

File System Auditor 1.0 Release Notes

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.

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.
- 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.

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.

- 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

Install the Console component on each workstation from which you want to audit events in the database.

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.
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.
 - 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.

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 **Set the server and database name** box 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.

- To remove a selected file mask, click **Remove** in the appropriate area.
6. 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.


1. 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.
2. 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 **Tools** 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 patten 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.

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.

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 fully functional 45-day 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.