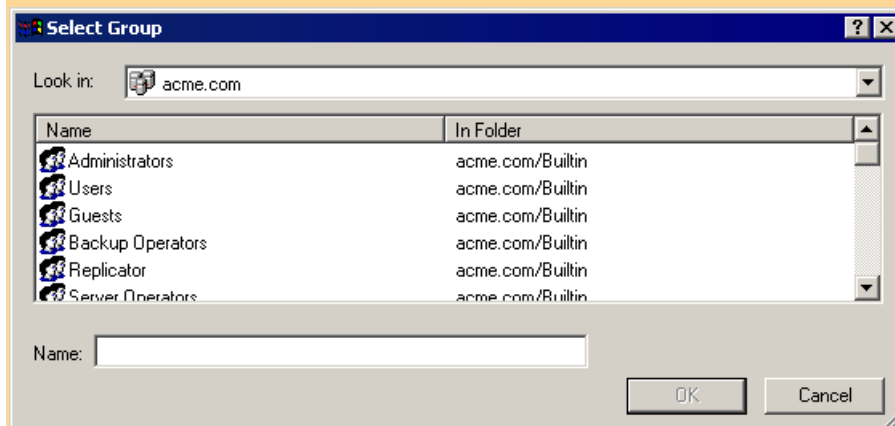
3. Click **OK**. The users and groups display in the **Users** box. If there is more than one, the users and groups are separated by commas.

Adding Groups

1. Choose either **Include Selected Users** or **Exclude Selected Users** to activate the lower portion of the **Users Filter** box.
2. In the **Group** box, type a group name or click [Select a group](#) to choose a group.



If you clicked [Select a group](#), the **Select Group** box lists all the groups in the current domain. To switch to another domain, select the domain or **Entire Directory** from the **Look in** list.

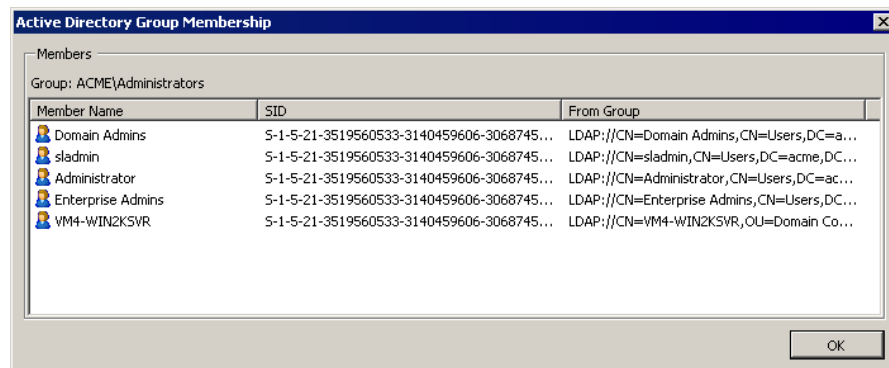


Select a group from the list or type a group name in the **Name** box, and then click **OK**. The group displays in the **Group** box.

- Click **Add Group**. The group name displays in the list. Repeat the process to add more groups if desired.




- To remove selected group(s) from the list, click **Remove Selected Groups**.
- To display the members of a selected group, click **Show Group Members...**. The **Members** box displays the group members. Click **OK** to close the box.

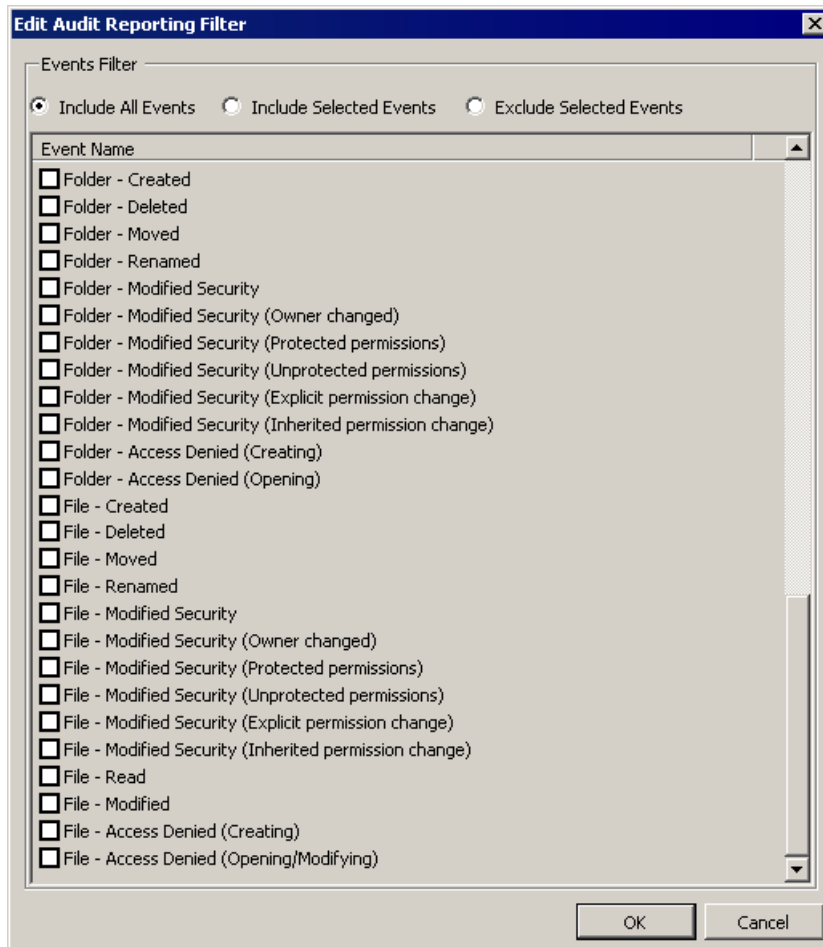


- Click **OK**. The users and groups display in the **Users** box. If there is more than one, the users and groups are separated by commas.

Setting the Events Filter

By default, all events captured by File System Auditor are included in the report. You can filter the results by including or excluding specific events.

1. Click  next to the **Events** filter setting in the **Selected Report Filter** area. The **Events Filter** box displays the events that can be reported upon. By default, all events are included.



Include All Events

Select to include all events. By default, all events are included in the report.

Include Selected Events

Select to specify specific events to include in the report.

Exclude Selected Events

Select to specify specific events to exclude from the report.

Important: If an event was filtered out from being captured in the auditing database, you will not see a result even if you select the filter from this list.

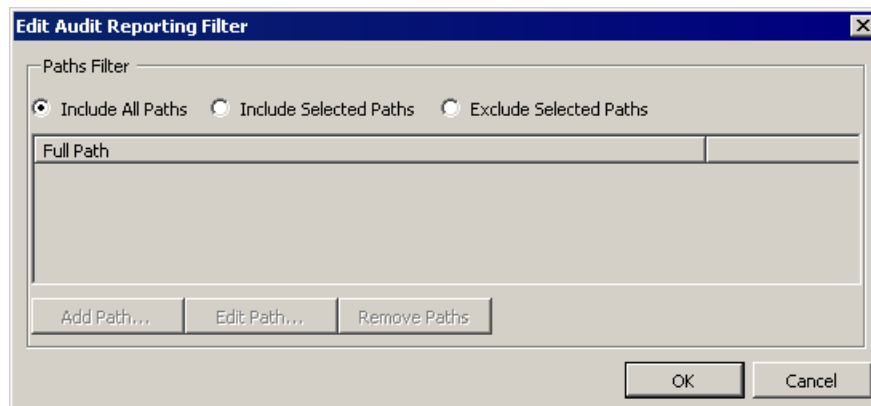
Note: Some applications generate a File Read event only when a file is opened for the first time. If the file is opened again, the application may pull from a memory cache and not from the disk. Since File System Auditor watches events going to NTFS, if an application pulls a file from a memory cache and never calls NTFS, a File Read event is not logged. If another user opens that same file for the first time, that File Read event is logged.

2. Click **OK**. The events displays in the **Events** box. If there is more than one, the events are separated by commas.

Setting the Paths Filter

By default, all paths are included in the report. You can filter the results by including or excluding specific paths.

1. Click **...** next to the **Paths** filter setting in the **Selected Report Filter** area. The **Paths Filter** box opens. Initially, the list is empty.



Include All Paths

Select to include all folders and files. By default, all paths are included in the report.

Include Selected Paths

Select to specify specific paths to include in the report.

Note: It is not advisable to select a root drive due to the amount of data that would be collected.

Exclude Selected Paths

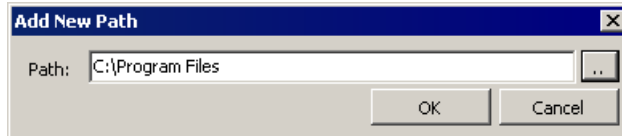
Select to specify specific paths to exclude from the report.

Button	Description
Add Path...	Add a path. See <i>Adding Paths</i> .
Edit Path...	Modify a selected path. See <i>Adding Paths</i> .
Remove Paths	Delete selected path(s).

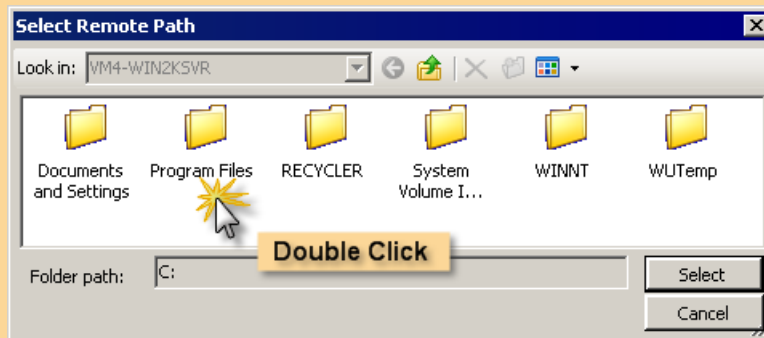
2. Click **OK**. The path displays in the **Paths** box. If there is more than one, the paths are separated by commas.

Adding Paths

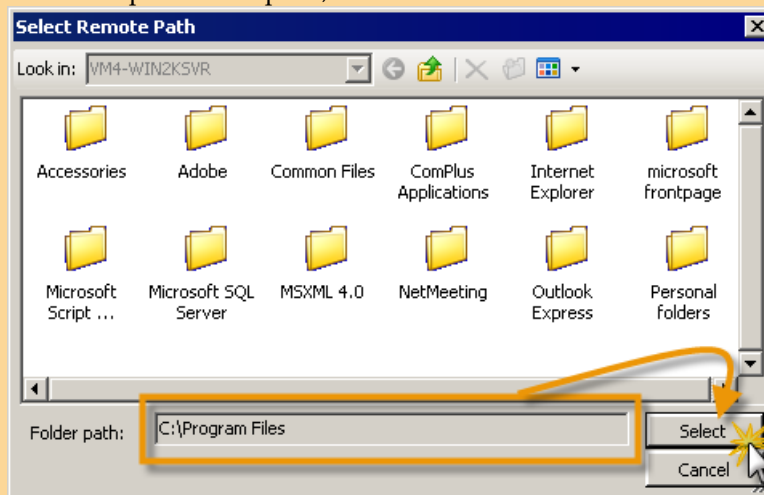
1. Select **Include Selected Paths** or **Exclude Selected Paths** to activate the lower portion of the **Paths Filter** box.
2. Click **Add Path...**. The **Add New Path** box appears.
3. In the **Path** box, type the path to which to apply the filter, or click **...** to locate a folder. You can use the * wildcard when typing the path.



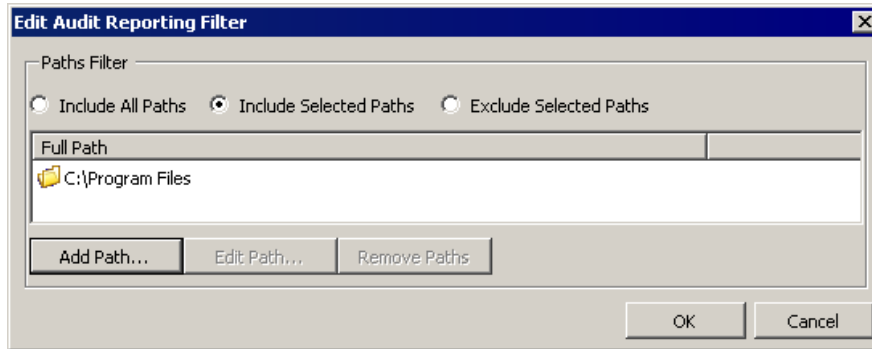
If you click **...** the **Select Remote Path** box appears. Double-click a selection to build the path in the **Folder path** box.

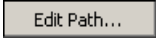



When the path is complete, click **Select**.



- Click **OK**. The path displays in the **Full Path** column. Repeat adding paths, if necessary.




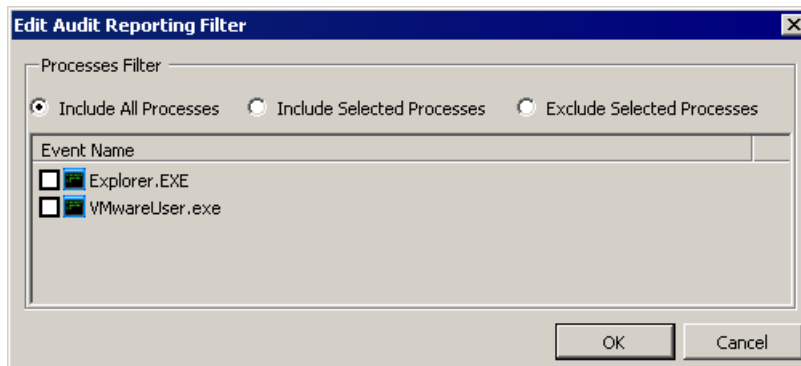
- To edit a selected path, click .
- To remove selected path(s), click .

- Click **OK**. The path displays in the **Paths** box. If there is more than one, the paths are separated by commas.

Setting the Processes Filter

By default, all processes captured in the database are included in the report. You can filter the results by including or excluding specific processes.

- Click  next to the **Processes** filter setting in the **Selected Report Filter** area. The **Processes Filter** box displays the processes included in the database. By default, all processes are included in the report.



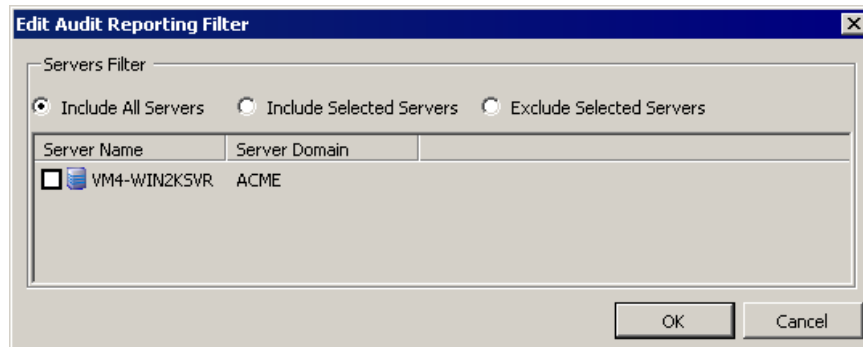
- Include All Processes**
By default, all configured processes are included in the report.
- Include Selected Processes**
Select to specify specific processes to include in the report.
- Exclude Selected Processes**
Select to specify specific processes to exclude from the report.

Note: Only local processes display in the list. Any file activity performed by a remote user displays under the System process. You can configure the service to ignore local virus scanning and backup software using the process filters in the File System Auditor Configuration Console. See the *Getting Started Guide*.

2. Click **OK**. If you chose a specific process, the process displays in the **Processes** box. If there is more than one, the processes are separated by commas.

Setting the Servers Filter

1. Click **...** next to the **Servers** filter setting in the **Selected Report Filter** area. The **Servers Filter** box lists the servers currently active in the system.



Include All Servers

Select to include all servers. By default, all servers in the list are included in the report.

Include Selected Servers

Select to specify specific servers to include in the report.

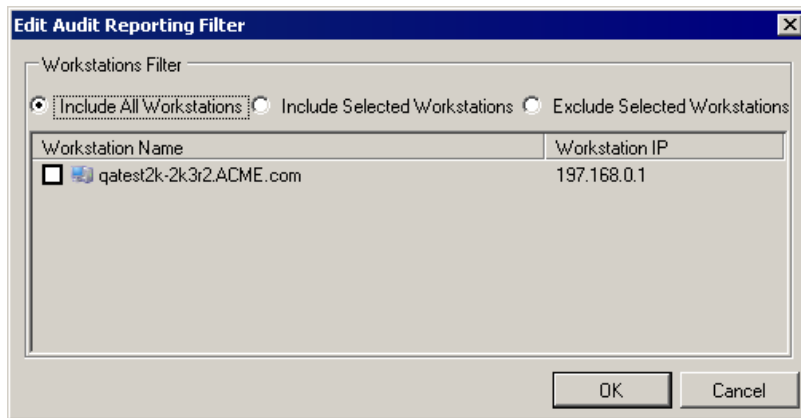
Exclude Selected Servers

Select to specify specific servers to exclude from the report.

2. Click **OK**. If you chose a specific server, the server displays in the **Servers** box. If there is more than one, the servers are separated by commas.

Setting the Workstations Filter

1. Click  next to the **Workstations** filter setting in the **Selected Report Filter** area. The **Workstations Filter** box lists the workstations currently active in the system.



Include All Workstations

Select to include all workstations. By default, all workstations in the list are included in the report.

Include Selected Workstations

Select to specify specific workstations to include in the report.

Exclude Selected Workstations






Select to specify specific servers to exclude from the report.

2. Click **OK**. If you chose a specific workstation, the workstation displays in the **Workstations** box. If there is more than one, the workstations are separated by commas.

VIEWING AND SORTING RESULTS

Only the first 1,000 results in the database display in the **Report Preview** area in ascending order by time of generation. You can use the navigation buttons to scroll through the database or go to a specific record in the database. You also can sort the results by column heading or group them by a column heading.

Navigating Through the Database

To Go To:	Click:
The last record in the database	
The first record in the database	
A specific record in the database, type the number in the box	
The next record in the database from the selected record	
The previous record in the database from the selected record	

Viewing Results


- To view truncated results, size the columns, or point to a value to view the entire value.

Report Preview (Maximum of 1000 Events)

Retrieved by Time Generated Desc

Server Name	Time Generated	Account	Event	Path
QATEST2K-2K3R2 (ACME)	9/15/2009 2:27:39 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Deleted	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:27:39 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Renamed	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:27:06 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Deleted	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:27:06 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Renamed	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:26:59 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Created	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:26:59 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Renamed	C:\WINDOWS\system32\dhcp\backu

Sorting Results

- To sort the results, click a column header, or choose a sort type from the **Retrieve by** list, and then click .


Report Preview (Maximum of 1000 Events)

Retrieved by Time Generated Desc

Server Name	Time Generated	Account Asc	Account Desc	Time Generated Asc	Time Generated Desc	Event	Path
QATEST2K-2K3R2 (ACME)	9/15/2009 2:27:39 PM	SYSTEM (NT AUTHORITY\SYSTEM)	SYSTEM (NT AUTHORITY\SYSTEM)	9/15/2009 2:27:39 PM	9/15/2009 2:27:39 PM	Folder - Deleted	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:27:39 PM	SYSTEM (NT AUTHORITY\SYSTEM)	SYSTEM (NT AUTHORITY\SYSTEM)	9/15/2009 2:27:39 PM	9/15/2009 2:27:39 PM	Folder - Renamed	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:27:06 PM	SYSTEM (NT AUTHORITY\SYSTEM)	SYSTEM (NT AUTHORITY\SYSTEM)	9/15/2009 2:27:06 PM	9/15/2009 2:27:06 PM	Folder - Deleted	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:27:06 PM	SYSTEM (NT AUTHORITY\SYSTEM)	SYSTEM (NT AUTHORITY\SYSTEM)	9/15/2009 2:27:06 PM	9/15/2009 2:27:06 PM	Folder - Renamed	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:26:59 PM	SYSTEM (NT AUTHORITY\SYSTEM)	SYSTEM (NT AUTHORITY\SYSTEM)	9/15/2009 2:26:59 PM	9/15/2009 2:26:59 PM	Folder - Created	C:\WINDOWS\system32\dhcp\backu
QATEST2K-2K3R2 (ACME)	9/15/2009 2:26:59 PM	SYSTEM (NT AUTHORITY\SYSTEM)	SYSTEM (NT AUTHORITY\SYSTEM)	9/15/2009 2:26:59 PM	9/15/2009 2:26:59 PM	Folder - Renamed	C:\WINDOWS\system32\dhcp\backu


EXPORTING REPORT DATA

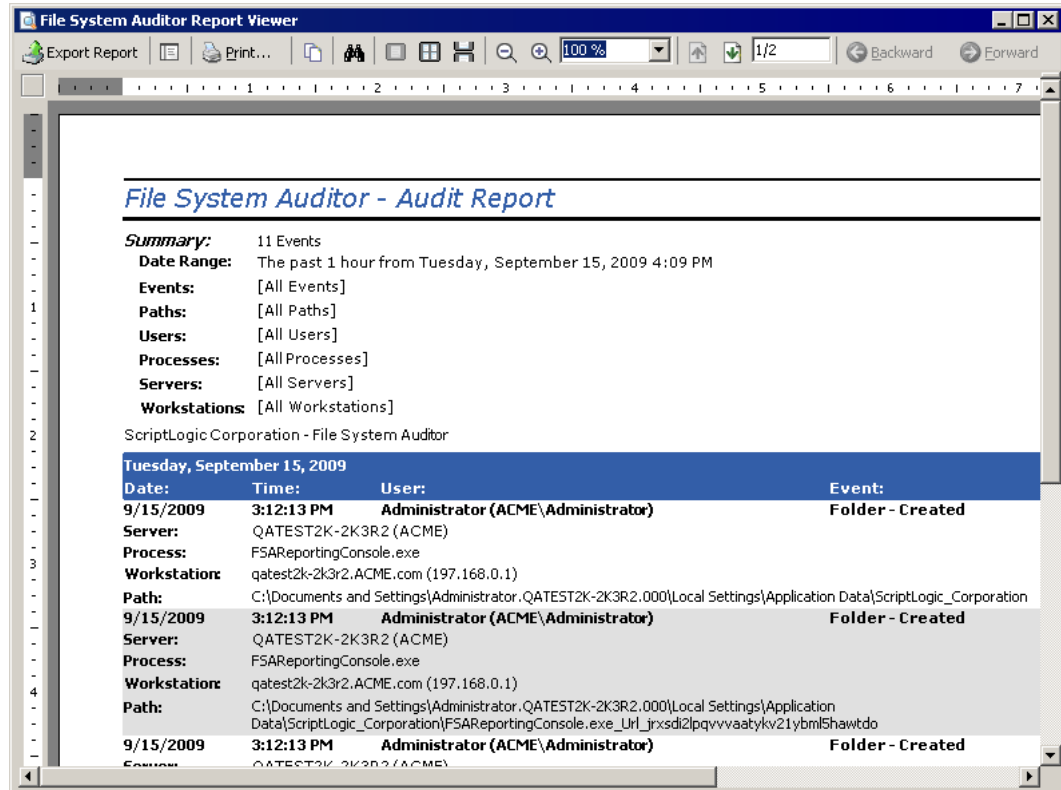
You can export the list of results to a .csv file. If you prefer to generate a report, you can export the report to other types of files. See *Exporting a Report*.








- When you have the list of results that you want, click .

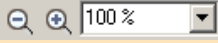
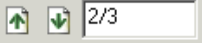
PRINTING A REPORT

You can prepare a report of the results that appear in the **Report Filter Results** area. The results print in the order in which they display. Filter and sort the results to obtain the report you want. See *Setting Filters* and *Viewing and Sorting Results*.

- ▶ When you have the list of results that you want, click . The **Report Preview** window displays the **Audit Report**, which you can view, print, or export.




Toolbar	Description
 Export Report	Export the report in HTML, PDF, RTF, TXT, TIFF, or XLS format. See <i>Exporting a Report</i> .
	Open a Contents pane to the left of the report. If the report groups data, such as by computer or account, you can quickly jump to a particular item by clicking the name in the Contents pane.
 Print...	Open the Print box. You can change printer properties and output settings before printing the report.
	Open the Find box. In the Find What box, type the text to find, and then click Find Next .
	Display one page at a time.
	Display multiple pages at a time.
	Display continuous pages.

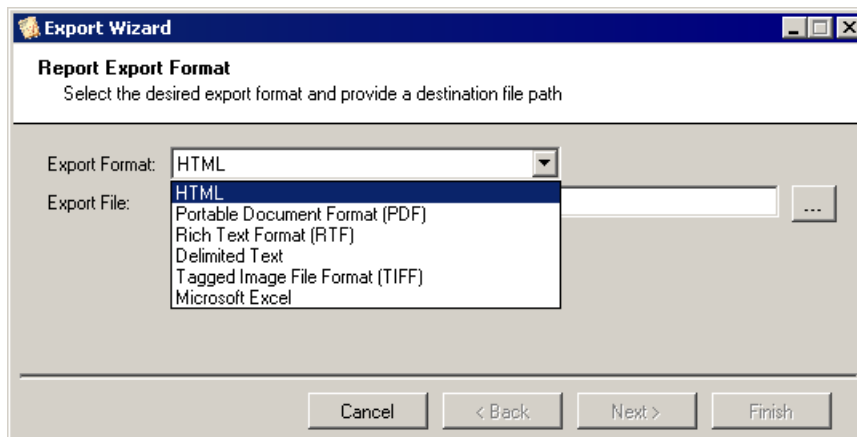
Toolbar	Description
	Zoom in or out. You also can select a zoom percentage from the list.
	Switch pages in the report. You also can type a page number in the box, and then press Enter .


EXPORTING A REPORT

You can export a report to another format, such as a PDF file for attaching to an email or a TIF file for including in a slide presentation.

Note: You also can just export the results without generating a report. See *Exporting Report Data*.

1. From the **Report Preview** window, click . The **Export Wizard** opens to the **Report Export Format** box.
2. From the **Export Format** list, select a format. The available options are **HTML**, **PDF**, **RTF**, **Delimited Text**, **TIFF**, and **Microsoft Excel**.



3. In the **Export File** box, type a path and name for the exported file, or click  to locate a path for the file.
4. Click **Next**. Depending on the format you chose, the next box displays the default settings for that format.

HTML (*.htm, *.html)

Export Wizard

HTML Export Options
Specify the details of the document to be exported as HTML

Title: Create Frameset

Character Set: Include HTML Header

Bookmark Style: Include Page Margins

Output Type: Multiple Pages

Remove Vertical Space

Cancel < Back Next > Finish

Portable Document Format (*.pdf)

Export Wizard

PDF Export Options
Specify the details of the document to be exported as a PDF

General Options | Document Security | Document Properties | Embedded Fonts

PDF Version: Export Bookmarks

Metfile Images:

Convert Windows Metafiles to PNG

Image Quality:

Image Resolution:

Cancel < Back Next > Finish

Rich Text Format (*.rtf)

No options.

Delimited Text (*.txt, *.csv)

Export Wizard

Text Export Options
Specify the details of the document to be exported as Plain Text

Page Delimiter:

Text Delimiter:

Encoding:

Suppress Empty Lines

Cancel < Back Next > Finish

Tagged Image File Format (*.tif)

The screenshot shows the 'TIFF Export Options' dialog box. The title bar reads 'Export Wizard'. Below the title bar, the text says 'TIFF Export Options' and 'Specify the details of the document to be exported as a TIFF'. There is a 'Compression Scheme' dropdown menu set to 'Ccitt3'. Below it is a checkbox for 'Dither' which is unchecked. At the bottom, there are four buttons: 'Cancel', '< Back', 'Next >', and 'Finish'.

Microsoft Excel (*.xls)

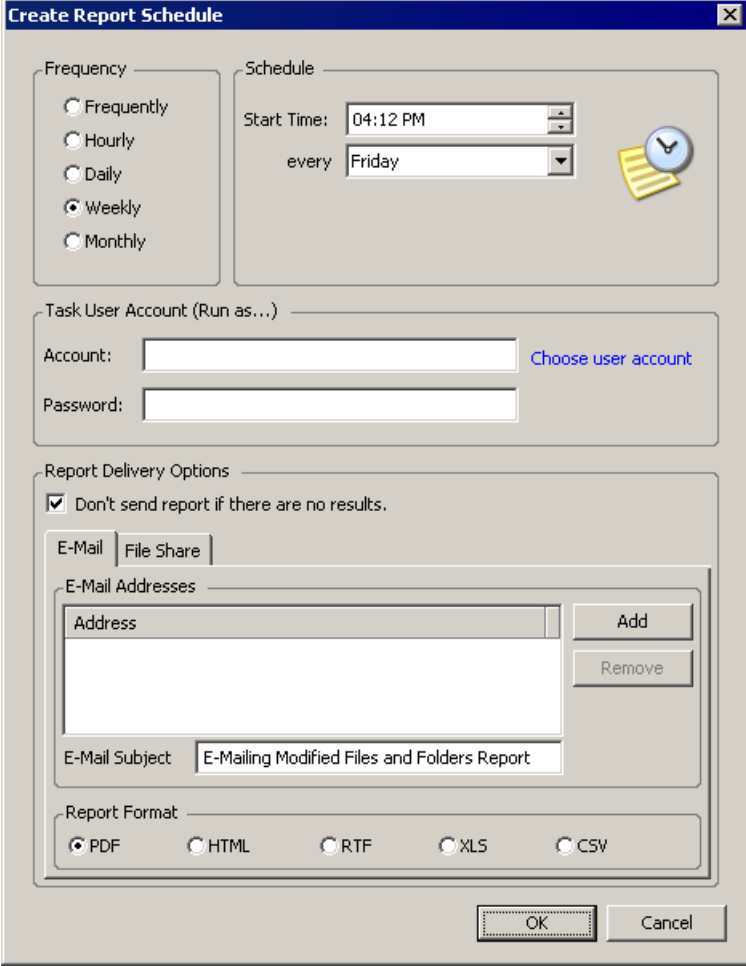
The screenshot shows the 'Excel Export Options' dialog box. The title bar reads 'Export Wizard'. Below the title bar, the text says 'Excel Export Options' and 'Specify the details of the document to be exported as an Excel Spreadsheet'. There is a 'File Format' dropdown menu set to 'Microsoft Excel 97 or newer'. Below it is a 'Columns & Rows' section with two spinners: 'Min Column Width' set to 0.10 (inches) and 'Min Row Height' set to 0.10 (inches). Below that is a 'Cell Formatting' section with five checkboxes: 'Auto Row Height' (unchecked), 'Display GridLines' (checked), 'Multisheet' (unchecked), 'Remove Vertical Space' (unchecked), and 'Use Cell Merging' (unchecked). At the bottom, there are four buttons: 'Cancel', '< Back', 'Next >', and 'Finish'.

5. After selecting options for the export file, click **Finish**.

SCHEDULING A REPORT

You can schedule a report that is sent to either an email address or to a file share.

1. Select a report and then click  **Create Schedule**. The **Create Report Schedule** box opens.



Frequency

Select a time frame for the report.

Schedule

Set the time frame for the report.

Task User Account (Run As)

Type an account name that has the appropriate permissions to run the report, or click [Choose user account](#) to choose an account. In the **Password** box, type the account's password.

Report Delivery Options

- Do not send report if there are no results**

By default, a report is not sent to the addresses specified on the **E-Mail** tab or the file shares specified on the **File Share** tab if there are no results in the report.

E-Mail

- To add email addresses, click **Add**. The **Enter email address** box opens. Type an email address, and then click **OK**.
- In the **Subject Line** box, type a subject line for the email that is sent. By default, the name of the report displays.
- To delete selected email addresses from the list, click **Remove**.

File Share



- To add a file share, click **Add**. The **Add File Share Path** box opens. Type a path to the location where you want to store the report, or click [Browse](#) to find a location, and then click **OK**.
- To delete selected paths from the list, click **Remove**.

Report Format

Select a format for the report.

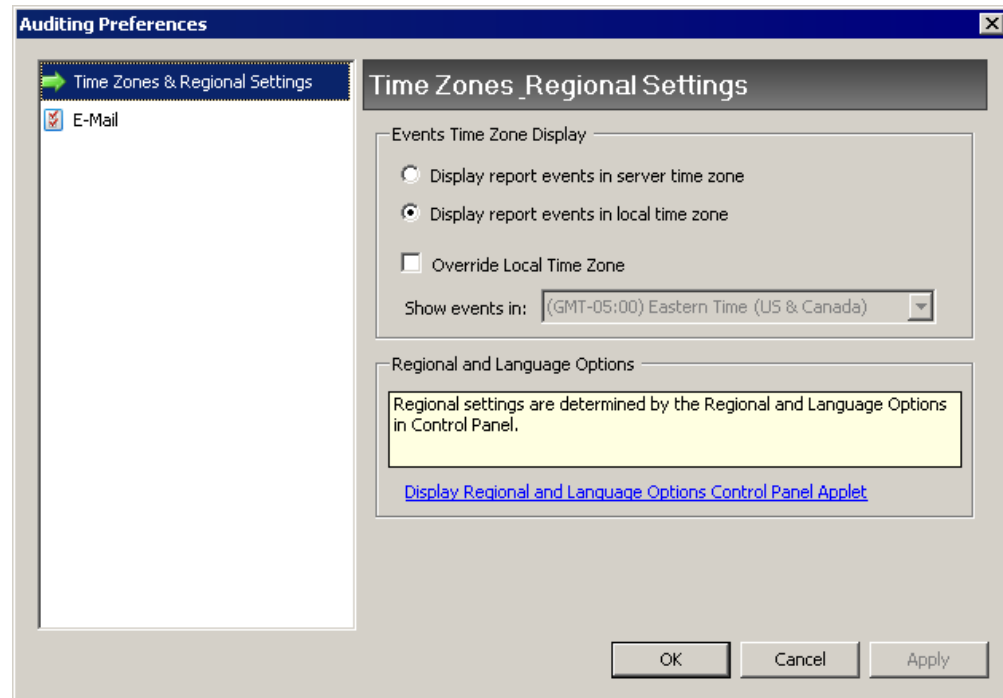
2. Click **OK**. The report header displays the schedule.

Report scheduled to run each week on Friday at 4:12 PM				
Report Preview (Maximum of 1000 Events)				
Server Name	Time Generated	Account	Event	
QATEST2K-2K3R2 (ACME)	9/15/2009 3:27:07 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Renamed	C:\WINDOWS\system32\
QATEST2K-2K3R2 (ACME)	9/15/2009 3:27:07 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Created	C:\WINDOWS\system32\
QATEST2K-2K3R2 (ACME)	9/15/2009 3:27:14 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Renamed	C:\WINDOWS\system32\
QATEST2K-2K3R2 (ACME)	9/15/2009 3:27:14 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Deleted	C:\WINDOWS\system32\
QATEST2K-2K3R2 (ACME)	9/15/2009 3:27:40 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Renamed	C:\WINDOWS\system32\
QATEST2K-2K3R2 (ACME)	9/15/2009 3:27:40 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Created	C:\WINDOWS\system32\
QATEST2K-2K3R2 (ACME)	9/15/2009 3:27:47 PM	SYSTEM (NT AUTHORITY\SYSTEM)	Folder - Renamed	C:\WINDOWS\system32\

- To change the schedule, click  **Edit Schedule**.
- To delete the schedule, click .

SETTING TIME ZONES AND REGIONAL SETTINGS

- ▶ Choose **Preferences** from the **Tools** menu. The **Auditing Preferences** box opens to the **Time Zones & Regional Settings** tab.



Events Time Zone Display

- Display report events in server time zone**

Choose to display events in the time zone set on the file server.

- Display report events in local time zone**

By default, events are listed with the time zone displayed in the **Show events in** box.

- Override Local Time Zone**

Select to choose the time zone where the computer on which you are installing File System Auditor resides.

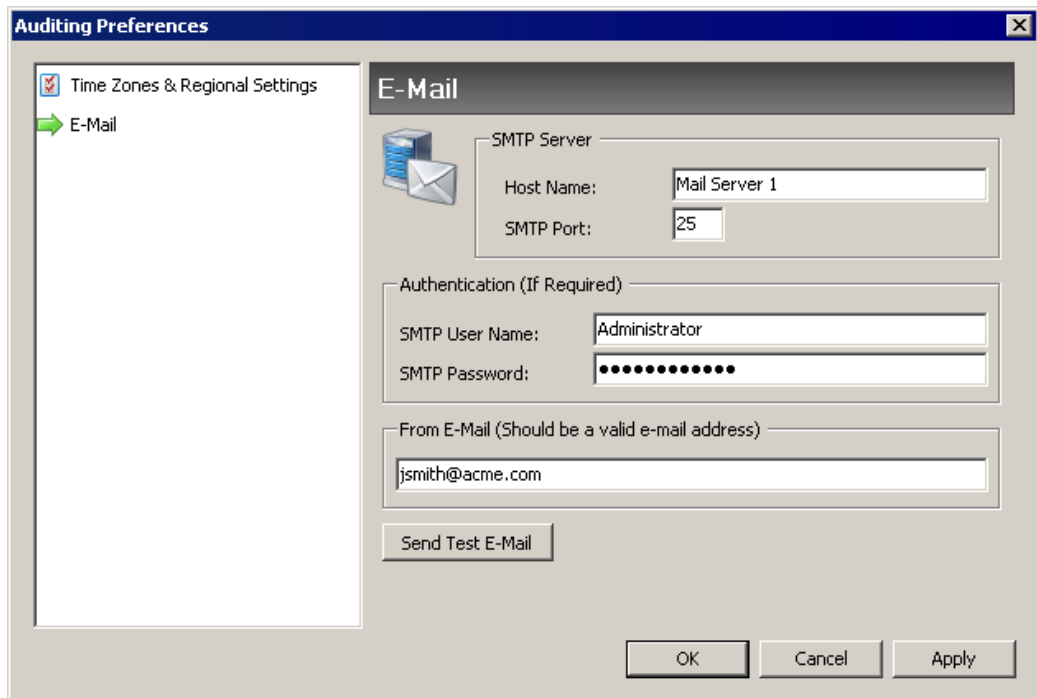
Regional and Language Options

[Display Regional and Language Options Control Panel Applet](#)

Regional settings are determined by the Regional and Language Options in the Control Panel.

SETTING THE EMAIL ACCOUNT

1. Choose **Preferences** from the **Tools** menu, and then click **E-Mail**.
2. In the **SMTP Server Host Name** box, type the name of the SMTP server that sends the scheduled report emails.
3. In the **SMTP Port** box, type the number of the TCP/IP port on which the SMTP server is listening. The default is 25.
4. If your SMTP server requires authentication, type the username and password in the **SMTP User Name** and **SMTP Password** boxes.
5. In the **From E-Mail** box, type the email address that to appear in the From box of the email.



The screenshot shows the 'Auditing Preferences' dialog box with the 'E-Mail' tab selected. The dialog has a left sidebar with 'Time Zones & Regional Settings' and 'E-Mail' (indicated by a green arrow). The main area is titled 'E-Mail' and contains the following fields and controls:

- SMTP Server** section:
 - Host Name: Mail Server 1
 - SMTP Port: 25
- Authentication (If Required)** section:
 - SMTP User Name: Administrator
 - SMTP Password: [masked with dots]
- From E-Mail (Should be a valid e-mail address)** section:
 - jsmith@acme.com

At the bottom of the dialog, there is a 'Send Test E-Mail' button and three standard buttons: 'OK', 'Cancel', and 'Apply'.

6. Click **Send Test E-Mail** to check the entries.

Troubleshooting

In its Knowledge Base, ScriptLogic Corporation has a library of articles that may provide an answer to a problem you are experiencing. Before calling technical support, check to see if your problem is documented here. You might also browse the Discussion Forums to see if anyone else is experiencing the same issue.

<http://www.scriptlogic.com/support>

Not seeing events in the database

Check that (a) you have set up the service configuration utility correctly to capture the events, and (b) you have not excluded the files and folders you are auditing.

Some applications generate a File Read event only when a file is opened for the first time. If the file is opened again, the application may pull from a memory cache and not from the disk. Since File System Auditor watches events going to NTFS, if an application pulls a file from a memory cache and never calls NTFS, a File Read event is not logged. If another user opens that same file for the first time, that File Read event is logged.

Auditing database fills up fast

Use caution if including **File-Read** or **File-Access Denied (Opening/ Modifying)** events as the number of events recorded by File System Auditor may overwhelm the auditing database. Any focus on a file in Windows Explorer, such as a mouse-over or using the arrow keys to scroll through the directory, causes a **File-Read** event in File System Auditor if the user has access to the file(s). If the user does not have access to the file(s), File System Auditor records a **File-Access Denied (Opening/Modifying)** event.

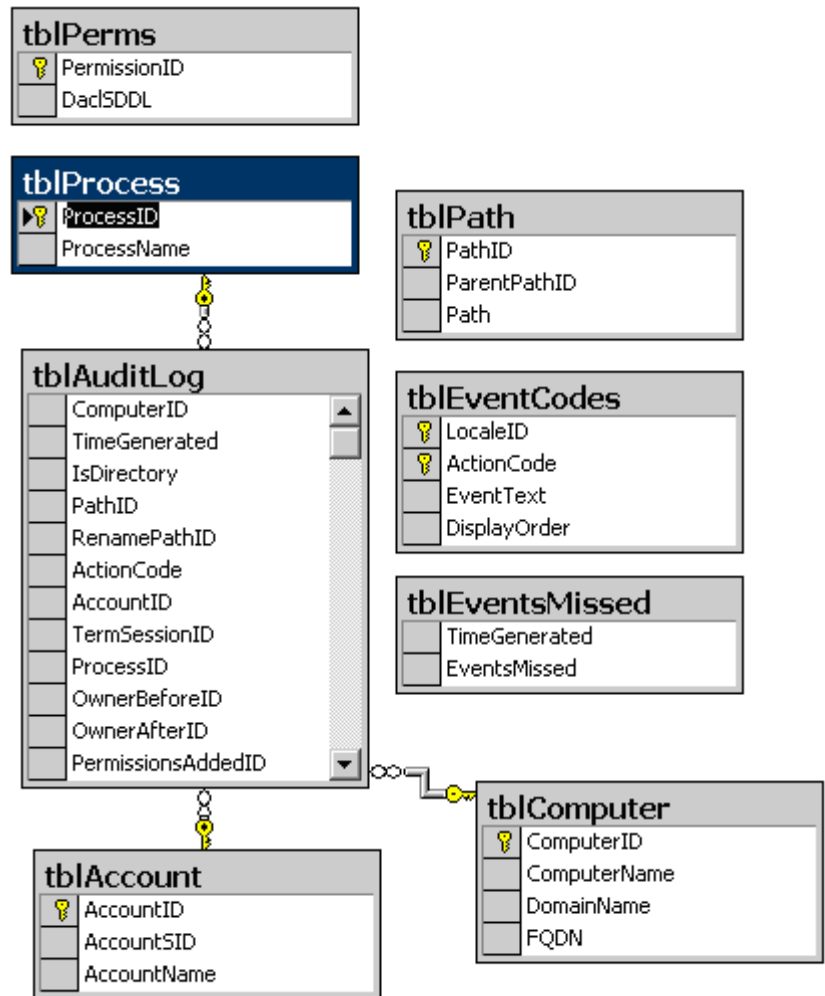
If you need to include the **File-Read** or **File-Access Denied (Opening/ Modifying)** events, restrict the path to a minimum number of files/folders, and to eliminate false positives, make sure you have Windows Access-Based Enumeration (available with Windows Server 2003 Service Pack 1) enabled and operational.

UNINSTALLING FILE SYSTEM AUDITOR

1. From the Windows Control Panel, double-click **Add/Remove Programs**.
2. Select **File System Auditor 2**, and then click **Remove**. A message box prompts you for confirmation.
3. To remove the application, click **Yes**.

Note: The installation directory that contained File System Auditor remains after the process is complete. This directory contains the license file for the product and any files created after the product was installed. These may be deleted manually if you wish to completely remove File System Auditor.

Audit Database Schema



Index

.

.cvs, 21
.htm, 21
.html, 21
.pdf, 21
.rtf, 21
.tiff, 22
.txt, 21
.xls, 22

A

adding
 groups to a filter, 10
audit report, 19
auditing database, 29

C

changing
 database authentication mode, 7
closing
 Reporting Console, 3
creating
 reports, 5

D

database
 changing authentication mode, 7
database schema, 29
date format
 setting, 25
date/time
 filter, 8
deleting
 email addresses, 24
 reports, 3
Delimited Text, 21

E

editing
 paths filter, 15
email accounts
 setting, 26
EULA, 4
events
 filter, 12
exiting
 Reporting Console, 3
exporting
 reports, 20

F

File menu, 3
File System Auditor
 removing, 28
 starting Report Configuration Console, 2
filters, 8
 date/time, 8
 events, 12
 groups, 10
 paths, 13
 processes, 15
 servers, 16, 17
 users, 9

G

general options, 25
groups
 adding to a filter, 10
 removing from a filter, 11
 viewing members, 11

H

help
 displaying online, 3
Help menu, 4
HTML, 21

L

language
 setting, 25
license agreement, 4

M

menus
 File, 3
 Help, 4
 Tools, 3
 View, 3
Microsoft Excel Worksheet (XLS), 22

N

new report
 creating, 5

O

opening
 Report Configuration Console, 2

P

- paths
 - filter, 13
- Portable Document Format (PDF), 21
- printing
 - reports, 19
- processes
 - filter, 15

R

- removing
 - groups from a filter, 11
 - paths from a filter, 15
- renaming
 - reports, 3
- report
 - exporting, 20
 - printing, 19
- Reporting Console
 - exiting, 3
- reports
 - creating, 5
 - deleting, 3
 - renaming, 3
- results
 - sorting, 17
 - viewing, 17
- Rich Text Format (RTF), 21

S

- servers
 - filter, 16, 17

- setting
 - date/time filter, 8
 - email account, 26
 - events filters, 12
 - filters, 8
 - general options, 25
 - group filters, 10
 - path filters, 13
 - process filters, 15
 - server filters, 16, 17
 - user filters, 9
- SLFileAuditor, 29
- Start Page, 2
 - displaying, 3
- starting
 - Report Configuration Console, 2

T

- Tagged Image Format (TIF), 22
- time zones
 - setting, 25
- Tools menu, 3

U

- users
 - filter, 9

V

- View menu, 3
- viewing
 - group members, 11
 - report results, 17