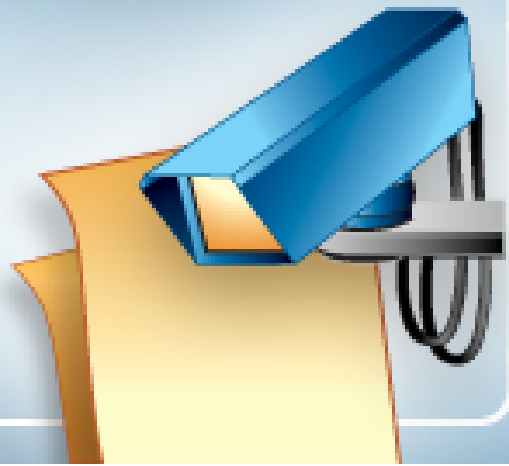


FILE SYSTEM AUDITOR™



ScriptLogic® File System Auditor Getting Started Guide

SCRIPTLOGIC

© 2005 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 1.x. It is possible that it may contain technical or typographical errors. ScriptLogic Corporation provides this publication "as is," without warranty of any kind, either expressed or implied.

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

1.561.886.2400
www.scriptlogic.com

Trademark Acknowledgements:

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

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

Printed in the United States of America (1/2006)

DOCUMENTATION CONVENTIONS

Typeface Conventions

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

CONTACTING SCRIPTLOGIC

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



ScriptLogic Corporation

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



561.886.2400 Sales and General Inquiries
561.886.2450 Technical Support



561.886.2499 Fax



www.scriptlogic.com

SCRIPTLOGIC ON THE WEB

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

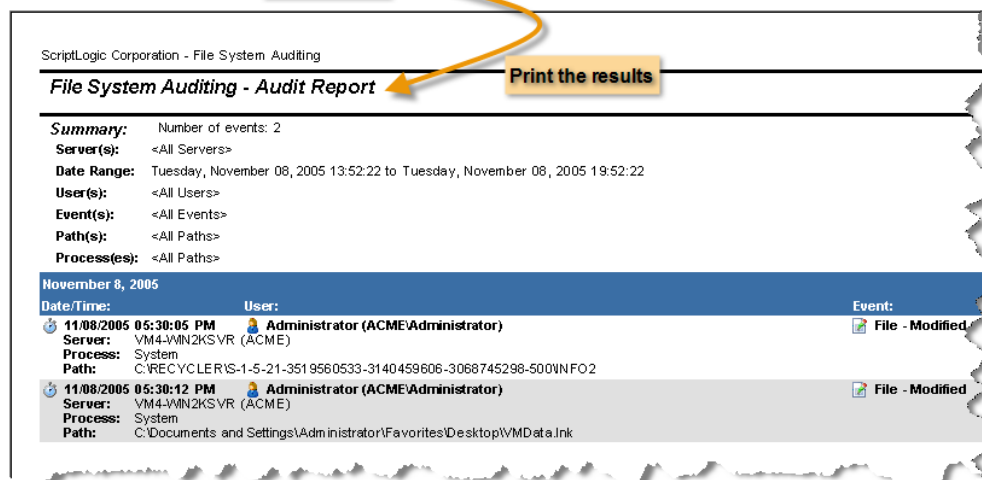
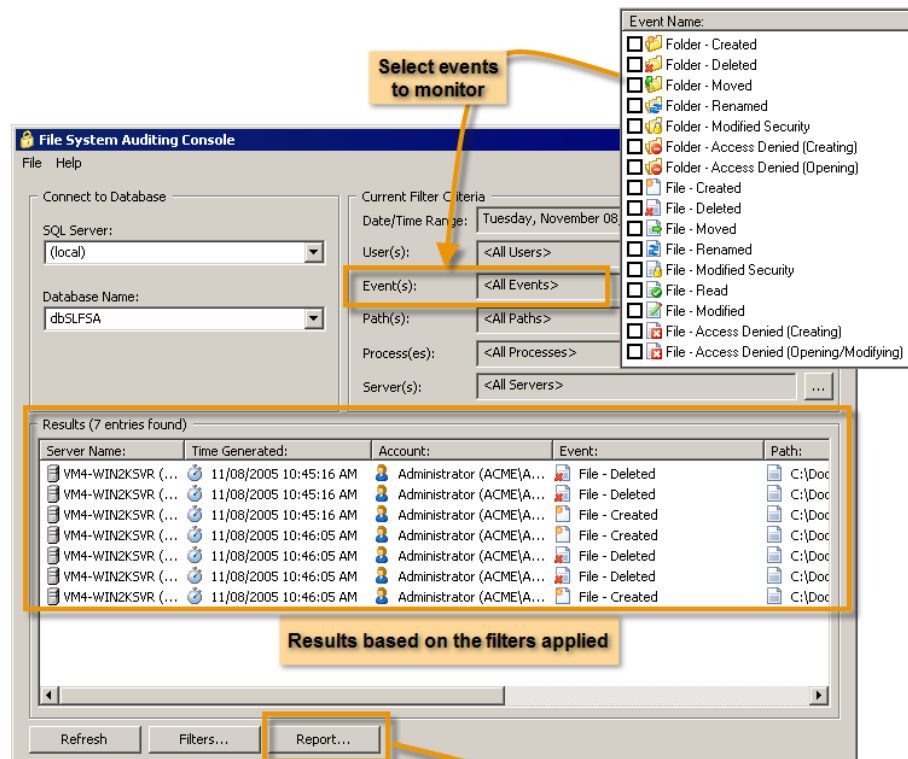
- Download product updates, patches and/or evaluation products.
- Locate product information and technical details.
- Find out about Product Pricing.
- Search the Knowledge Base for Technical Notes containing an extensive collection of technical articles, troubleshooting tips and white papers.
- Search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

Contents

WHAT IS FILE SYSTEM AUDITOR?	5
INSTALLING FILE SYSTEM AUDITOR	7
BEFORE YOU BEGIN	8
<i>User Privilege Requirements</i>	8
RUNNING THE SERVER SETUP WIZARD	8
RUNNING THE CONSOLE SETUP WIZARD.....	15
STARTING FILE SYSTEM AUDITOR	18
<i>Starting the Evaluation Version</i>	18
<i>Applying a License File</i>	19
<i>Evaluating the Product</i>	19
CONFIGURING FILE SYSTEM AUDITOR.....	20
STARTING FSA SERVICE CONFIGURATION.....	20
EXAMINING THE MAIN WINDOW.....	20
SETTING THE AUDITING DATABASE	22
SETTING THE DATABASE LOGON ACCOUNT.....	22
SETTING FILE PATH FILTERS	23
SETTING PROCESS FILTERS	25
SETTING ADVANCED OPTIONS	26
MANAGING THE AUDITING DATABASE.....	27
STARTING THE DATABASE MAINTENANCE UTILITY	27
CREATING A NEW DATABASE	28
REMOVING AN EXISTING DATABASE.....	30
INCREASING DATABASE SIZE	31
SHRINKING A DATABASE.....	32
RUNNING AN SQL SCRIPT	32
VIEWING DATABASE STATISTICS	33
ATTACHING A DATABASE	34
DETACHING A DATABASE	34
TRUNCATING THE TRANSACTION LOG	35
SAVING CONNECTION INFORMATION	35
PERFORMING DATABASE MAINTENANCE.....	36
RESETTING DATABASE SECURITY	37
SWITCHING THE SERVER SECURITY MODE.....	38
SETTING THE 'SA' PASSWORD	38
MOVING A DATABASE TO ANOTHER SERVER	39
TROUBLESHOOTING	40
UNINSTALLING FILE SYSTEM AUDITOR	40
INDEX	41

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 whenever specific file system events occur, such as failed access attempts, or modifications of a particular set of files and folders. Reports can be sent out on a daily or weekly basis, or frequently in 5, 10, 15, 20, 30, or 60 minute increments.

Edit Scheduled Report

Description: Deleted Folders

Schedule

Schedule Task: Daily Start Time: 12:00 AM

Do not send report if there are no results

Filter Criteria

User(s): <All Users> ...

Event(s): Folder - Deleted ...

Path(s): <All Paths> ...

Process(es): <All Processes> ...

Server(s): <All Servers> ...

Send To

Email address(es):

Email: jsmith@ACME.com Add... Remove

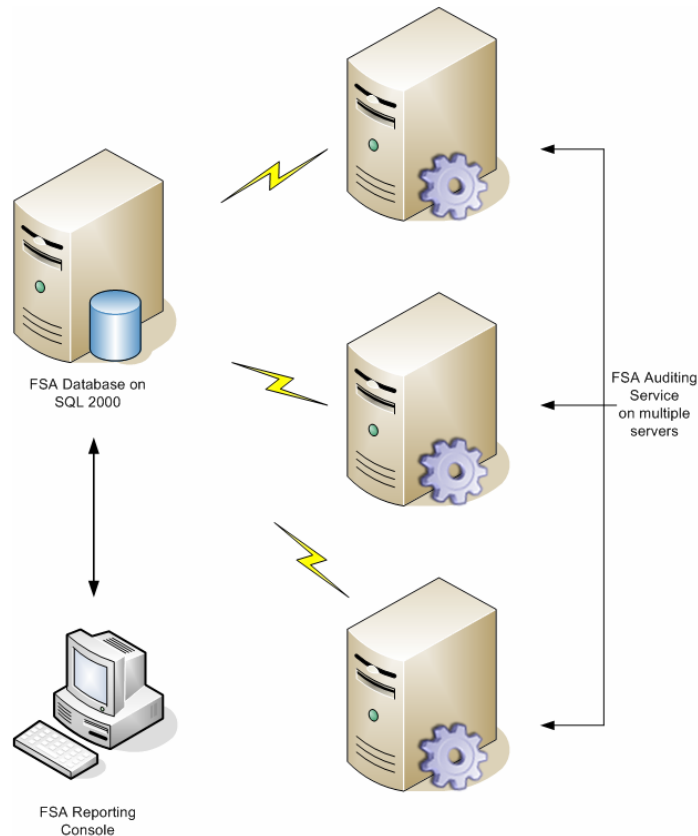
Subject line: Daily Deleted Folders Report

OK Cancel

Installing File System Auditor

There are two installation files for File System Auditor: Server and Console.

- Install the Server component on each file server that you want to audit. During the installation process, you are prompted to create an auditing database, which should be installed in one central location for all audited file servers. You can choose to use the MSDE database that File System Auditor automatically creates for you during the Server installation process, or you can use another specified MSDE or SQL database on a remote computer. If you want to use a MSDE or SQL database on a remote computer, choose the **Custom** setup during the Server installation process, and choose not to install MSDE – see page 11 for more details.
- Install the Console component on each workstation from which you want to audit events in the database.



File System Auditor is provided in a Windows Installer package format, which allows for robust, self-repairing of application files, and ease of installation and software distribution. The Windows Installer service is included with Microsoft Windows 2000 and later.

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.

Supported Management Platforms

- Windows 2000: Professional, Server
- Windows XP Professional
- Windows Server™ 2003: Standard, Server, Enterprise Edition

Recommended Hardware

- 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

Export Requirements

- Microsoft Data Engine (MSDE) 2000; or Microsoft SQL Server 2000 and Data Access Components (MDAC) 2.7

Note: MSDE and MDAC are included with File System Auditor.

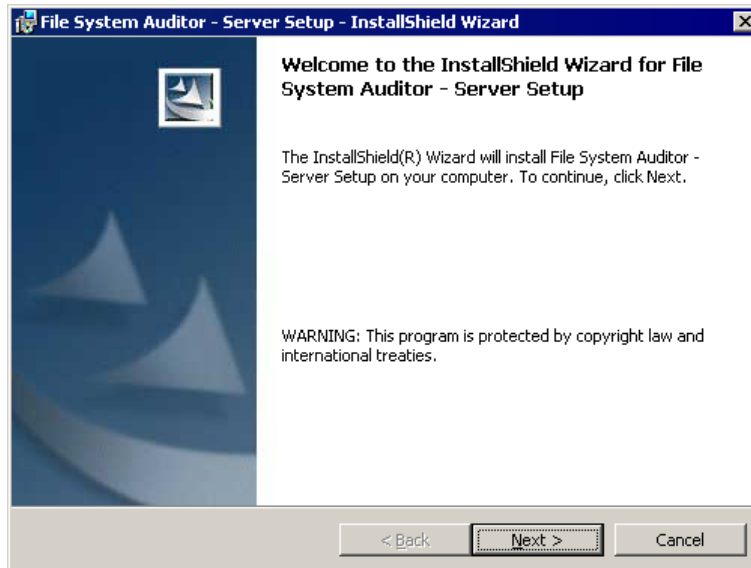
RUNNING THE SERVER SETUP WIZARD

Install the Server component on each server that you want to audit. During the installation process, you are prompted to create an auditing database, which should be located on only one server. You can choose to use the MSDE database that File System Auditor automatically creates for you or you can use another specified MSDE or SQL database on a remote computer. If you want to use another specified MSDE or SQL database, choose the Custom option when prompted to not install MSDE.

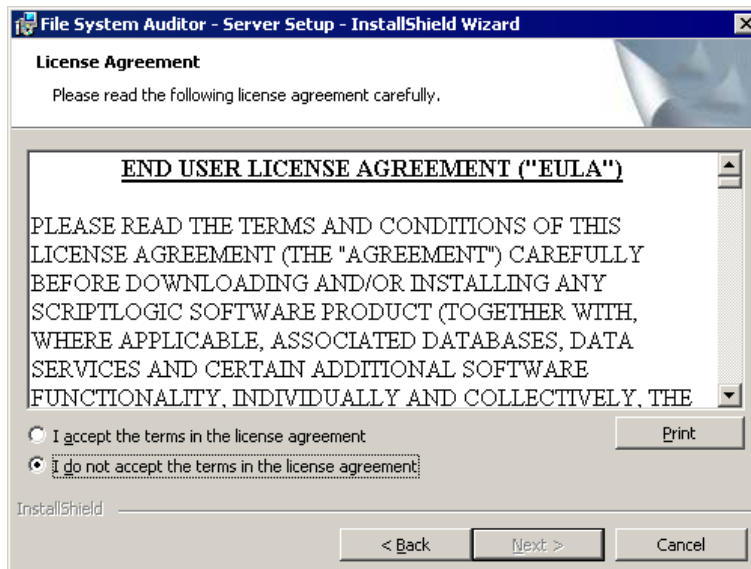
Important: If you are running Active Administrator on the same computer as File System Auditor, exit Active Administrator and stop all Active Administrator services before installing File System Auditor.

Important: You are prompted to restart the computer upon completion of the installation process.

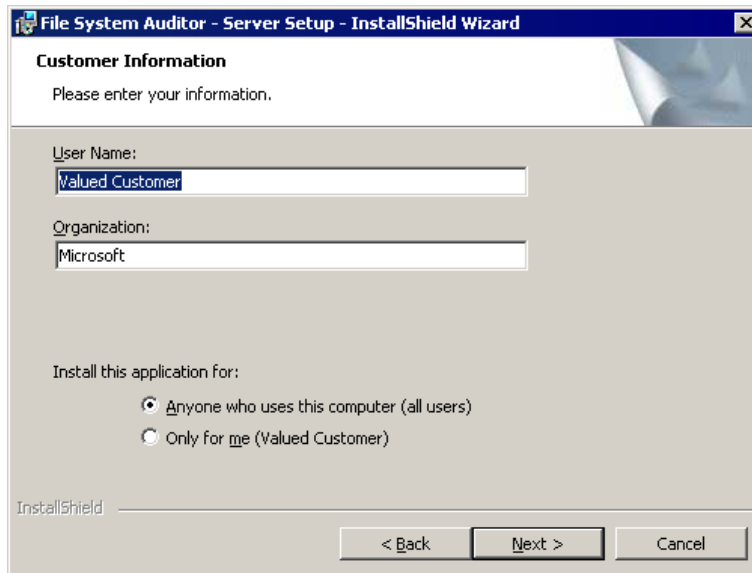
1. Double-click the **FSA_Server_Setup_Beta.msi** file. The **Welcome** box appears.



2. Click **Next**. The **License Agreement** box appears.



3. Select **I accept the terms in the license agreement**, and then click **Next**. The **Customer Information** box appears.



File System Auditor - Server Setup - InstallShield Wizard

Customer Information

Please enter your information.

User Name:
Valued Customer

Organization:
Microsoft

Install this application for:

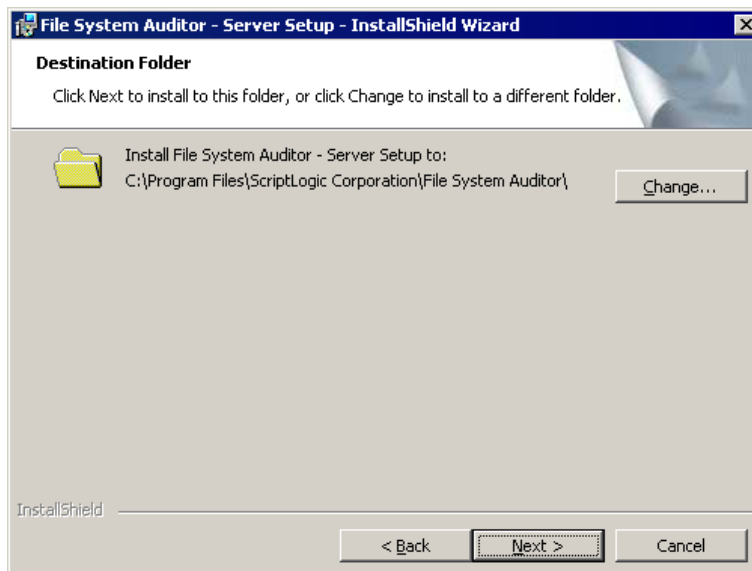
Anyone who uses this computer (all users)

Only for me (Valued Customer)

InstallShield

< Back Next > Cancel

4. If necessary, change the default values in the **User Name** and **Organization** boxes. Also choose whether to permit access to all users or just yourself. Click **Next**. The **Destination Folder** box displays the default installation path.



File System Auditor - Server Setup - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

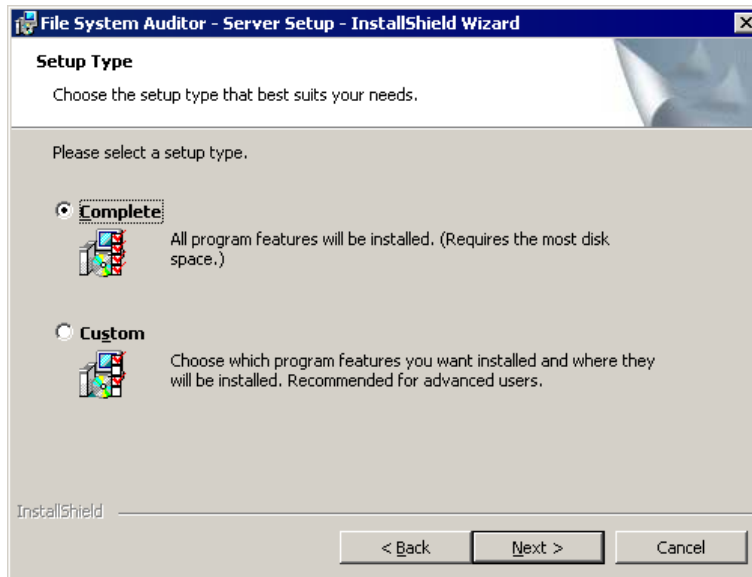
Install File System Auditor - Server Setup to:
C:\Program Files\ScriptLogic Corporation\File System Auditor\ Change...

InstallShield

< Back Next > Cancel

- To change the installation path, click **Change**, and then select a new path.

5. Click **Next**. The **Setup Type** box appears.

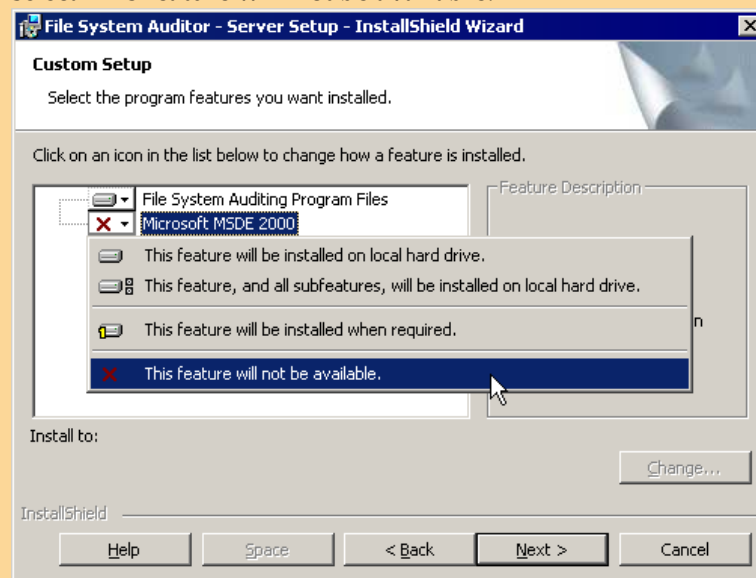


Note: MSDE 2000 is installed with the complete install of File System Auditor. To omit installing MSDE 2000, choose **Custom**.

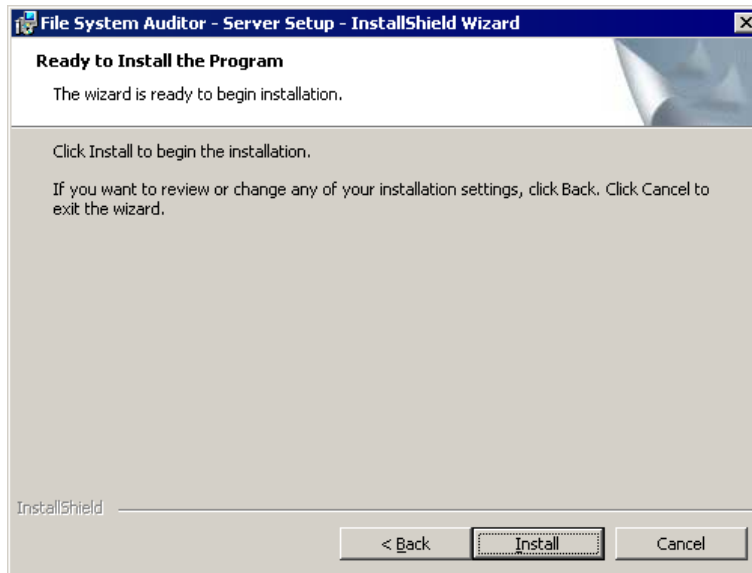
Important: You must select **Custom** if you are going to use a database that is located on another server.

6. Choose whether to do a complete or custom installation.

Note: If you chose a custom installation, expand **Microsoft MSDE 2000**, and then select **This feature will not be available**.



7. Click **Next**. The **Ready to Install the Program** box appears.

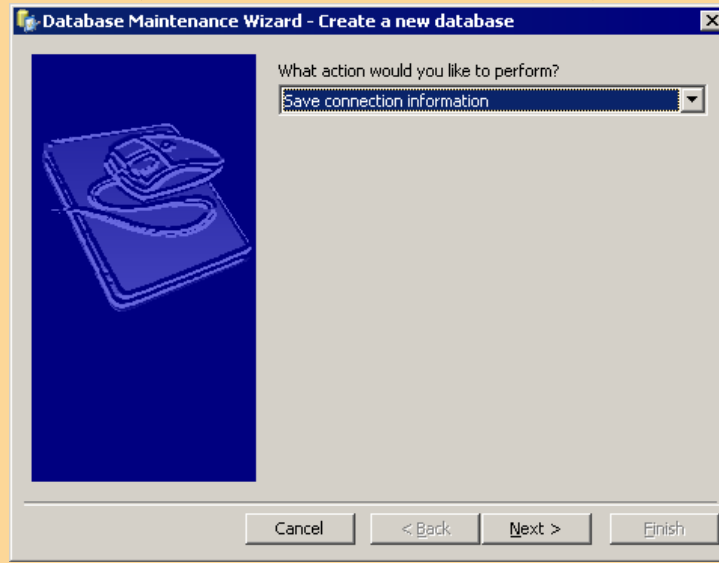


8. Click **Install**. A progress bar displays the installation process. When the installation is complete, the **Database Maintenance Wizard** opens.

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



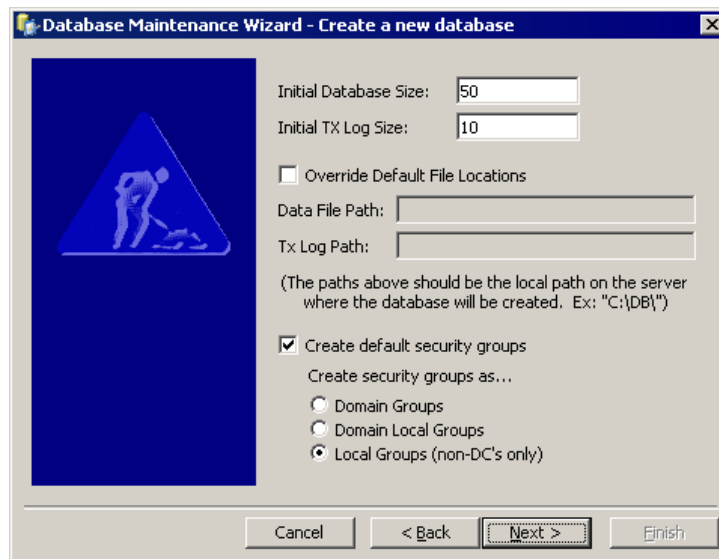
Important: If you chose to not install MSDE 2000, you must click **Back**. In the **Action** box, choose **Save connection information**, and then click **Next**.



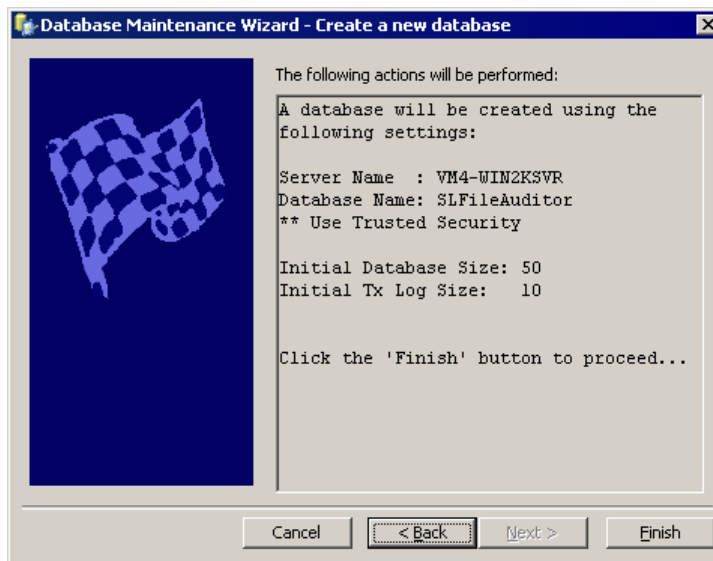
9. In the **SQL Database Server Name** box, type the name of the server that is running MSDE 2000 or Microsoft SQL Server 2000, or click **...** to locate a server.
10. In the **Database Name** box, type the name of the database to create or click **...** to locate existing database names. The default database is SLFileAuditor.
11. 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.

Important: If you want to use Windows Authentication, the SQL Server must be configured to use trusted security.

12. Click **Next**. The database definition dialog box displays the default sizes for the database (*.mdf) and transaction log (*.ldf) files.



13. In the **Initial Database Size** box, type an initial size for the database file (*.mdf). If the database needs to grow the data file, it will do so automatically.
14. In the **Initial TX Log Size** box, type an initial size for the transaction log file (*.ldf). If the database needs to grow the log file, it will do so automatically.
15. To create the database transaction log files in a location other than the default location, select the **Override Default File Locations** check box, and then type the physical path in the appropriate boxes. Express the path as a logical path and not as a UNC path.
16. By default, default security groups are created as local groups on non-domain controllers only. You can select to create default domain groups or domain local groups. To bypass the creation of default security groups, clear the **Create default security groups** check box.
17. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.




18. To create the specified database, click **Finish**.

As the action runs, a progress bar displays the action occurring and the progress towards completion. When the action is finished, The **Login as** box appears.

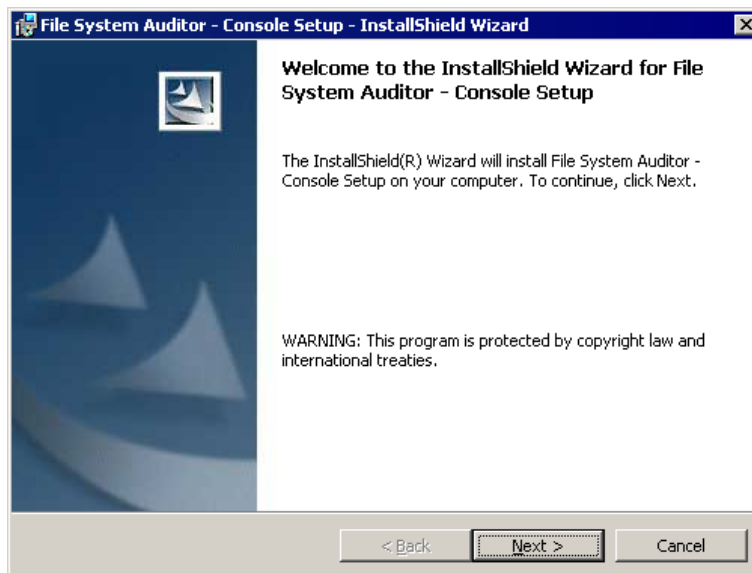


By default, the ScriptLogic File System Auditing Service runs as Local Administrator. If you need to, you can set a domain username and password that will be used by the service (through impersonation) to access the auditing database.

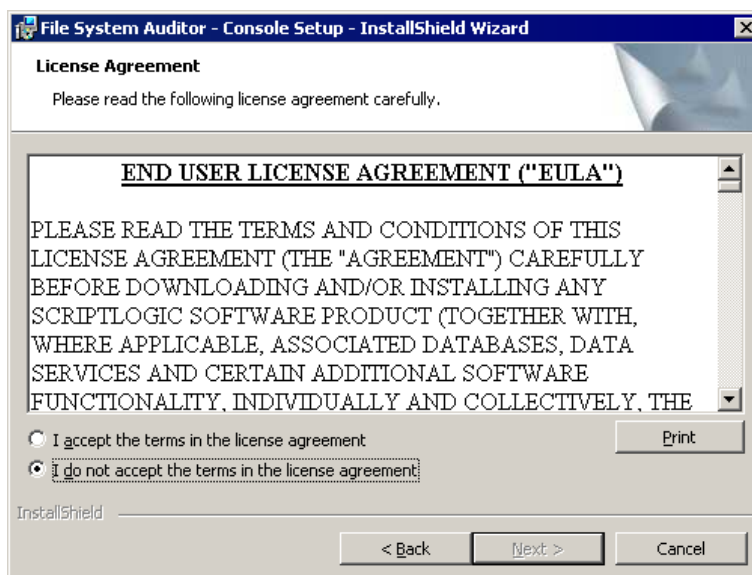
19. In the **Account** box, type an account name or click  to locate an account name, type the password, and then click **OK**.
20. Click **Finish**. You are prompted to restart the computer.

RUNNING THE CONSOLE SETUP WIZARD

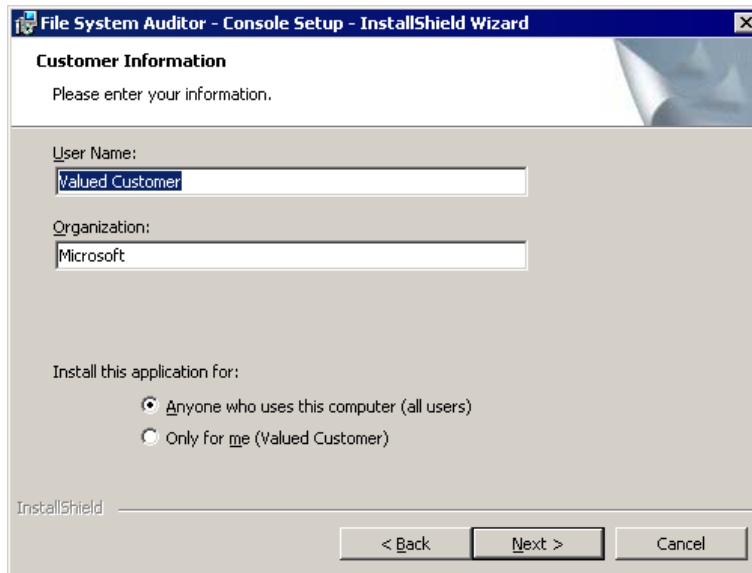
1. Double-click the `FSA_Console_Setup_Beta.msi` file. The **Welcome** box appears.



2. Click **Next**. The **License Agreement** box appears.



3. Select **I accept the terms in the license agreement**, and then click **Next**. The **Customer Information** box appears.



File System Auditor - Console Setup - InstallShield Wizard

Customer Information

Please enter your information.

User Name:
Valued Customer

Organization:
Microsoft

Install this application for:

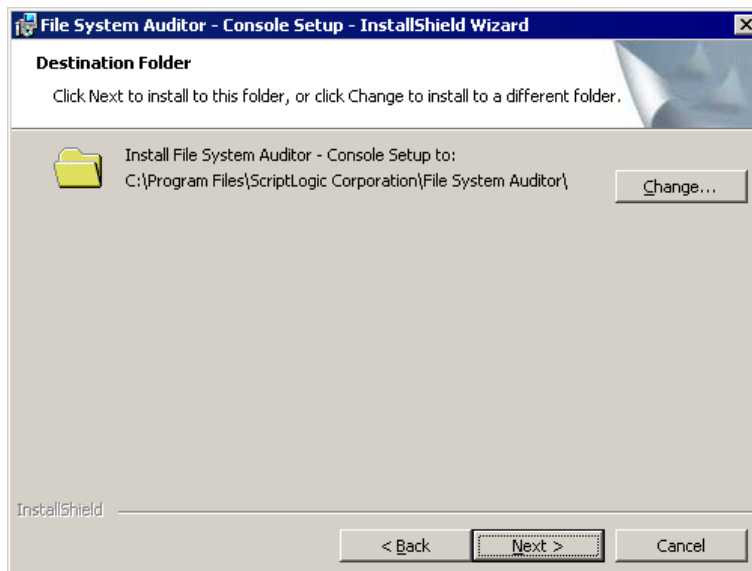
Anyone who uses this computer (all users)

Only for me (Valued Customer)

InstallShield

< Back Next > Cancel

4. If necessary, change the default values in the **User Name** and **Organization** boxes. Also choose whether to permit access to all users or just yourself. Click **Next**. The **Destination Folder** box displays the default installation path.



File System Auditor - Console Setup - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

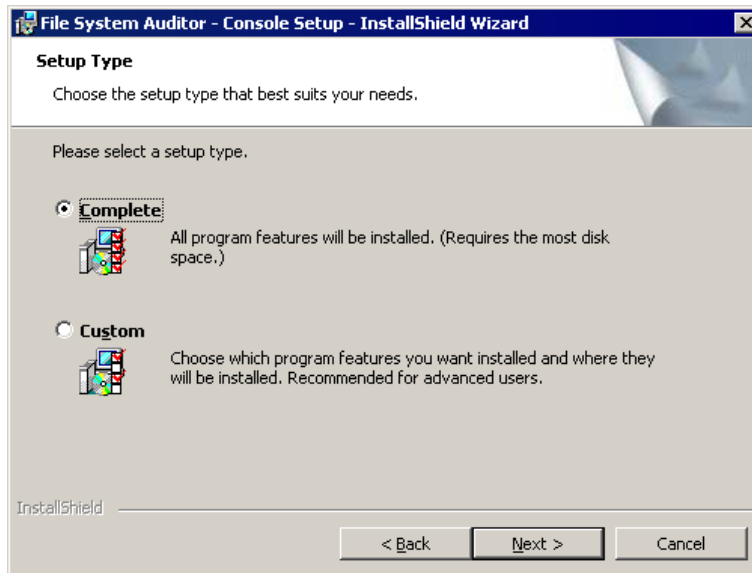
Install File System Auditor - Console Setup to:
C:\Program Files\ScriptLogic Corporation\File System Auditor\ Change...

InstallShield

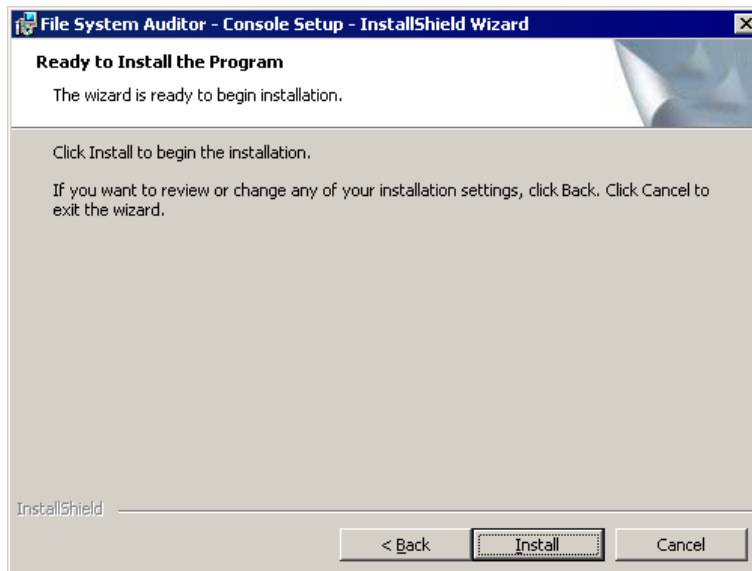
< Back Next > Cancel

- To change the installation path, click **Change**, and then select a new path.

5. Click **Next**. The **Setup Type** box appears.



6. Choose whether to do a complete or custom installation, and then click **Next**. The **Ready to Install the Program** box appears.



7. Click **Install**. A progress bar displays the installation process.
8. When the installation is complete, click **Finish**.

STARTING FILE SYSTEM AUDITOR

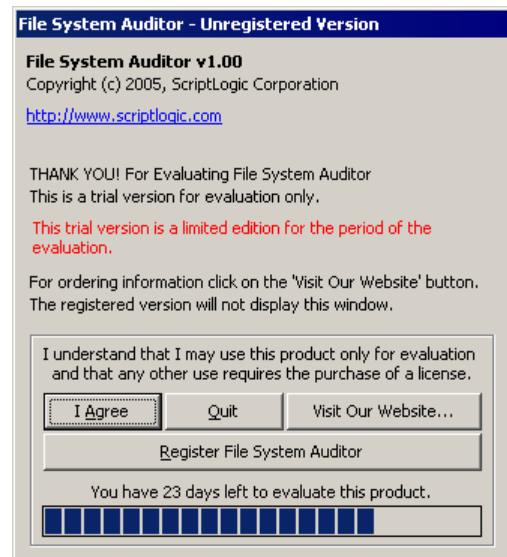
- ▶ Click **Start**, point to **Programs > ScriptLogic Corporation > File System Auditing**, and then select one of the following options:

Programs	Use
Create Database	Create an auditing database
FSA Service Configuration	Configure File System Auditor for data collection
FSA Reporting Console	Filter and report on data in the auditing database

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

Starting the Evaluation Version

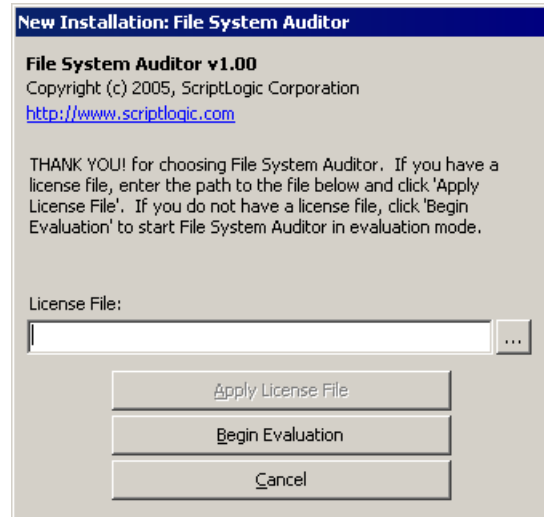
During the evaluation period, the first time you start File System Auditor, the Unregistered Version window opens.



To:	Click:
Start the evaluation version	I agree
Exit	Quit
Go to the ScriptLogic web site	Visit Our Website
Apply a License File	Register File System Auditor


Applying a License File

The first time you start File System Auditor, you see the **New Installation** dialog 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 Support Team specialist should have sent this file to you as an email attachment.

- ▶ Click  to locate the license file, and then click **Apply License File**.

Evaluating the Product

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

Note: The full and evaluation versions of File System Auditor are identical. The license file is the sole determinant of program functionality.

Configuring File System Auditor

The File Service Configuration module 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.

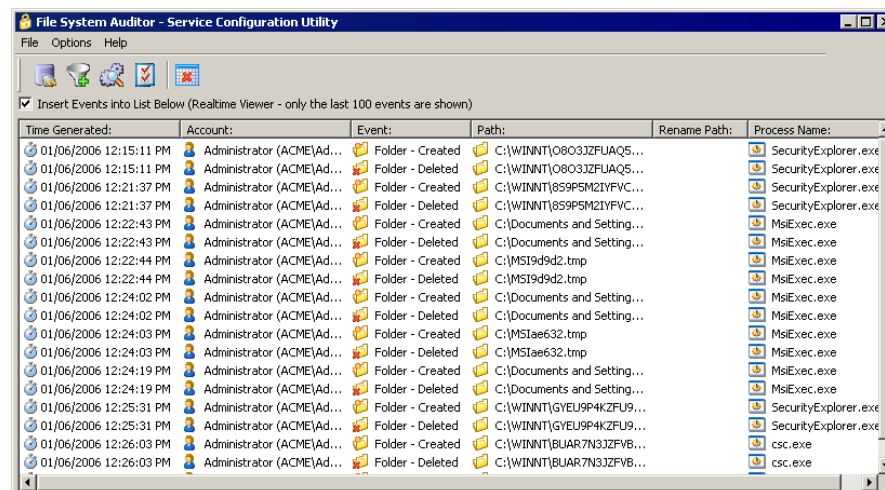
STARTING FSA SERVICE CONFIGURATION

- ▶ Click **Start**, point to **Programs > ScriptLogic Corporation > File System Auditing**, and then select **FSA Service Configuration**.

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

EXAMINING THE SERVICE CONFIGURATION UTILITY MAIN WINDOW

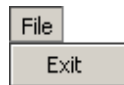
The **Service Configuration Utility** main window can list events as they occur. This window is blank until you create at least one file path filter.



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

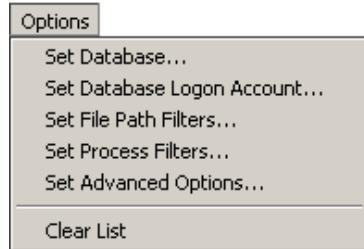
Select to list events as they occur. By default, events display. To suppress the display of events, clear the check box. The events that are listed do not disappear until you select **Clear List** from the **Options** menu.







File Menu



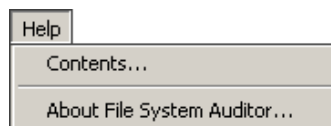
Menu Option	Description
Exit	Closes File System Auditor.

Options Menu and Toolbar Icons



Toolbar	Menu Option	Description
	Set Database	Sets the SQL Sever and database to use to collect event data. See <i>Setting the Auditing Database</i> .
	Set Database Logon Account	Set the account which the ScriptLogic File Auditing Service uses to access the auditing database. See <i>Setting the Database Logon Account</i> .
	Set File Path Filters	Defines the path and filters upon which the collection is based. You can exclude or include specific events and files. See <i>Setting File Path Filters</i> .
	Set Process Filters	Excludes specific processes from event collection. See <i>Setting Process Filters</i> .
	Set Advanced Options	Sets the length of time in which duplicates are suppressed from the list of events. See <i>Setting Advanced Options</i> .
	Clear List	Clears the list of events on the main window.


Help Menu

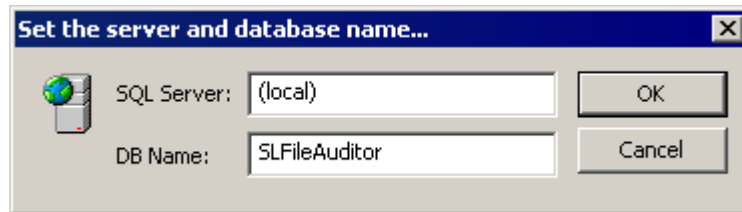


Menu Option	Description
Contents	Access online help
About File System Auditor	View information about the version of File System Auditor installed on your computer, to apply a license file, or to visit the ScriptLogic website.

SETTING THE AUDITING DATABASE

Events are recorded in an SQL database that you created, either during installation, or with the **Create Database** module. You can create more than one database and use this feature to switch among the various databases.


- ▶ Click  or choose **Set Database** from the **Options** menu. The **SQL Server** and **DB Name** boxes displays the names of the current SQL server and database.



To change the names of the SQL server and database, type the name in the appropriate box, and then click **OK**.

SETTING THE DATABASE LOGON ACCOUNT

By default, the ScriptLogic File System Auditing Service runs as Local Administrator. If you need to, you can set a domain username and password that will be used by the service (through impersonation) to access the auditing database.

- ▶ Click  or choose **Set Database Logon Account** from the **Options** menu. The **Set Database Logon Account** box displays the current account and password.




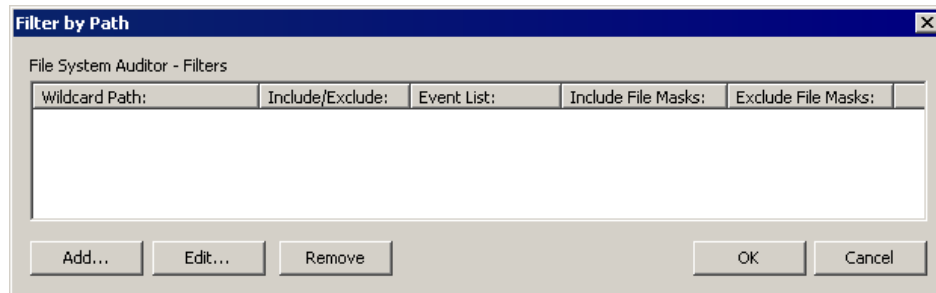
To change the account, type an account name or click  to locate an account name, type the password, and then click **OK**. Restart the ScriptLogic File System Auditing Service.


SETTING FILE PATH FILTERS

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.

Note: Upon installation, you must create at least one filter. File System Auditor cannot collect data unless you define a filter.

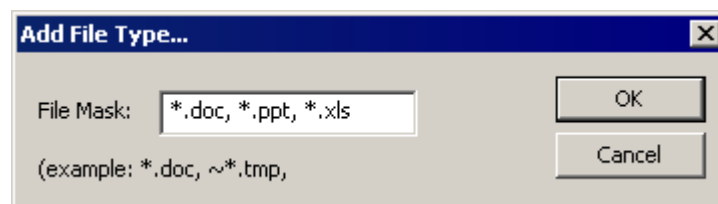
1. Click  or choose **Set File Path Filters** from the **Options** menu. The **Filter by Path** box displays the current filters. Upon initial installation, the box is empty.



2. Click **Add**. The **Edit Filter** box appears.
3. In the **Folder/File Wildcard** box, type the path to which to apply the filter, or click  to locate a folder.
4. In the **Include/Exclude Action Codes** list, select the events that you want to include or exclude from the path.

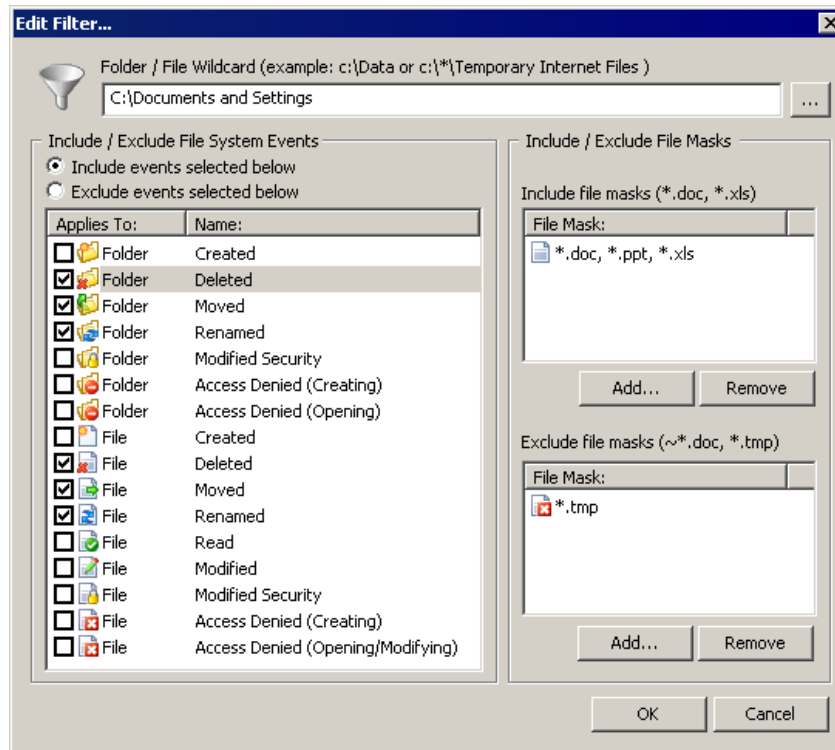
Note: You can select to include or exclude events, but not both in the same filter. Create separate filters to include and exclude events.

5. 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 File Type** box appears. Type the mask in the box using wildcards as needed, and then click **OK**.



Note: You can type more than one mask in the **File Mask** box by separating each mask with a comma.

The **Edit Filter** box displays the selections.

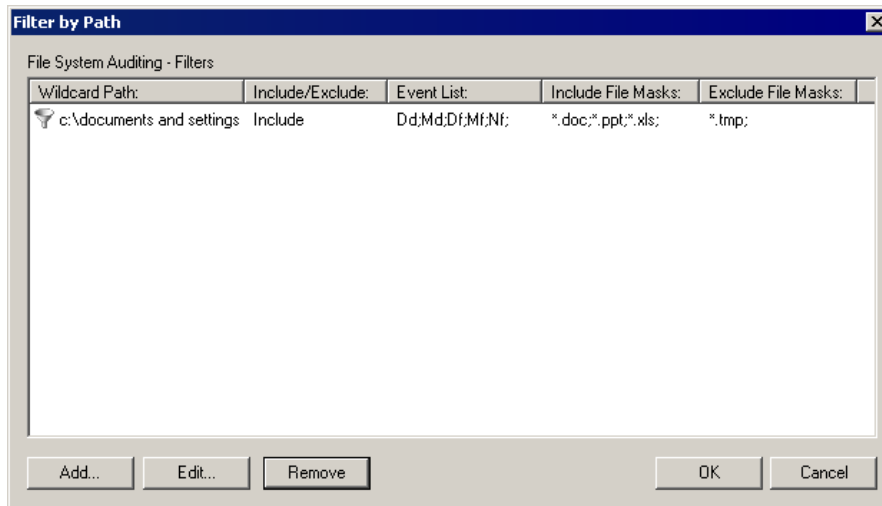


Important: Use caution if including **File-Read** or **File-Access Denied (Opening/Modifying)** events as the number of events recorded by File System Auditor may overwhelm the auditing database. Any focus on a file in Windows Explorer, such as a mouse-over or using the arrow keys to scroll through the 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 either ScriptLogic's WinCloak, or Windows Access-Based Enumeration (available with Windows Server 2003 Service Pack 1) enabled and operational.

- To remove a selected file mask, click **Remove** in the appropriate area.

- Click **OK**. The **Filter by Path** box displays the filter.

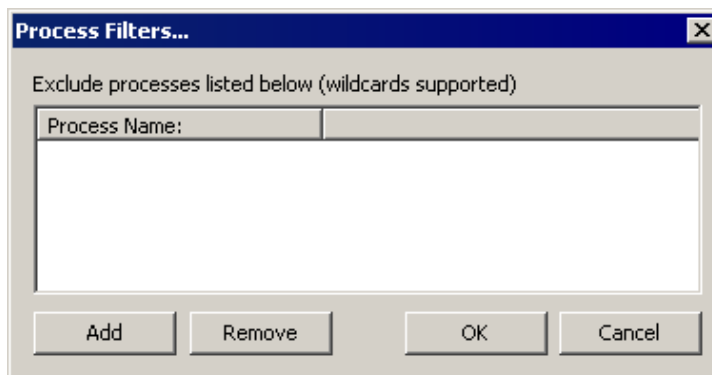


- To edit a selected file path filter, click **Edit**.
- To delete selected file path filters, click **Remove**.

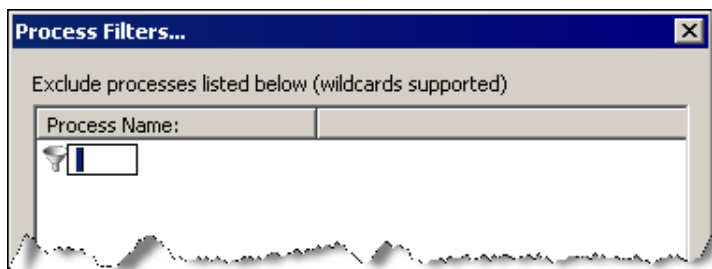
SETTING PROCESS FILTERS

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

- Click  or choose **Set Process Filters** from the **Options** menu. The **Process Filters** box displays the current filters. Upon initial installation, the box is empty.

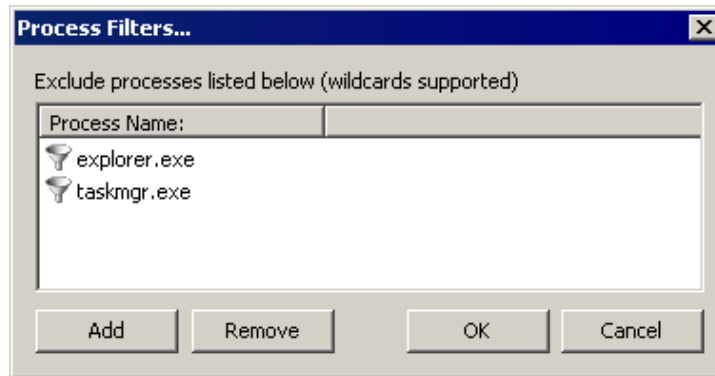


- Click **Add**. The cursor appears under the **Process Name** column.



3. Type the process name, using wildcards if needed, and then press **Enter**.

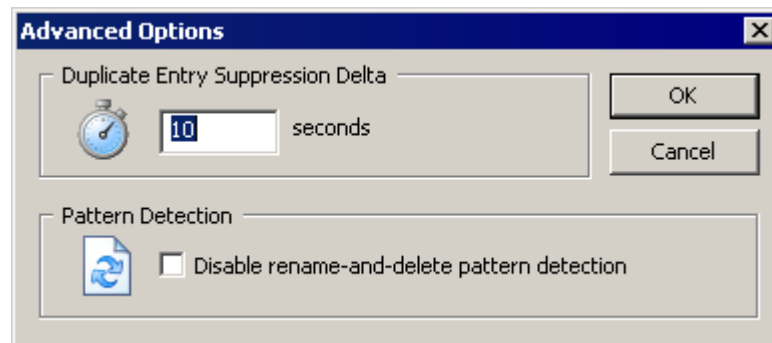
Note: If you make a mistake while typing, you can click the name in the **Process Name** column, and then correct the misspelling.



- To remove selected process filters, click **Remove**.

SETTING ADVANCED OPTIONS

- ▶ Click  or choose **Set Advanced Options** from the **Options** menu. The **Advanced Options** box displays the current settings.



Duplicate Entry Suppression Delta

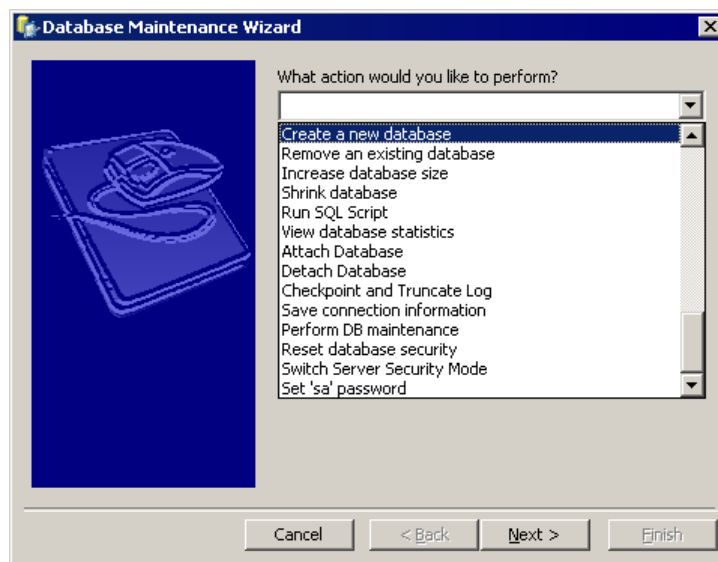
By default, duplicate entries that occur within 10 seconds of each other are suppressed. Only the first entry appears in the event list. You can increase this value to reduce the length of the event list. Changes apply to new event collection only. Existing data is not affected.

Disable 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.

Managing the Auditing Database

When you first install File System Auditor, the **Database Maintenance Wizard** opens automatically for you to create a new database. Follow these this procedure if you bypassed this step during installation, or wish to create another database to use.



Note: File System Auditor includes a run-time version of Microsoft SQL Server 2000 Desktop Engine (MSDE 2000), which is data engine built and based on core SQL Server technology. This database engine has some limitations over the full version of Microsoft SQL Server 2000, such as a 2GB database limit and a restriction on the number of concurrent users. If you have a large enterprise, you may want to consider purchasing a full version of Microsoft SQL Server 2000 for use with this product.

STARTING THE DATABASE MAINTENANCE UTILITY

- ▶ Click **Start**, point to **Programs > ScriptLogic Corporation > File System Auditing**, and then select **Create Database**.

CREATING A NEW DATABASE

When you first install File System Auditor, the Database Maintenance Wizard opens automatically for you to create a new auditing database. Follow these this procedure if you bypassed this step during installation, or wish to create another database to use.

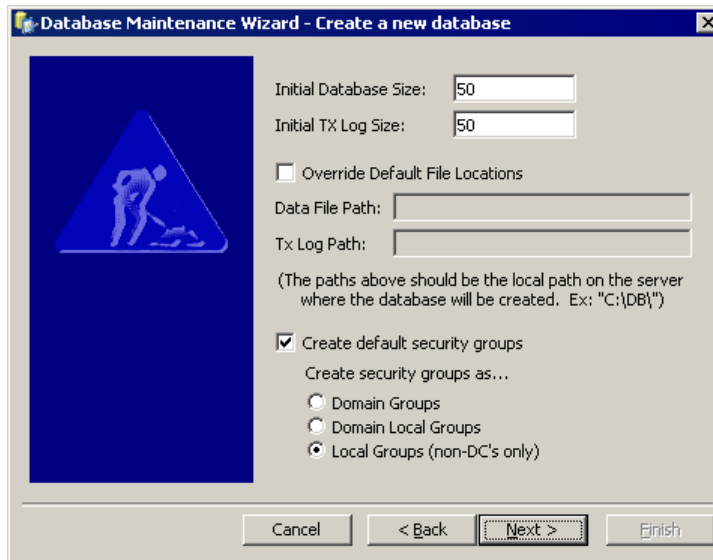
Important: You must create an auditing database before you can perform any tasks using File System Auditor.

1. From the **Database Maintenance Wizard** main page, select **Create a new database** from the list, and then click **Next**. The database selection dialog box displays the current computer and database names (default).



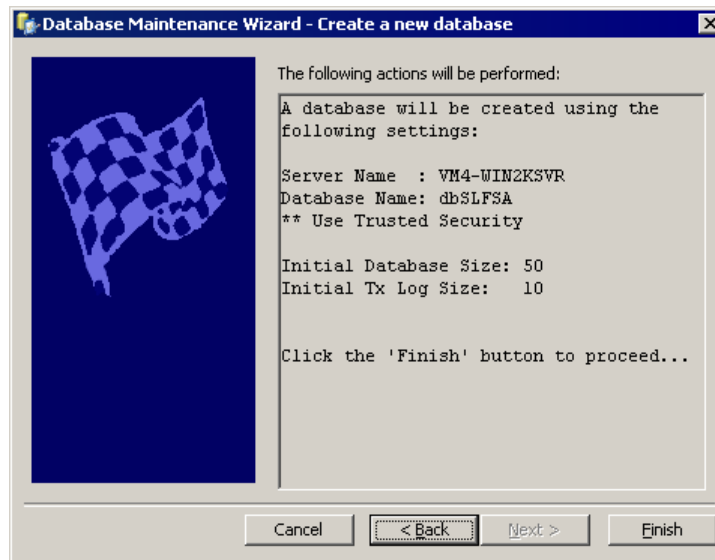
2. In the **SQL Database Server Name** box, type the name of the server that is running MSDE 2000 or Microsoft SQL Server 2000, or click **...** to locate a server.
3. In the **Database Name** box, type the name of the auditing database to create or click **...** to locate existing database names.
4. 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.

5. Click **Next**. The database definition dialog box displays the default sizes for the database (*.mdf) and transaction log (*.ldf) files.



6. In the **Initial Database Size** box, type an initial size for the database file (*.mdf). If the database needs to grow the data file, it will do so automatically.
7. In the **Initial TX Log Size** box, type an initial size for the database transaction log file (*.ldf). If the database needs to grow the log file, it will do so automatically.
8. To create the database transaction log files in a location other than the default location, select **Override Default File Locations**, and then type the physical path in the appropriate boxes. Express the path as a logical path and not as a UNC path.
9. By default, default security groups are created as local groups on non-domain controllers only. You can select to create default domain groups or domain local groups. To bypass the creation of default security groups, clear the **Create default security groups** check box.

- Click **Next**. The **Database Maintenance Wizard** displays the options you chose.



- To create the specified database, click **Finish**.

As the action runs, a progress bar displays the action occurring and the progress towards completion. When the action is finished, a message box appears.

- Click **OK**.

REMOVING AN EXISTING DATABASE

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.

- From the **Database Maintenance Wizard** main page, select **Remove an existing database** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
- In the **SQL Database Server Name** 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 to remove 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 **Database Maintenance Wizard** displays the options you chose.

Caution: Removing a database deletes it permanently from the system.

6. To permanently delete the database, click **Finish**.

As the action runs, a progress bar displays the action occurring and the progress towards completion. When the action is finished, a message box appears.

7. Click **OK**.

INCREASING DATABASE SIZE

Microsoft SQL Server automatically increases the size of the database file as needed, but if this happens while discoveries are running, it can significantly slow down the discovery process. If a discovery process seems to be running normally, and then suddenly slows down, you may want to increase the size of the database manually.

1. From the **Database Maintenance Wizard** main page, select **Increase database size** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click to locate the server.
3. In the **Database Name** box, type the name of the database to resize or click to locate the database.
4. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the existing size of the database.



Note: Enter the total size of the new 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.

6. In the **New Database Size** box, type a numeric value in megabytes that is greater than the existing value and represents the total size of the database, and then click **Next**. The **Database Maintenance Wizard** displays the options you chose.
7. Click **Finish**, and then click **OK**.

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.

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.

1. From the **Database Maintenance Wizard** main page, select **Shrink database** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click to locate the server.
3. In the **Database Name** box, type the name of the database to shrink, or click to locate the database.
4. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
6. Click **Finish**, and then click **OK**.

RUNNING AN SQL SCRIPT

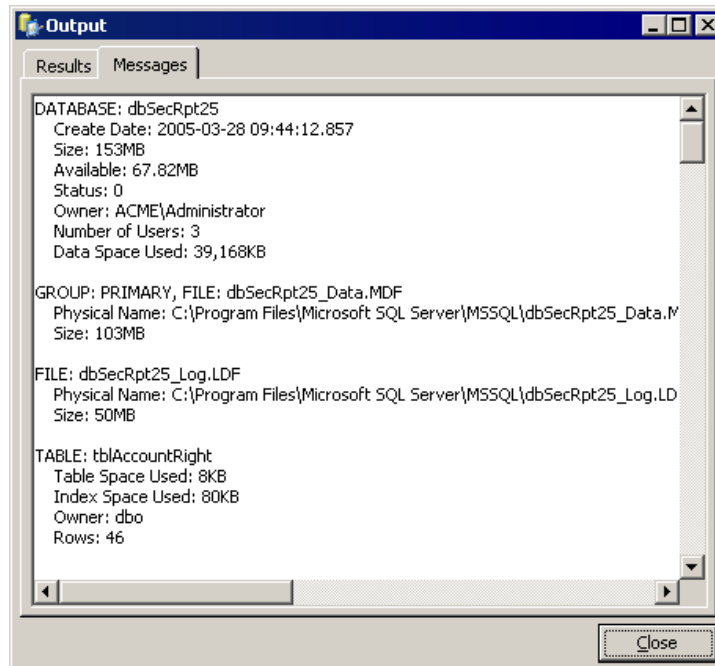
1. From the **Database Maintenance Wizard** main page, select **Run SQL Script** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the Microsoft Windows server where the database is located, or click to locate the server.
3. In the **Database Name** box, type the name of the database on which to run the SQL script, or click to locate the database.
4. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the SQL Script selection box.
6. In the **Select a SQL Script file to run** box, type the full path to the SQL Script File (*.sql) or click to locate the file. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.

7. Click **Finish**. A progress bar shows the progress of the action. Upon completion, the **Output** message box opens to the **Results** tab. To see messages regarding the action, open the **Messages** tab.
8. Click **Close**, and then click **OK**.

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 Maintenance Wizard** main page, select **View database statistics** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click **...** to locate the server.
3. In the **Database Name** box, type the name of the database, or click **...** to locate the database.
4. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
6. Click **Finish**, and then click **OK**. The **Output** dialog box opens to the **Messages** tab, which displays the database statistics.



- ▶ To save or print the output, right-click in the box, choose **Select All**. Right-click the selection, and then choose **Copy**. Paste from the clipboard into an application of your choice.
7. When you are finished viewing the statistics, click **Close**.

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 Maintenance Wizard** main page, select **Attach database** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click to locate the server.
3. In the **Database Name** box, type the name of the database to attach, or click to locate the database.
4. 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.
5. Click **Next**. The data file selection box appears.
6. In the **Select the MDF (data) file to attach** box, type the full path to the data file or click to locate the data file to attach.
7. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
8. Click **Finish**, and then click **OK**.

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.

1. From the **Database Maintenance Wizard** main page, select **Detach database** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click to locate the server.
3. In the **Database Name** box, type the name of the database to detach, or click to locate the database.

4. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
6. Click **Finish**. The **Output** message box opens to the **Messages** tab, which displays information about the process.
 - ▶ To save or print the output, right-click in the box, choose **Select All**. Right-click the selection, and then choose **Copy**. Paste from the clipboard into an application of your choice.
7. Click **Close**, and then click **OK**.

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 Maintenance Wizard** main page, select **Checkpoint and Truncate Log** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click to locate the server.
3. In the **Database Name** box, type the name of the database whose log file you want to truncate, or click to locate the database.
4. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the options you chose.
6. Click **Finish**, and then click **OK**.

SAVING CONNECTION INFORMATION

This option writes the database connection settings to the registry.

1. From the **Database Maintenance Wizard** main page, select **Save connection information** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click to locate the server.
3. In the **Database Name** box, type the name of the database, or click to locate the database.

4. 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the settings to be written to the registry.
6. Click **Finish**, and then click **OK**.

PERFORMING DATABASE MAINTENANCE

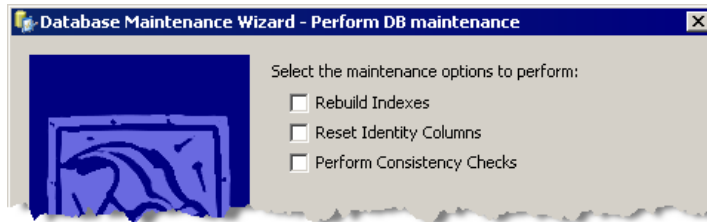
Performing regular database maintenance can help maintain the performance of SQL Server. Run this action if you feel SQL Server is not performing at the same level it once did. You can select to rebuild indexes, reset identify columns, and perform consistency checks.

Many SQL database administrators are familiar with Database Consistency Checker (DBCC) commands. The **Perform DB Maintenance** action performs the following 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 Maintenance Wizard** main page, select **Perform DB Maintenance** from the drop-down list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click to locate the server.
3. In the **Database Name** box, type the name of the database, or click to locate the database.
4. 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 maintenance options selection box appears.



Rebuild Indexes

Select to run CHECKINDEX and CHECKTABLE REPAIR_REBUILD.

Reset Identify Columns

Select to run CHECKIDENT.

Perform Consistency Checks

Select to run CHECKCATALOG, CHECKFILEGROUP, CHECKTABLE REPAIR_REBUILD, and CHECKINDEX.

- Choose the maintenance options to perform, and then click **Next**. The **Database Maintenance Wizard** displays the actions to be performed.
- Click **Finish**. When the process is complete, the **Database Maintenance Results** box opens to the **Messages** tab.
 - ▶ To save or print the output, right-click in the box, choose **Select All**. Right-click the selection, and then choose **Copy**. Paste from the clipboard into an application.
- Click **Close**, and then click **OK**.

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 Maintenance Wizard** main page, select **Reset database security** from the list, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
- In the **SQL Database Server Name** box, type the name of the server where the auditing 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 to use Windows or SQL Server 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 **Database Maintenance Wizard** displays actions to be performed.
- Click **Finish**, and then click **OK**.

SWITCHING THE SERVER 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 **SQL Server and Windows**.

1. From the **Database Maintenance Wizard** main page, select **Switch Server Security Mode**, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click **...** to locate the server.
3. In the **Database Name** box, type the name of the database, or click **...** to locate the database.
4. Choose whether to use Windows or SQL Server 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.
5. Click **Next**. The **Database Maintenance Wizard** displays the security mode options.



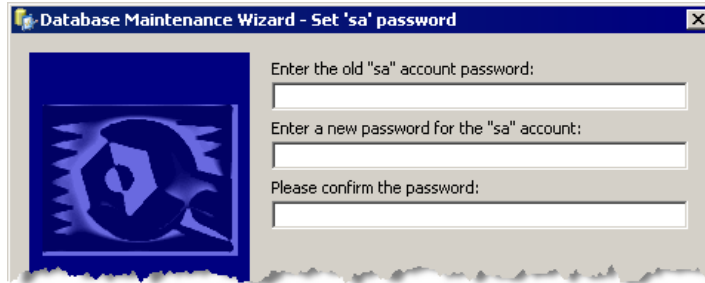
6. Select either **SQL Server and Windows** or **Windows only**, and then click **Next**. The **Database Maintenance Wizard** displays the actions to be performed.
7. Click **Finish**, and then click **OK**.

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 Maintenance Wizard** main page, select **Set 'sa' password**, and then click **Next**. The **Database Maintenance Wizard** displays the database selection options.
2. In the **SQL Database Server Name** box, type the name of the server where the database is located, or click **...** to locate the server.
3. In the **Database Name** box, type the name of the database, or click **...** to locate the database.

4. 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.
5. Click **Next**. The “sa” password box opens.



6. In the **Enter the old “sa” account password** box, type the existing password.
7. In the **Enter a new password for the “sa” account** box, type the new password.
8. In the **Please confirm the password** box, retype the new password.
9. Click **Next**. The **Database Maintenance Wizard** displays the actions to be performed.
10. Click **Finish**, and then click **OK**.

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 client utilities.

Note: Client utilities are available only on a full version of SQL Server 2000, 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.

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 either ScriptLogic's WinCloak, or Windows Access-Based Enumeration (available with Windows Server 2003 Service Pack 1) enabled and operational.

UNINSTALLING FILE SYSTEM AUDITOR

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

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.

Index

A

- adding
 - file masks, 23
 - file path to filter, 23
 - process filters, 25
- attaching
 - database, 34

C

- creating
 - database, 28

D

- database
 - attaching, 34
 - creating, 28
 - detaching, 30, 34
 - increasing size, 31
 - maintenance, 36
 - moving to another server, 39
 - removing, 30
 - setting, 22
 - setting logon account, 22
 - shrinking, 32
 - viewing statistics, 33
- DBCC commands, 36
- detaching
 - database, 30, 34
- duplicate entries
 - suppressing, 26

E

- editing
 - file path filter, 25
- excluding
 - files, 23
 - folders, 23

F

- file extensions
 - .ldf, 13
 - .mdf, 13
 - .sql, 32
- file masks
 - adding, 23
 - removing, 24
- File menu, 21
- File System Auditor
 - starting, 20
- filters

- file path, 23
- process, 25

H

- Help menu, 21

I

- including
 - files, 23
 - folders, 23
- increasing
 - database size, 31

M

- masks. *See* file masks
- menus
 - File, 21
 - Help, 21
 - Options, 21
- Microsoft Data Engine 2000, 27
- moving
 - database to another server, 39
- MSDE, 27

O

- opening
 - FSA Service Configuration, 20
- Options menu, 21

P

- path filter
 - editing, 25
 - removing, 25
- pattern detection
 - rename-and-delete, 26
- process filters
 - adding, 25
 - removing, 26

R

- reducing
 - database size, 32
- removing
 - database, 30
 - file masks, 24
 - file path filter, 25
 - process filters, 26
- rename-and-delete
 - disable pattern detection, 26

S

- sa password
 - setting, 38
- saving
 - connection information, 35
- Security Explorer
 - removing, 40
- servers
 - moving a database, 39
- setting
 - database, 22
 - database logon account, 22
 - process filters, 25
 - sa password, 38
 - SQL server, 22
 - suppression delta, 26
- setting filters
 - file path, 23
- shrinking
 - database, 32

- SQL Script
 - running, 32
- SQL Script File, 32
- SQL server
 - setting, 22
- starting
 - Enterprise Security Reporter, 18
 - FSA Service Configuration, 20
- suppression delta, 26

T

- tempdb database, 32
- transation log
 - truncating, 35
- truncate
 - transaction log, 35

V

- viewing
 - database statistics, 33