



# *FILE SYSTEM AUDITOR*<sup>®</sup>

*VERSION 2*

## **ScriptLogic<sup>®</sup>**

# **File System Auditor**

# **Agent Configuration**

# **Getting Started 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 System 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](http://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](http://www.scriptlogic.com)

## SCRIPTLOGIC ON THE WEB

ScriptLogic can be found on the web at [www.scriptlogic.com](http://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

<b>WHAT IS FILE SYSTEM AUDITOR?</b> .....	<b>1</b>
<b>INSTALLING FILE SYSTEM AUDITOR</b> .....	<b>2</b>
MINIMUM SYSTEM REQUIREMENTS .....	3
<i>Supported Management Platforms</i> .....	3
<i>Export Requirements</i> .....	3
<i>Support for iSCSI disks</i> .....	3
BEFORE YOU BEGIN .....	4
<i>User Privilege Requirements</i> .....	4
INSTALLING FILE SYSTEM AUDITOR .....	4
STARTING FILE SYSTEM AUDITOR .....	8
<i>Applying a License File</i> .....	8
<i>Evaluating the Product</i> .....	9
<b>CONFIGURING FILE SYSTEM AUDITOR</b> .....	<b>10</b>
STARTING THE AGENT CONFIGURATION CONSOLE .....	10
EXAMINING THE AGENT CONFIGURATION CONSOLE START PAGE.....	10
UPGRADING THE AUDIT AGENT .....	13
CREATING AN AUDIT DATABASE .....	14
ADDING FILE SERVERS.....	14
STOPPING AND STARTING THE AUDIT AGENT .....	22
SETTING PATH FILTERS .....	23
SETTING PROCESS EXCLUSION FILTERS .....	27
SETTING USER EXCLUSION FILTERS.....	29
CHANGING DATABASE SETTINGS.....	31
CHANGING ADVANCED SETTINGS.....	32
SETTING DEFAULT FILTERS.....	33
<b>USING THE REAL TIME VIEWER</b> .....	<b>35</b>
<b>PURGING THE AUDIT DATABASE</b> .....	<b>36</b>
PURGING DATA FROM THE COMMAND LINE.....	43
<i>Using Interactive Mode</i> .....	44
<b>MANAGING THE AUDITING DATABASE</b> .....	<b>45</b>
STARTING THE DATABASE WIZARD .....	45
CREATING A NEW DATABASE .....	47
REMOVING AN EXISTING DATABASE.....	49
INCREASING DATABASE SIZE .....	49
SHRINKING A DATABASE.....	50
RUNNING AN SQL SCRIPT .....	52
VIEWING DATABASE STATISTICS .....	52
ATTACHING A DATABASE .....	53
DETACHING A DATABASE .....	54
TRUNCATING THE TRANSACTION LOG .....	55
CHANGING THE SECURITY MODE.....	55
SETTING THE SA PASSWORD.....	56
SAVING CONNECTION INFORMATION .....	57
PERFORMING DATABASE MAINTENANCE.....	58
RESETTING DATABASE SECURITY .....	59
MOVING A DATABASE TO ANOTHER SERVER .....	60

<b>TROUBLESHOOTING .....</b>	<b>61</b>
REMOVING A FILE SERVER .....	62
UNINSTALLING THE AUDIT AGENT .....	62
UNINSTALLING FILE SYSTEM AUDITOR .....	63
<b>AUDIT DATABASE SCHEMA .....</b>	<b>64</b>
<b>STORED PROCEDURES .....</b>	<b>65</b>
<b>INDEX .....</b>	<b>67</b>

# 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 interface. The main window is titled "ScriptLogic File System Auditor [Report Configuration Console]". It features a menu bar (File, View, Tools, Help) and a toolbar with buttons for "New Report", "Start Page", and a help icon. The interface is divided into several sections:

- Reports:** A sidebar on the left with a "Modified Files and Folders" section.
- Modified Files and Folders:** The main area, containing a "Database Connection" section with fields for "SQL Server Instance" (QATEST2K-2K3R2), "Database Name" (SLFileAuditor), and "Authentication Mode" (Windows). A "Selected Report Filter" section includes "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]), and "Workstations" ([All Workstations]).
- Report Preview:** A section below the filters, indicating "Report Not Scheduled". It shows a table of events with columns for "Server Name", "Time Generated", "Account", and "Event".

Below the main window, a "File System Auditor Report Viewer" window is open, displaying a detailed report titled "File System Auditor - Audit Report". The report includes a summary and a list of events:

**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

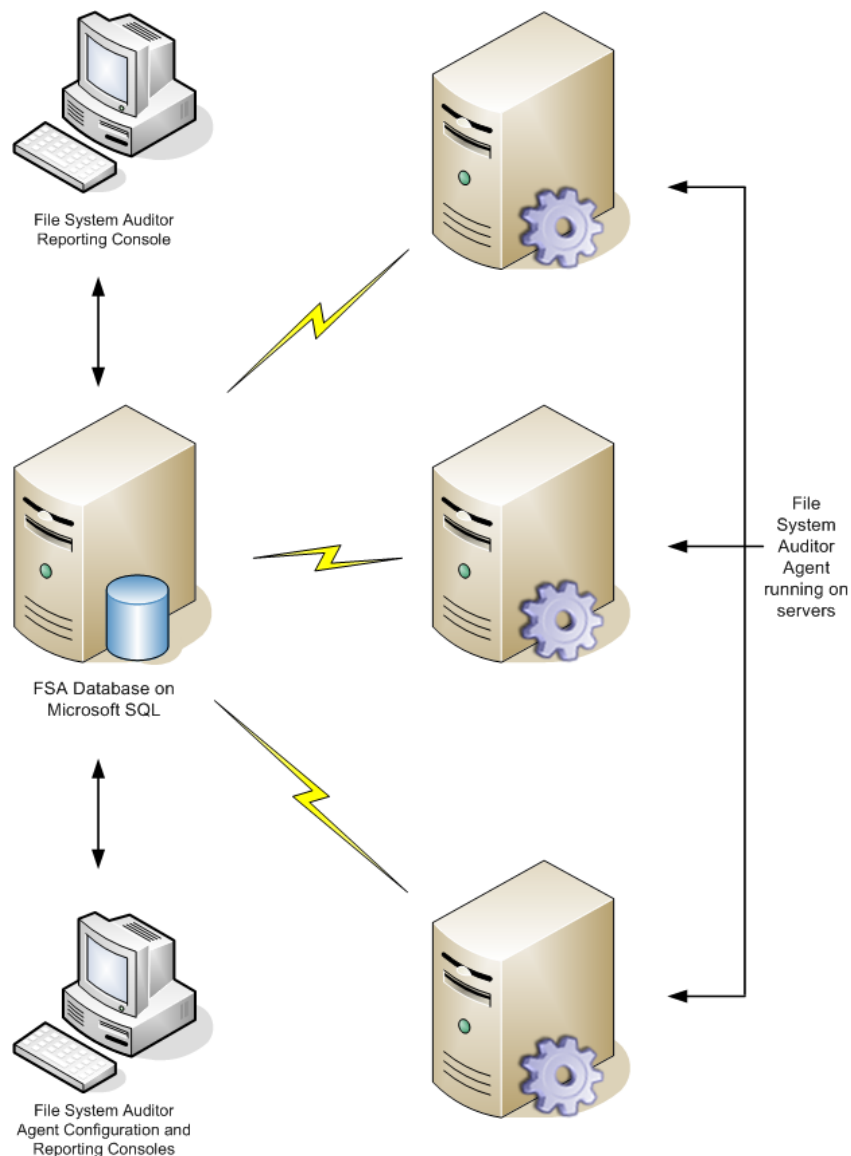
**Tuesday, September 15, 2009**

Date:	Time:	User:	Event:
9/15/2009	3:12:13 PM	Administrator (ACME\Administrator)	Folder - Created
<b>Server:</b> QATEST2K-2K3R2 (ACME) <b>Process:</b> FSAReportingConsole.exe <b>Workstation:</b> qatest2k-2k3r2.ACME.com (197.168.0.1) <b>Path:</b> 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
<b>Server:</b> QATEST2K-2K3R2 (ACME) <b>Process:</b> FSAReportingConsole.exe <b>Workstation:</b> qatest2k-2k3r2.ACME.com (197.168.0.1) <b>Path:</b> C:\Documents and Settings\Administrator.QATEST2K-2K3R2.000\Local Settings\Application Data\ScriptLogic_Corporation\F SAReportingConsole.exe_url_jrsd2lqqvvaatykv21ybm5hawtdo			
9/15/2009	3:12:13 PM	Administrator (ACME\Administrator)	Folder - Created

# Installing File System Auditor

There are two components to File System Auditor: the Agent Configuration Console and the Reporting Console. From the Agent Configuration Console, you can remotely install the File System Auditor Agent on systems to be audited. The Agent consists of a file system driver and a service. You can install just the Reporting Console on systems to be used for report generation.

SQL 2000, SQL 2005, and SQL 2008 database instances (default and named) are supported, including SQL 2005 Express.



## MINIMUM SYSTEM REQUIREMENTS

- Intel®Pentium® III or higher processor
- 512 MB RAM
- 50 MB free hard disk space for installation
- 100 MB free hard disk space for the database

## Supported Management Platforms

### Agent Configuration and Report Configuration Consoles

**Note:** Microsoft .NET Framework 2 is required on the Agent Configuration and Report Configuration Consoles.

- Windows 2000 SP4 with Update Rollup 1: Professional, Server
- Windows XP Professional with SP2
- Windows Server™ 2003 Family with SP1
- Windows Vista
- Windows Server 2008 Family including R2
- Windows 7

### Agent

- Windows Server 2000 SP4 with Update Rollup 1
- Windows Server 2003 family with SP1
- Windows Server 2008 Family, including R2 and Server Core

## Export Requirements

- Microsoft SQL Server 2000, Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, and Data Access Components (MDAC) 2.7

## Support for iSCSI disks

File System Auditor 2 is supported on iSCSI target disks using Microsoft iSCSI Software Initiator Version 2.06 (build 3497). If you are using an earlier version of this software and are experiencing issues auditing an iSCSI target disk with File System Auditor 2, upgrade to the latest version of the Microsoft iSCSI Software Initiator, which you can find at the Microsoft Download Center: <http://www.microsoft.com/downloads/>

## BEFORE YOU BEGIN

Download the latest version of the File System Auditor program from the ScriptLogic Web site: <http://www.scriptlogic.com/support>

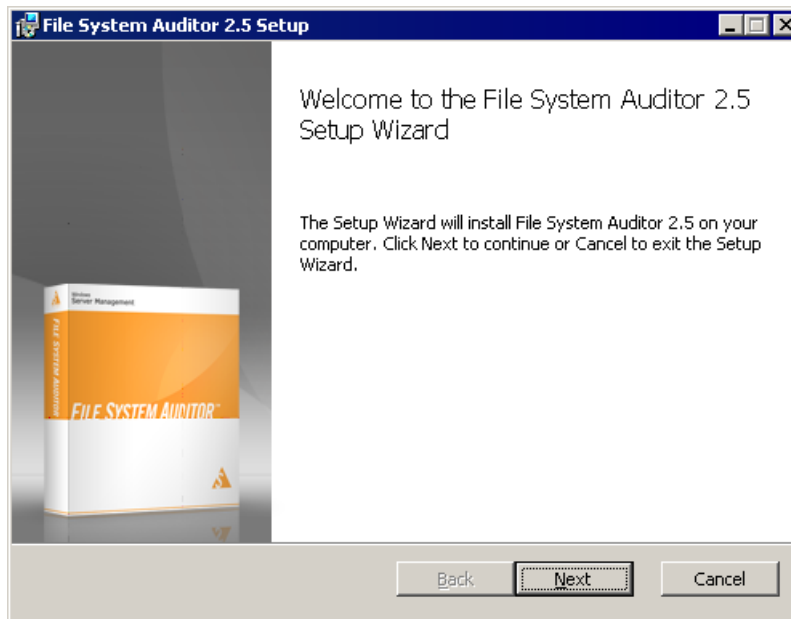
### User Privilege Requirements

In order to install and configure File System Auditor, a user must hold administrative rights.

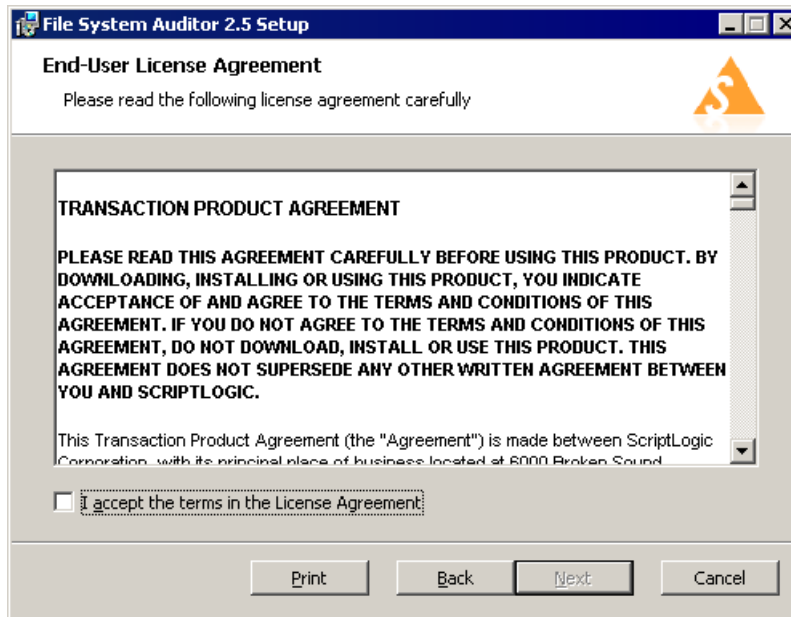
## INSTALLING FILE SYSTEM AUDITOR

During the install process, you can choose to install the Agent Configuration Console and/or the Report Configuration Console. After the Agent Configuration Console is installed, you can remotely install the File System Auditor Agent on those computers you want to audit. Install the Report Configuration Console on those computers whose users need to generate reports.

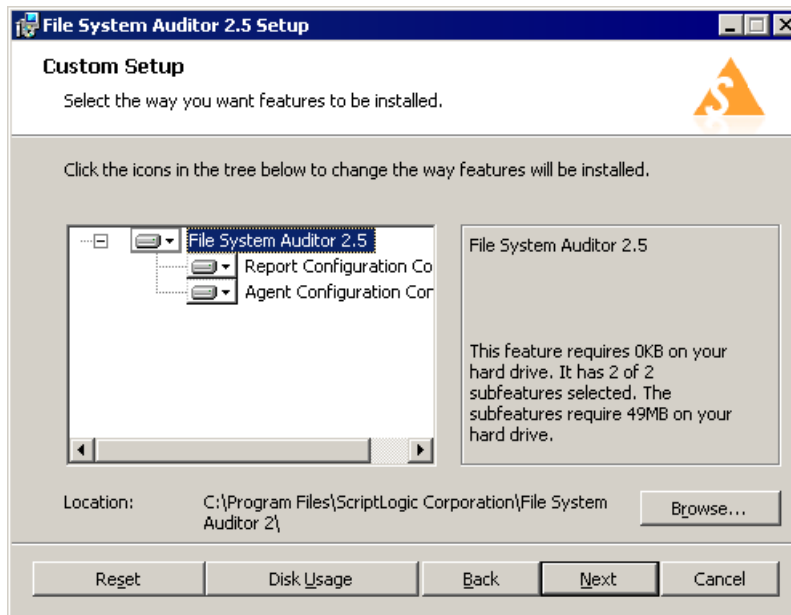
1. Double-click the **FSASetup.msi** file. The **Welcome** page opens.



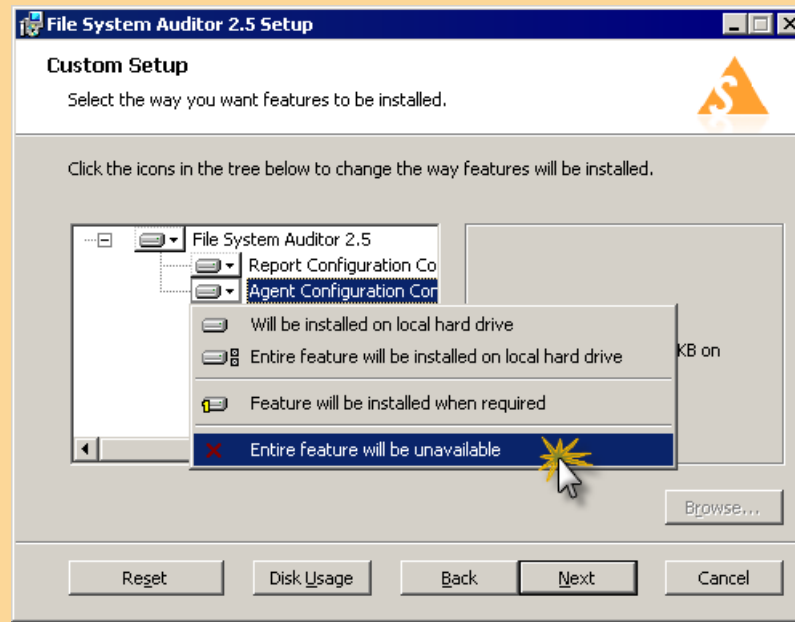
2. Click **Next**. The **License Agreement** page opens.



3. Select the **I accept the terms in the License Agreement** check box, and then click **Next**. The **Custom Setup** page opens.

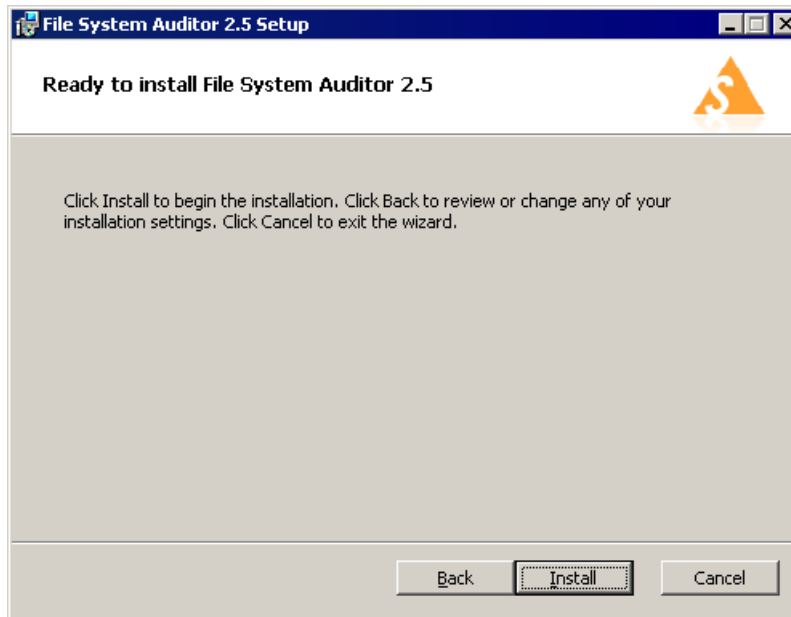


**Note:** By default, both the Agent Configuration Console and the Report Configuration Console are installed. If you want to install just the Report Configuration Console, open the **Agent Configuration Console** list, and then choose **Entire feature will be unavailable**.

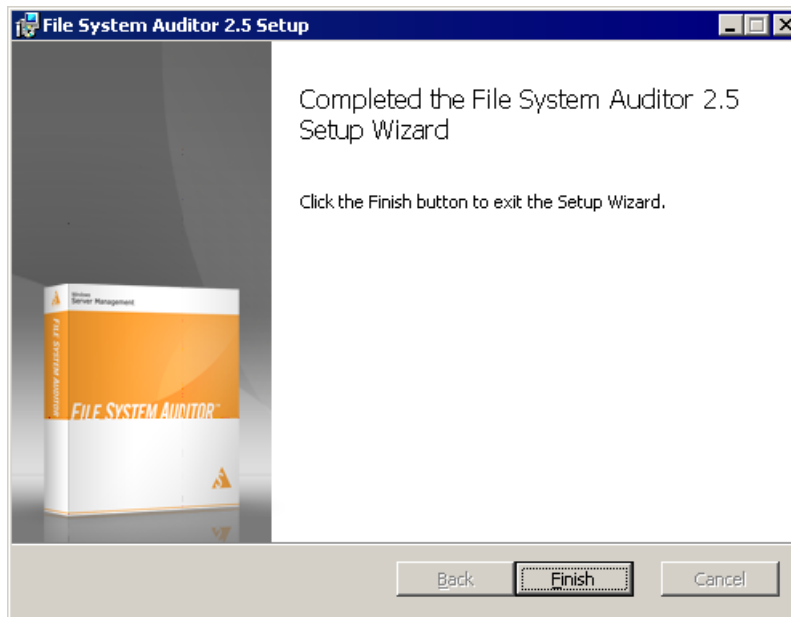


To:	Click:
Return the selections to the default	<input type="button" value="Reset"/>
Change the location of the program files	<input type="button" value="Browse..."/> The <b>Change Current Destination Folder</b> page opens. Choose a new location for the installation directory.
See if there is enough space to install the programs	<input type="button" value="Disk Usage"/> The <b>Disk Requirements</b> page shows the disk space available on the drive displayed in the <b>Install to</b> area.

4. Click **Next**. The **Ready to install** page opens.



5. Click **Next**. The installation process begins. When the process is complete, the **Completed** page opens.



6. Click **Finish**.

## STARTING FILE SYSTEM AUDITOR

- ▶ Click **Start**, point to **Programs** ▶ **ScriptLogic Corporation** ▶ **File System Auditor 2**, and then select one of the following options:

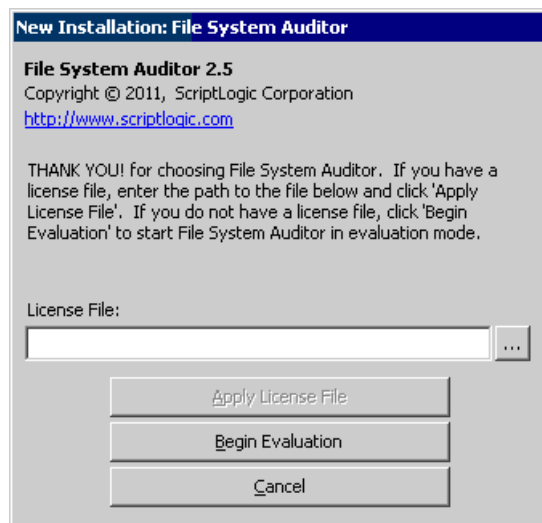
Option	Description
Agent Configuration Console	Configure File System Auditor for data collection. See <i>Configuring File System Auditor</i> .
Database Wizard	Create and manage the auditing database[s]. See <i>Managing the Audit Database</i> .
FSA Getting Started Guide (PDF)	Opens the installation and configuration document for the Agent Configuration Console.
FSA User Guide (PDF)	Opens the user guide for the Report Configuration Console.
Report Configuration Console	Filter and report on data in the auditing database. See the <i>File System Auditor Report Configuration User Guide</i> .
Real Time Viewer	View data in the audit database in real-time. See <i>Starting the Real Time Viewer</i> .

Each time you run File System Auditor or File System Audit Reporter, you will be greeted by the splash screen, which displays the initialization of the program and the version number.


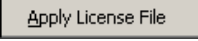
### Applying a License File

The first time you start File System Auditor, you see the **New Installation** box, which allows you to apply a license file or evaluate the product without a license, as well as contact ScriptLogic Corporation and visit our website for further information.

File System Auditor requires a valid license file in order to function properly. If you have a company license file or were provided with an evaluation or temporary license file, you must enter the location and filename in the **License File** box.

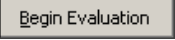


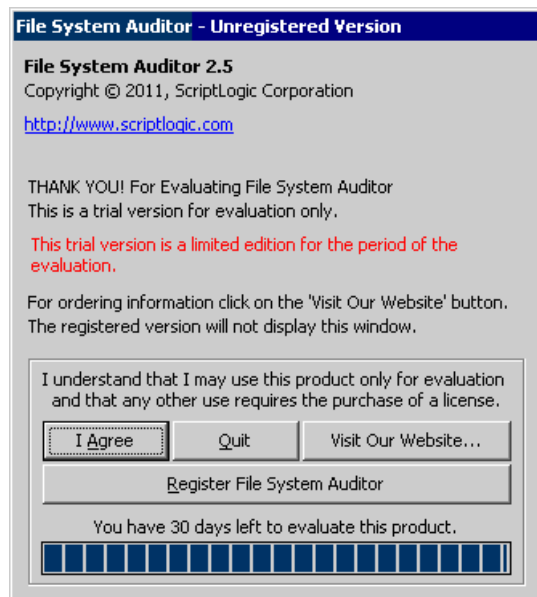
The license file is approximately 1KB in size and has a .lic file extension. Your Sales Account Executive or Licensing Specialist should have sent this file to you as an email attachment.

- ▶ Click  to locate the license file, and then click .

## Evaluating the Product

**Note:** The full and evaluation versions of File System Auditor are identical. The license file is the sole determinant of program functionality. The evaluation period is 30 days and limited to 2 servers.

- ▶ If you are evaluating the software and would like to use the preset values for the number of licenses, objects, and evaluation days, click .



To:	Click:
Start the evaluation version	
Exit	
Go to the ScriptLogic web site	
Apply a License File	

# Configuring File System Auditor

The File Service Auditor Agent Configuration Console enables you to manage the data that goes into the auditing database. Only the data that resides in the auditing database is available to the File System Auditor console for reporting.

Before File System Auditor can begin to collect data, you must define a path and choose the types of events to monitor. To manage the number of events that are collected, you can specify to include or exclude certain file types, or exclude certain processes from the collection. Lastly, you can specify a length of time during which duplicate events are suppressed from the list, which also helps manage the amount of data collected.

## STARTING THE AGENT CONFIGURATION CONSOLE

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

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










## EXAMINING THE AGENT CONFIGURATION CONSOLE START PAGE

If this is the first time you have installed File System Auditor, the **Configuration Console Start Page** displays. To set up File System Auditor, you must add at least one file server and create an auditing database.

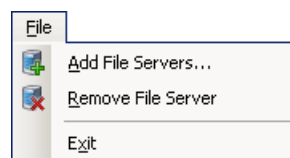


Option	Description
<a href="#">Add File Servers</a>	Add file servers. See <i>Adding File Servers</i> .
<a href="#">Run Database Wizard</a>	Create and manage auditing databases. See <i>Starting the Database Wizard</i> .
<a href="#">Purge Audit Log</a>	Purge selected data from an auditing database. See <i>Purging the Audit Database</i> .
<a href="#">Modify Application Preferences</a>	Create and manage default filters. See <i>Setting Default Filters</i> .
<a href="#">Display Help</a>	Display online help.
<a href="#">Launch Reporting Console</a>	Open the File System Audit Report Configuration Console where you can produce reports based on the data in the auditing database. See the <i>File System Auditor Report Configuration User Guide</i> .

## Tool Bar

Icon	Description
 Add File Servers	Add file servers. See <i>Adding File Servers</i> .
	Remove selected file servers.
 Start Auditing	Start the auditing process.
	Stop the auditing process.
	Refresh the display.
 Reporting Console	Open the File System Audit Report Configuration Console where you can produce reports based on the data in the auditing database. See the <i>File System Auditor Report Configuration User Guide</i> .
 Upgrade File Server	Upgrade the Audit Agent from a previous installation of File System Auditor. See <i>Upgrading the Audit Agent</i> .
 Start Page	Display the Start Page.
	Access online help

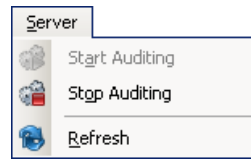
## Menus



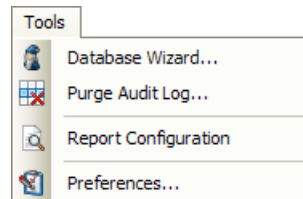
Menu Option	Description
Add File Servers	Add file servers. See <i>Adding File Servers</i> .
Remove File Server	Remove selected file servers.
Exit	Close File System Auditor.



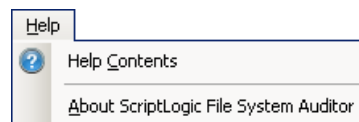
Menu Option	Description
Start Page	Display the Start Page.



Menu Option	Description
Start Auditing	Start the auditing process.
Stop Auditing	Stop the auditing process.
Refresh	Refresh the display.



Menu Option	Description
Database Wizard	Create and manage auditing databases. See <i>Starting the Database Wizard</i> .
Purge Audit Log	Purge selected data from an auditing database. See <i>Purging the Audit Database</i> .
Report Configuration	Open the File System Audit Report Configuration Console where you can produce reports based on the data in the auditing database. See the <i>File System Auditor Report Configuration User Guide</i> .
Preferences	Create and manage default filters. See <i>Setting Default Filters</i> .



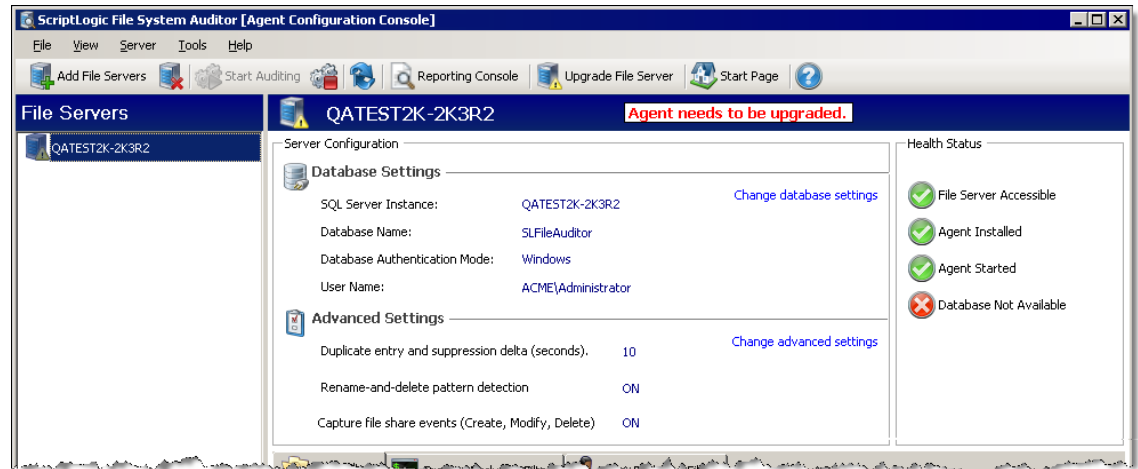
Menu Option	Description
Help Contents	Access online help
About ScriptLogic File System Auditor	View information about the version of File System Auditor installed on your computer, to apply a license file, or to visit the ScriptLogic website.

## UPGRADING THE AUDIT AGENT

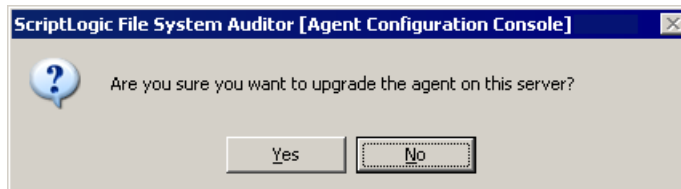
**Note:** If you are installing File System Auditor for the first time, proceed to *Creating an Audit Database*.

If you are updating from a previous version, you need to upgrade the Audit Agent following the installation of the latest version of File System Auditor.

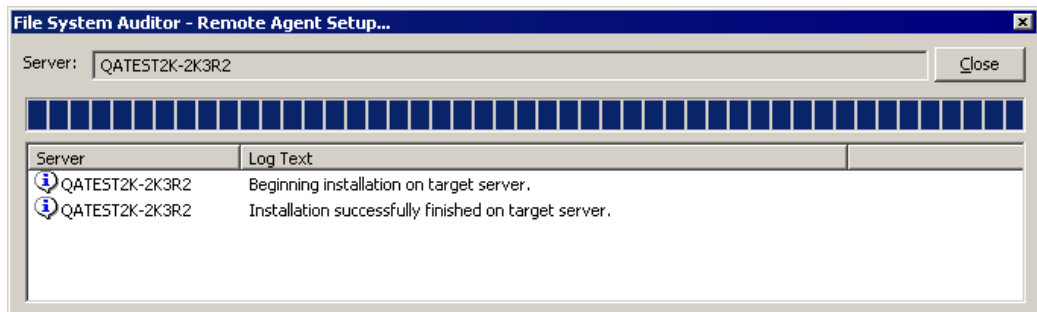
After starting File System Auditor, you see your file servers listed with a notice that the Agent needs to be upgraded.



1. Select the file server, and then click . A warning message displays.



2. To upgrade the agent, click Yes.



3. Click Close.

## CREATING AN AUDIT DATABASE

**Important:** File System Auditor requires an instance of Microsoft SQL Server.

**Important:** You must create an auditing database before you can perform any tasks using File System Auditor.

There are several methods that you can choose to start the Database Wizard where you can create an audit database.


- ▶ Click **Start**, point to **Programs** ▶ **ScriptLogic Corporation** ▶ **File System Auditor 2**, and then choose **Database Wizard**.
- ▶ Click [Run Database Wizard](#) on the **Agent Configuration Console Start Page**.
- ▶ Choose **Database Wizard** from the **Tools** menu on the **Agent Configuration Console Start Page**.

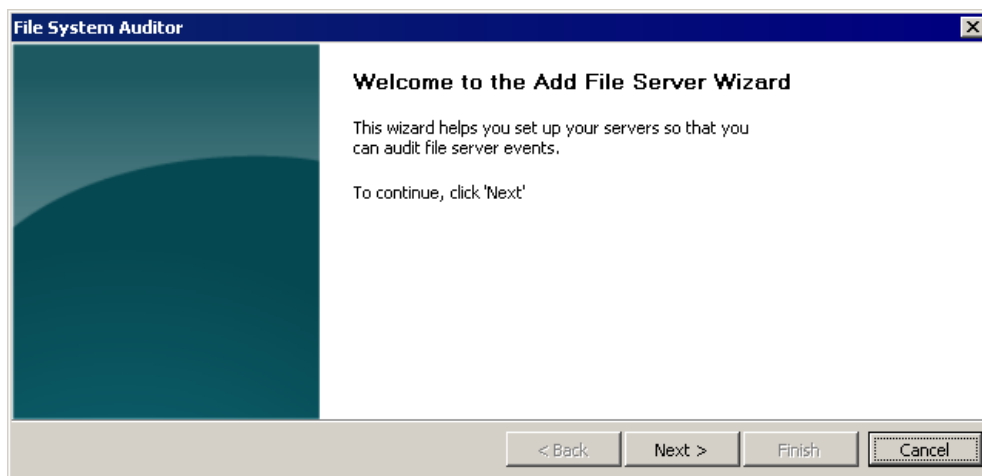
See *Creating a New Database* in the *Database Wizard* chapter.

**Note:** You also have an opportunity to access the Database Wizard to create a database during the process of adding file servers. See *Adding File Servers*.

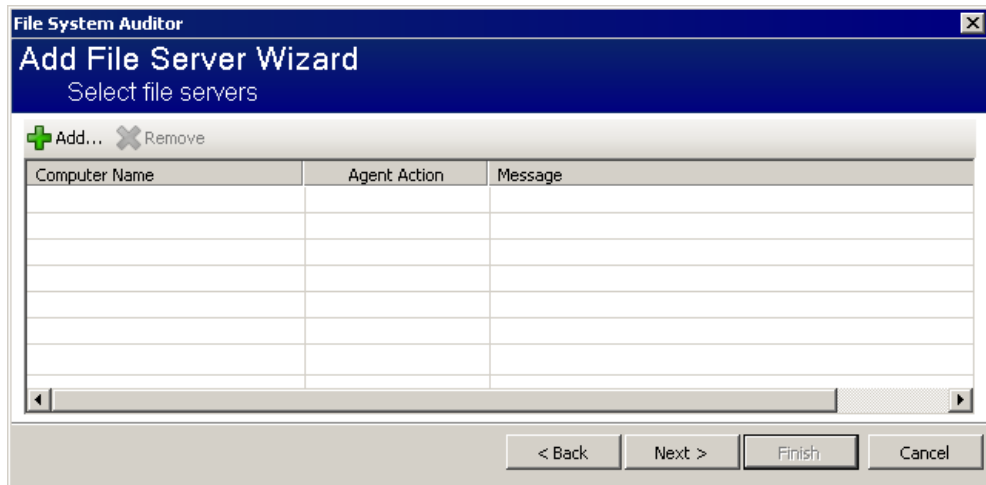
## ADDING FILE SERVERS

To audit a computer, you must add it to the list of file servers. During the process, the Audit Agent is installed on the target computers, the connection to the Audit Database is established, and you can define filters to manage the data that is collected.

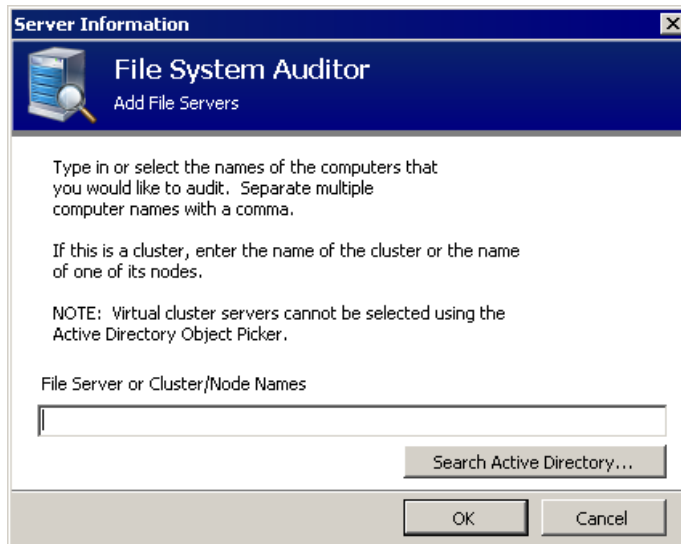
1. Click . Alternatively, choose **Add File Servers** from the **File** menu or click [Add File Servers](#) on the **Agent Configuration Console Start Page**. The **Add File Server Wizard** opens.



2. Click **Next**. The **Select file servers** page opens.

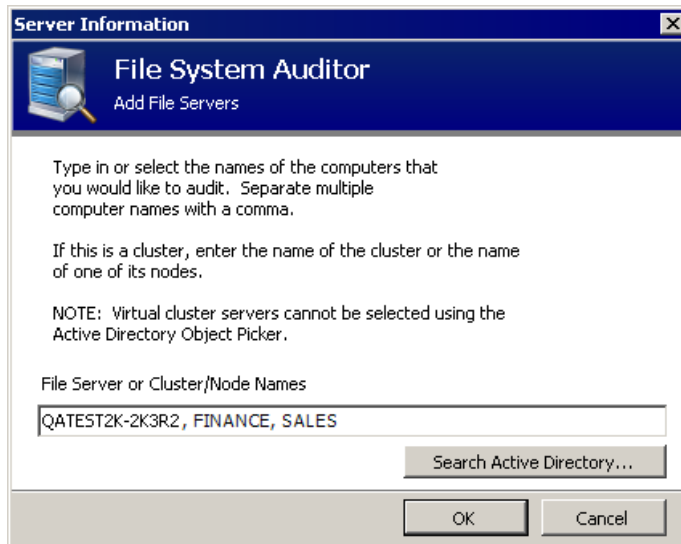


3. Click **+ Add...**. The **Add File Servers** page opens.

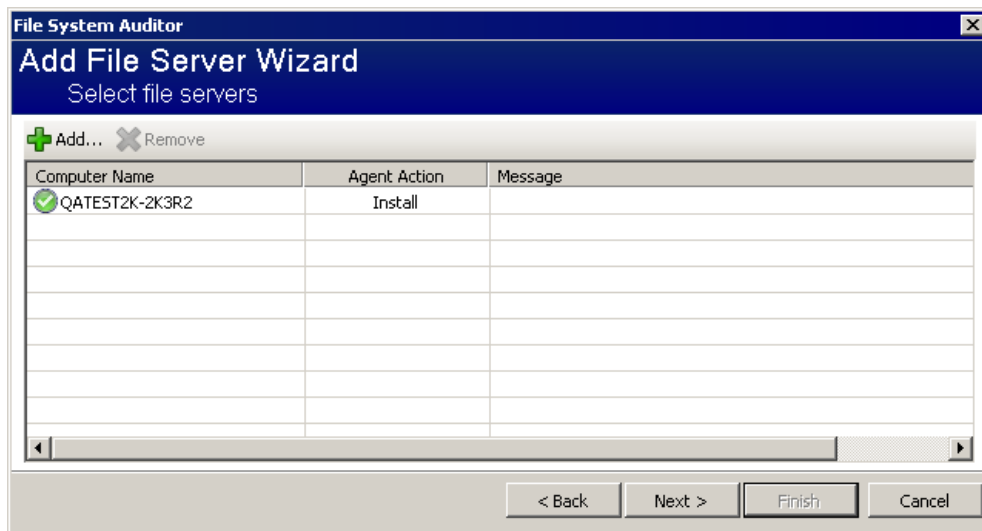


- In the **File Server or Cluster/Node Names** box, type the names of the file servers or cluster servers separated with commas, or click  and choose the servers.

**Note:** You cannot select virtual cluster servers from the Active Directory Object Picker. You must type the names in the box.



- Click **OK**. The server name(s) displays in the **Computer Name** column and the **Agent Action** column indicates the Audit Agent will be installed.



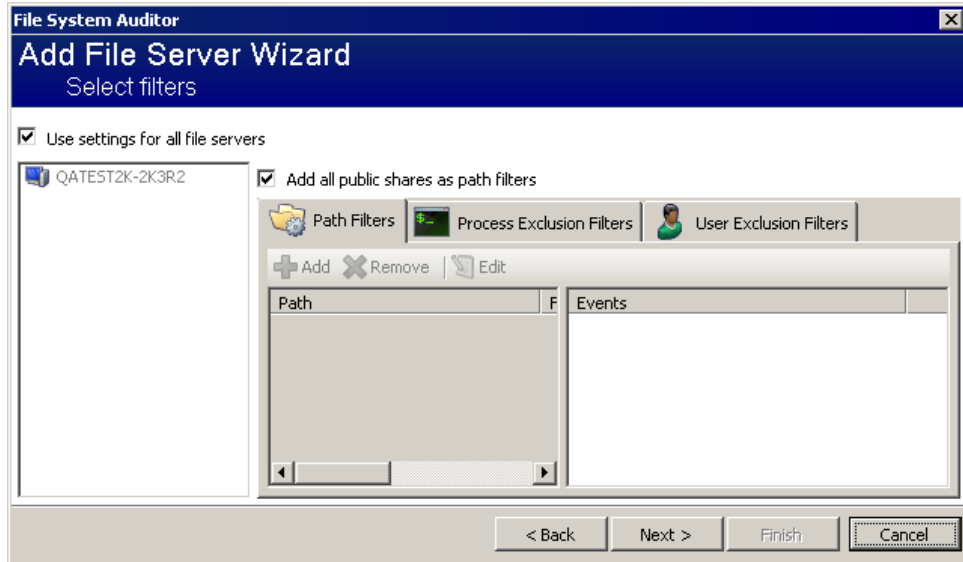
6. Click **Next**. The **Choose database and set authentication** page opens.

The screenshot shows the 'Add File Server Wizard' dialog box with the title 'Choose database and set authentication'. It features a blue header bar with the text 'File System Auditor' and 'Add File Server Wizard'. Below the header, there is a database icon and a 'Create New Database...' button. The 'SQL Server Instance' dropdown is set to 'QATEST2K-2K3R2'. The 'Database Name' dropdown is set to 'SLFileAuditor'. A 'Database Authentication' section contains a key icon and a text box with instructions: 'Enter a username and password for an account that has permissions to write to the above database. The password for this account should not expire.' Below this, there are radio buttons for 'Windows Authentication' (selected) and 'SQL Server Authentication'. The 'Username' field contains 'ACME\Administrator' and has a 'Search Active Directory...' button. The 'Password' and 'Confirm Password' fields are masked with dots. At the bottom, there are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

- a. From the **SQL Server Instance** list, select the name of the server where the auditing database resides.
- b. From the **Database Name** list, select the name of the auditing database.
- c. Choose whether to use Windows or SQL Server authentication.
- d. In the **Username** box, type the name of the account with the permissions necessary to write to the auditing database, or click **Search Active Directory...** to select an account.
- e. In the **Password** and **Confirm Password** boxes, type the password for the account you selected.

7. Click **Next**. The **Select filters** page lists the servers you added.

On the **Select filters** page, you can define filters that will include or exclude items from the auditing process. On initial installation, you may want to accept the default settings as you can define filters once installation is complete.



**Use settings for all file servers**

By default, the filters that you add here apply to all the file servers in the list. If you want to define filters separately for each server, clear the check box.

**Path Filters**

**Add all public shares as path filters**

By default, all public shares are added as path filters. If you want to add different path filters, clear the **Use settings for all file servers** check box, and then clear this check box.

You can specify specific folders to include or filter out any folders you do not want to include in the data. In addition, you can specify specific events and files to include or exclude. See *Stopping and Starting the Audit Agent*.

**Process Exclusion Filters**

See *Setting Process Exclusion Filters*.

**User Exclusion Filters**

See *Setting User Exclusion Filters*.

8. Click **Next**. The **Set advanced install options** page opens.

#### Advanced Options

##### **Duplicate entry and suppression delta (seconds)**

By default, duplicate entries that occur within 10 seconds of each other are suppressed. Only the first entry appears in the event list. You can increase this value to reduce the length of the event list. Changes apply to new event collection only. Existing data is not affected.

##### **Rename-and-delete pattern detection**

In some software applications, when saving a file, instead of overwriting the original file, the application saves to a temporary file, renames the original file, renames the temporary file to the current file name, and then deletes the temporary file. This process occurs so you can recover the original file. By default, File System Auditor detects this behavior and logs it in the database as a file modification on the file you were editing, rather than as a rename and delete process. To disable this detection, select the check box.

##### **Capture file share events (Create, Modify, Delete)**

If you are running Windows Server 2003 or later, file share events are included in the data collection by default. To disable this feature, clear the check box.

#### Agent Start Options

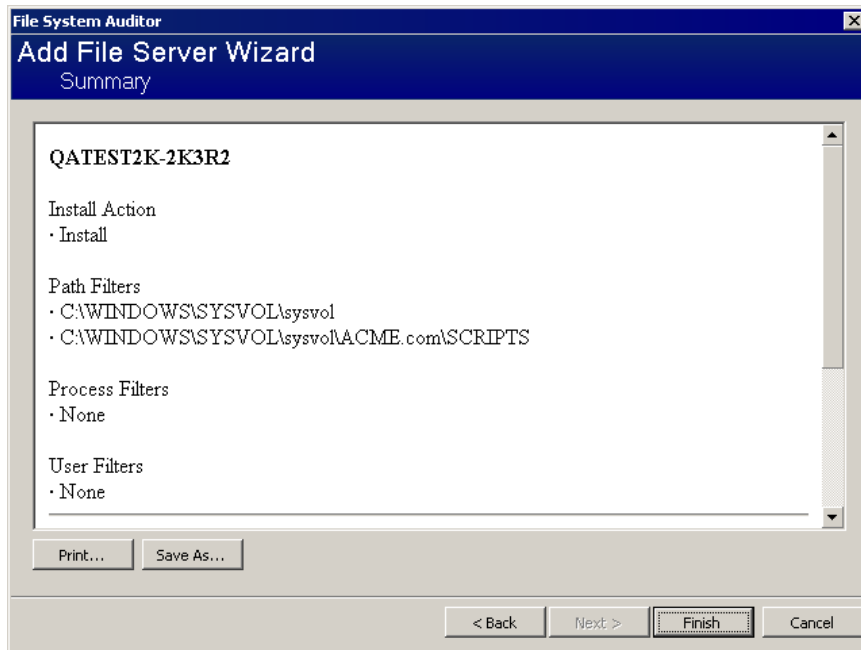
##### **Start agent(s) immediately after install**

By default, the agents are started after installation is complete.

##### **Only install agents. User will start agents later**

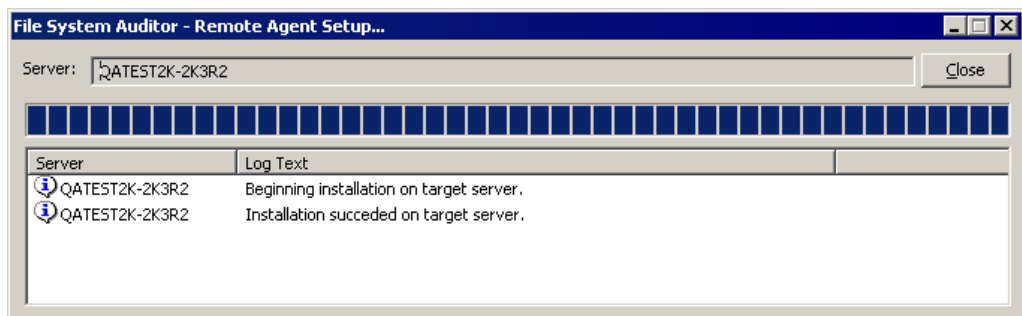
Select to install agents only. To start the agents after installation, see *Stopping and Starting the Audit Agent*.

9. Click **Next**. The **Summary** page displays the selections you made.



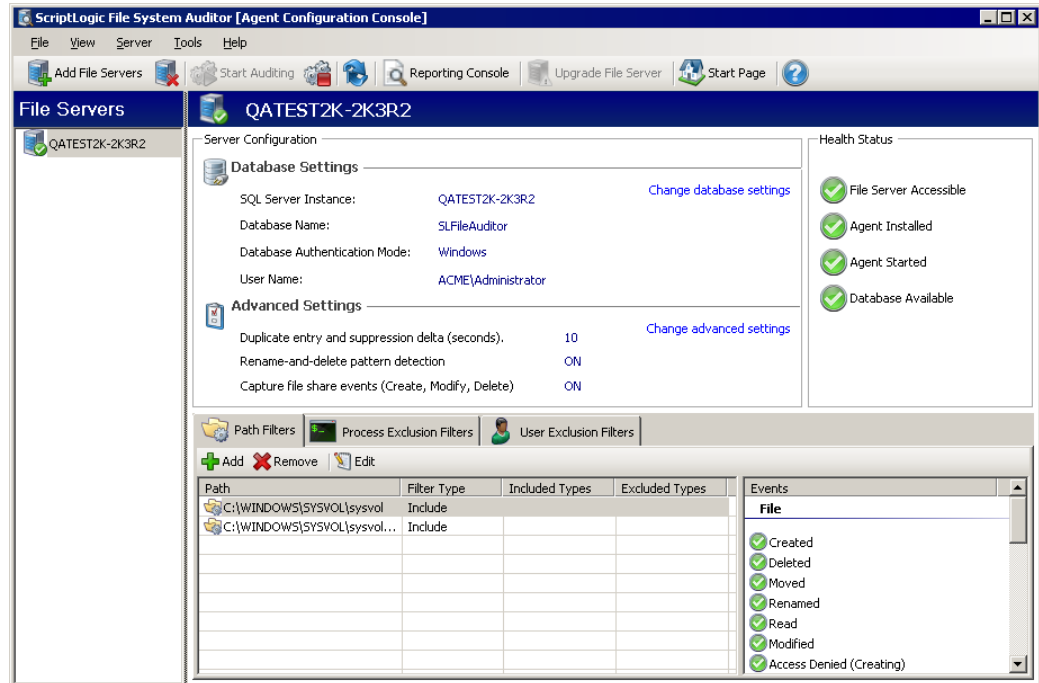
Button	Description
Print...	Print the summary information.
Save As...	Save the summary information to a file.

10. Click **Finish**.




11. Click **Close**.

The main window displays the file servers that you installed. You can select each server individually to view information and to create filters.



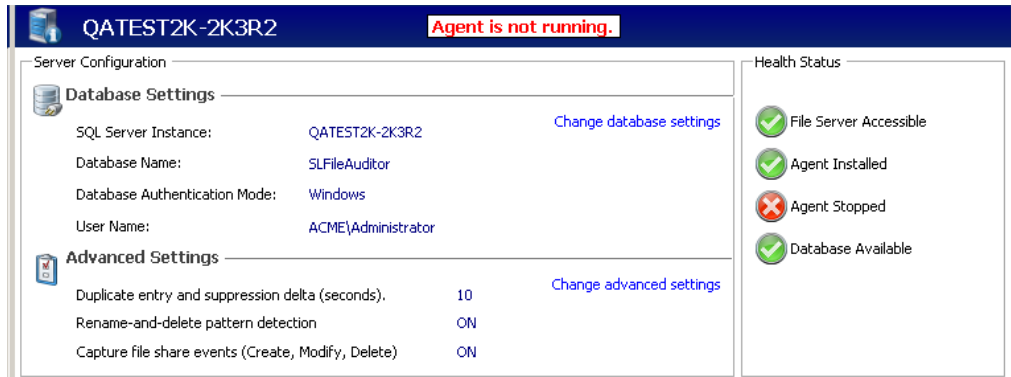
- The **Database Settings** area displays information about the SQL Server Instance and the auditing database. See *Changing Database Settings*,
- The **Advanced Settings** area displays the choices made during installation of the file server. See *Changing Advanced Settings*.
- The **Health Status** area shows the status of the File Server, Agent, and Audit Database.

**Note:** You may need to click  to refresh the status. Alternatively, choose **Refresh** from the **Server** menu.

- The **Filters** area contains three tabs. You had the option to add filters during the process of adding a filter. If you chose to bypass that step, you can add them now, or if you did add filters, you can edit or remove them.
  - See *Setting Path Filters*
  - See *Setting Process Exclusion Filters*
  - See *Setting User Exclusion Filters*

## STOPPING AND STARTING THE AUDIT AGENT

- To stop the Audit Agent, click . Alternatively, choose **Stop Auditing** from the **Server** menu.



The screenshot shows the File System Auditor console for server QATEST2K-2K3R2. The status bar at the top right indicates "Agent is not running." The console is divided into two main sections: "Server Configuration" and "Health Status".

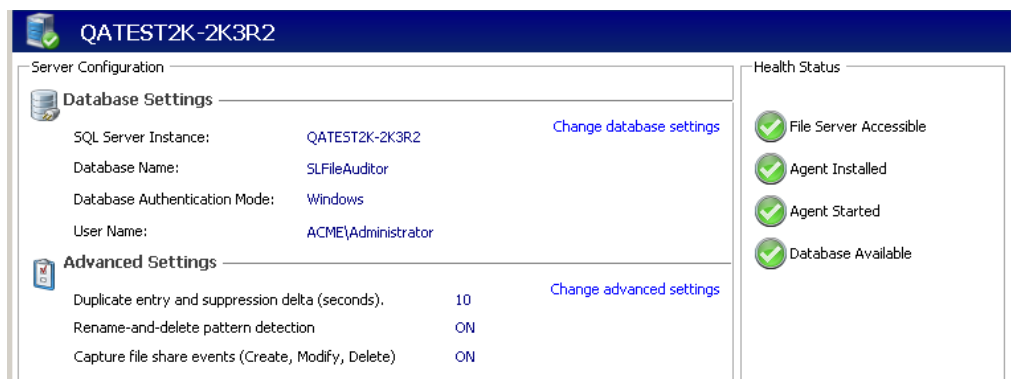
**Server Configuration:**

- Database Settings:**
  - SQL Server Instance: QATEST2K-2K3R2
  - Database Name: SLFileAuditor
  - Database Authentication Mode: Windows
  - User Name: ACME\Administrator
- Advanced Settings:**
  - Duplicate entry and suppression delta (seconds): 10
  - Rename-and-delete pattern detection: ON
  - Capture file share events (Create, Modify, Delete): ON

**Health Status:**

- File Server Accessible (Green checkmark)
- Agent Installed (Green checkmark)
- Agent Stopped (Red X)
- Database Available (Green checkmark)

- To start a stopped Audit Agent, click . Alternatively, choose **Start Auditing** from the **Server** menu.



The screenshot shows the File System Auditor console for server QATEST2K-2K3R2. The status bar at the top left now shows a green checkmark. The console is divided into two main sections: "Server Configuration" and "Health Status".

**Server Configuration:**

- Database Settings:**
  - SQL Server Instance: QATEST2K-2K3R2
  - Database Name: SLFileAuditor
  - Database Authentication Mode: Windows
  - User Name: ACME\Administrator
- Advanced Settings:**
  - Duplicate entry and suppression delta (seconds): 10
  - Rename-and-delete pattern detection: ON
  - Capture file share events (Create, Modify, Delete): ON

**Health Status:**

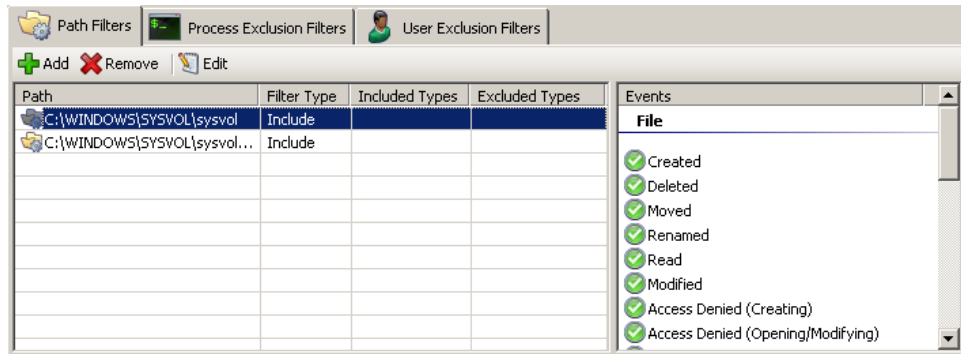
- File Server Accessible (Green checkmark)
- Agent Installed (Green checkmark)
- Agent Started (Green checkmark)
- Database Available (Green checkmark)

## SETTING PATH FILTERS

You can specify specific folders or files to include or filter out any folders or files you do not want to include in the data.

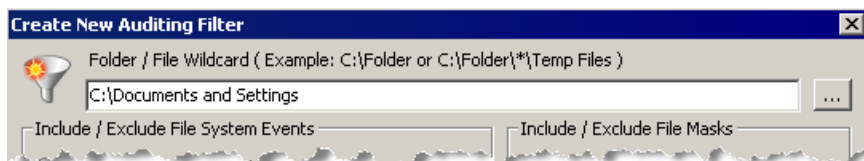
**Note:** If you are running Windows Server 2003 or later, file share events (Create, Modify, and Delete) are included in the data collection by default. To disable this feature, see *Changing Advanced Settings*.


1. Open the **Path Filters** tab to display the current filters.

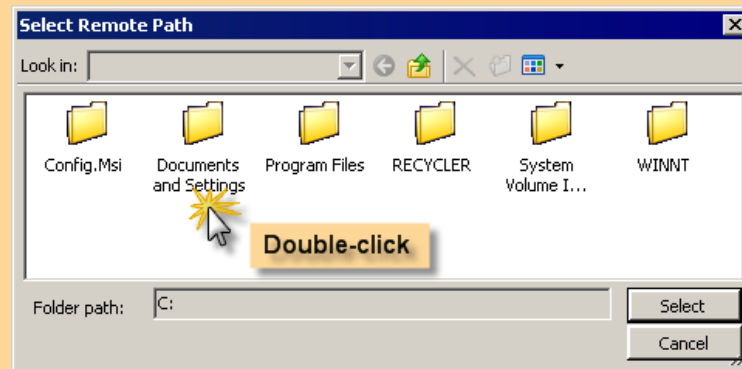


Button	Description
	Add a new filter
	Remove selected filters
	Edit the selected filter

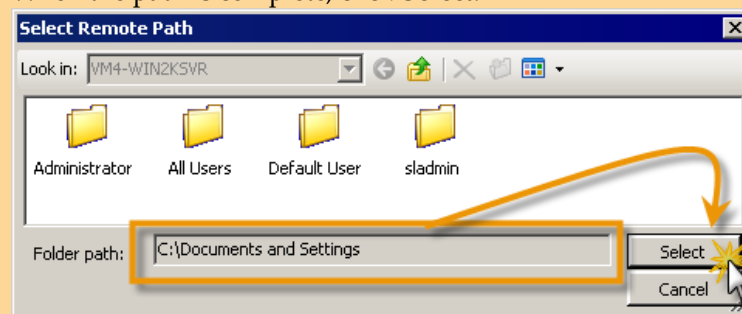
2. Click . The **Create New Auditing Filter** box opens.
3. In the **Folder/File Wildcard** box, type the path to which to apply the filter, or click to locate a folder. You can use the \* wildcard when typing the path.



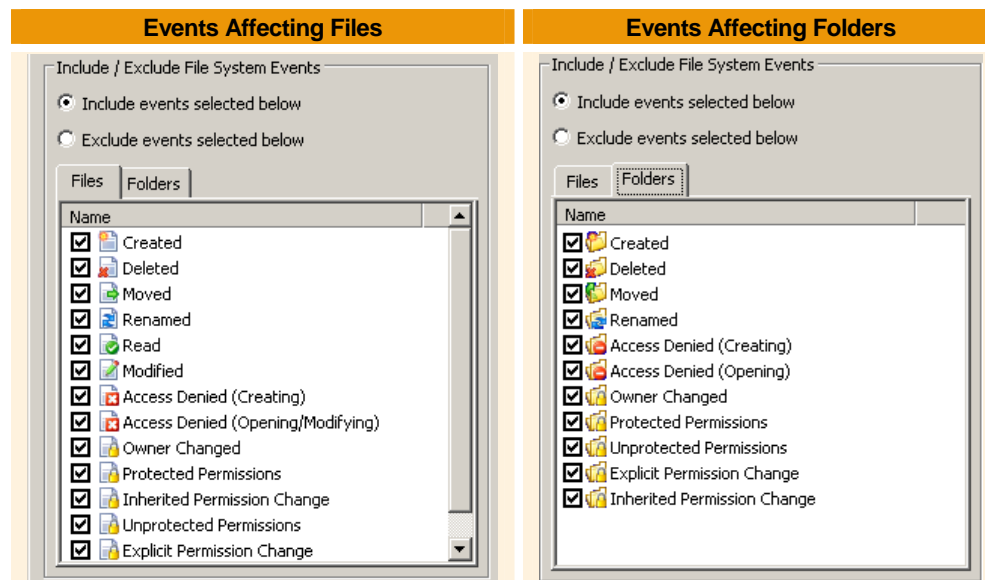
If you click  the **Select Remote Path** box opens. Double-click a selection to build the path in the **Folder path** box.



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



4. In the **Include/Exclude File System Events** area, select the file and folder events that you want to include or exclude from the path. By default, all events are selected.



**Note:** Protected Permissions are those where the parent permissions do not apply to the child objects. Unprotected Permissions are those where the parent permissions do apply to the child objects.

**Note:** You can select to include or exclude events, but not both in the same filter. Create separate filters to include and exclude events.

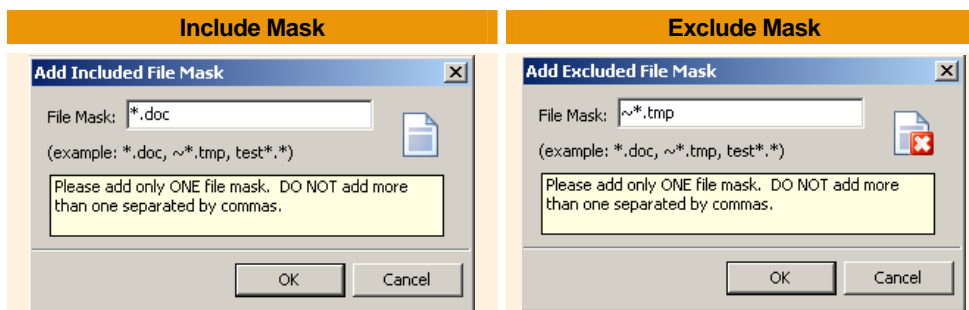
**Important:** Use caution if including **File-Read** or **File-Access Denied (Opening/Modifying)** events as the number of events recorded by File System Auditor may overwhelm the auditing database. Any focus on a file in Windows Explorer, such as a mouse-over or using the arrow keys to scroll through 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.

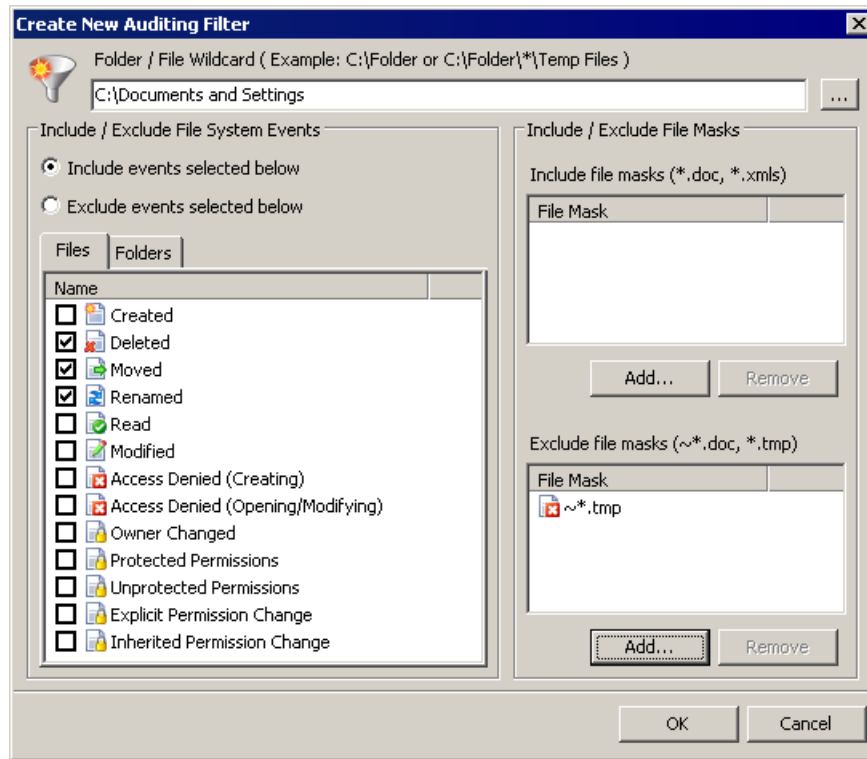
**Note:** Some applications generate a **File Read** event only when a file is opened for the first time. If the file is opened again, the application may pull from a memory cache and not from the disk. Since File System Auditor watches events going to NTFS, if an application pulls a file from a memory 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.



- In the **Include/Exclude File Masks** area, you can specify files to include or exclude. To add a mask, click **Add** in the appropriate area. The **Add Included File Mask** or **Add Excluded File Mask** box appears. Type the mask in the box using wildcards as needed, and then click **OK**.

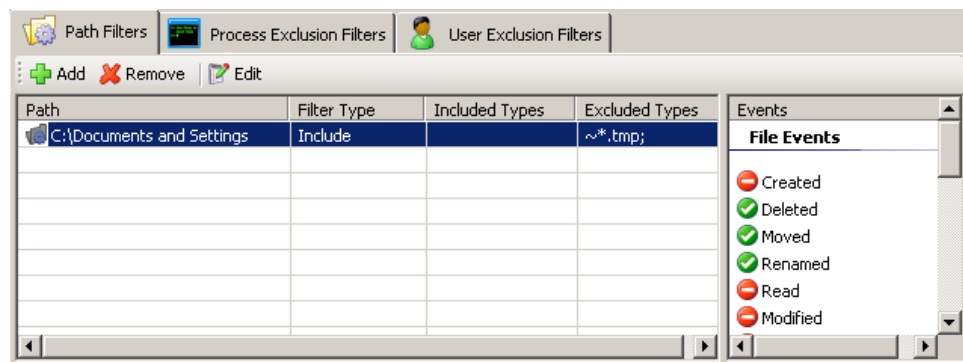
**Note:** To include or exclude events for files that have no extension, type \*. (asterisk, dot). If you then rename a file without an extension to a file name with an extension, you will see the event because it shows up for the file name with the extension.





The **Create New Auditing Filter** box displays the selections.



- To remove a selected file mask, click **Remove** in the appropriate area.
6. Click **OK**. The **Path Filters** tab displays the filter. The **Events** list displays the **File Events** first in the list, and then the **Folder Events**.
- Events included in the filter are indicated with .
  - Events excluded from the filter are indicated with .



- To edit a selected path filter, click  or double-click the path filter.
- To delete selected path filters, click .

## SETTING PROCESS EXCLUSION FILTERS

By default, all processes are included in the event collection. You can exclude specific processes from the event collection.

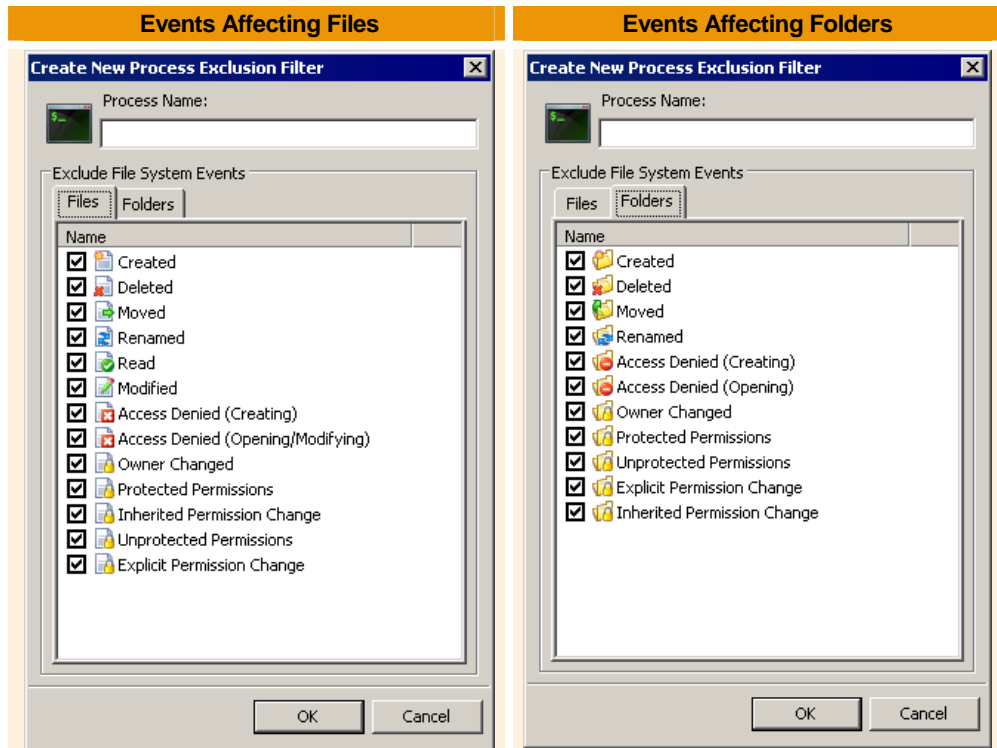
1. Open the **Process Exclusion Filters** tab to display the current filters.





Button	Description																					
	Add a new filter																					
	Remove selected filters																					
	Edit a selected filter																					
	Add filters that exclude all events for the following processes:																					
	<table border="0"> <tr> <td>abackup.exe</td> <td>ntbackup.exe</td> <td>slfsasvc.exe</td> </tr> <tr> <td>cavtray.exe</td> <td>NtrsScan.exe</td> <td>spybotsd.exe</td> </tr> <tr> <td>cobbu.exe</td> <td>rbserve.exe</td> <td>spysweeper.exe</td> </tr> <tr> <td>fsm32.exe</td> <td>rtvscan.exe</td> <td>webscanx.exe</td> </tr> <tr> <td>mcshield.exe</td> <td>savscan.exe</td> <td>winbackup.exe</td> </tr> <tr> <td>mssrv.exe</td> <td>slase.exe</td> <td>ws_rep.exe</td> </tr> <tr> <td>navapw32.exe</td> <td></td> <td></td> </tr> </table>	abackup.exe	ntbackup.exe	slfsasvc.exe	cavtray.exe	NtrsScan.exe	spybotsd.exe	cobbu.exe	rbserve.exe	spysweeper.exe	fsm32.exe	rtvscan.exe	webscanx.exe	mcshield.exe	savscan.exe	winbackup.exe	mssrv.exe	slase.exe	ws_rep.exe	navapw32.exe		
abackup.exe	ntbackup.exe	slfsasvc.exe																				
cavtray.exe	NtrsScan.exe	spybotsd.exe																				
cobbu.exe	rbserve.exe	spysweeper.exe																				
fsm32.exe	rtvscan.exe	webscanx.exe																				
mcshield.exe	savscan.exe	winbackup.exe																				
mssrv.exe	slase.exe	ws_rep.exe																				
navapw32.exe																						

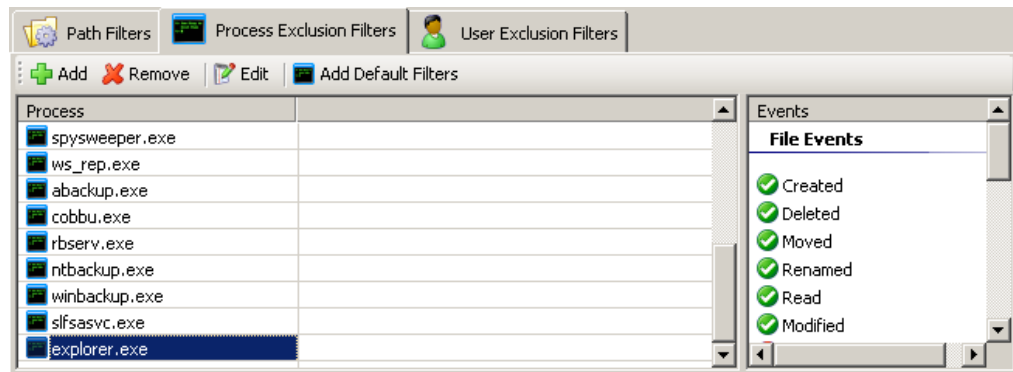
2. Click . The **Process Exclusion Filter** box lists the events you can choose to exclude from the process. By default, all events are selected.
3. In the **Process Name** box, type the name of the process, using wildcards as needed.

- In the **Exclude File System Events** area, select the file and folder events that you want to exclude from the process.



- Click **OK**. The **Process Exclusion Filters** tab displays the filter. The **Events** list displays the **File Events** first in the list, and then the **Folder Events**.

- Events included in the filter are indicated with .
- Events excluded from the filter are indicated with .

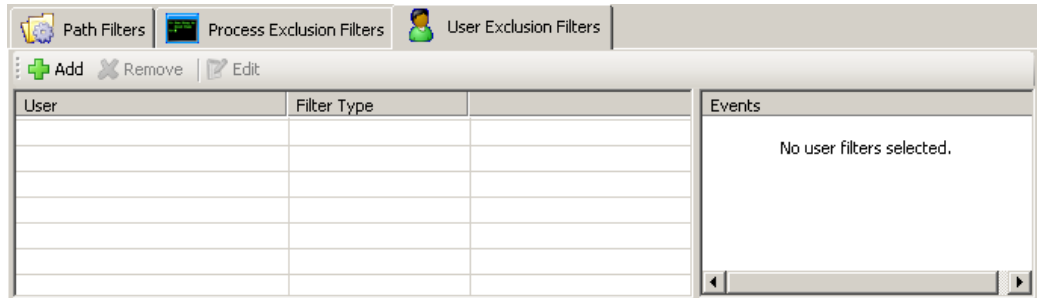


- To edit a selected process exclusion filter, click  or double-click the filter.
- To delete selected process exclusion filters, click .

## SETTING USER EXCLUSION FILTERS

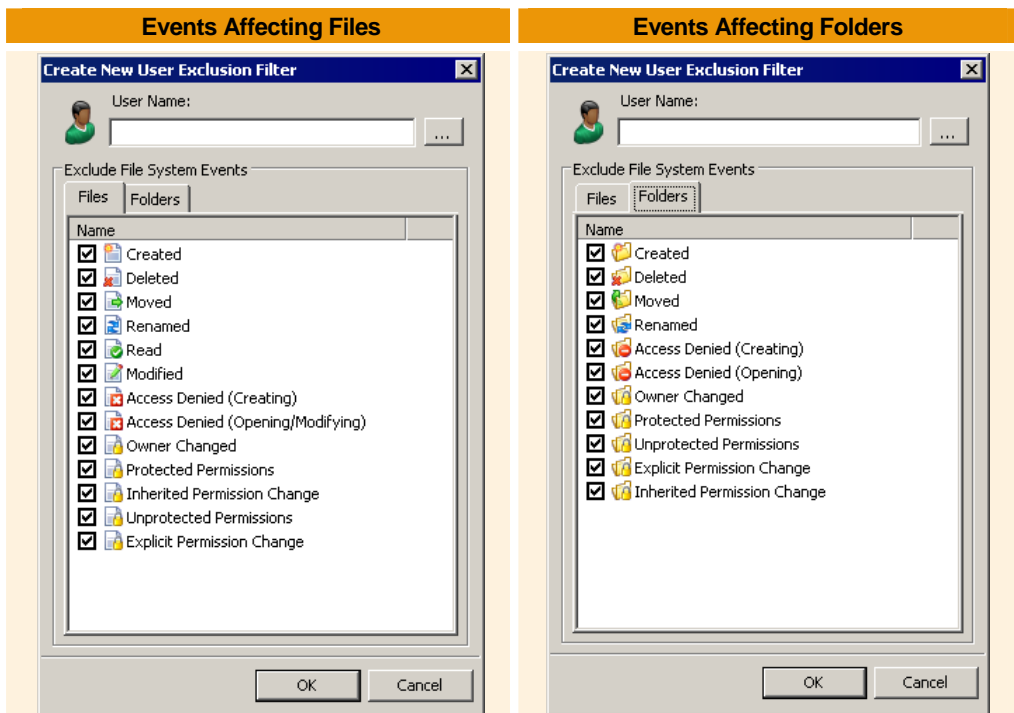
By default, all users are included in the event collection. You can exclude specific users from the event collection.



1. Open the **User Exclusion Filters** tab to display the current filters.

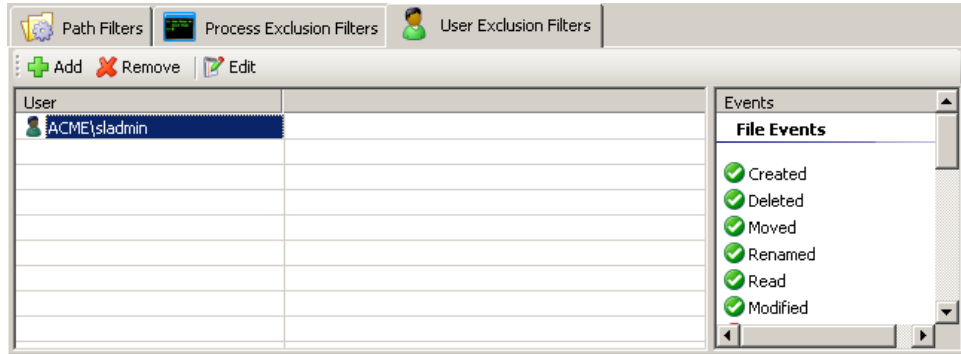


Button	Description
	Add a new filter
	Remove selected filters
	Edit the selected filter

2. Click . The **User Exclusion Filter** box appears. In the **User Name** box, type a user name, or click to locate a user name. You can use the \* wildcard when typing the user name.
3. In the **Exclude File System Events** area, select the file and folder events that you want to exclude for the selected user.



4. Click **OK**. The **User Exclusion Filters** tab displays the filter. The **Events** list displays the **File Events** first in the list, and then the **Folder Events**.
  - Events included in the filter are indicated with .
  - Events excluded from the filter are indicated with .



- To edit a selected user exclusion filter, click  or double-click the filter.
- To delete selected user exclusion filters, click .

## CHANGING DATABASE SETTINGS

The **Server Configuration** area for the selected server displays the database being used to collect the events. You can change to a different database, change the database authentication, or change the account used to write to the database.



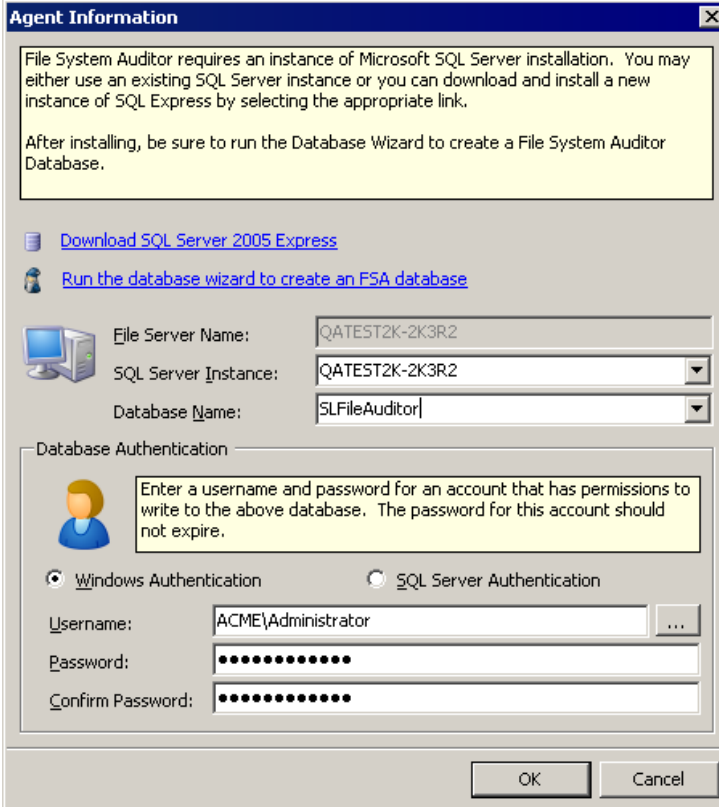
Server Configuration

**Database Settings**

Database Server:	VM4-WIN2KSVR	<a href="#">Change database settings</a>
Database Name:	FSA Audit Database	
Database Authentication Mode:	Windows	
User Name:	ACME\Administrator	

- ▶ To change any database settings, click [Change database settings](#) in the **Server Configuration** area for the selected server. The **Agent Information** box displays the current database settings. Make any necessary changes, and then click **OK**.

**Note:** You can create a new database, if necessary, by clicking [Run the database wizard to create an FSA database](#).



**Agent Information**

File System Auditor requires an instance of Microsoft SQL Server installation. You may either use an existing SQL Server instance or you can download and install a new instance of SQL Express by selecting the appropriate link.

After installing, be sure to run the Database Wizard to create a File System Auditor Database.

[Download SQL Server 2005 Express](#)

[Run the database wizard to create an FSA database](#)

File Server Name: QATEST2K-2K3R2

SQL Server Instance: QATEST2K-2K3R2

Database Name: SLFileAuditor

**Database Authentication**

Enter a username and password for an account that has permissions to write to the above database. The password for this account should not expire.

Windows Authentication  SQL Server Authentication

Username: ACME\Administrator

Password: .....

Confirm Password: .....

OK Cancel

## CHANGING ADVANCED SETTINGS

By default, the **Duplicate entry and suppression delta** is set to 10 seconds, and **Rename-and-delete pattern detection** and **Capture file share events** are turned on.

Advanced Settings		
Duplicate entry and suppression delta (seconds).	10	<a href="#">Change advanced settings</a>
Rename-and-delete pattern detection	ON	
Capture file share events (Create, Modify, Delete)	ON	

- ▶ To change the advanced settings, click [Change advanced settings](#) in the **Server Configuration area** for a selected file server. The **Advanced Settings** box displays the current settings.



### **Duplicate entry and suppression delta (seconds)**

By default, duplicate entries that occur within 10 seconds of each other are suppressed. Only the first entry appears in the event list. You can increase this value to reduce the length of the event list. Changes apply to new event collection only. Existing data is not affected.

### **Rename-and-delete pattern detection**

In some software applications, when saving a file, instead of overwriting the original file, the application saves to a temporary file, renames the original file, renames the temporary file to the current file name, and then deletes the temporary file. This process occurs so you can recover the original file. By default, File System Auditor detects this behavior and logs it in the database as a file modification on the file you were editing, rather than as a rename and delete process. To disable this detection, clear the check box.

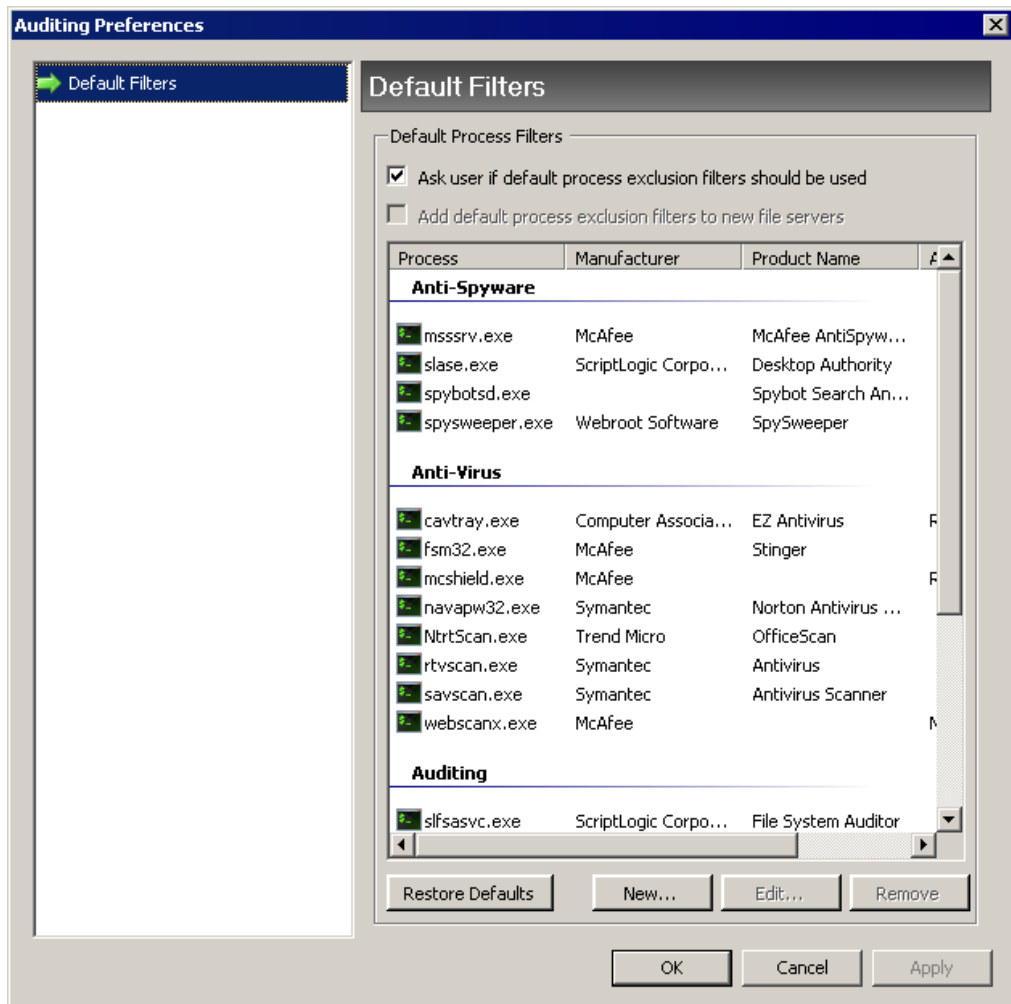
### **Capture file share events (Create, Modify, Delete)**

If you are running Windows Server 2003 or later, file share events are included in the data collection by default. To disable this feature, clear the check box.

## SETTING DEFAULT FILTERS

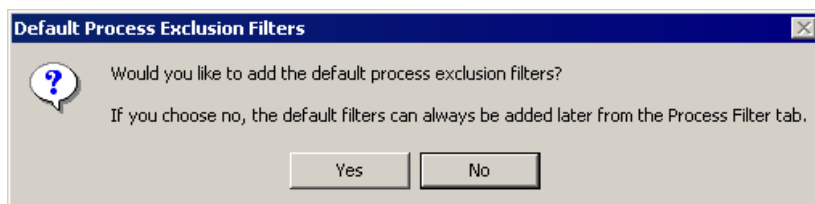
When adding file servers, users can choose to add default process exclusion filters. You can determine the processes in the exclusion filter

1. Choose **Preferences** from the **Tools** menu. The **Auditing Preferences** box displays the default filters.



- Ask user if default process exclusion filters should be used**

By default, the user is asked to include the default process exclusion filters when adding a file server. If you want to suppress the display of this message box, clear the check box.



**Add default process exclusion filters to new file servers**

To activate this check box, clear the **Ask user if default process exclusion filters should be used** check box. By default, process exclusion filters are added to new file servers. Clear the check box if you do not want the default filters added automatically.

Button	Description
New...	Add a new filter
Edit...	Edit a selected filter
Remove	Remove selected filters
Restore Defaults	Return the default filters list to the default:

### Default Filters

Process	Manufacturer	Product Name	Application Name
<b>Anti-Virus</b>			
cavtray.exe	Computer Associates	EZ Antivirus	Real-time AV Scanner
fsm32.exe	McAfee	Stinger	
mcshield.exe	McAfee		Real-time Scanner
Navapw32.exe	Symantec	Norton Antivirus Agent	
ntsrScan.exe	Trend Micro	OfficeScan	
rtvscan.exe	Symantec	Antivirus	
savscan.exe	Symantec	Antivirus Scanner	
webscanx.exe	McAfee		Network Traffic Monitor
<b>Anti-Spyware</b>			
mssrv.exe	McAfee	McAfee AntiSpyware	
slase.exe	ScriptLogic	Desktop Authority	
spybotsd.exe		Spybot Search and Destroy	
spysweeper.exe	Webroot Software	SpySweeper	
<b>Backup Software</b>			
abackup.exe	Modular Software	aBackup	
cobbu.exe	Cobian	Cobian Backup	
ntbackup.exe	Microsoft	Windows Backup	
rbserve.exe	Mike Lin	Rapid Backup	
winbackup.exe	UniBlue Systems Ltd.	WinBackup	
<b>File Replication</b>			
ws_rep.exe	Xosoft	WANSynchA Agent	
<b>Auditing</b>			
Slsasvc.exe	ScriptLogic Corporation	File System Auditor	ScriptLogic File System Auditor Service

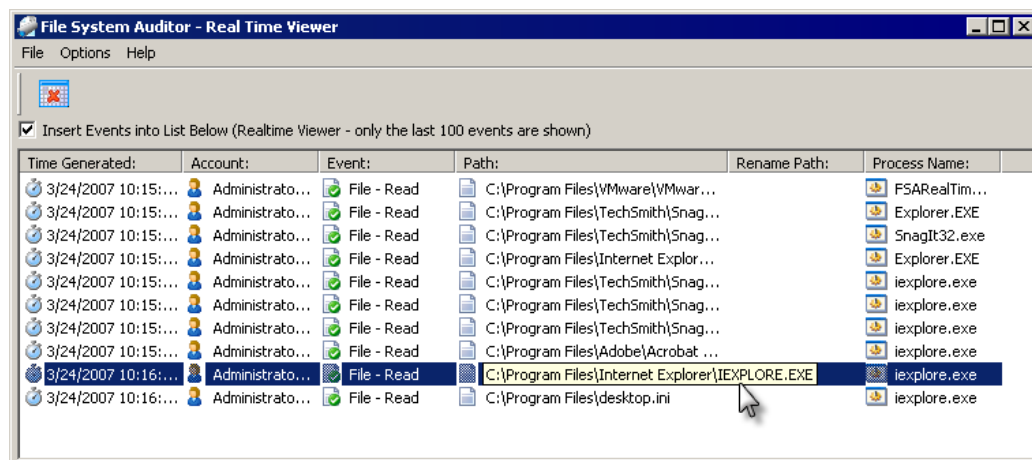
# Using the Real Time Viewer

Once you have set up File System Auditor, you can use the Real Time Viewer to look at events as they occur.

**Note:** You cannot view events that occur prior to the time you opened the Real Time Event Viewer. To view events that occurred in the past, use the Reporting Console.

## STARTING THE REAL TIME VIEWER

- ▶ On the computer where the Audit Agent is installed, click **Start**, point to **Programs** ▶ **ScriptLogic Corporation** ▶ **File System Auditor 2**, and then select **Real Time Viewer**. Events start to display as they occur.



You can size the columns to view the complete entry, or select a record and then point to the entry.

- Insert Events into List Below (Realtime Viewer – only the last 100 events are shown)**

By default, events begin to appear in the list as soon as you open the Real Time Viewer. To turn off the capture of events, clear the check box.

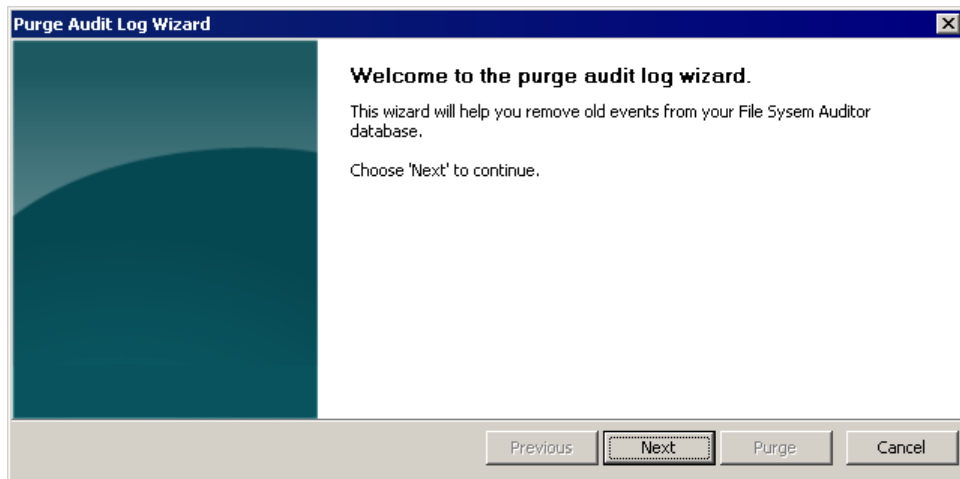
## Menus and Toolbar Icons

Menu	Menu Option	Icon	Description
File Exit	Exit		Close the Real Time Event Viewer
Options Clear List	Clear List		Clear the list of events
Help About File System Auditor...	About File System Auditor		View the copyright information

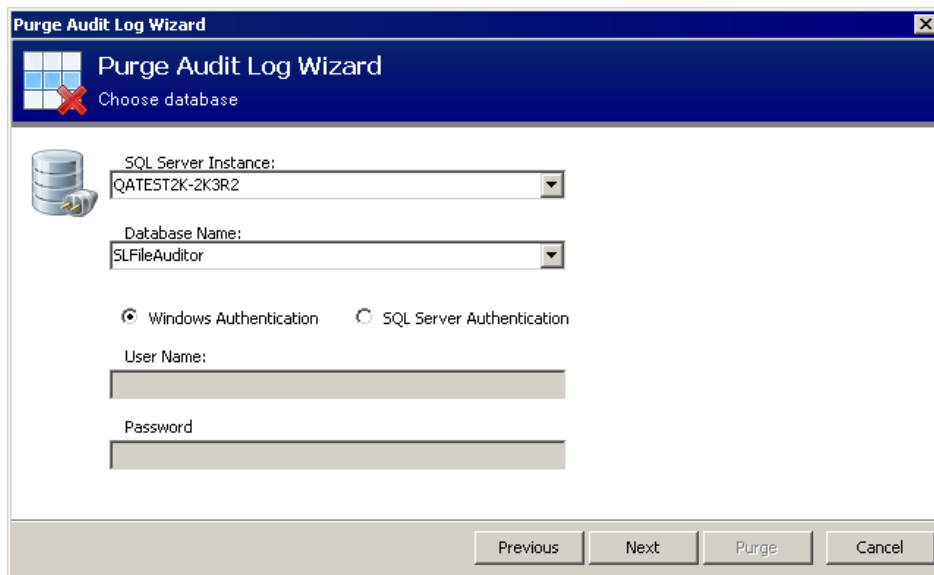
# Purging the Audit Database

The **Purge Database Wizard** helps you purge specific data from the auditing database.

1. From the **Tools** menu, choose **Purge Audit Log**. Alternatively, click [Purge Audit Log](#) on the **Start Page**. The **Purge Database Wizard** opens to the **Welcome** page.



2. Click **Next**. The **Choose database** page opens. Choose a server from the **SQL Server Instance** list. Choose a database from the **Database Name** list. Choose whether the database uses **Windows** or **SQL Server Authentication**. If you choose **SQL Server Authentication**, type the user name and password in the appropriate boxes.



3. Click **Next**. The **Select data/time range** page opens.

The screenshot shows the 'Purge Audit Log Wizard' dialog box with the title 'Select date/time range'. It contains two radio button options:

- Delete file system events for the following number of hours:
  - Hours:
- Delete file system events between the following times
  - Date / Time From:
 

August, 2009						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	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	29
30	31	1	2	3	4	5

 Today: 8/24/2009  
 Time:
  - Date / Time To:
 

August, 2009						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	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	29
30	31	1	2	3	4	5

 Today: 8/24/2009  
 Time:

At the bottom, there are four buttons: 'Previous', 'Next' (highlighted with a dashed border), 'Purge', and 'Cancel'.

- Delete file system events for the following number of hours**

By default, all file system events for the past hour are deleted. Type a number in the **Hours** box to increase or decrease the time range.

- Delete file system events between the following times**

Select to choose a date and time range. Click the calendar to select a date. Either type or scroll the values in the time boxes.

4. Click **Next**. The **Select user filters** page displays the users in the audit database.

**Include All Users**

By default, all users are included in the purge.

**Include Selected Users**

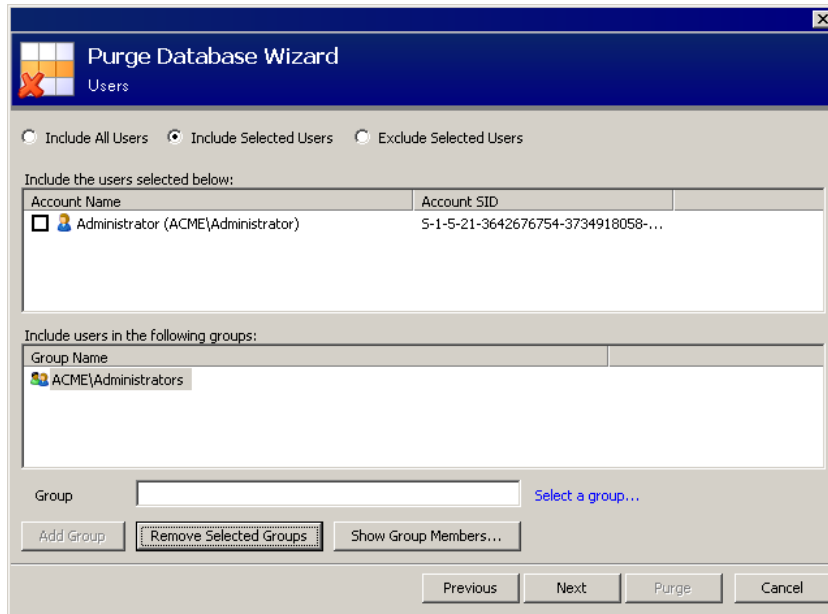
Select to activate the **Users** area. Select users in the list to include in the purge. You can also add groups to include in the purge. See *Adding a Group*.

**Exclude Selected Users**

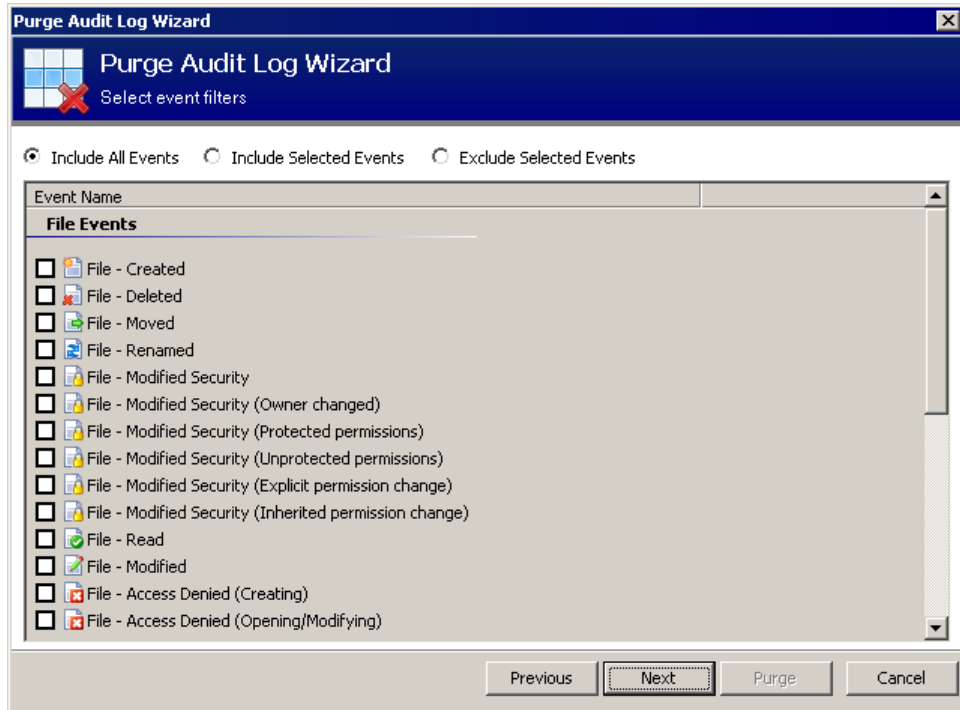
Select to activate the **Users** area. Select users in the list to exclude from the purge. You can also add groups to exclude from the purge. See *Adding a Group*.

### Adding a Group

- a. Type a group name in the **Group** box. Alternatively, click [Select a group](#), and then search for a group to add.
- b. Click **Add Group**. The name displays in the list.
  - To show a selected groups members, click **Show Group Members**.
  - To remove selected groups from the list, click **Remove Selected Groups**.



5. Click **Next**. The **Select event filters** page lists all the events present in the Audit Database.



**Include All Events**

By default, all events are included in the purge.

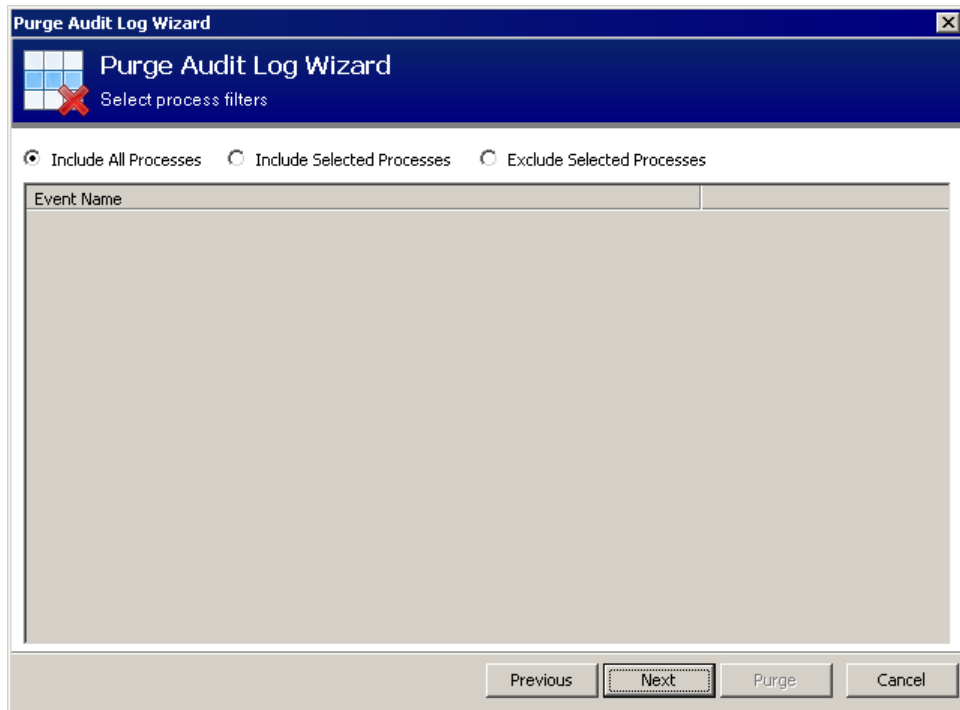
**Include Selected Events**

Select to activate the **Events** area. Select events in the list to include in the purge.

**Exclude Selected Events**

Select to activate the **Events** area. Select events in the list to exclude from the purge.

6. Click **Next**. The **Processes** box lists the processes included in the auditing database.



**Include All Processes**

By default, all processes are included in the purge.

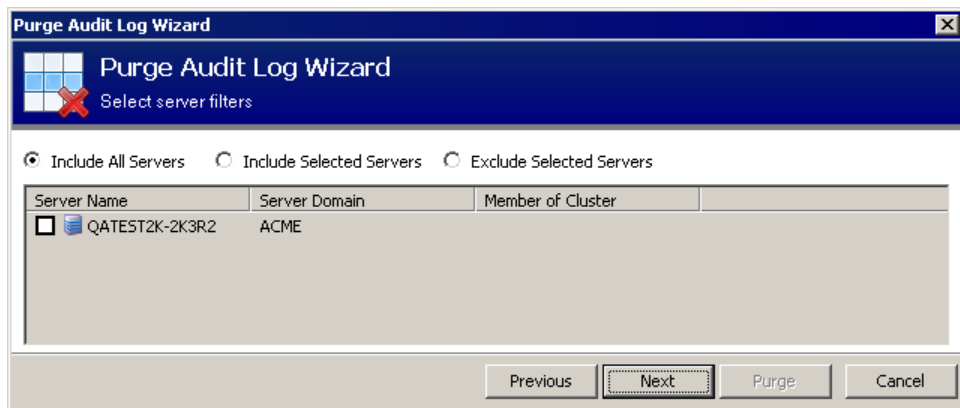
**Include Selected Processes**

Select to activate the **Processes** area. Select processes in the list to include in the purge.

**Exclude Selected Processes**

Select to activate the **Processes** area. Select processes in the list to exclude from the purge.

7. Click **Next**. The **Select server filters** page displays the servers in the Audit Database.



**Include All Servers**

By default, all servers are included in the purge.

**Include Selected Servers**

Select to activate the **Servers** area. Select servers in the list to include in the purge.

**Exclude Selected Servers**

Select to activate the **Servers** area. Select servers in the list to exclude from the purge.

8. Click **Next**. The **Select workstation** page displays the workstations in the auditing database.

The screenshot shows the 'Purge Audit Log Wizard' dialog box with the title 'Select workstation filters'. It features three radio buttons: 'Include All Workstations' (selected), 'Include Selected Workstations', and 'Exclude Selected Workstations'. Below these is a table with two columns: 'Workstation Name' and 'Workstation IP'. The table is currently empty. At the bottom, there are four buttons: 'Previous', 'Next' (highlighted with a dashed border), 'Purge', and 'Cancel'.

**Include All Workstations**

By default, all workstations are included in the purge.

**Include Selected Workstations**

Select to activate the **Workstation** area. Select workstations in the list to include in the purge.

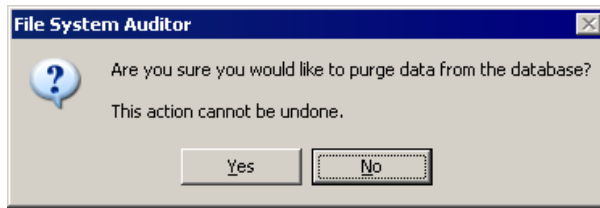
**Exclude Selected Workstations**

Select to activate the **Workstations** area. Select workstations in the list to exclude from the purge.

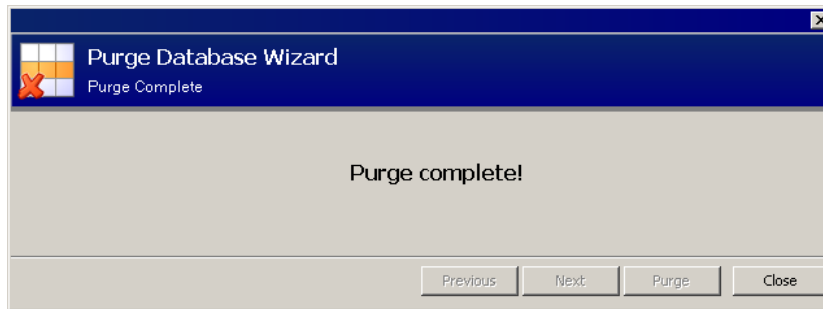
9. Click **Next**. The **Preview results** page displays the selections you made. The number of events to be purged displays in the **Events to be Purged** area. To examine the actual data, click [Display first 1000 events](#).

The screenshot shows the 'Purge Audit Log Wizard' dialog box with the title 'Preview results'. It contains several input fields for filtering: 'Date/Time Range' (The past 1 hour from Monday, August 24, 2009 12:50 PM), 'Users' ([All Users]), 'Events' ([All Events]), 'Paths' ([All Paths]), 'Processes' ([All Processes]), 'Servers' ([All Servers]), and 'Workstations' ([All Workstations]). Below these fields is a link that says 'Display first 1000 events'. Underneath is a section titled 'Events to be Purged' which contains a table with the following columns: 'Server Name', 'Time Generated', 'Account', 'Event', and 'Path'. The table is empty and contains the text 'No events were found.' At the bottom, there are four buttons: 'Previous', 'Next' (highlighted with a dashed border), 'Purge', and 'Cancel'.

10. Click **Purge**. A message asks for confirmation.



11. Click **Yes** to continue with the purge process. The **Purge Complete** box displays.



12. Click **Close**.

## PURGING DATA FROM THE COMMAND LINE

### Usage

```
PurgeData.exe [/? |
               [/CS="<conn_str>"
               [/Date="<date>" | /Days="<number_of_days>"]]]
```

### where

```
/?                Display this help message

<conn_str>       Connection string for DB
                  e.g. "Server=SqlServer1;Database=SLFileAuditor;
                  Integrated Security=SSPI;Asynchronous Processing=true"

<date>           All events older than the specified date
                  (but not including) are removed from the database.

<number_of_days> All events that were happened at least
                  the number of days specified prior to
                  the current date are removed from the database.
                  If 0 specified all the events are removed.
```

### Example

```
C:\Program Files\ScriptLogic Corporation\File System Auditor 2\PurgeData.exe
/CS="Server=VM2K3FSAAGENT\FSA;Database=SLFileAuditor2; Asynchronous
Processing=true;Integrated Security=SSPI" /Days=5
```

## Using Interactive Mode

---

Run PurgeData.exe without arguments to begin interactive mode.

```
C:\Program Files\ScriptLogic Corporation\File System Auditor 2>purgedata.exe

FSA Data Purge Tool
=====
Enter the SQL Server Instance:VM2K3FSAAGENT\FSA

Enter the Database Name:SLFileAuditor2

Select the SQL Server authentication
  1 -- Windows authentication
  2 -- SQL Server authentication
Enter number, then press (ENTER) to continue (1): 1

Select the events to purge
  1 -- All events at least a specific number of days old
  2 -- All events older than a given date
Enter number, then press (ENTER) to continue (1): 1

You selected to remove all events at least a specific number of days old.
Please enter the number of days (10): 5

Preparing to purge data using the following parameters:
  Purge all events at least 5 days old
```

### Command Line Example

```
C:\Program Files\ScriptLogic Corporation\File System Auditor 2\PurgeData.exe
/CS="Server=VM2K3FSAAGENT\FSA;Database=SLFileAuditor2; Asynchronous
Processing=true;Integrated Security=SSPI" /Days=5
```

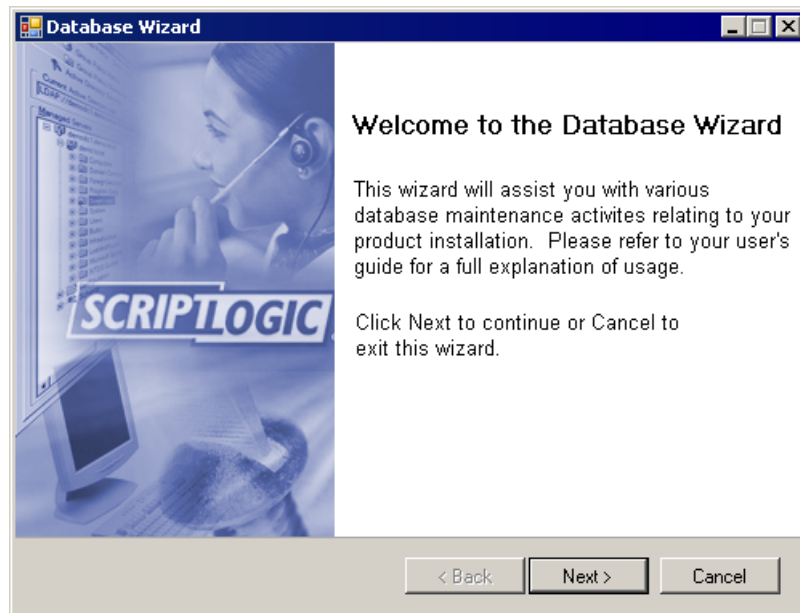
# Managing the Auditing Database

**Important:** You must create an auditing database before you can perform any tasks using File System Auditor.

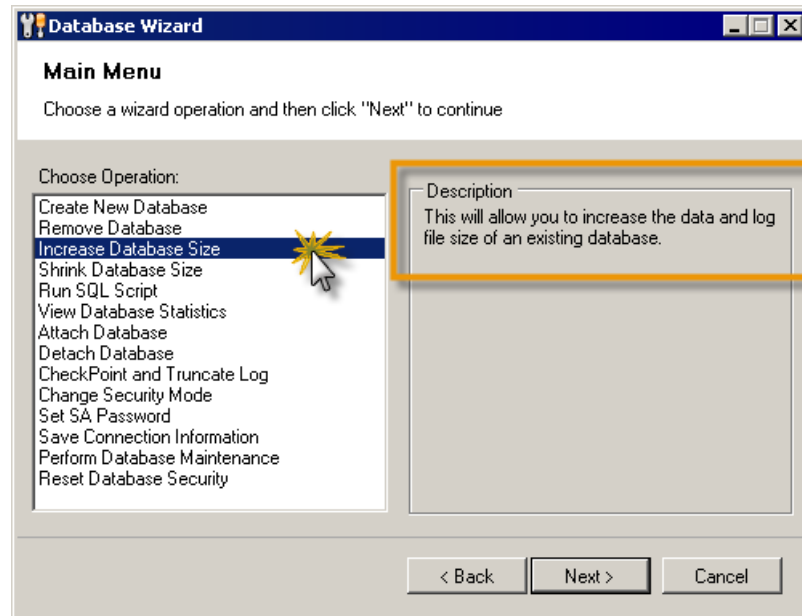
## STARTING THE DATABASE WIZARD

- ▶ Click **Start**, point to **Programs** ▶ **ScriptLogic Corporation** ▶ **File System Auditor 2**, and then select **Database Wizard**.
- ▶ Choose **Database Wizard** from the **Tools** menu on the **Agent Configuration Console Start Page**. See *Error! Reference source not found.*

The **Welcome to the Database Wizard** box appears.



Click **Next** to display the main menu. When you choose an operation from the list, a brief description displays.

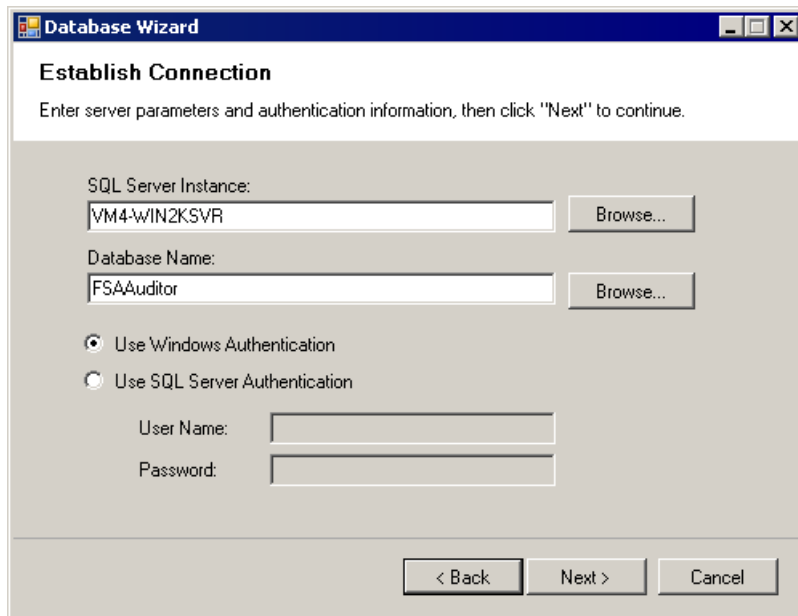


Operation	Description
Create New Database	Create a new database.
Remove Database	Remove (drop) an existing database.
Increase Database Size	Increase data and log file size of an existing database.
Shrink Database Size	Decrease the data and log file size of an existing database.
Run SQL Script	Run any SQL script.
View Database Statistics	View statistics for an existing database.
Attach Database	Attach an existing database.
Detach Database	Detach an existing database.
CheckPoint and Truncate Log	Perform a checkpoint operation on the specified database. This checks to see if there are 'dirty' pages in memory that need to be flushed to the hard drive. The log file will be marked accordingly and then a truncate operation will be performed.
Change Security Mode	Change the security mode of a SQL server instance to integrated mode (Windows only) or mixed mode (Windows and SQL Server).
Set SA Password	Change the current SA login account password for SQL Server.
Save Connection Information	Save the database-related connection information into the registry.
Perform Database Maintenance	Perform several tasks, such as Rebuilding Indexes, Resetting Identity Columns, and Performing Consistency Checks.
Reset Database Security	Reset security related principles, such as roles, logins, and permissions to their default settings.

## CREATING A NEW DATABASE

**Important:** You must create an auditing database before you can perform any tasks using File System Auditor.

1. From the **Database Wizard Main Menu**, select **Create New Database**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server that is running Microsoft SQL Server, or click **Browse...** to locate the server.
4. In the **Database Name** box, type the name of the auditing database to create. To view existing database names, click **Browse...**.



The screenshot shows the 'Database Wizard' dialog box with the 'Establish Connection' step. The title bar reads 'Database Wizard'. Below the title bar, the text 'Establish Connection' is displayed, followed by the instruction: 'Enter server parameters and authentication information, then click "Next" to continue.' The dialog contains two text input fields: 'SQL Server Instance:' with the value 'VM4-WIN2KSVR' and a 'Browse...' button to its right; and 'Database Name:' with the value 'FSAAuditor' and a 'Browse...' button to its right. Below these fields are two radio button options: 'Use Windows Authentication' (which is selected) and 'Use SQL Server Authentication'. Under the 'Use SQL Server Authentication' option, there are two text input fields: 'User Name:' and 'Password:'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. The default selection for authentication is **Use Windows Authentication**. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.

- Click **Next**. The **Enter Database Settings** box displays the default initial sizes for the database (\*.mdf) and log (\*.ldf) files.

The screenshot shows the 'Enter Database Settings' dialog box. It has a title bar 'Database Wizard' and a subtitle 'Enter Database Settings'. Below the subtitle is the instruction 'Choose create database settings and then click "Next" to continue'. The dialog is divided into three main sections: 'File Sizes', 'Security Groups', and 'File Paths'. In the 'File Sizes' section, there are two input boxes: 'Initial Database Size' and 'Initial Log File Size', both containing the value '50' and followed by 'MB'. In the 'Security Groups' section, there is a checked checkbox 'Create default security groups as...' and three radio buttons: 'Local Group (Non DC)' (selected), 'Global', and 'Domain Local'. In the 'File Paths' section, there is an unchecked checkbox 'Override Default File Locations' and two empty text boxes labeled 'Data File Path' and 'Log File Path'. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

#### File Sizes

By default, the database and log files are created at 50 MB each. If you want to change the default, type a value in the appropriate box. The data and log files grow automatically starting from the initial value specified here. You can change the size of the data file at a later time. See *Increasing Database Size*.

#### Create default security groups

By default, default security groups are created as local groups on non-domain controllers only. You can select to create default domain global or local groups. To bypass the creation of default security groups, clear the check box.

#### Override Default File Locations

Select to create the database transaction log files in a location other than the default location, Type the physical path in the appropriate boxes. Express the path as a logical path and not as a UNC path.

- Click **Next**. The **Create New Database** box displays the database name.
- Click **Finish**.

## REMOVING AN EXISTING DATABASE

**Caution:** Removing a database permanently removes it from the system. If you just want to detach the database, see *Detaching a Database*.

**Note:** The database cannot be in use. Exit File System Auditor, if necessary.

1. From the **Database Wizard Main Menu**, select **Remove Database**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click  to locate the server.
4. In the **Database Name** box, type the name of the database, or click  to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.
6. Click **Next**. The **Remove Database** box displays the name of the database you chose.
7. Click **Finish**.

## INCREASING DATABASE SIZE

Microsoft SQL Server automatically increases the size of the database file, which can sometimes cause performance issues. To avoid this, you may want to increase the size of the database manually.

1. From the **Database Wizard Main Menu**, select **Increase Database Size**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click  to locate the server.
4. In the **Database Name** box, type the name of the database, or click  to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.

- Click **Next**. The **Enter Database Size** box displays the current combined size of the database and log files in the **Total Database Size** area.

- In the **Enter New Database Size** box, type a numeric value in megabytes that is greater than the existing value and represents the size of the database file.

**Note:** Enter the total size of the database, not the additional size of the database. For example, if the database is 50MB and you want to add another 50MB, then you would enter 100 as the new database size.

**Note:** The log file is not affected by this process.

- Click **Next**. The **Increase Database Size** box displays the database you chose.
- Click **Finish**.

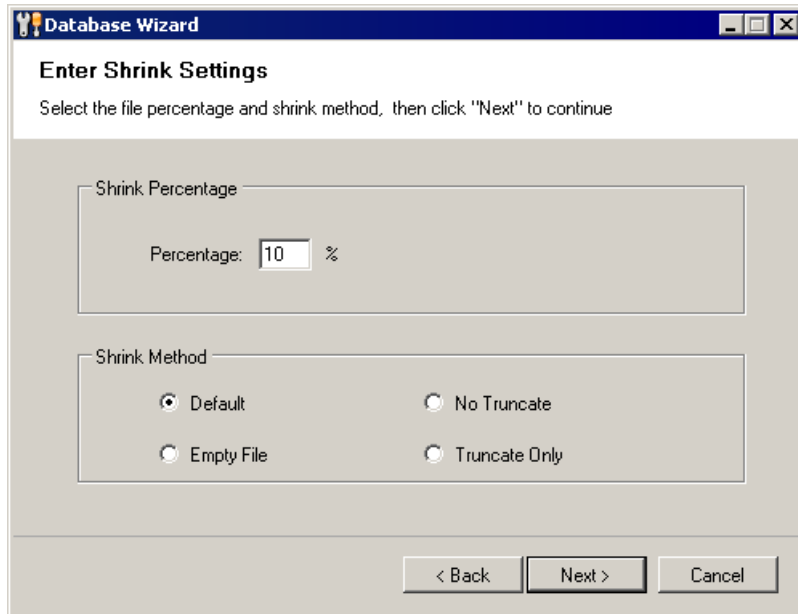
## SHRINKING A DATABASE

If you need to reclaim space, you can shrink the database, which reduces the size of the database to the minimum amount based on the size of the data.

**Note:** Another database to monitor is the tempdb database, which is the working area that Microsoft SQL Server uses to process queries and perform other actions. You might shrink the tempdb database periodically to reclaim the disk space that is no longer needed.

- From the **Database Wizard Main Menu**, select **Shrink Database Size**.
- Click **Next**. The **Establish Connection** box appears.
- In the **SQL Server Instance** box, type the name of the server where the database is located, or click **Browse...** to locate the server.

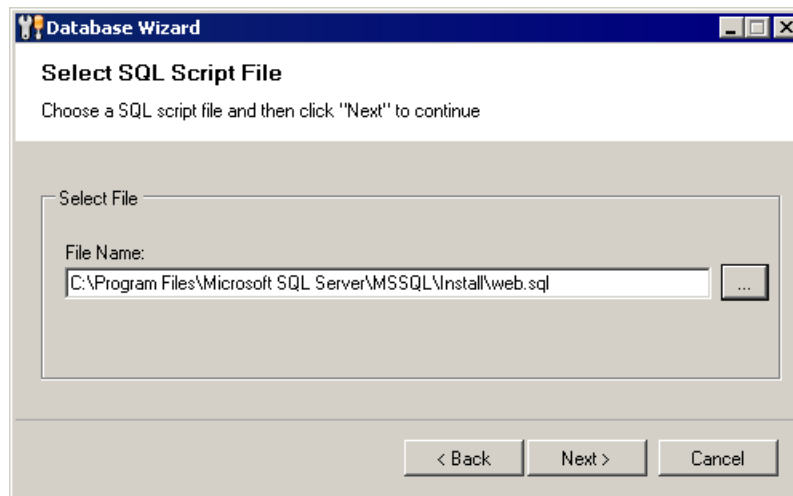
4. In the **Database Name** box, type the name of the database, or click **Browse...** to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.
6. Click **Next**. The **Enter Shrink Settings** box appears.



7. In the **Shrink Percentage** box, type the percentage by which to shrink the database. By default, the database shrinks by 10%.
8. In the **Shrink Method** area, select a method to use when shrinking the database.
  - Default**  
Data at the end of the file is moved to earlier in the file. File is truncated by the value in the **Shrink Percentage** box.
  - Empty File**  
Remove all data from the database and reduce the size by the value in the **Shrink Percentage** box.
  - No Truncate**  
Data at the end of the file is moved to earlier in the file. Database size is reduced by the value in the **Shrink Percentage** box.
  - Truncate Only**  
File is truncated by the value in the **Shrink Percentage** box. Data is not moved.
9. Click **Next**. The **Shrink Database** box displays the database you chose.
10. Click **Finish**.

## RUNNING AN SQL SCRIPT

1. From the **Database Wizard Main Menu**, select **Run SQL Script**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click **Browse...** to locate the server.
4. In the **Database Name** box, type the name of the database, or click **Browse...** to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.
6. Click **Next**. The **Select SQL Script File** box appears.
7. In the **File Name** box, type the full path to the SQL Script File (\*.sql) or click **...** to locate the file.



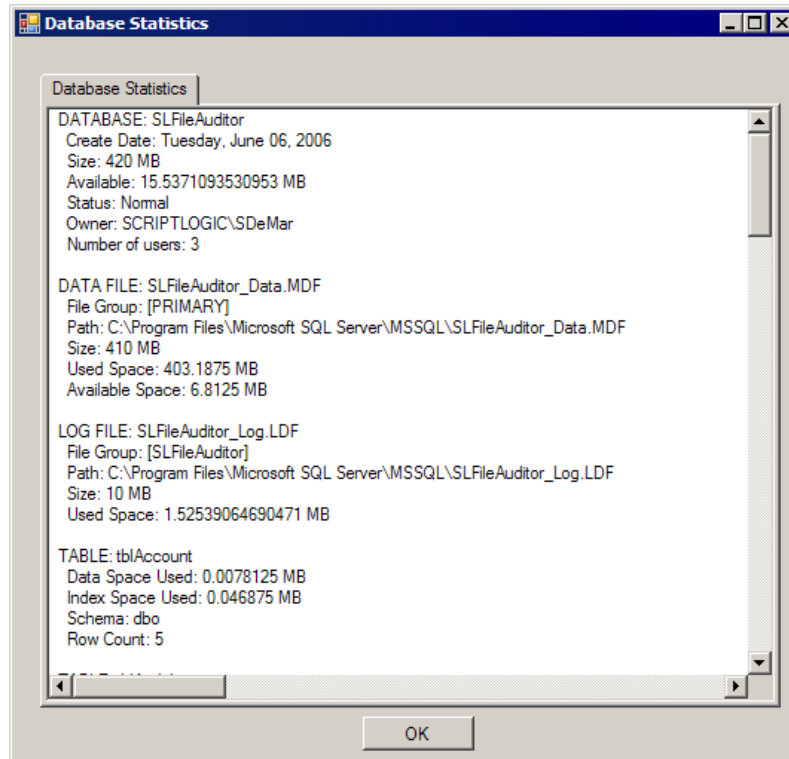
8. Click **Next**. The **Run SQL Script** box displays the path to the file you chose.
9. Click **Finish**.

## VIEWING DATABASE STATISTICS

View the current database settings and statistics on the size of the database and each table in the database, which is helpful for diagnosing problems in the event that SQL Server is not functioning properly.

1. From the **Database Wizard Main Menu**, select **View Database Statistics**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click **Browse...** to locate the server.
4. In the **Database Name** box, type the name of the database, or click **Browse...** to locate the database.

5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.
6. Click **Next**. The **View Database Statistics** box displays the database you chose.
7. Click **Finish**. The **Database Statistics** box displays the database statistics.

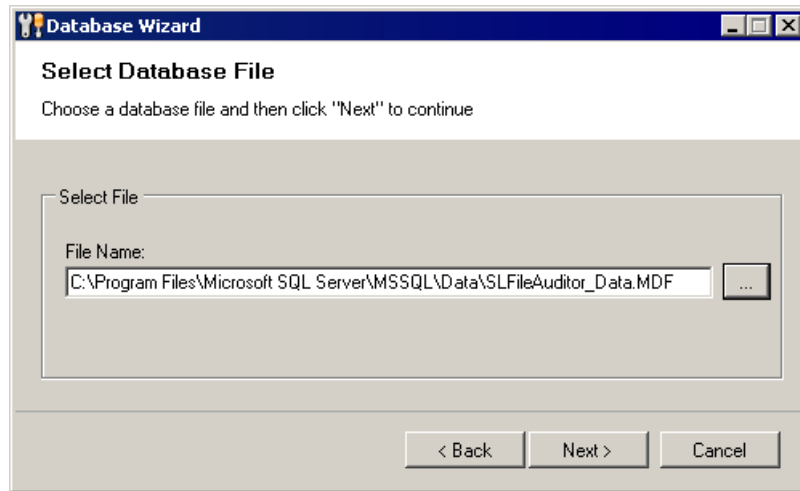


## ATTACHING A DATABASE

When you create a database, it is automatically attached to File System Auditor. If you detach a database, you can attach it again to use it.

1. From the **Database Wizard Main Menu**, select **Attach Database**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click **Browse...** to locate the server.
4. In the **Database Name** box, type the name of the database, or click **Browse...** to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.
6. Click **Next**. The **Select Database File** box appears.

- In the **File Name** box, type the full path to the data file or click  to locate the data file to attach.



- Click **Next**. The **Attach Database** box displays the database you chose.
- Click **Finish**.

## DETACHING A DATABASE

Detaching a database removes it from File System Auditor, but does not delete it from the system. To permanently delete a database, see *Removing an Existing Database*.

**Note:** The database cannot be in use. Exit File System Auditor, if necessary.

- From the **Database Wizard Main Menu**, select **Detach Database**.
- Click **Next**. The **Establish Connection** box appears.
- In the **SQL Server Instance** box, type the name of the server where the database is located, or click  to locate the server.
- In the **Database Name** box, type the name of the database, or click  to locate the database.
- Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.
- Click **Next**. The **Detach Database** box displays the database you chose.
- Click **Finish**.

## TRUNCATING THE TRANSACTION LOG

When a transaction log becomes full, it forces the database to expand it. However, since File System Auditor does not use the transaction log, and there is no way to disable the transaction log for a database, you may need to periodically truncate the transaction log to tell the SQL Server that the data is no longer needed.

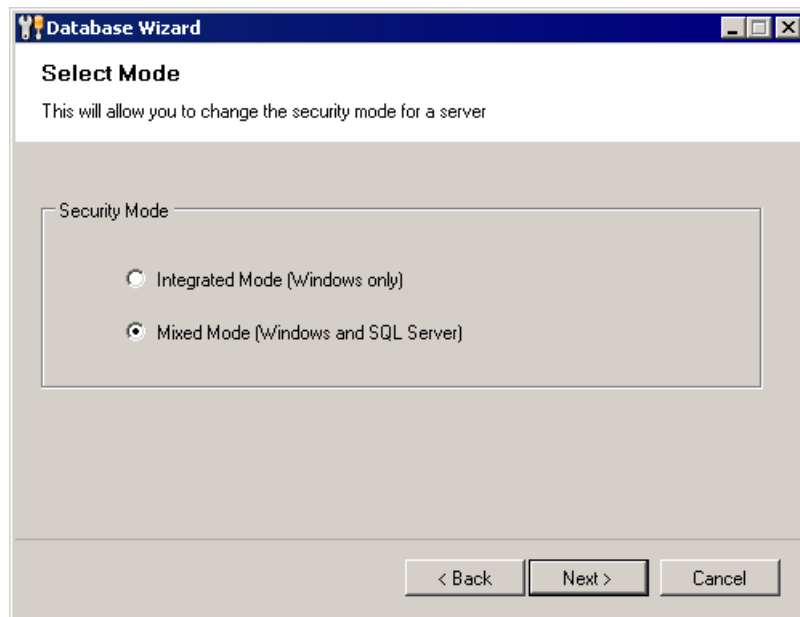
1. From the **Database Wizard Main Menu**, select **Checkpoint and Truncate Log**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click  to locate the server.
4. In the **Database Name** box, type the name of the database, or click  to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.
6. Click **Next**. The **Checkpoint and Truncate Log** box displays the database you chose.
7. Click **Finish**.

## CHANGING THE SECURITY MODE

Depending on your system setup, you may want to switch the security mode on the SQL Server to enhance performance of some applications. For example, if you have Active Administrator™ set up to use one mode and File System Auditor to use the other, you may want to switch the security mode on the SQL Server to **Mixed Mode (Windows and SQL Server)**.

1. From the **Database Wizard Main Menu**, select **Change Security Mode**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click  to locate the server.
4. In the **Database Name** box, type the name of the database, or click  to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.

6. Click **Next**. The **Select Mode** box displays the security mode options.



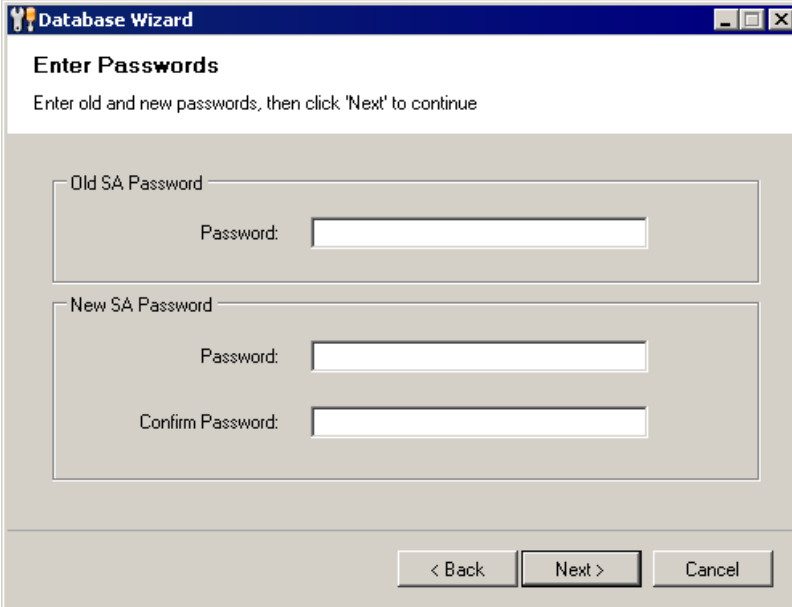
7. Select the security mode.
  - Integrated Mode (Windows only)**  
Select to use the Integrated Mode (Windows only) on the selected server.
  - Mixed Mode (Windows and SQL Server)**  
Select to use Mixed Mode (Windows and SQL Server) on the selected server.
8. Click **Next**. The **Change Security Mode** box displays the server you chose.
9. Click **Finish**.

## SETTING THE SA PASSWORD

If the SQL Server is set up in mixed mode (SQL Server and Windows), set a password for the SQL Server administrator (sa account). You also can use this option to change the password for security purposes.

1. From the **Database Wizard Main Menu**, select **Set SA Password**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click **Browse...** to locate the server.
4. In the **Database Name** box, type the name of the database, or click **Browse...** to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.

6. Click **Next**. The **Enter Passwords** box appears.



The screenshot shows a dialog box titled "Database Wizard" with a sub-header "Enter Passwords". Below the sub-header is the instruction "Enter old and new passwords, then click 'Next' to continue". The dialog contains two main sections: "Old SA Password" and "New SA Password". Each section has a "Password:" label followed by a text input field. The "New SA Password" section also includes a "Confirm Password:" label followed by another text input field. At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

7. In the **Old SA Password** box, type the existing password.
8. In the **New SA Password** box, type the new password.
9. In the **Confirm Password** box, retype the new password.
10. Click **Next**. The **Set SA Password** box displays the server you chose.
11. Click **Finish**.

## SAVING CONNECTION INFORMATION

This option writes the database connection settings to the registry.

1. From the **Database Wizard Main Menu**, select **Save Connection Information**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click **Browse...** to locate the server.
4. In the **Database Name** box, type the name of the database, or click **Browse...** to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.
6. Click **Next**. The **Save Connection Information** box displays the registry key to which the database connection settings is written.
7. Click **Finish**.

## PERFORMING DATABASE MAINTENANCE

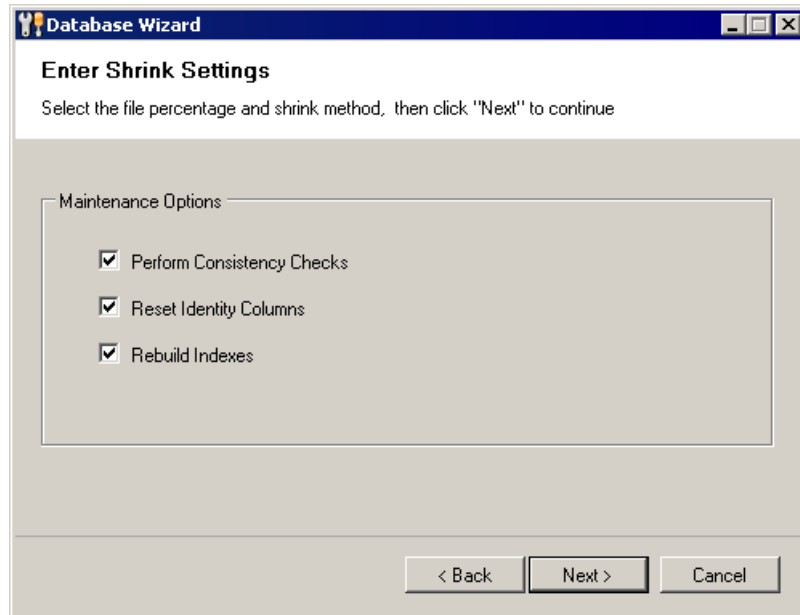
Performing regular database maintenance can help maintain the performance of SQL Server. Run this action if you feel SQL Server is not performing at the same level it once did. You can select to rebuild indexes, reset identity columns, and perform consistency checks.

The **Perform Database Maintenance** action performs the following Database Consistency Checker (DBCC) commands.

DBCC Command	Description
CHECKCATALOG	Checks the system tables for consistency.
CHECKFILEGROUP	Performs a physical consistency check on all indexes and tables.
CHECKTABLE REPAIR_REBUILD	Performs a consistency check of the data in each table and rebuilds indexes if necessary.
CHECKIDENT	Checks the identity values of each table and resets them if necessary.
CHECKINDEX	Checks the physical database allocation of indexes and repairs if necessary.

1. From the **Database Wizard Main Menu**, select **Perform Database Maintenance**.
2. Click **Next**. The **Establish Connection** box appears.
3. In the **SQL Server Instance** box, type the name of the server where the database is located, or click  to locate the server.
4. In the **Database Name** box, type the name of the database, or click  to locate the database.
5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.

- Click **Next**. The **Perform Database Maintenance** box appears.



- Choose the maintenance options to perform. By default all options are selected.

**Perform Consistency Checks**

Select to run CHECKCATALOG, CHECKFILEGROUP, CHECKTABLE REPAIR\_REBUILD, and CHECKINDEX.

**Reset Identify Columns**

Select to run CHECKIDENT.

**Rebuild Indexes**

Select to run CHECKINDEX and CHECKTABLE REPAIR\_REBUILD.

- Click **Next**. The **Perform Database Maintenance** box displays the database and actions to be performed.
- Click **Finish**.

## RESETTING DATABASE SECURITY

Resetting the database security re-creates the Windows NT security groups, database roles, and logins, and then re-applies the default security to all tables/functions/stored procedures in the auditing database.

- From the **Database Wizard Main Menu**, select **Reset Database Security**.
- Click **Next**. The **Establish Connection** box appears.
- In the **SQL Server Instance** box, type the name of the server where the database is located, or click **Browse...** to locate the server.
- In the **Database Name** box, type the name of the database, or click **Browse...** to locate the database.

5. Choose whether Windows or SQL Server Authentication is used. If you select **Use SQL Server Authentication**, type the name of the SQL Server user account in the **User Name** box and the password in the **Password** box.
6. Click **Next**. The **Reset Database Security** box displays the database you chose.
7. Click **Finish**.

### MOVING A DATABASE TO ANOTHER SERVER

If you need to move a database from one server to another, we recommend using the Microsoft SQL Server 2000/2005/2008 Client Utilities, SQL 2005 Management Studio, or Management Studio Express for SQL 2005 Express.

**Note:** Client utilities are available only on a full version of SQL Server, which is not included with File System Auditor.

1. Open SQL Enterprise Manager.
2. Locate the database to move, right-click, point to **All Tasks**, and then choose **Detach Database**.
3. Open the folder where the data files for that database are stored, and then copy the \*.mdf and \*.ldf files for that database to the new server.
4. In SQL Enterprise Manager, navigate to the new server where you want to attach the database, right-click on the **Database** folder, point to **All Tasks**, and then choose **Attach Database**.
5. Select the \*.mdf file you just copied to the computer, and then complete the operation.

# 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

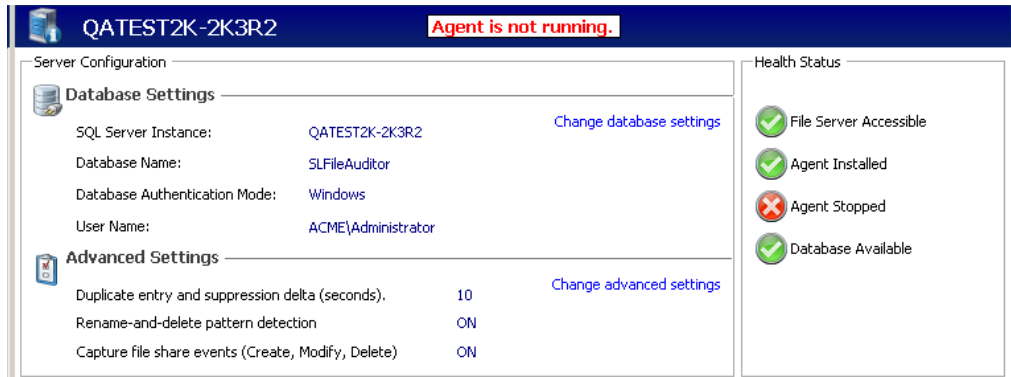
Use caution if including **File-Read** or **File-Access Denied (Opening/ Modifying)** events as the number of events recorded by File System Auditor may overwhelm the auditing database. Any focus on a file in Windows Explorer, such as a mouse-over or using the arrow keys to scroll through the directory, 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.

## REMOVING A FILE SERVER

When you remove a file server from the list of servers, the Audit Agent is uninstalled as part of the process. To add the server back to the list, see *Adding File Servers*.

1. Select the server from the list of file servers, and then click . Alternatively, choose **Stop Auditing** from the **Server** menu.



2. With the server still selected, click . Alternatively, choose **Remove File Server** from the **File** menu.
3. To remove the server, click **Yes**. During the process of removing the server, the Audit Agent is uninstalled.

## UNINSTALLING THE AUDIT AGENT

You can uninstall the Audit Agent without removing a file server from the list. To reinstall the Audit Agent on the file server, add the file server again. See *Adding File Servers*.

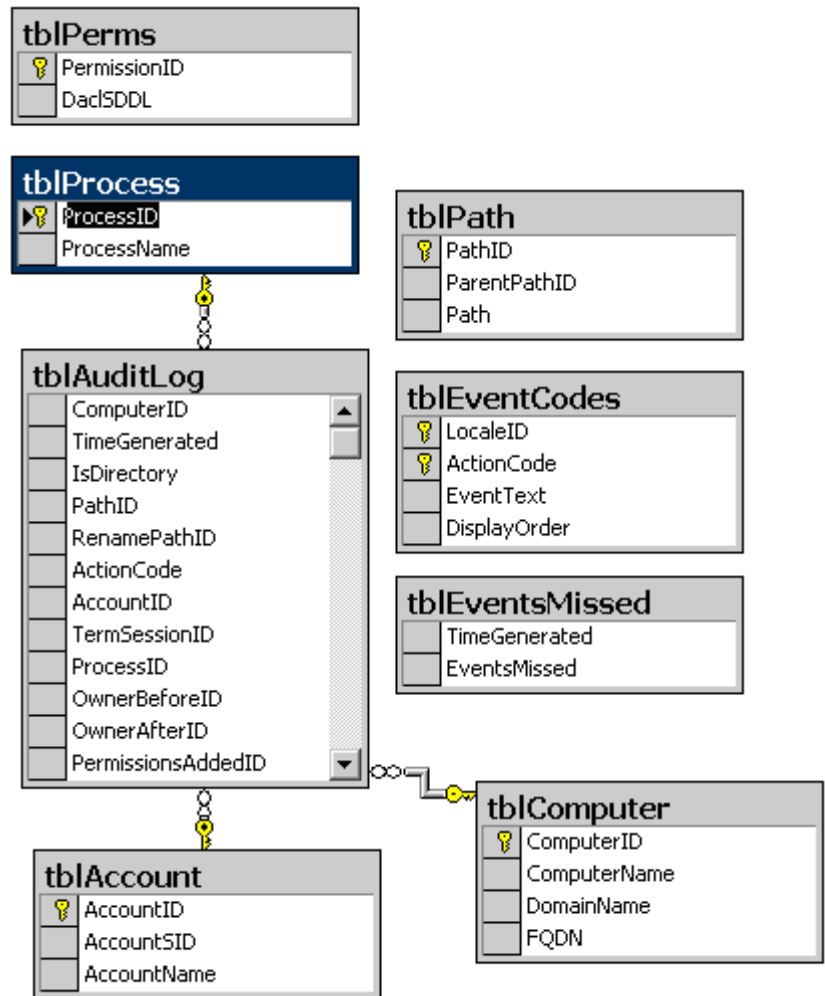
1. From the Windows Control Panel, choose **Add/Remove Programs**.
2. Select **File System Auditor – Agent Setup**, and then click **Remove**. A message box prompts you for confirmation.
3. To remove the agent, click **Yes**.

## UNINSTALLING FILE SYSTEM AUDITOR

1. From the Windows Control Panel, choose **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



# Stored Procedures

Name	Owner	Type	Create Date
CleanUpTables	dbo	User	3/21/2007 11:05
DeleteFullPath	dbo	User	3/21/2007 11:05
dt_addtosourcecontrol	dbo	System	3/21/2007 11:26
dt_addtosourcecontrol_u	dbo	System	3/21/2007 11:26
dt_adduserobject	dbo	System	3/21/2007 11:26
dt_adduserobject_vcs	dbo	System	3/21/2007 11:26
dt_checkinobject	dbo	System	3/21/2007 11:26
dt_checkinobject_u	dbo	System	3/21/2007 11:26
dt_checkoutobject	dbo	System	3/21/2007 11:26
dt_checkoutobject_u	dbo	System	3/21/2007 11:26
dt_displayoerror	dbo	System	3/21/2007 11:26
dt_displayoerror_u	dbo	System	3/21/2007 11:26
dt_droppropertiesbyid	dbo	System	3/21/2007 11:26
dt_dropuserobjectbyid	dbo	System	3/21/2007 11:26
dt_generateansiname	dbo	System	3/21/2007 11:26
dt_getobjwithprop	dbo	System	3/21/2007 11:26
dt_getobjwithprop_u	dbo	System	3/21/2007 11:26
dt_getpropertiesbyid	dbo	System	3/21/2007 11:26
dt_getpropertiesbyid_u	dbo	System	3/21/2007 11:26
dt_getpropertiesbyid_vcs	dbo	System	3/21/2007 11:26
dt_getpropertiesbyid_vcs_u	dbo	System	3/21/2007 11:26
dt_isundersourcecontrol	dbo	System	3/21/2007 11:26
dt_isundersourcecontrol_u	dbo	System	3/21/2007 11:26
dt_removefromsourcecontrol	dbo	System	3/21/2007 11:26
dt_setpropertybyid	dbo	System	3/21/2007 11:26
dt_setpropertybyid_u	dbo	System	3/21/2007 11:26
dt_validateloginparams	dbo	System	3/21/2007 11:26

Name	Owner	Type	Create Date
dt_validateloginparams_u	dbo	System	3/21/2007 11:26
dt_vcsenabled	dbo	System	3/21/2007 11:26
dt_verstamp006	dbo	System	3/21/2007 11:26
dt_verstamp007	dbo	System	3/21/2007 11:26
dt_whocheckedout	dbo	System	3/21/2007 11:26
dt_whocheckedout_u	dbo	System	3/21/2007 11:26
GetAccountID	dbo	User	3/21/2007 11:05
GetComputerID	dbo	User	3/21/2007 11:05
GetPathID	dbo	User	3/21/2007 11:05
GetPathIDEx	dbo	User	3/21/2007 11:05
GetPermissionID	dbo	User	3/21/2007 11:05
GetProcessID	dbo	User	3/21/2007 11:05
InsertEntry	dbo	User	3/21/2007 11:05
InsertEntry2	dbo	User	3/21/2007 11:05
PopulateEventNames	dbo	User	3/21/2007 11:05
PurgeDataByDate	dbo	User	3/21/2007 11:05
Update1	dbo	User	3/21/2007 11:05
Update2	dbo	User	3/21/2007 11:05

# Index

- 
- .lic, 9
- A**
- adding
  - default filters, 34
  - file path to filter, 24
  - file servers, 15
  - process filters, 28
  - user filters, 30
- Advanced Settings, 33
- attaching
  - database, 54
- Audit Agent
  - starting, 23
  - stopping, 23
  - upgrading, 14
- Audit Database
  - creating, 15
  - viewing data, 36
- auditing database, 65
- C**
- creating
  - Audit Database, 15
  - database, 48
- D**
- database
  - attaching, 54
  - changing settings, 32
  - creating, 15, 48
  - detaching, 50, 55
  - increasing size, 50
  - maintenance, 59
  - moving to another server, 61
  - purging, 37
  - shrinking, 51
  - viewing data, 36
  - viewing statistics, 53
- database schema, 65
- Database Wizard, 46
- DBCC commands, 59
- default filters, 34
- detaching
  - database, 50, 55
- duplicate entries
  - suppressing, 33
- E**
- editing
  - default filters, 35
  - file path filter, 27
  - process exclusion filter, 29
  - user exclusion filter, 31
- evaluation period, 10
- excluding
  - files, 24
  - folders, 24
  - processes, 28
  - users, 30
- F**
- file extensions
  - .sql, 53
- file masks
  - removing, 27
- file servers
  - adding, 15
- File System Auditor
  - starting, 11
- filters
  - file path, 24
  - process, 28
  - user, 30
- I**
- including
  - files, 24
  - folders, 24
- increasing
  - database size, 50
- installing
  - SQL Server 2005 Express, 32
- iSCSI disks, 3
- L**
- license file
  - applying, 9
- M**
- moving
  - database to another server, 61

**O**

- opening
  - Agent Configuration, 11

**P**

- path filter
  - editing, 27
  - removing, 27
- process filters
  - adding, 28
  - editing, 29
  - removing, 29
- purging
  - audit database, 37

**R**

- reducing
  - database size, 51
- register product, 10
- removing
  - default filters, 35
  - file masks, 27
  - file path filter, 27
  - process exclusion filter, 29
  - user exclusion filter, 31

**S**

- saving
  - connection information, 58
- servers
  - moving a database, 61
- setting
  - process filters, 28
  - user filters, 30
- setting filters
  - file path, 24
- shrinking
  - database, 51

- SLFileAuditor, 65
- SQL Script
  - running, 53
- SQL Script File, 53
- SQL Server 2005 Express, 32
- starting
  - Agent Configuration, 11
  - Audit Agent, 23
- stopping
  - Audit Agent, 23
- suppressing
  - duplicate entries, 33
- system requirements, 3

**T**

- tempdb database, 51
- transaction log
  - truncating, 56
- truncate
  - transaction log, 56

**U**

- upgrading
  - Audit Agent, 14
- user filters
  - adding, 30
  - editing, 31
  - removing, 31

**V**

- viewing
  - data, 36
  - database statistics, 53

**W**

- web site, 10