ScriptLogic®
File System Auditor
User Guide

SCRIPTLOGIC

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

1.561.886.2400
www.scriptlogic.com

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

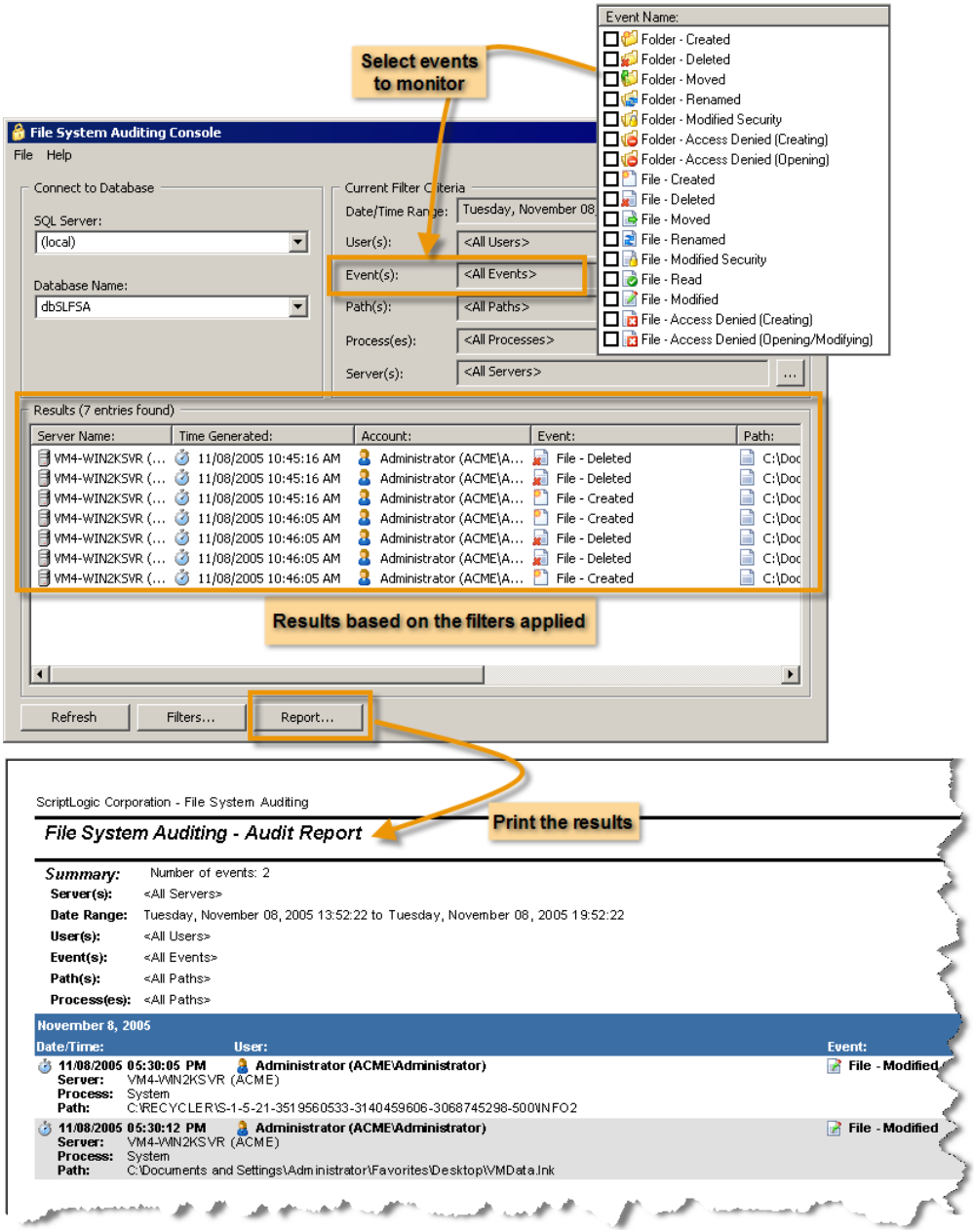
ScriptLogic can be found on the web at www.scriptlogic.com. Our web site offers customers a variety of information:

- 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.

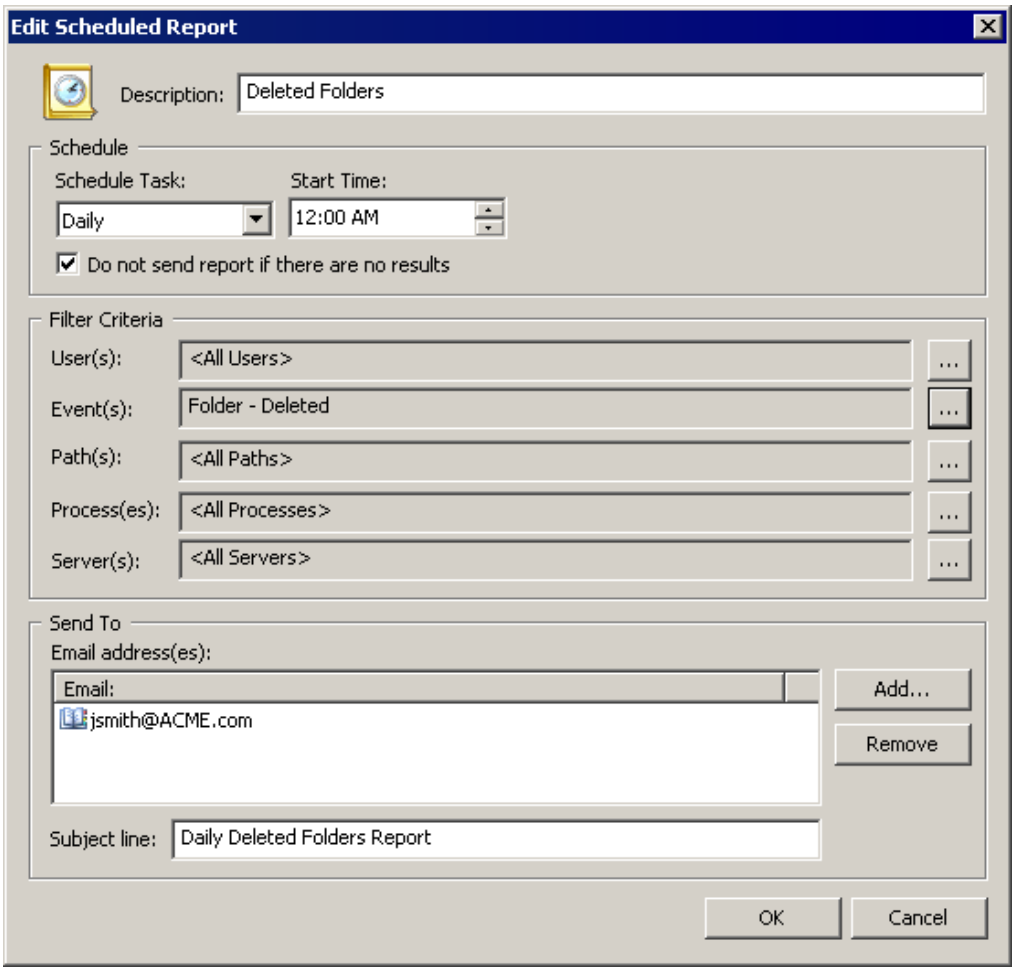
Contents

What is File System Auditor?

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.



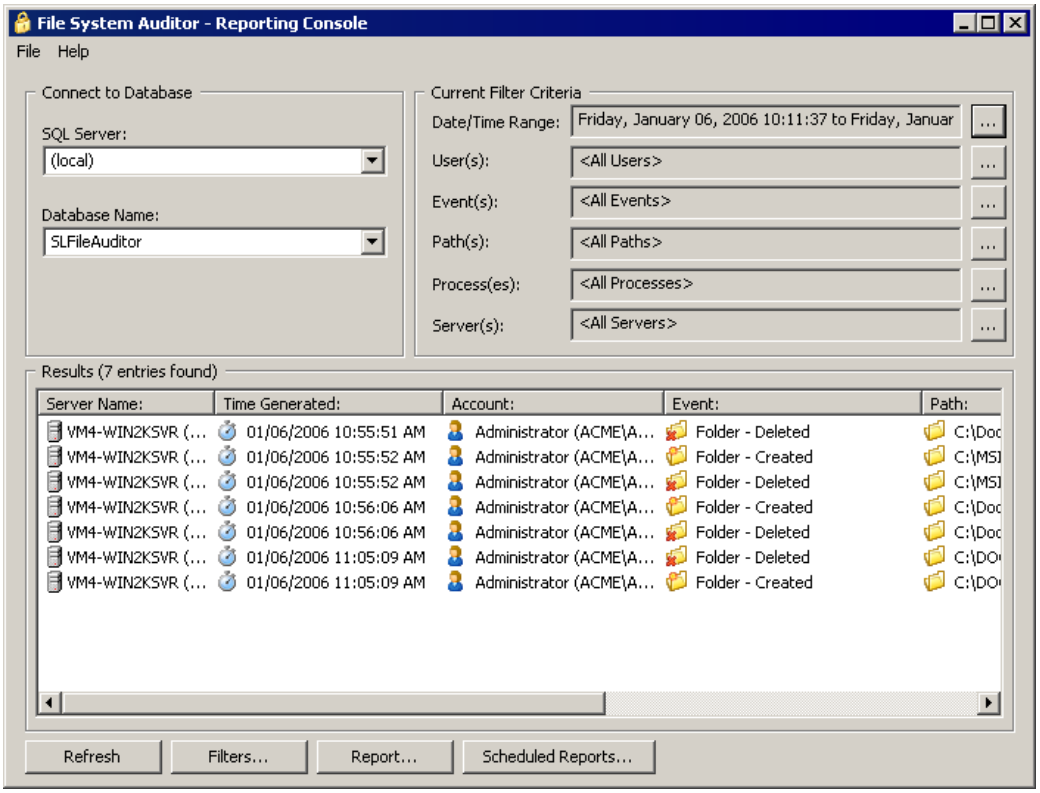
File System Auditor assists in security management by sending email alerts whenever specific file system events occur, such as failed access attempts, or modifications of a particular set of files and folders. Reports can be sent out on a daily or weekly basis, or frequently in 5, 10, 15, 20, 30, or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



Reporting Events

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

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



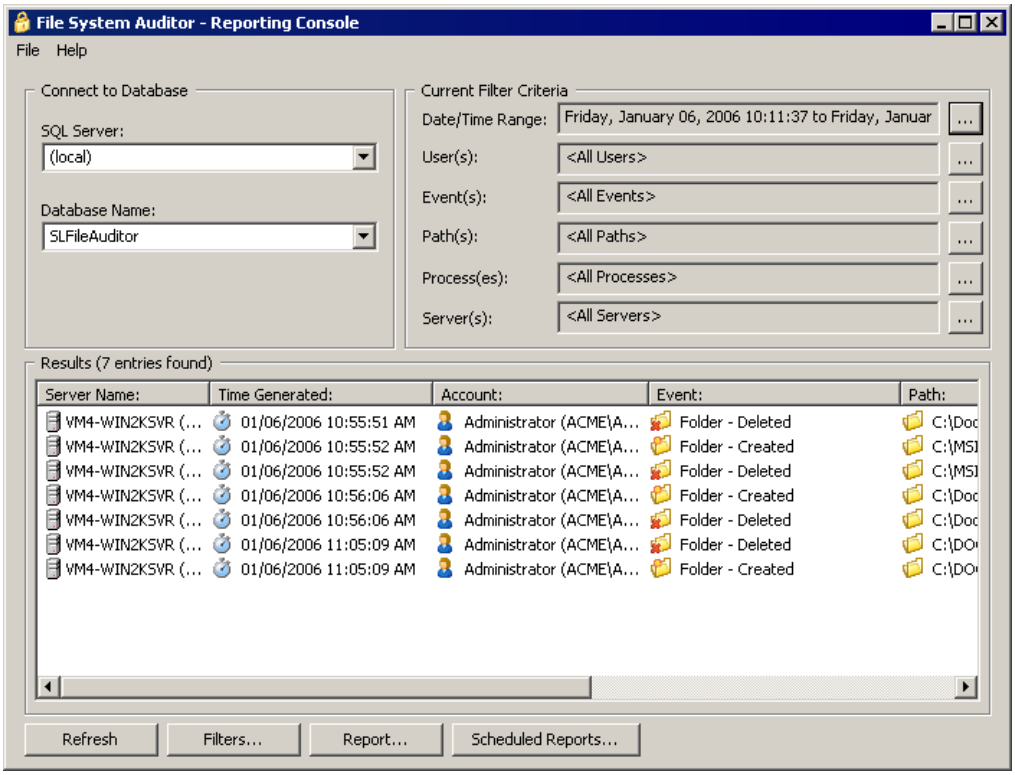
STARTING FSA REPORTING

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

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 REPORTING CONSOLE MAIN WINDOW

The **File System Auditor Reporting Console** displays the current database, filters, and results.

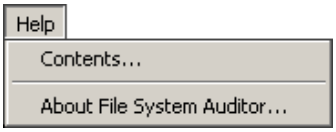


Button	Description
...	Define criteria to filter the results. See *Setting Filters*.
Stop / Refresh	Stop the collection of data or update the list in the **Results** area.
Filters	Define criteria to filter the results. See *Setting Filters*.
Report	Display a report based on the results list that you can view or print. See *Printing a Report*.
Scheduled Reports	Create a filter under which to run a report on a scheduled basis. See *Managing Scheduled Reports*.

File Menu

Menu Option	Description
Exit	Closes File System Auditor.

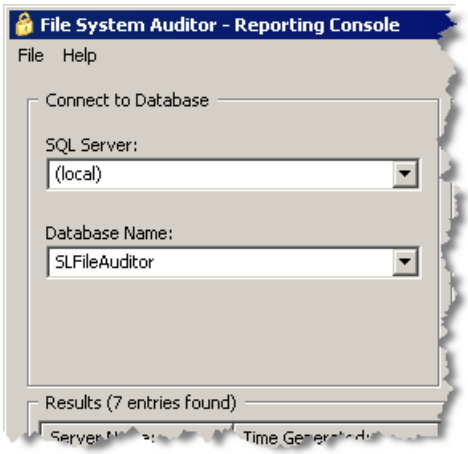
Help Menu



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.

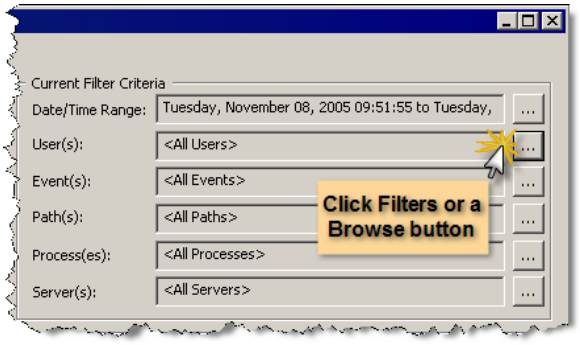
CONNECTING TO A DATABASE

Initially, the database created during installation displays in the **Connect to Database** area of the **File System Auditing Console** window. If more than one SQL Server or database exists, you can select them from the appropriate list.



SETTING FILTERS

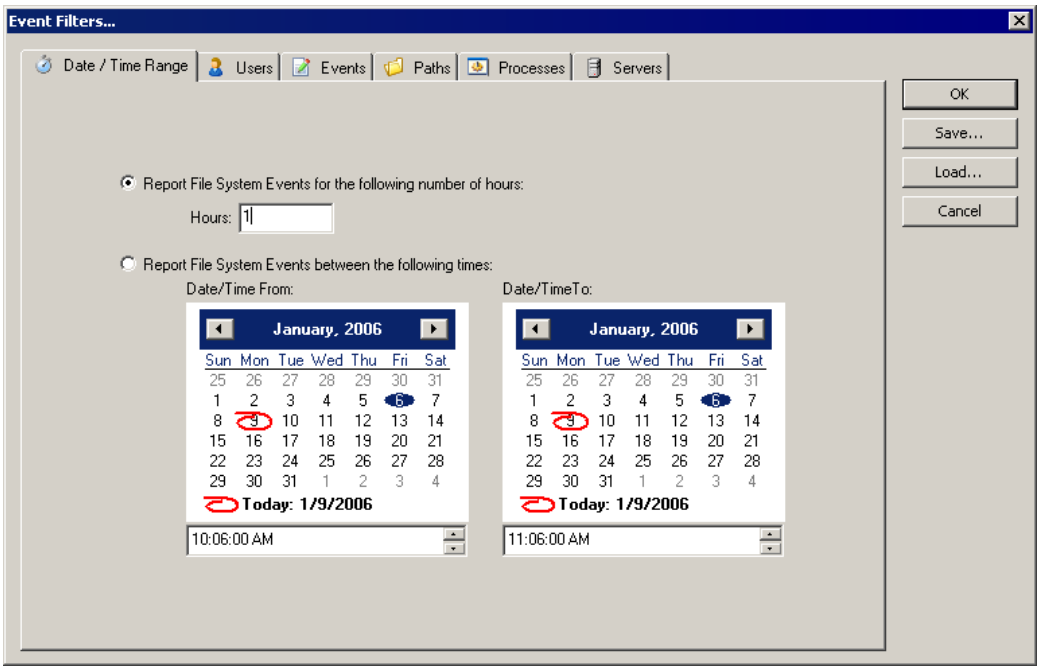
- Click **Filters**. The **Event Filters** dialog box opens to the **Date/Time Range** tab. You also can click ... next to each filter setting in the **Current Filter Criteria** area to open the associated tab.



Note: It is not advisable to select a root drive and audit every folder and file action because of the amount of data that would be collected.

Setting the Date/Time Range Filter

- Click **Filters**, or click … next to the **Date/Time Range** filter setting in the **Current Filter Criteria** area. The **Date/Time Range** tab opens.



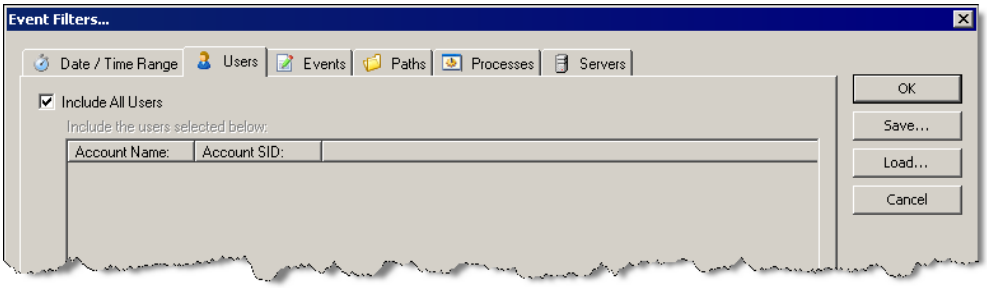
Report File System Events to the following number of hours
Select to include events in the report for the number of hours as indicated in the **Hours** box. By default, reports include file system events for one hour.

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

Button	Description
OK	Closes the window and saves the selections for the current session.
Save	Saves the selections to a filter file. See *Saving Filters*.
Load	Loads the selections from a saved filter file. See *Loading Filters*.
Cancel	Closes the window without saving the selections for the current session.

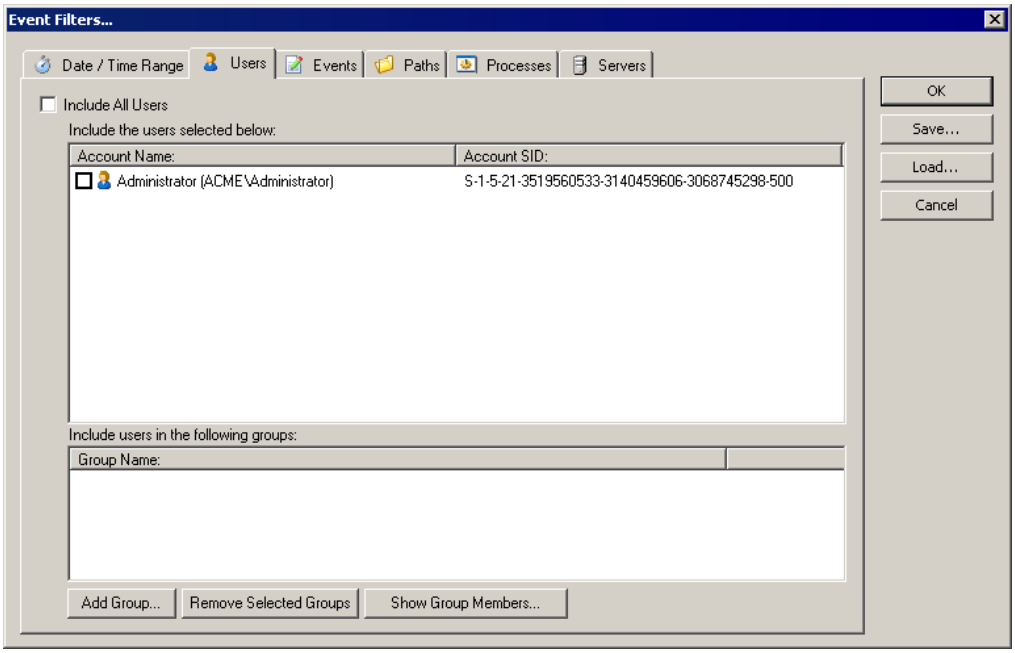
Setting the Users Filter

- Click **Filters**, and then open the **Users** tab, or click … next to the **Users** filter setting in the **Current Filter Criteria** area. The **Users** tab opens. Initially, the list is empty.



Include All Users

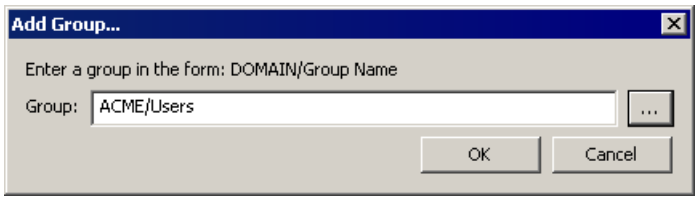
By default, all users who are currently signed on to the system are included in the report. To select specific users, clear the check box. The display refreshes showing all the users who are currently in the auditing database. Select the check box next to each user.



Button	Description
Add Group	Add groups to the list. See *Adding Groups*.
Remove Selected Groups	Remove selected groups from the list. See *Adding Groups*.
Show Group Members	Displays the members of the selected group. See *Adding Groups*.
OK	Closes the window and saves the selections for the current session.
Save	Saves the selections to a filter file. See *Saving Filters*.
Load	Loads the selections from a saved filter file. See *Loading Filters*.
Cancel	Closes the window without saving the selections for the current session.

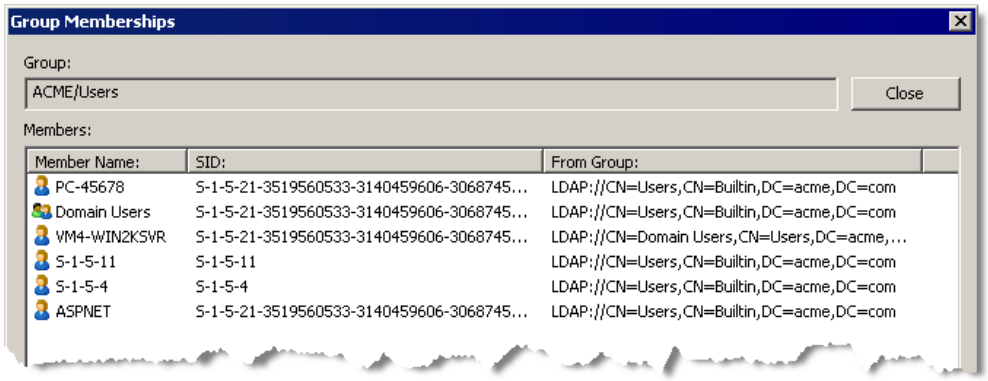
Adding Groups

1. Open the **Users** tab, and then click **Add Group**.
2. In the **Group** box, type a group name in the format DOMAIN/Group Name, or click … to locate a group.



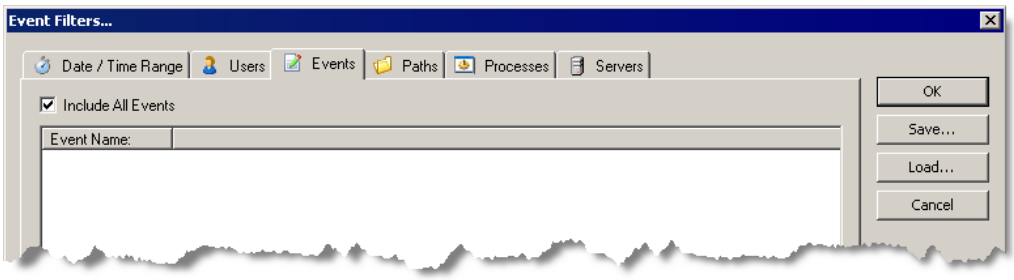
3. Click **OK**. The group displays in the **Group Name** area.

- To remove selected group(s) from the list, click **Remove Selected Groups**.
- To display the members of a selected group, click **Show Group Members**. The **Group Memberships** window displays the group members.



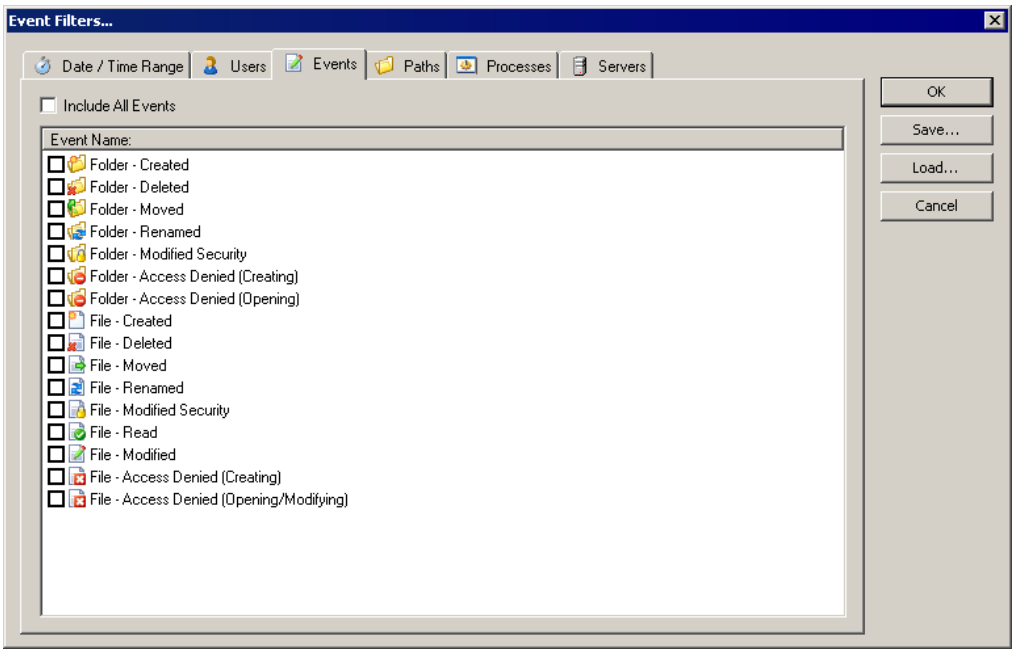
Setting the Events Filter

- Click **Filters**, or click … next to the **Events** filter setting in the **Current Filter Criteria** area. The **Events** tab opens. Initially, the list is empty.



Include All Events

Select to include all events. By default, all events are included in the report. To select specific events, clear the check box. The display refreshes showing the events that you can select.



Button	Description
OK	Closes the window and saves the selections for the current session.
Save	Saves the selections to a filter file. See *Saving Filters*.
Load	Loads the selections from a saved filter file. See *Loading Filters*.
Cancel	Closes the window without saving the selections for the current session.

Note: It is not advisable to audit every folder and file action due to the amount of data that would be collected.

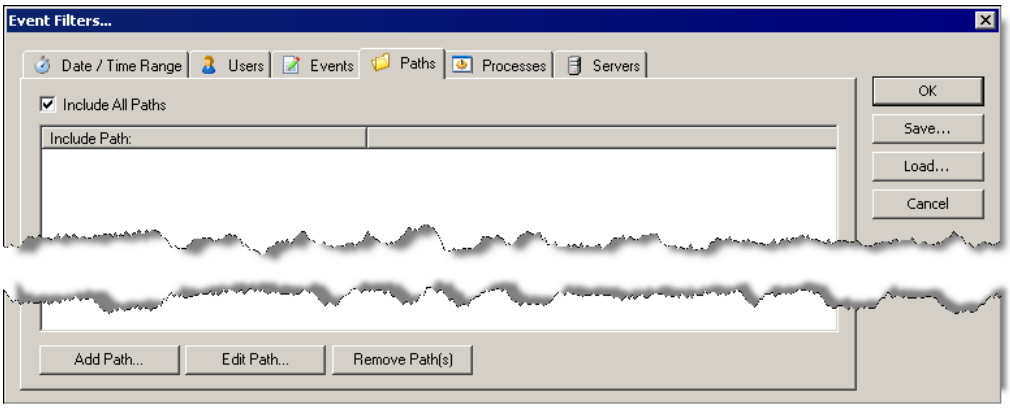
Important: If an event was filtered out from being captured in the auditing database, you will not see a result even if you select the filter from this list.

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.

Setting the Paths Filter

- Click **Filters**, and then open the **Paths** tab, or click ... next to the **Paths** filter setting in the **Current Filter Criteria** area. The **Paths** tab opens. Initially, the list is empty.



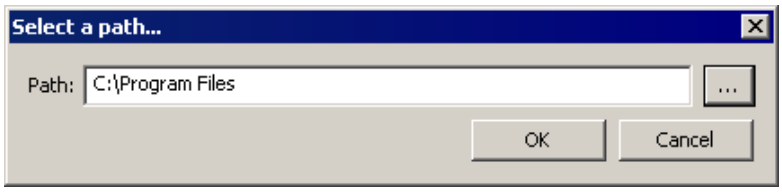
Include All Paths
Select to include all folders and files. By default, all paths are included in the report. To select specific folders and files, clear the check box, or click **Add Path**.

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

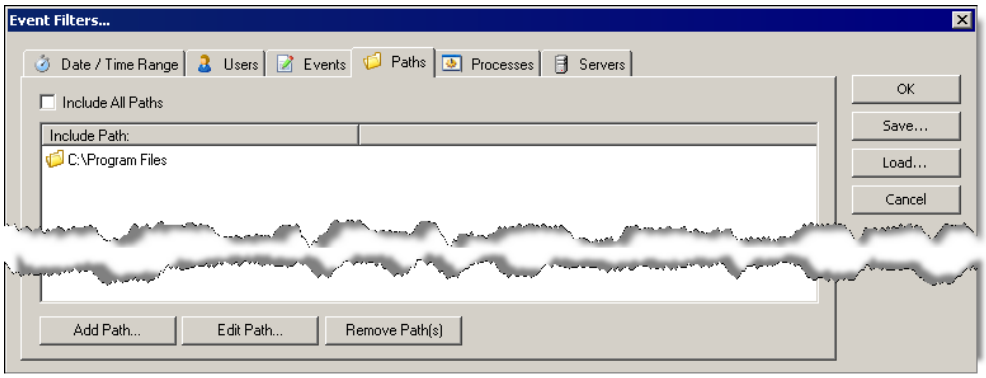
Button	Description
Add Path	Add a file path filter. See *Adding a Path*.
Edit Path	Edit selected file path filter. See *Adding a Path*.
Remove Path(s)	Delete selected path(s).
OK	Closes the window and saves the selections for the current session.
Save	Saves the selections to a filter file. See *Saving Filters*.
Load	Loads the selections from a saved filter file. See *Loading Filters*.
Cancel	Closes the window without saving the selections for the current session.

Adding a Path

1. On the **Paths** tab, clear the **Include All Paths** check box, or click **Add Path**. The **Select a Path** box appears.



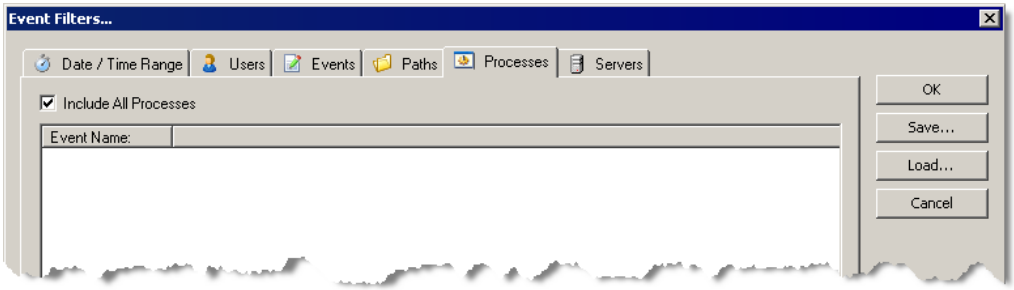
2. Type a path in the box or click ... to locate a path, and then click **OK**. The path displays in the **Include Path** column.



- To edit a selected path, click **Edit Path**.
- To remove selected path(s), click **Remove Path(s)**.

Setting the Processes Filter

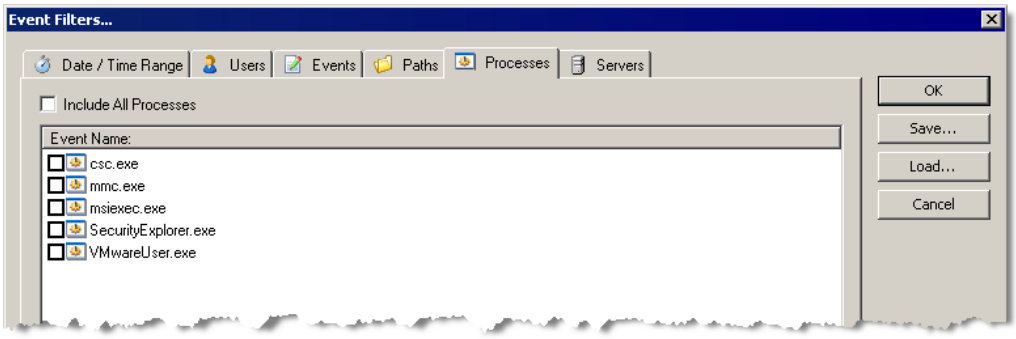
- Click **Filters**, and then open the **Processes** tab, or click … next to the **Processes** filter setting in the **Current Filter Criteria** area. The **Processes** tab opens. Initially, the list is empty.



Include All Processes

By default, all configured processes are included in the report. To select specific processes, clear the check box. The display refreshes showing the processes that you can select.

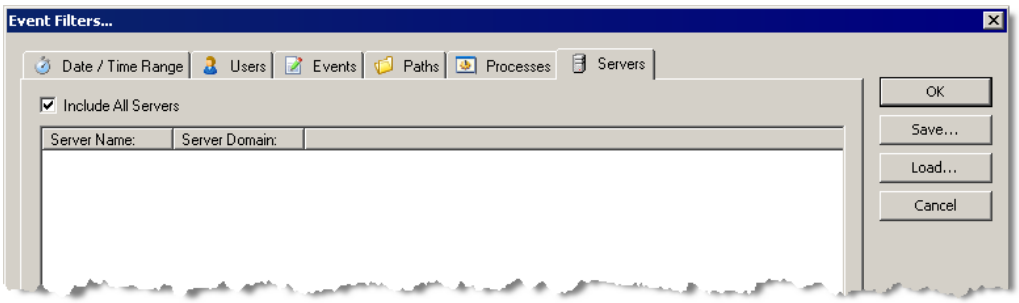
Note: Only local processes display in the list. Any file activity performed by a remote user displays under the System process. You can configure the service to ignore local virus scanning and backup software using the process filters in the Service Configuration Utility. See the *Getting Started Guide*.



Button	Description
OK	Closes the window and saves the selections for the current session.
Save	Saves the selections to a filter file. See *Saving Filters*.
Load	Loads the selections from a saved filter file. See *Loading Filters*.
Cancel	Closes the window without saving the selections for the current session.

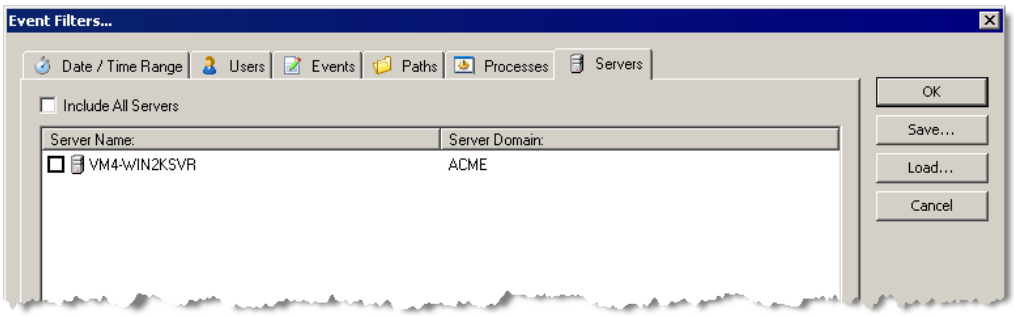
Setting the Servers Filter

- Click **Filters**, and then open the **Servers** tab, or click … next to the **Servers** filter setting in the **Current Filter Criteria** area. The **Servers** tab opens. Initially, the list is empty.



Include All Servers

Select to include all servers. By default, all servers are included in the report. To select specific servers, clear the check box. The display refreshes showing the servers that you can select.

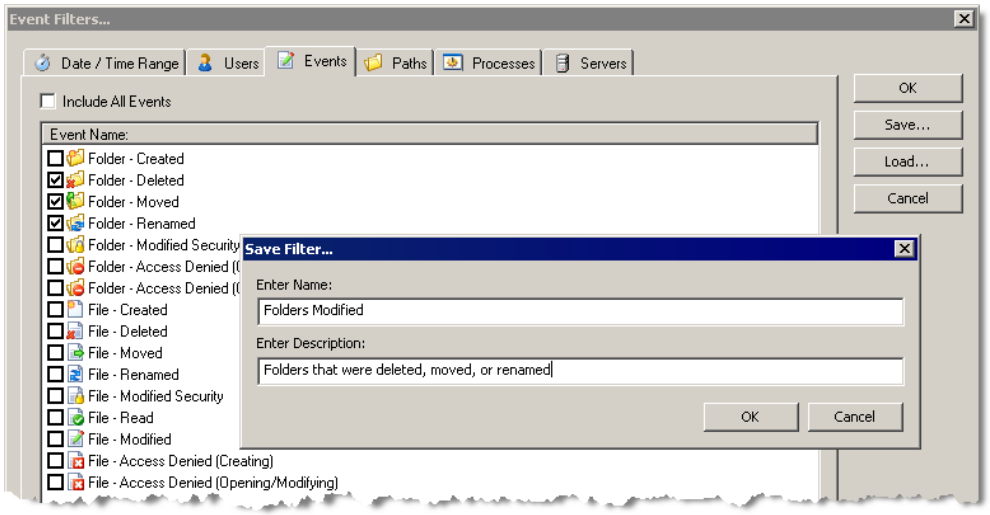


Button	Description
OK	Closes the window and saves the selections for the current session.
Save	Saves the selections to a filter file. See *Saving Filters*.
Load	Loads the selections from a saved filter file. See *Loading Filters*.
Cancel	Closes the window without saving the selections for the current session.

SAVING FILTERS

From each event filter tab, you can save your selections to a File System Auditor Filter File (.fsv) for reuse.

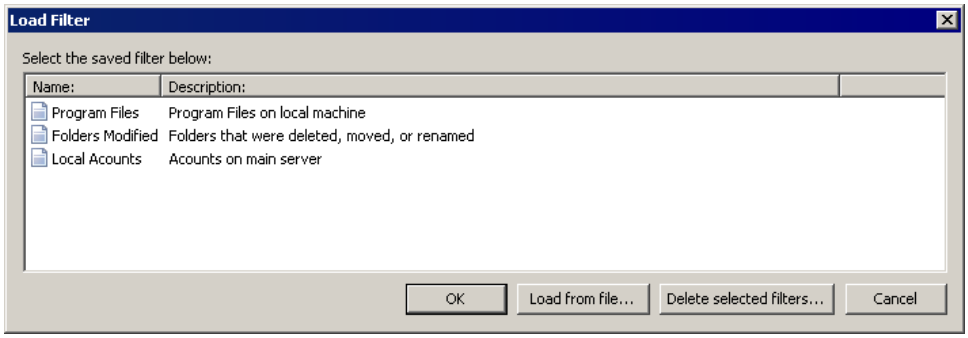
1. From an event filter tab, set up the filter, and then click **Save**. The **Save Filter** box appears.



2. Type a name and description for the filter, and then click **OK**. The filter settings are saved in a **File System Auditor Filter File (.fsv)** in the **Program Files\ ScriptLogic Corporation\File System Auditor** folder.

LOADING FILTERS

1. From an event filter tab, click Load. The Load Filter box displays the saved File System Auditor Filter Files (.fsv).

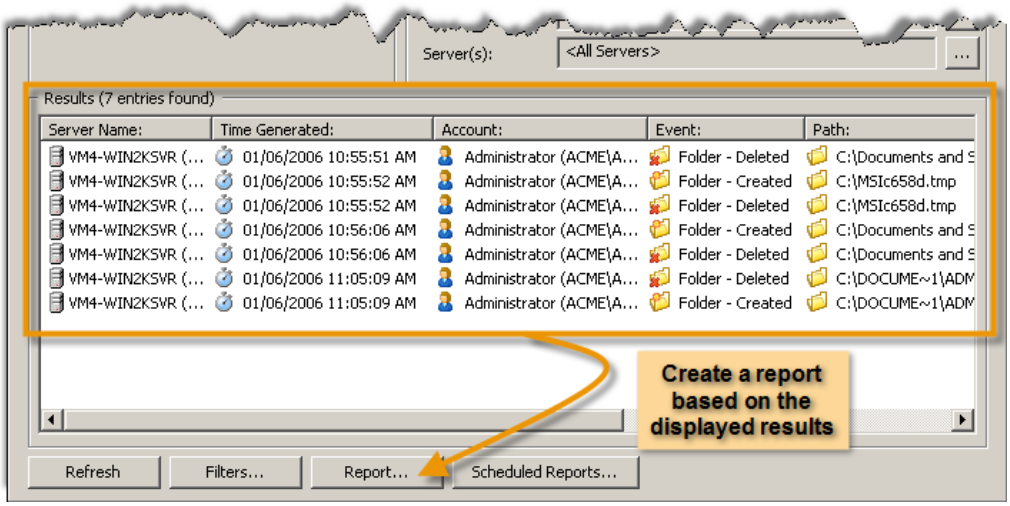


   - To delete selected filter files, click **Delete selected filters**.

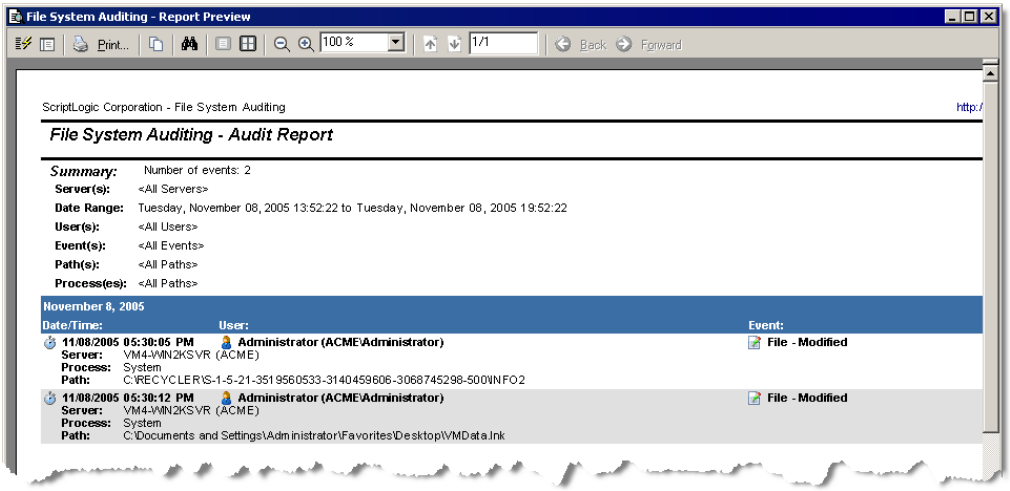
2. Select a saved filter file, and then click **OK**. Alternatively, you can click **Load from file**, and then select a filter file.

PRINTING A REPORT

You can prepare a report of the results that appear in the **Results** area of the main window.

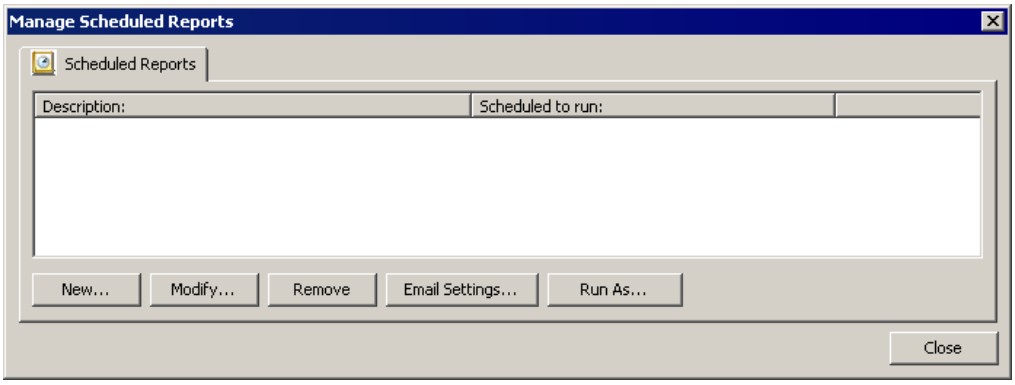


- When you have the list of results that you want, click **Report**. The **Report Preview** window displays the **Audit Report**, which you can view or print.



MANAGING SCHEDULED REPORTS

- From the Reporting Console, click **Scheduled Reports**. The **Manage Scheduled Reports** box appears.

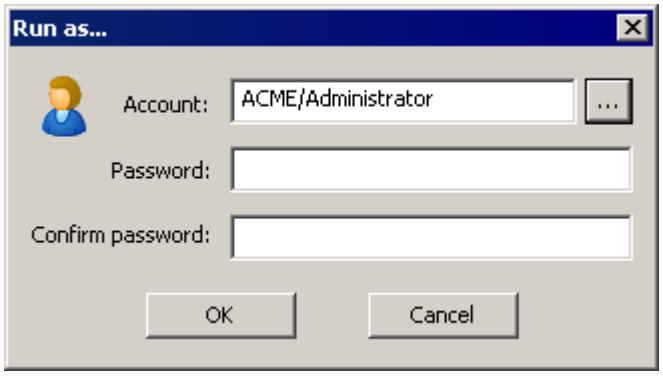


Button	Description
New	Create a new scheduled report. See *Creating a New Scheduled Report*.
Modify	Modify a scheduled report. See *Creating a New Scheduled Report.*
Remove	Remove selected scheduled reports.
Email Settings	Set up email for scheduled reports. See *Setting the Email Account*.
Run As	Set the account under which scheduled reports jobs run. See *Setting the Scheduled Reports Logon Account.*

SETTING THE SCHEDULED REPORTS 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.

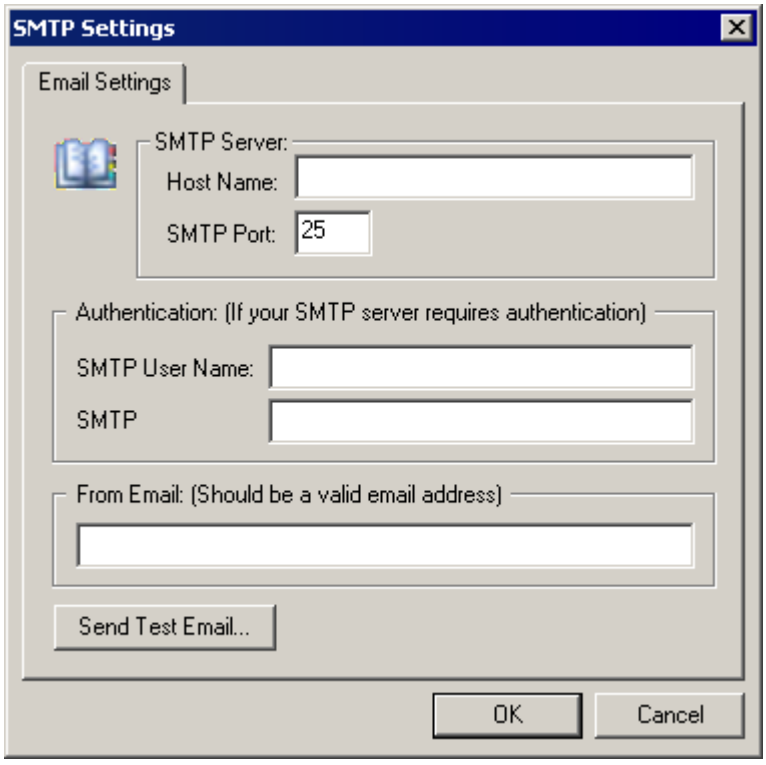
1. From the **Scheduled Reports** tab, click **Run As**. The **Run as** box opens.
2. In the **Account** box, type the account name under which the scheduled reports will run, or click ... to locate an account.



3. In the **Password** and **Confirm password** boxes, type the password for the account, and then click **OK**.

SETTING THE EMAIL ACCOUNT

1. From the **Scheduled Reports** tab, click **Email Settings**. The **SMTP Settings** box appears.

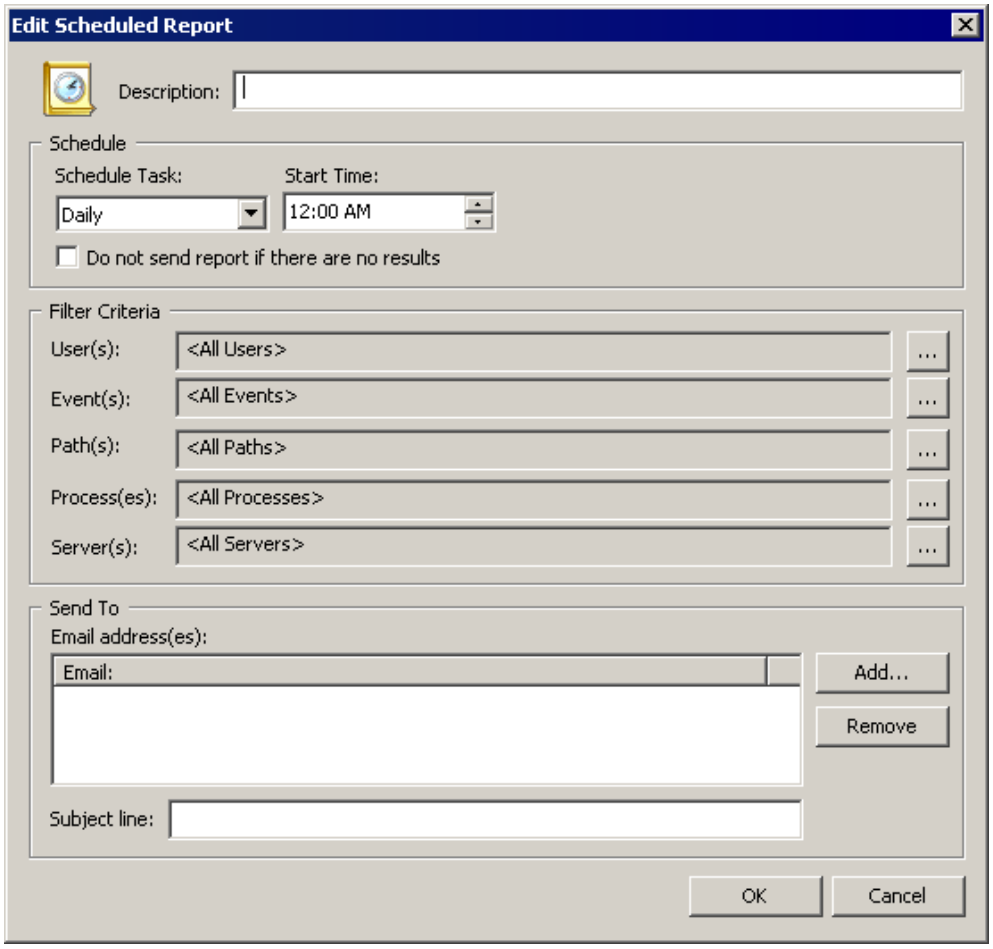


2. In the **SMTP Server Host Name** box, type the name of the SMTP server that sends the scheduled report emails.
3. In the **SMTP Port** box, type the number of the TCP/IP port on which the SMTP server is listening. The default is 25.
4. If your SMTP server requires authentication, type the username and password in the **SMTP User Name** and **SMTP Password** boxes.
5. In the **From Email** box, type the email address that to appear in the From box of the email.
6. Click **Send Test Email** to check the entries.

CREATING A NEW SCHEDULED REPORT

1. Click **New**. The **Edit Scheduled Report** box appears.

Note: If you have not set up an account under which the scheduled report job will run, you see an error message. Click **OK** and then set up the run as account. See *Setting the Scheduled Reports Logon Account*.



2. In the **Description** box, type a name for the report.
3. In the **Schedule** area, select a time frame for the report.

Schedule Task	Start Time
Frequently	Chose every 5, 10, 15, 20, 30, or 60 minutes
Daily	Choose a time
Weekly	Choose a time and day

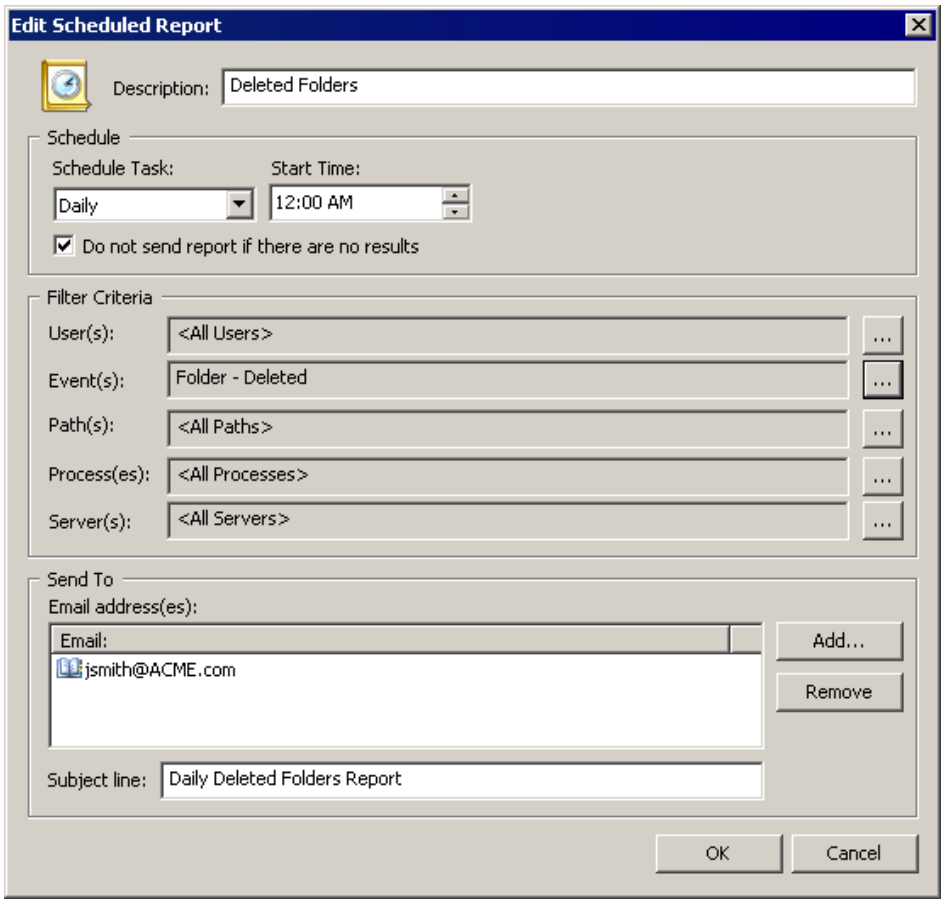
☐ **Do not send report if there are no results**
Select to not send a report if there are no results. By default, a report is sent to the addresses specified in the **Send to** area even if there are no results in the report.

4. In the **Filter Criteria** area, set up the filters by which to filter the data collected. See *Setting Filters*.

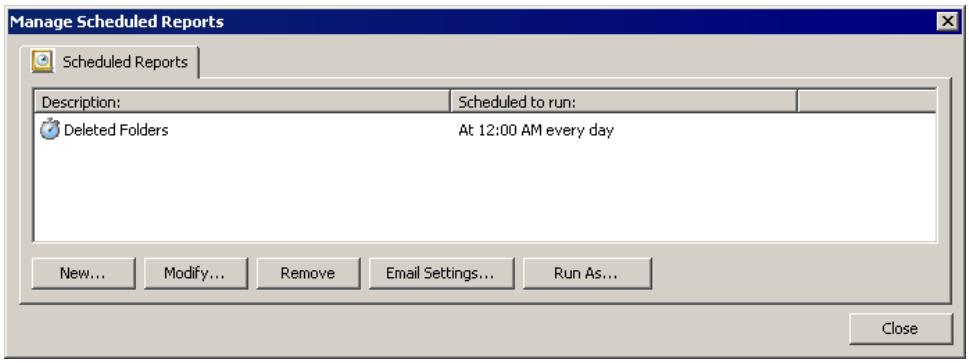
5. In the **Send to** area, click **Add**. The **Enter email address** box appears. Type an email address, and then click **OK**.

   - To delete selected email addresses from the list, click **Remove**.

6. In the **Subject line** box, type a subject line for the email that is sent.



7. Click **OK**. The scheduled report displays.



   - To modify a selected report, click **Modify**.
   - To delete selected reports from the list, click **Remove**.

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**.

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

U