



# FileAudit

GETTING STARTED GUIDE

5

VERSION



[www.isdecisions.com](http://www.isdecisions.com)



## Introduction

FileAudit monitors access or access attempts to sensitive files and folders on Microsoft Windows servers. FileAudit allows you to proactively track, audit, report and alert on all access to files and folders on your file servers. Agentless and non-intrusive, you can remotely audit your servers without installing anything on them.

The 'FileAudit Getting Started Guide' is designed to provide step by step installation instructions and configuration for the main features. The goal is to quickly get comfortable with the console and basic FileAudit concepts. Additional features are fully described into the [software help file](#).

If you run into issues or questions during your evaluation, installation or migration, we invite you to contact our [Technical Support Team](#).

## Table of contents

- 1. Install FileAudit.....3**
- 2. Configure your first audit path and define an alert on it. ....5**
  - 2.1. Configure your first audit path..... 5
  - 2.2. Define an alert on this audited folder. .... 9
- 3. Display the file access events ..... 16**
- 4. Set an automatic report. .... 18**
- 5. Additional settings..... 21**
  - 5.1. Exclude users, programs and extensions from the audit. ....21
  - 5.2. Granularly authorize FileAudit access for specific accounts. ....22



## 1. Install FileAudit

The FileAudit installation package (*FileAudit-Setup.exe*) is available [here](#).

The English and French language versions are identical and are compatible with 32- and 64-bit platforms.

FileAudit supports the following operating systems for Audit service installation (as for Console installation):

- Windows 10
- Windows 8
- Windows 2012 R2 Server
- Windows 2012 Server
- Windows 7
- Windows 2008 R2 Server
- Windows 2008 Server
- Windows Vista
- Windows 2003 Server
- Windows XP

The .Net Framework 4 is required for installation.

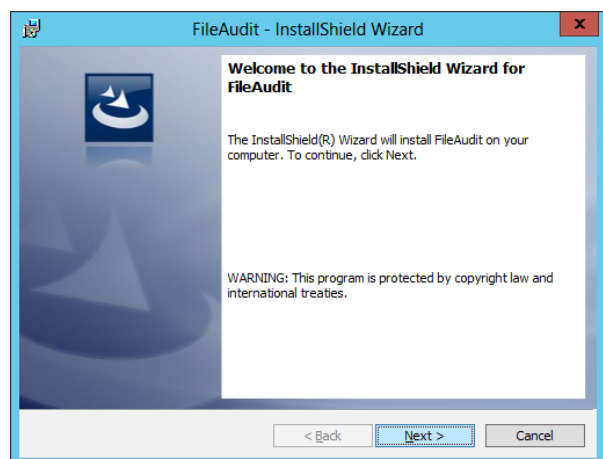
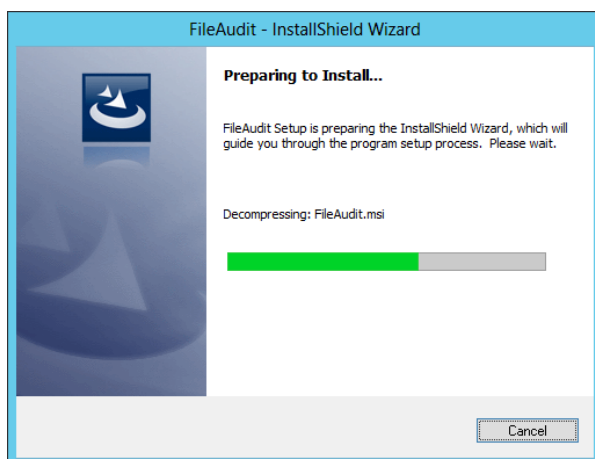
Installation of FileAudit on the system to be audited is not mandatory. Any machine meeting the system requirements can be used as a remote host for FileAudit, and the system to be remotely audited requires no further installations.

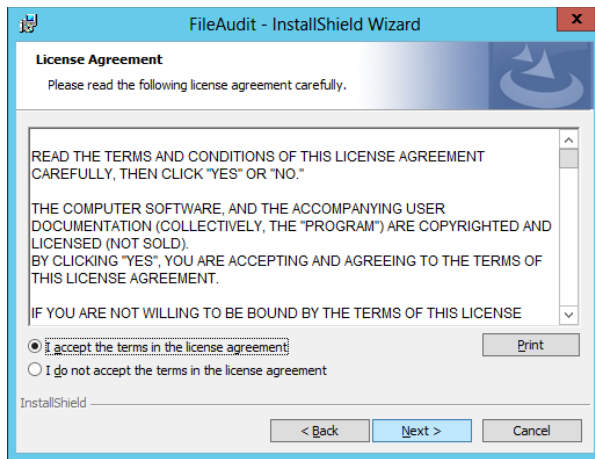
FileAudit will store all detected events in a database. FileAudit supports the following database systems:

- Microsoft Access database file (mdb)
- Microsoft SQL Express 2005/2008/2008 R2
- Microsoft SQL Server 2005/2008/2008 R2/2012

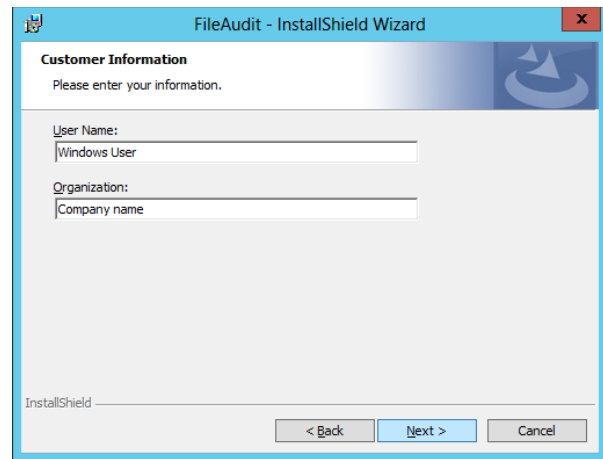
The FileAudit package also provides a free Microsoft Access database facility.

To launch the FileAudit installation process, run *FileAudit\_x86.exe* using an administrator account:

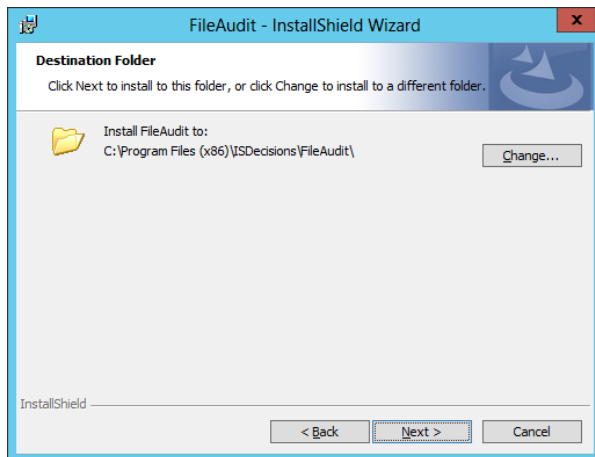




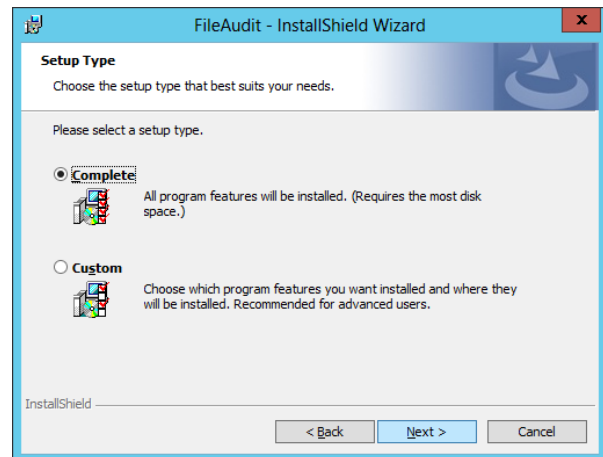
Carefully read and accept the *End User License Agreement*, and click 'Next >'.



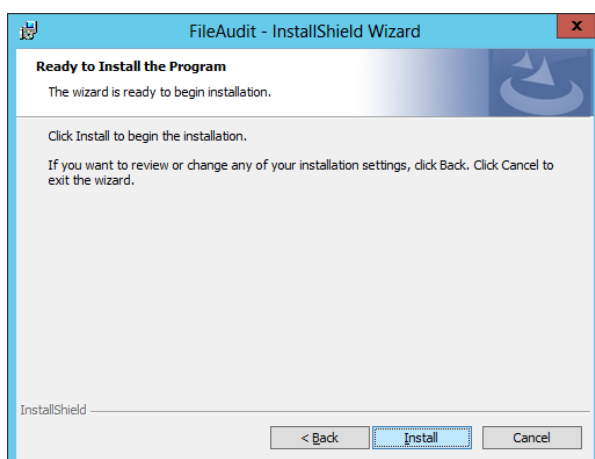
Enter your customer references and click 'Next >'.



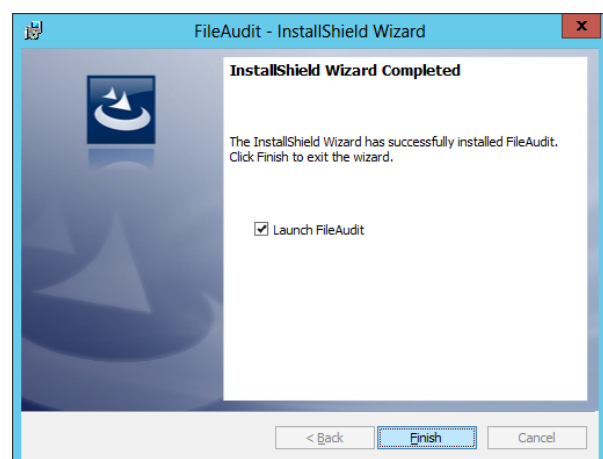
The installation folder can be changed if required



Keep the 'Complete' box checked and click 'Next >'.



Click 'Install' to begin FileAudit installation.



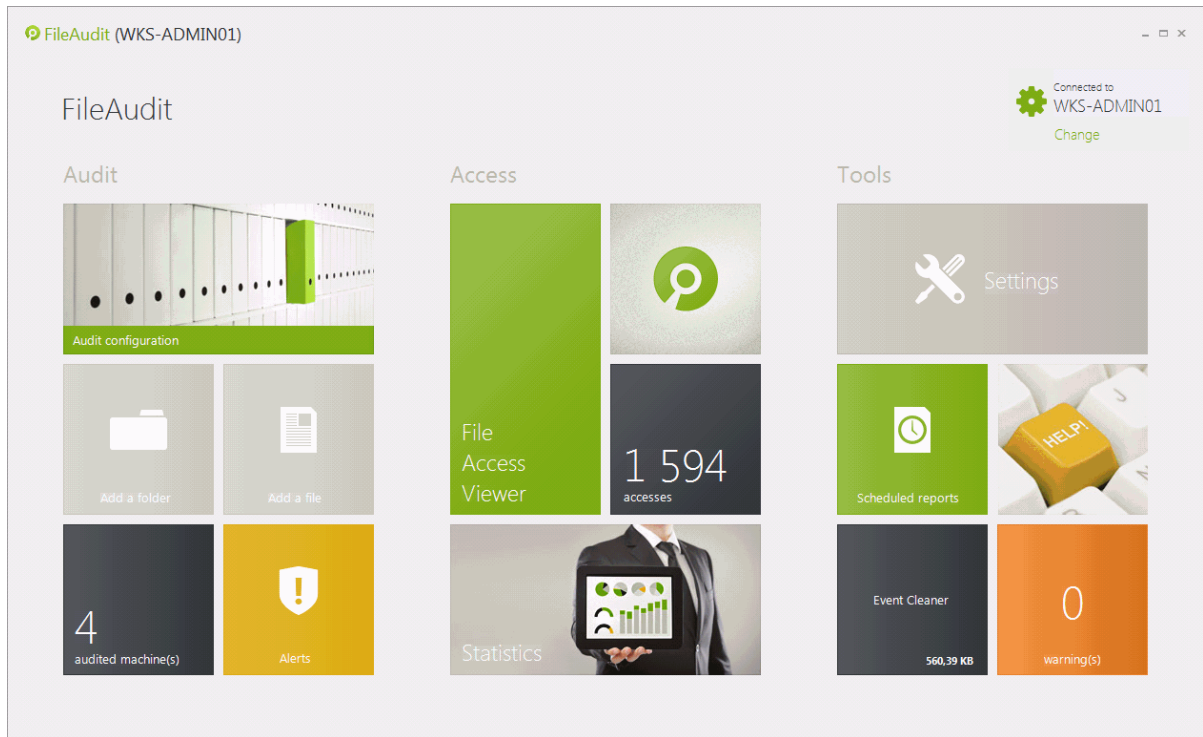
FileAudit has been successfully installed.  
Click 'Finish'.



## 2. Configure your first audit path and define an alert on it

### 2.1. Configure your first audit path.

Launch FileAudit.



FileAudit Hub

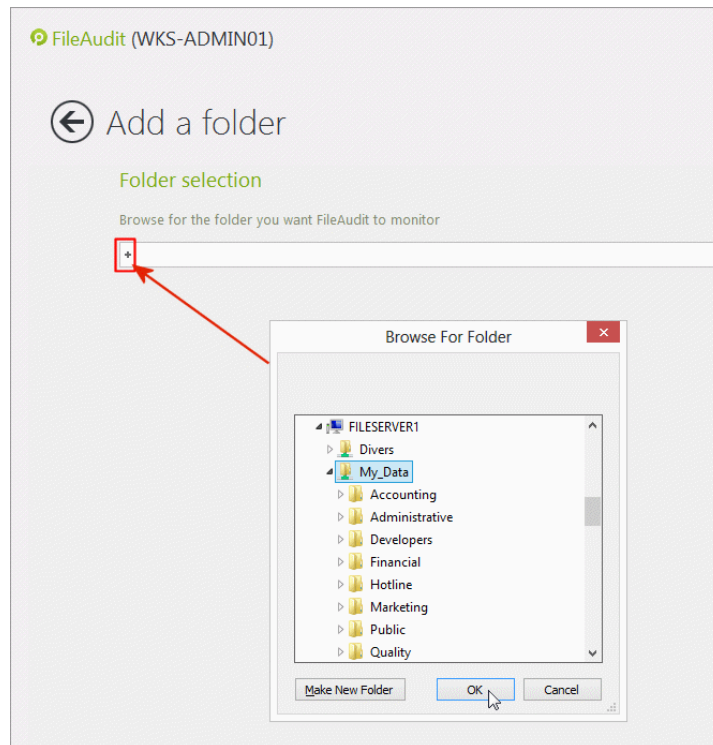
You will find 3 main tile groups:

- **Audit:** Tiles allowing you to configure your audit and alerts.
- **Access:** Tiles displaying the 'File Access Viewer' and the 'Statistics' view.
- **Tools:** Tiles customizing FileAudit settings, scheduling automatic reports, cleaning database and accessing the help file.

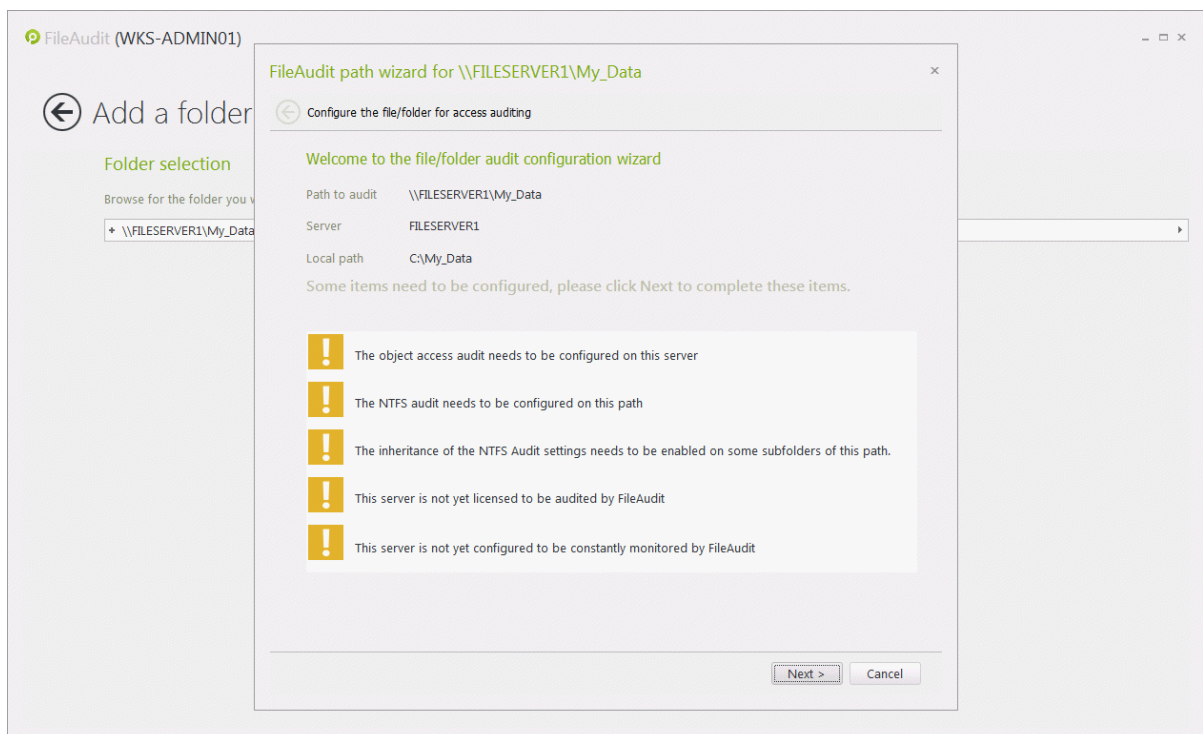
The additional '**Connect**' button at the top right hand corner allows you to remotely connect to another system running the 'FileAudit service'.



To set your first path to audit, click the 'Add a folder' tile in the FileAudit hub. Click the '+' button and browse for your target folder:

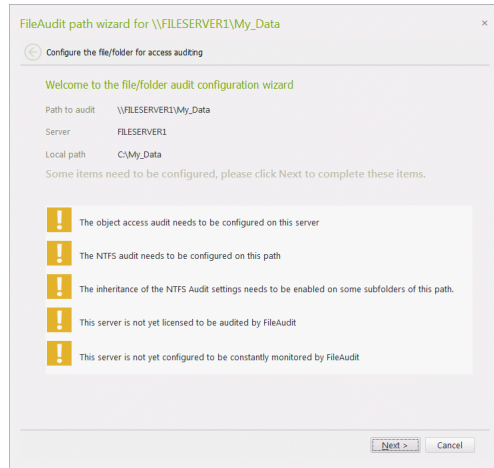


Having validated your selection, the 'FileAudit path wizard' will pop up to guide you through the process of configuring the folder audit.

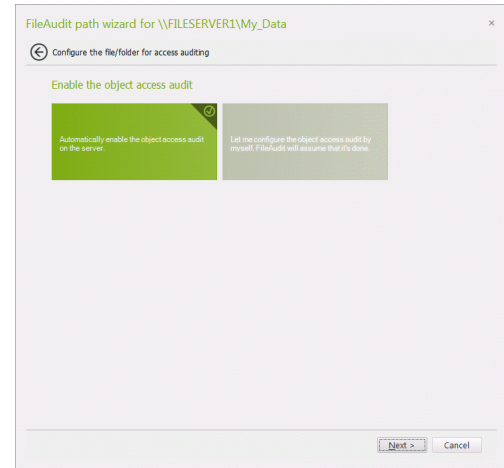




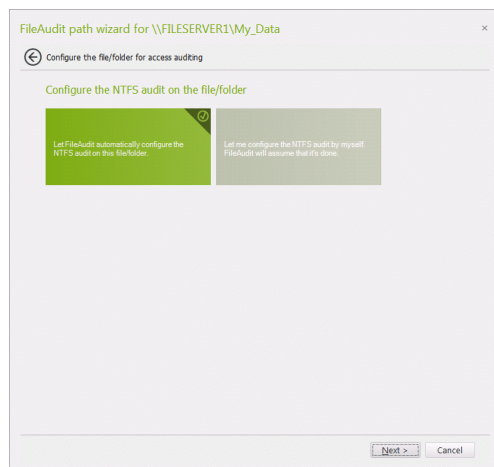
This wizard will display the status of the Audit configuration for the selected folder and highlight any missing requirements or settings. For each necessary action, you have the choice of completing it automatically (via the wizard) or manually. **We strongly recommend that FileAudit automatic configuration be used for all audit settings.**



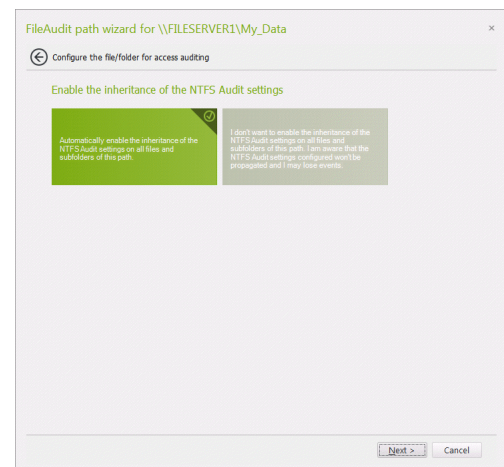
List of required actions.



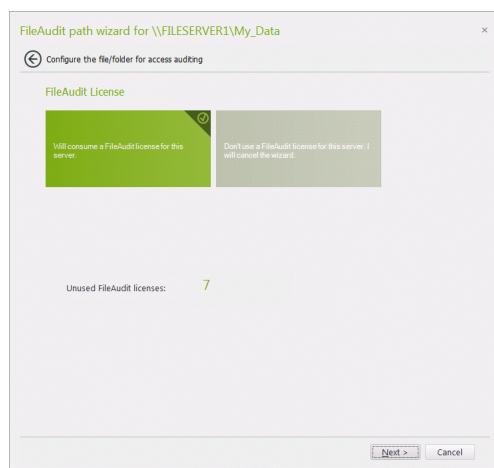
Select automatic or manual processing.



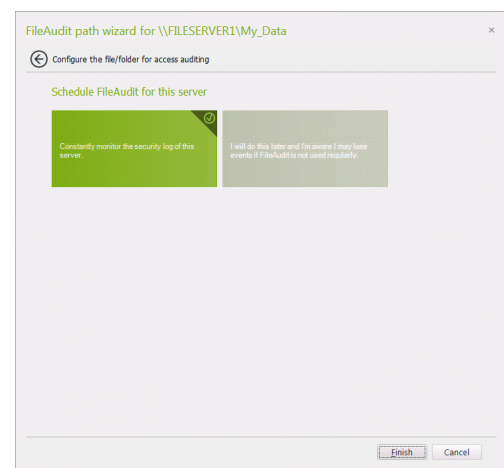
FileAudit will optimize the NTFS audit settings.



FileAudit checks when the inheritance of the NTFS Audit settings are disabled and can enable it.



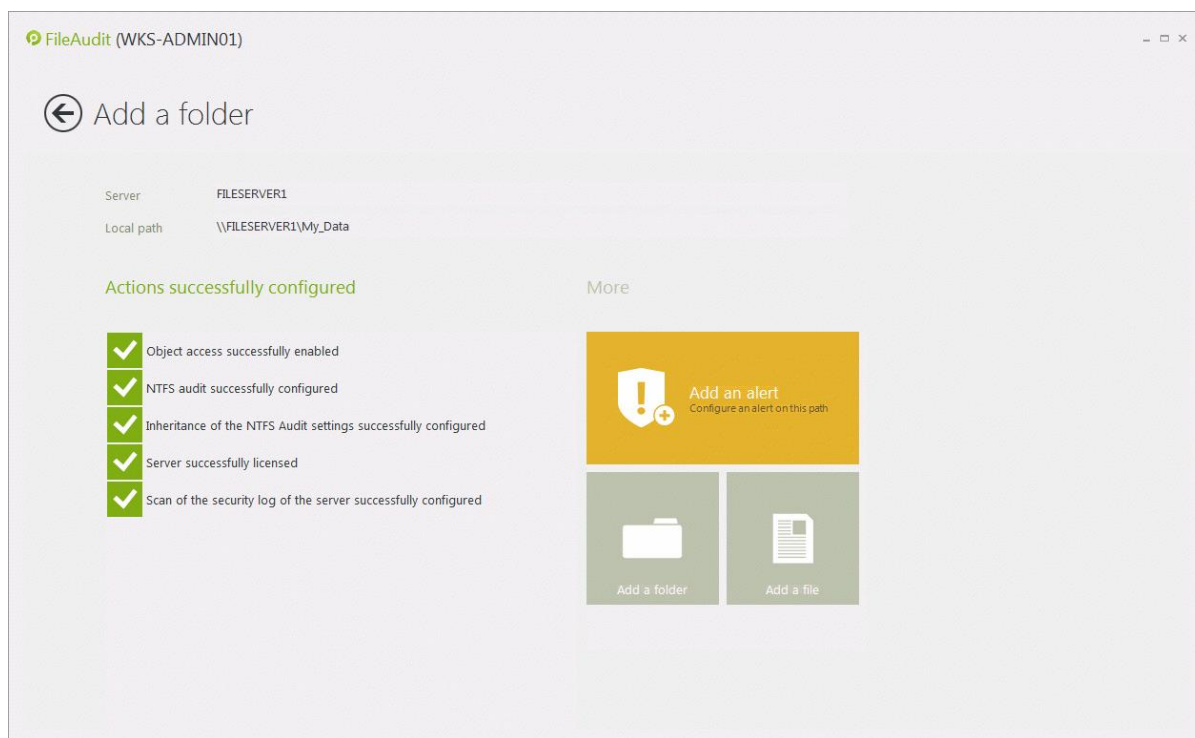
The folder host will be added to the 'Licensed servers' list.



Enable real-time event monitoring.



The folder you have selected is now monitored by FileAudit. All access events will be stored in the FileAudit database. We invite you to stay on this view as we will begin the next paragraph from here.



**Take note:** There are different ways to select a file/folder path to audit. Additionally to the method previously followed, you can:

- Launch the console by right-clicking directly on a file or folder in Windows Explorer and select FileAudit in the 'Context Menu'. In this case, the previous steps are skipped as the file/folder path is directly imported into the FileAudit Console.
- Display the 'File Access Viewer' and type the target path directly in the 'Path(s)' field. You can also find two buttons in the 'File Access Viewer' to add a folder or a file.
- Simply use the two tiles 'Add a folder' or 'Add a file' in the 'Audit configuration' section.

Additionally, FileAudit always checks the audit configuration status for every path entered in its different views and settings, for example in:

- The 'File access viewer',
- A scheduled report configuration,
- An alert rule definition.





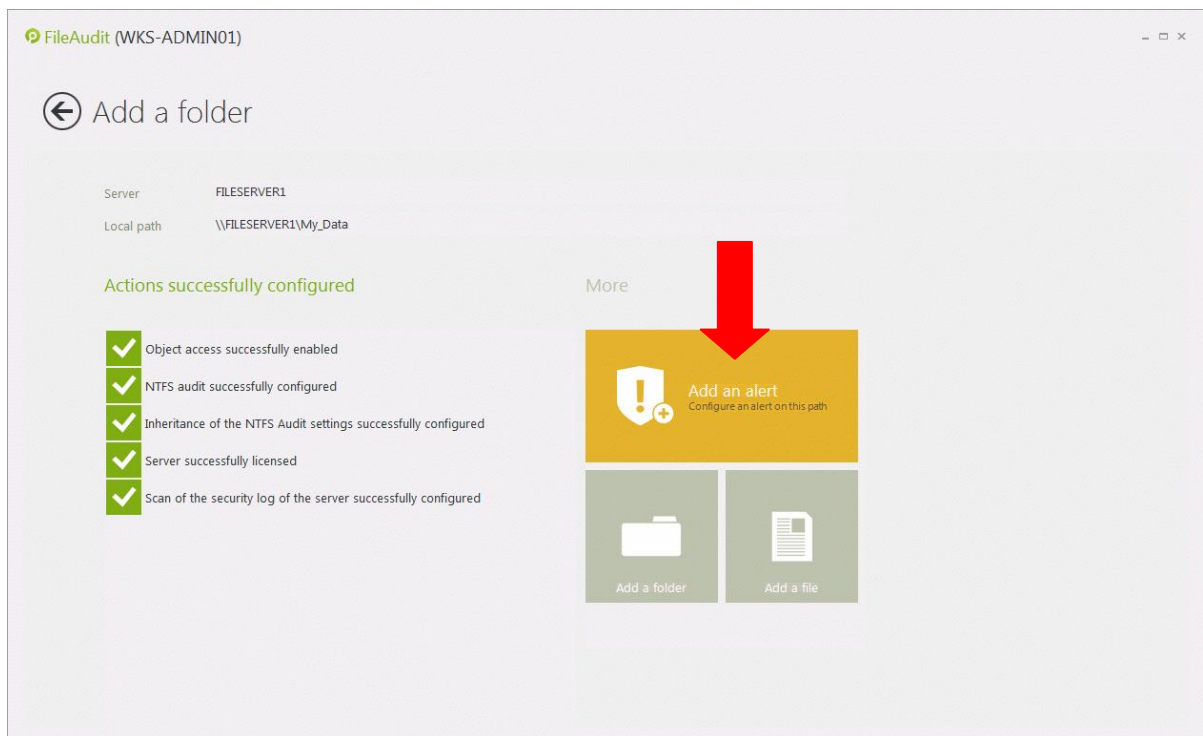
## 2.2. Define an alert on this audited folder.

FileAudit e-mail alerts can be automatically and immediately triggered when specific access events are detected. There are two types of alerts available: Alerts on single access and alerts on mass access:

- A 'Single access' alert is triggered to notify a predetermined access event corresponding to specific criteria. The alert is triggered the defined criteria are matched.
- The 'Mass access' alert brings an additional criterion to those available in the 'Single access': the frequency with which accesses are performed by the same user. This alert is triggered when the tolerated threshold is reached for a defined period of time.

### 2.2.1. Single access alert.

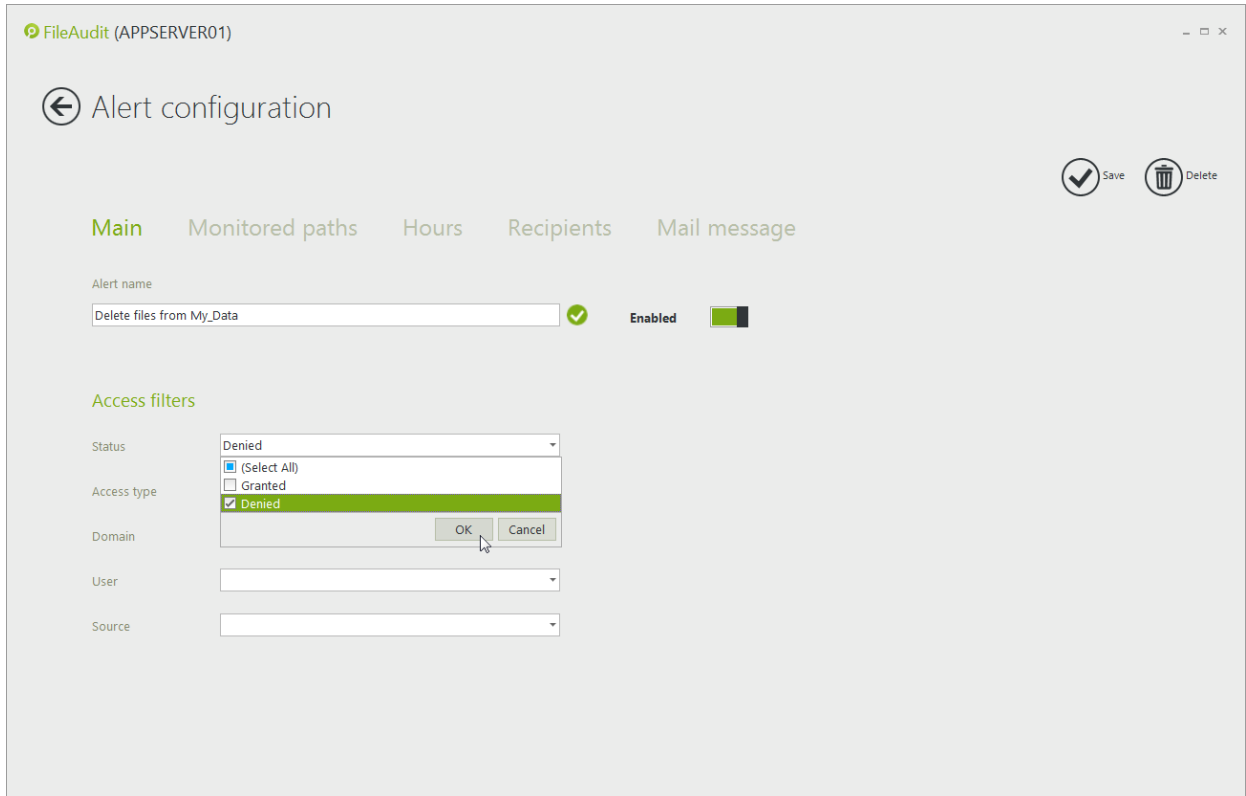
Once FileAudit has displayed the results of the audit configuration for your target folder, you can define from here a 'Single access' alert. You will find on the right-hand side the tile named 'Add an alert'. Click on it.



FileAudit will switch to the 'Alert' configuration section for the specific audited folder previously set. In this example, we will define an alert triggered for a successful deleted event on 'My\_Data' folder.



The first 'Main' tab allows you to define the event that will trigger the E-mail alert. FileAudit can send an alert when the access has been granted or denied. In our example, we will choose to receive this alert for any attempt of file deletion. In the 'Status' field, check the 'Granted' and 'Denied' box.



FileAudit (APPSERVER01)

Alert configuration

Save Delete

Main Monitored paths Hours Recipients Mail message

Alert name  
Delete files from My\_Data

Enabled

Access filters

Status: Denied

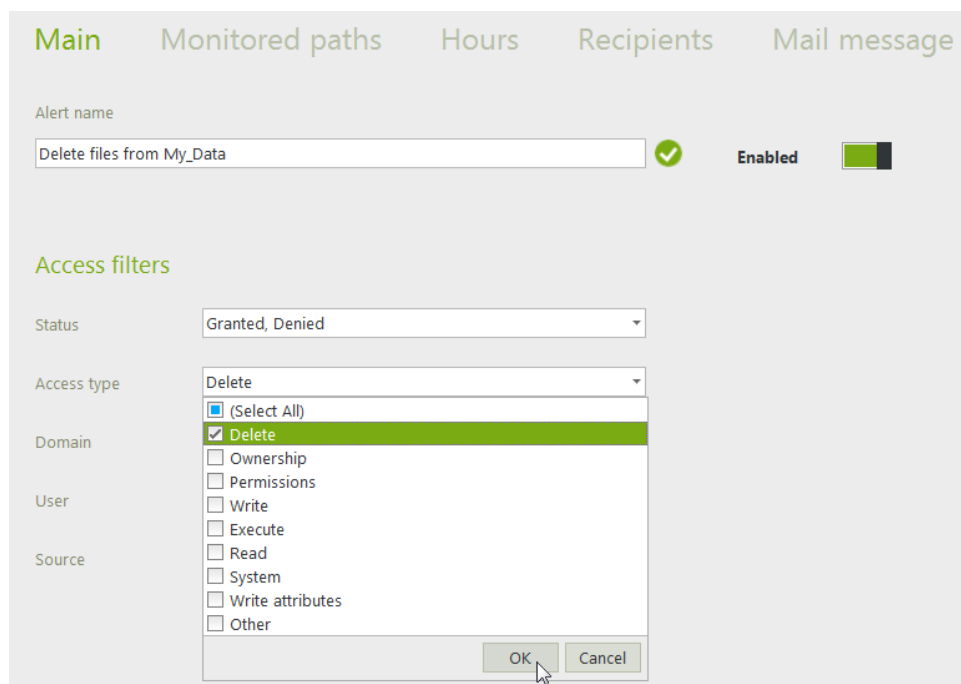
Access type: (Select All), Granted, **Denied**

Domain: OK Cancel

User:

Source:

Select then the 'Delete' access type. Take note that the event is generated for an attempted access. If a user attempts to delete a file on a monitored folder without sufficient rights, you will be alerted about a 'Delete' access event with a status 'Denied'.



Main Monitored paths Hours Recipients Mail message

Alert name  
Delete files from My\_Data

Enabled

Access filters

Status: Granted, Denied

Access type: Delete

Domain: (Select All), **Delete**, Ownership, Permissions, Write, Execute, Read, System, Write attributes, Other

User:

Source:

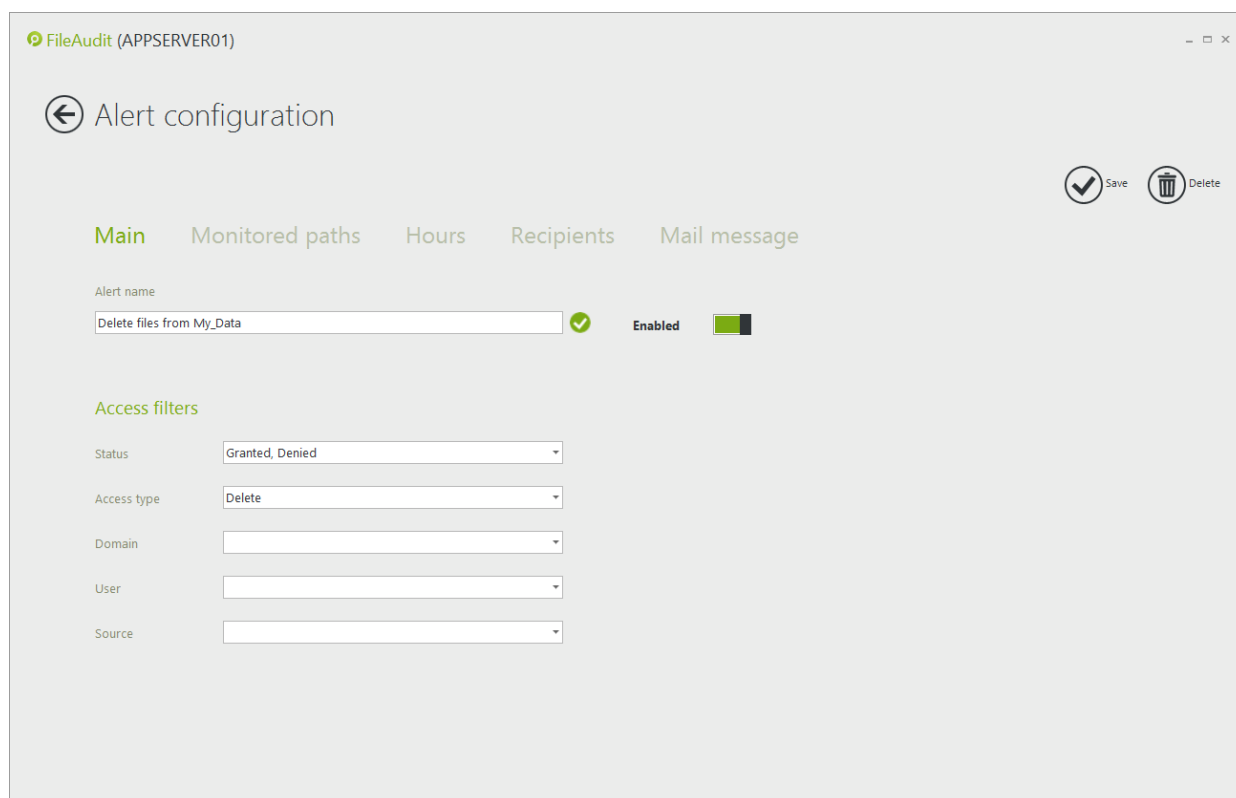
OK Cancel



The final parameters allow for the definition of a specific 'Domain', 'User' and/or 'Source' to trigger an alert. The fields 'Domain', 'User' and 'Source' should be kept empty if you want to be alerted for any 'Domain', 'User' or 'Source' that generates an event.

**Take note:** The 'Source' field allows you to specify the name of the process generating the access attempt when the file/folder is accessed locally (i.e. on the machine hosting the file/folder) or the IP address of the machine from which the access has been performed when the access is performed through the network.

The switch at the bottom of the 'Main' tab permits to enable/disable this alert.



FileAudit (APPSERVER01)

Alert configuration

Save Delete

Main Monitored paths Hours Recipients Mail message

Alert name

Delete files from My\_Data ☒ Enabled

Access filters

Status: Granted, Denied

Access type: Delete

Domain:

User:

Source:

The 'Monitored paths' section is already defined as we created this alert just after having set the audit on the path. This 'Alert' will be sent if any user successfully deletes a file or a folder in 'My\_Data'.

We will now define a recipient for this alert. Click on the 'Recipients' tab.



To create a new recipient, click on 'Add a recipient'. This will bring up a panel on the right-hand side of the screen. Directly enter a name and valid e-mail address for the recipient, and click on Validate to add this contact to the 'Recipients' list. You can reproduce this action to add several recipients.

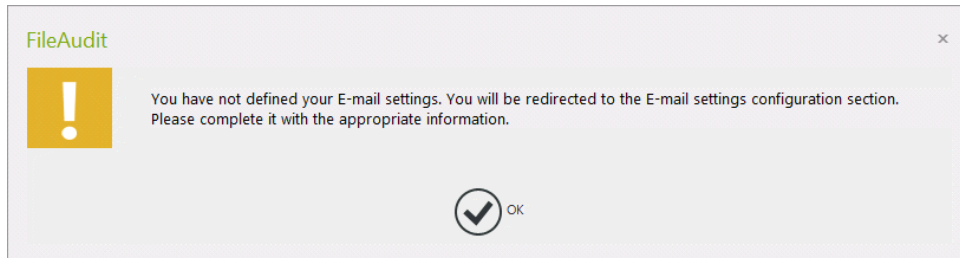
Take note: All previously-defined recipients of scheduled reports or alerts are stored as general parameters by FileAudit, allowing selection of existing recipients from this list.

The content of the e-mail message can be personalized via the 'Mail message' tab. The dynamic variables are enclosed in square brackets { }. Their definitions are available in the [Help file](#).

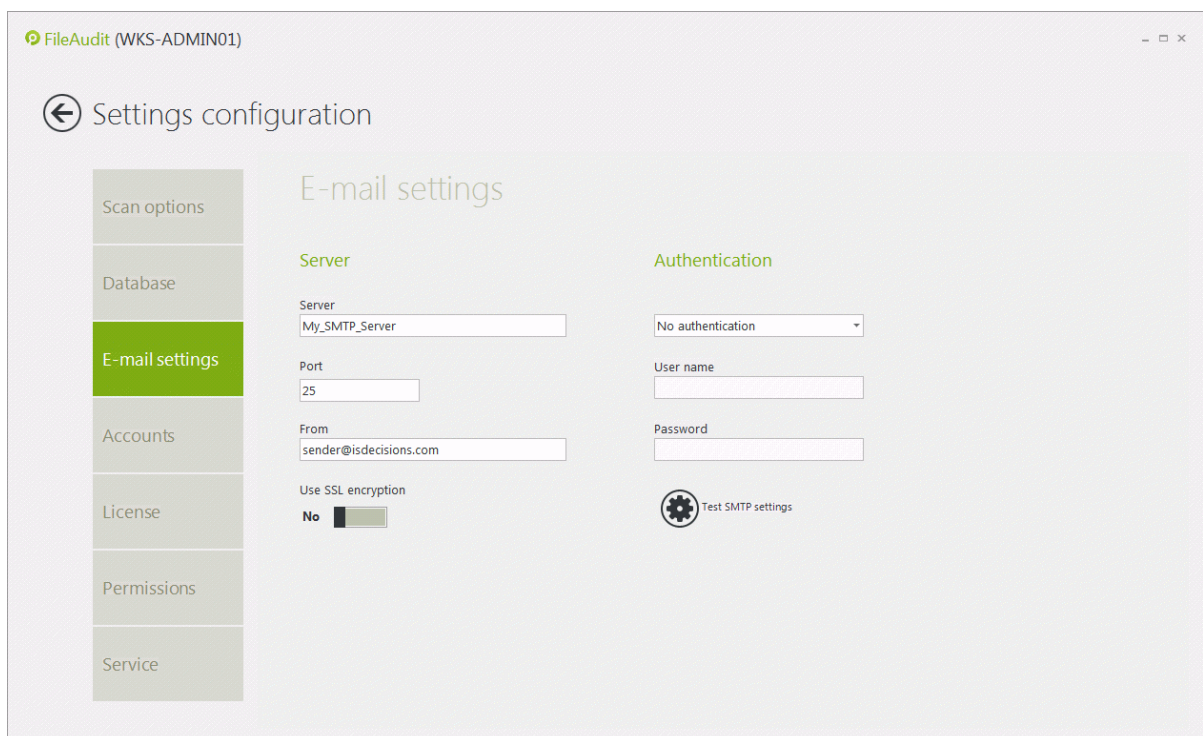


Once all configuration tabs are defined as required, click 'Save'. This alert will be directly activated.

When you add an alert, FileAudit checks if the required E-mail settings are defined to send this alert. Until now, we have not defined the E-mail server settings and from which E-mail box the alert will be sent. That is why this popup is displayed when you clicked on 'Save'.



Clicking on 'OK' will redirect you to the 'E-mail settings' section from FileAudit 'Settings configuration'. Enter your SMTP server, the port to use and the E-mail sender's address (requires an existing address).



Validate the configuration by clicking on the back arrow button which will bring you back to the FileAudit Hub.

The audit and the alert are now set on 'My\_Data' folder. Let's see now the file access events generated for this folder.

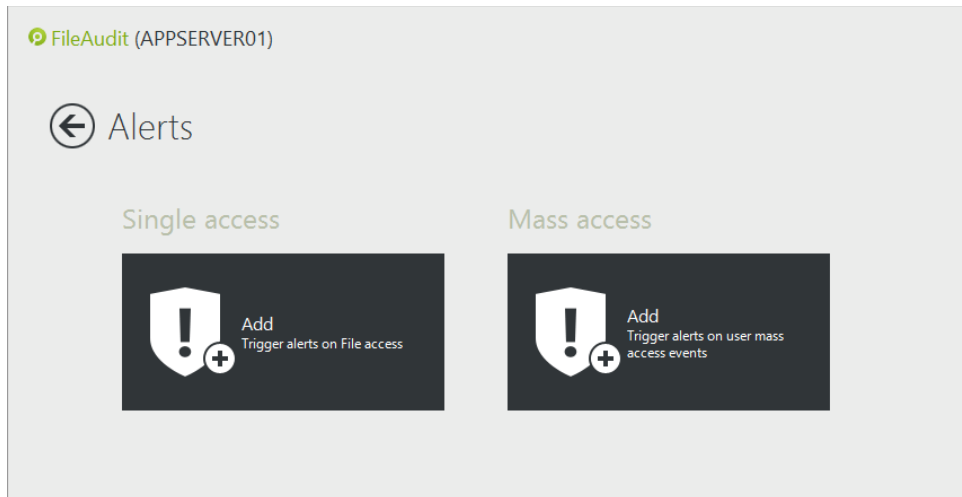
Take note: You can also create an alert directly from the FileAudit Hub clicking on the 'Alerts' tile.



### 2.2.2. Mass access alert.

This type of alert is triggered by certain mass access events performed by the same user. Alerts to bulk file copying are when a significant number of read accesses are performed during short period of time. Alerts to bulk file deletion or movements are when a significant number of deletions are performed during a short period of time.

You can create a mass access alert via the 'Alerts' tile in the FileAudit hub.



This alert type proposes the same criteria as those available when defining a 'Single access' alert and described previously. In addition the frequency criteria determine the number of accesses performed of the same type by the same user.





These frequency criteria are:

- **Threshold:** The number of accesses, corresponding to the criteria defined in this tab, beyond which the alert will be triggered.
- **Time period:** The defined period of time for the number of accesses corresponding to the criteria in this tab.
- **Latency period:** The time period during which the alert will be temporary disabled once triggered. Enter '0' as value to disable the latency period. Take note that disabling the latency period means that the alert will be triggered for each event over the threshold.



### 3. Display the file access events

The 'File access viewer' allows you to display, search, schedule and print reports on all access attempts generated for monitored files/folders configured on FileAudit. Open the 'File access viewer' using the central tile in the FileAudit Hub.

Enter a file/folder into the 'Path(s)' field to display the file access events generated for it. To validate this entry, press 'Enter' or click the refresh button. You can also select a path using the drop-down list which displays the path registered in the 'Audit configuration view'.

As said previously, if FileAudit is not yet open, you can right-click on the monitored folder in Windows Explorer and select FileAudit directly from the context menu. This will open FileAudit 'File access viewer' for this folder.

You can also click on 'Audit a folder' or 'Audit a file' buttons in the bottom left hand of the screen.

FileAudit (APPSERVER01)

File access viewer

Path(s) \\fileserver1\\My\_Data

Server Date and Time

File	Access type	Status	Date and Time	User	Source
<b>Server: FILESERVER1 (41 accesses)</b>					
<b>Date and Time: Today (24 accesses)</b>					
C:\My_Data\Technical\Project25\Table of content.txt	Read	Granted	22/07/2015 12:29:22.823	Cameron	10.1.13.12
C:\My_Data\Accounting\Draft - ideas.txt	Write	Granted	22/07/2015 12:28:54.523	administrator	notepad.exe
C:\My_Data\Accounting\Draft - ideas.txt	Read	Granted	22/07/2015 12:28:49.913	administrator	notepad.exe
C:\My_Data\Financial\Meetings\RD-28-03-2012.doc	Read	Granted	22/07/2015 12:28:43.857	Addison	10.1.13.11
C:\My_Data\Financial\Meetings\Questions.txt	Write	Denied	22/07/2015 12:28:32.810	Addison	10.1.13.11
C:\My_Data\Financial\Meetings\Questions.txt	Read	Granted	22/07/2015 12:28:29.557	Addison	10.1.13.11
C:\My_Data\Accounting\Price list.xls	Read	Granted	22/07/2015 12:28:10.053	administrator	explorer.exe
C:\My_Data\Accounting\Invoices\Invoice 023003.pdf	Read	Granted	22/07/2015 12:28:00.950	administrator	AcroRd32.exe
C:\My_Data\Financial\template.doc	Read	Granted	22/07/2015 12:27:15.973	Addison	10.1.13.11
C:\My_Data\Developers	Read	Denied	22/07/2015 12:27:10.293	Addison	10.1.13.11
C:\My_Data\Accounting\Invoices\Invoice 023014.pdf	Delete	Granted	22/07/2015 12:27:03.383	Addison	10.1.13.11
C:\My_Data\Technical\Project25\Specifications\Validation.doc	Read	Granted	22/07/2015 12:26:38.333	Cameron	10.1.13.12
C:\My_Data\Accounting\Invoices\Invoice 023034.pdf	Read	Granted	22/07/2015 12:26:21.170	Addison	10.1.13.11
C:\My_Data\Technical\Dev\Root\Products\UserLock\Pricing.aspx	Delete	Granted	22/07/2015 12:26:07.533	Administrator	10.1.13.4
C:\My_Data\Accounting	Read	Denied	22/07/2015 12:25:26.417	Cameron	10.1.13.12

From: 14/07/2015 00:00:00

Audit a folder Audit a file Schedule

Real time

Status 41 Events  
Query time 0:00:00.328  
Display time 0:00:00.000

The events are detected and stored into the database in real-time. If you also want the console to display events in real-time, enable the 'Real time' switch on the bottom right hand and click on 'Refresh'.

The File Access Viewer data grid offers several grouping and filtering options. To group the view by a specific column, drag and drop the column name below the Path(s) field.

To access the filter and perform a search action, click on the magnifying glass button. The filter form will pop up on the right-hand side of screen. Select your criteria and apply the filter.

You can use filters and search options directly from the event grid through the context menu displayed by right-clicking the column name line. This menu allows personalization of the data grid display (manage column display, sort, etc.) and is where the 'Filter Editor', 'Find Panel' and 'Auto Filter Rows' options can be enabled/disabled.

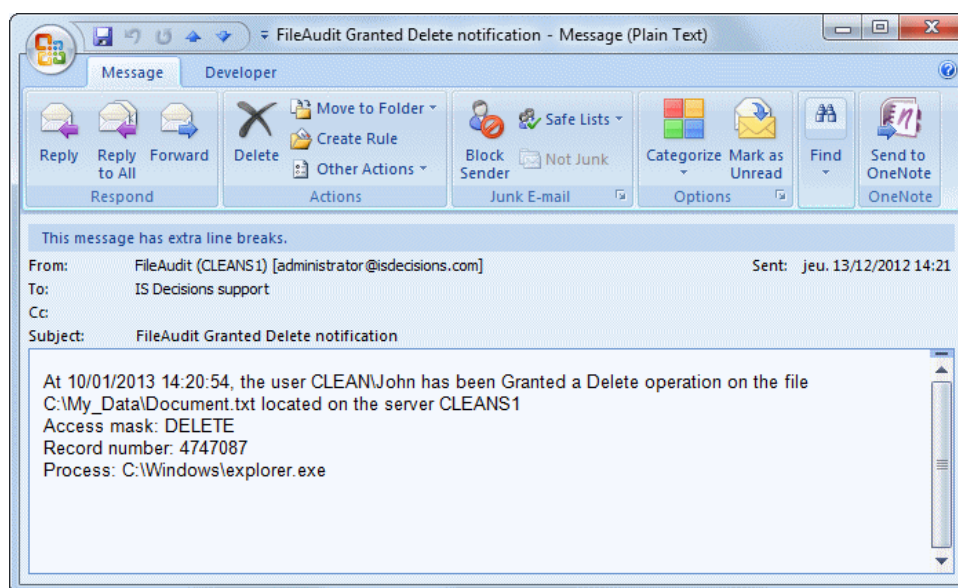
A quick search feature is available on every column's name. When you roll over a column's name with the mouse pointer, you can see a funnel icon on the top right hand corner of the column's name row. Click on it to access the quick search options.



The Print button will allow you to display a printable version of the File access viewer that you can directly print or export in several file formats.

Take note: The grouping and filtering options from the event grid affect only the data displayed. To perform a search of the entire events database, use the filters from the magnifying glass button.

Meanwhile, as some users have deleted file/folder, the E-mail alert was also sent in real-time:



## 4. Set an automatic report

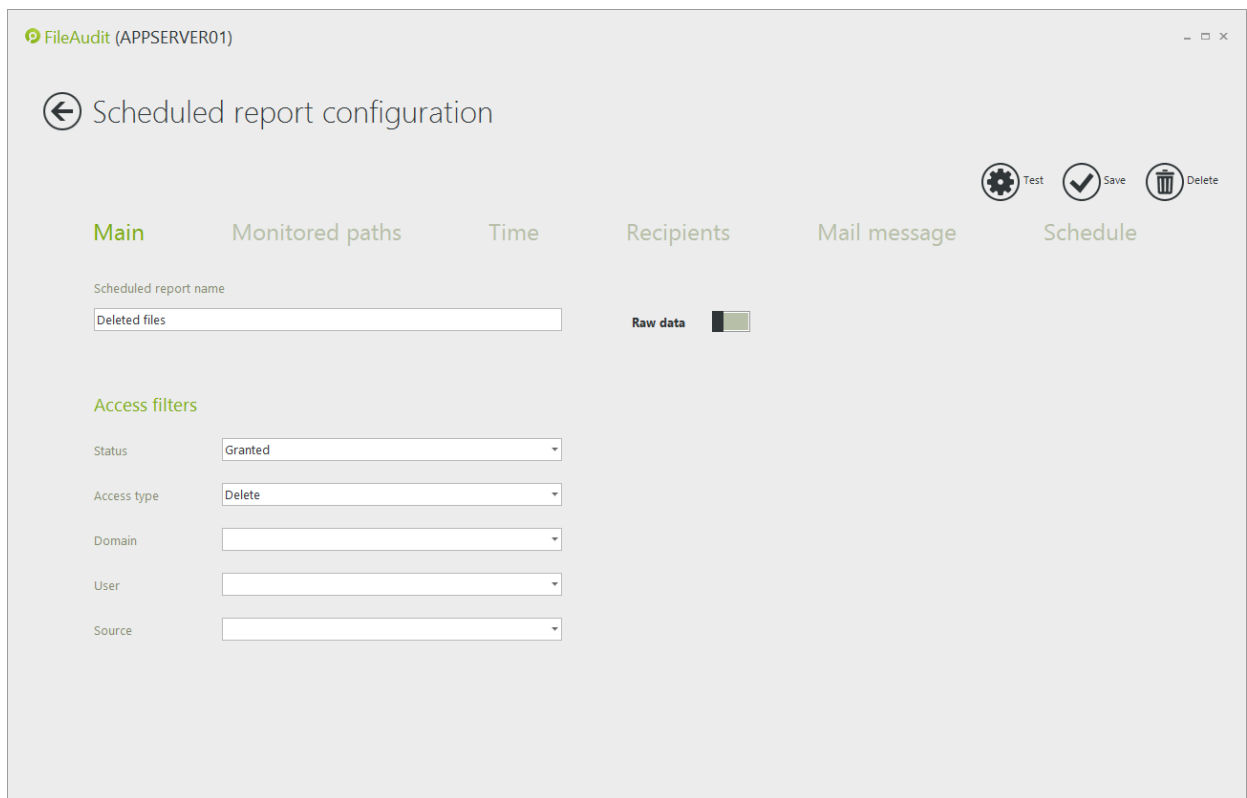
You can set a scheduled report to be sent by e-mail in two ways. The first is by clicking on the 'Scheduled reports' tile in the FileAudit Hub and clicking 'Add a scheduled report' to create a new report.

Alternatively, this feature can be enabled by personalizing the File Access Viewer in your report and clicking on the Schedule button. You will be redirected to the Scheduled report configuration section. All previously-defined filter settings will be imported in the first three tab settings (Main, Monitored paths and Time). We will use this method here.

Open the 'File access viewer' and personalize the view using the filter. For example, if you want to set a report for every deleted file event occurred during the previous day, set the filter with:

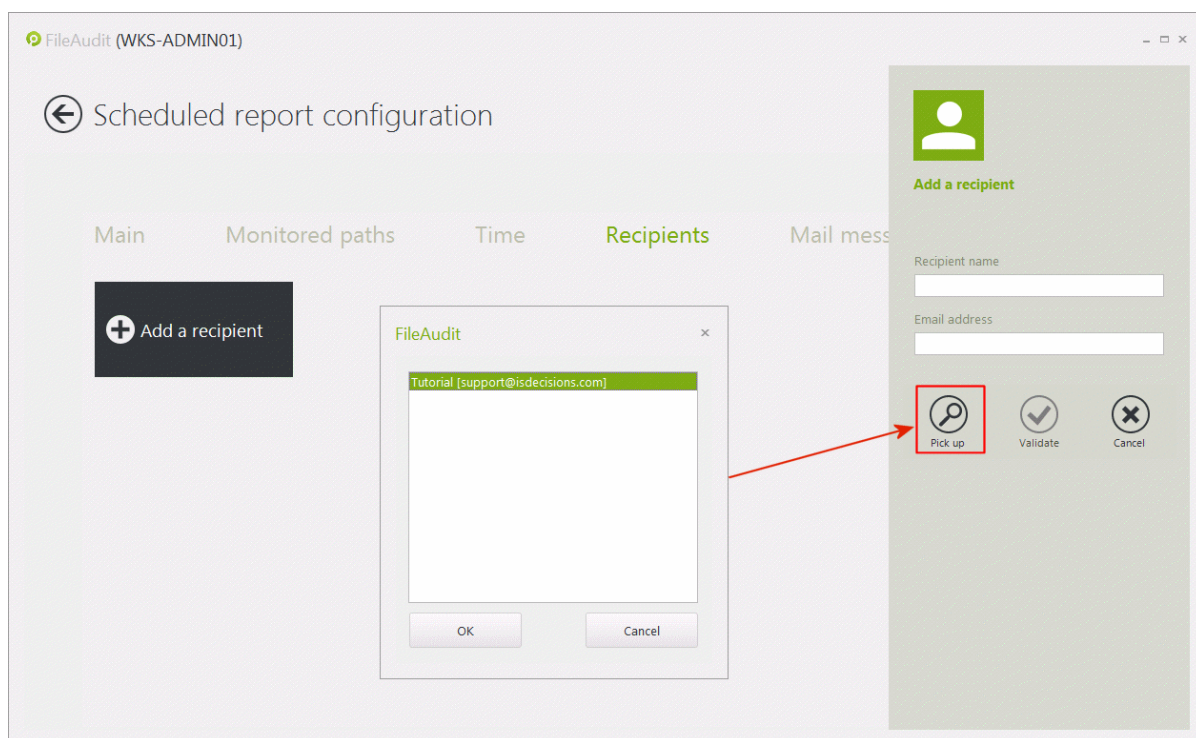
- Define the 'From' field to 'Event from' and set yesterday's date and time at 08:00 AM.
- Define the 'To' field to 'Event to' and set yesterday's date, and time at 6:00 PM.
- Set the 'Status' to 'Grant'.
- Set 'Delete' as the 'Access type'.
- Click on 'Apply'.

The 'File access viewer' will refresh the displayed events according to this filter configuration. Click on the 'Schedule' button. You will be redirected to the 'Scheduled report configuration' section. All the previously filter settings you defined and applied to the 'File access viewer' will be imported in the 3 first settings tabs 'Main', 'Monitored paths' and 'Time'. In the 'Main' section, enter a name for this report.



Click on the 'Recipients' tab to define the E-mail recipients for this report. As we already defined a recipient for an alert, we can pick up the recipient E-mail address if appropriate. Click on 'Add a recipient' and a form will pop up on the right side of the console.

Click on the 'Pick up button', select the recipient in the list and click 'OK'.

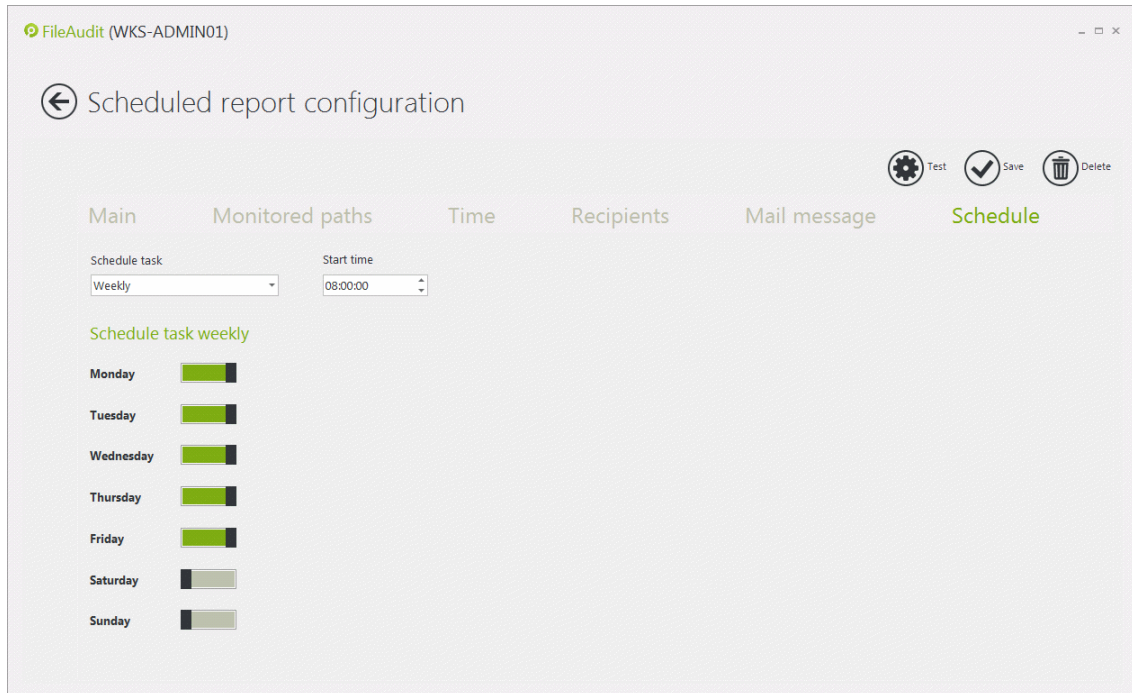


All the information about this recipient is imported into the 'Add a recipient' form. Validate the recipient. You can of course add several recipients for a same report.

The 'Mail message' section is already defined with default text. You can personalize it.



The last tab 'Schedule' defines the time trigger for the report task.

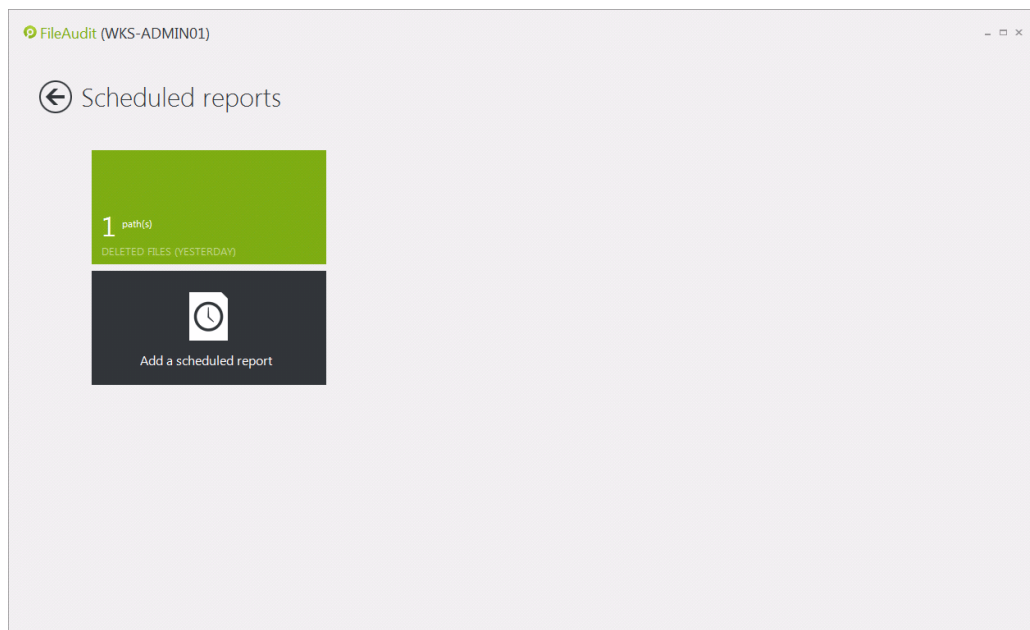


The FileAudit scheduler interprets the time period you have set for your report to dynamically generate the report on the same period. We have chosen here the previous day as the monitored time period. The report will always contain events from the previous day of the execution day. The report will be attached in PDF format in the E-mail.

Some predefined filters are available in the 'Time' tab to easily adjust the desired period time like 'Yesterday', 'The current week', 'The previous week', etc...

You can test the report definition clicking on the 'Test' button. A popup will confirm that the test has launched. If all goes well, you will receive an e-mail with the report attached. This allows you to check that the result corresponds to your needs and make any changes to the settings if needed.

Click on 'Save' to validate your first automatic report. You will be redirected to the 'Scheduled reports' section. You can modify all settings about this automatic report from this specific section.

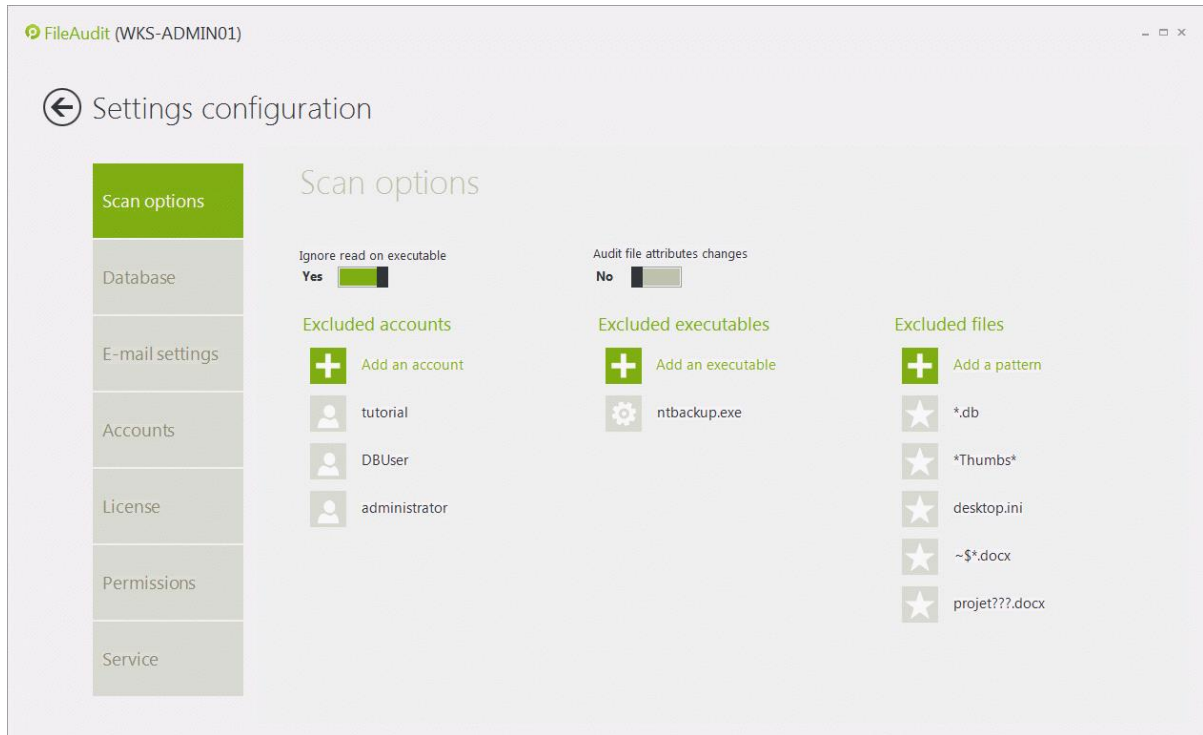




## 5. Additional settings.

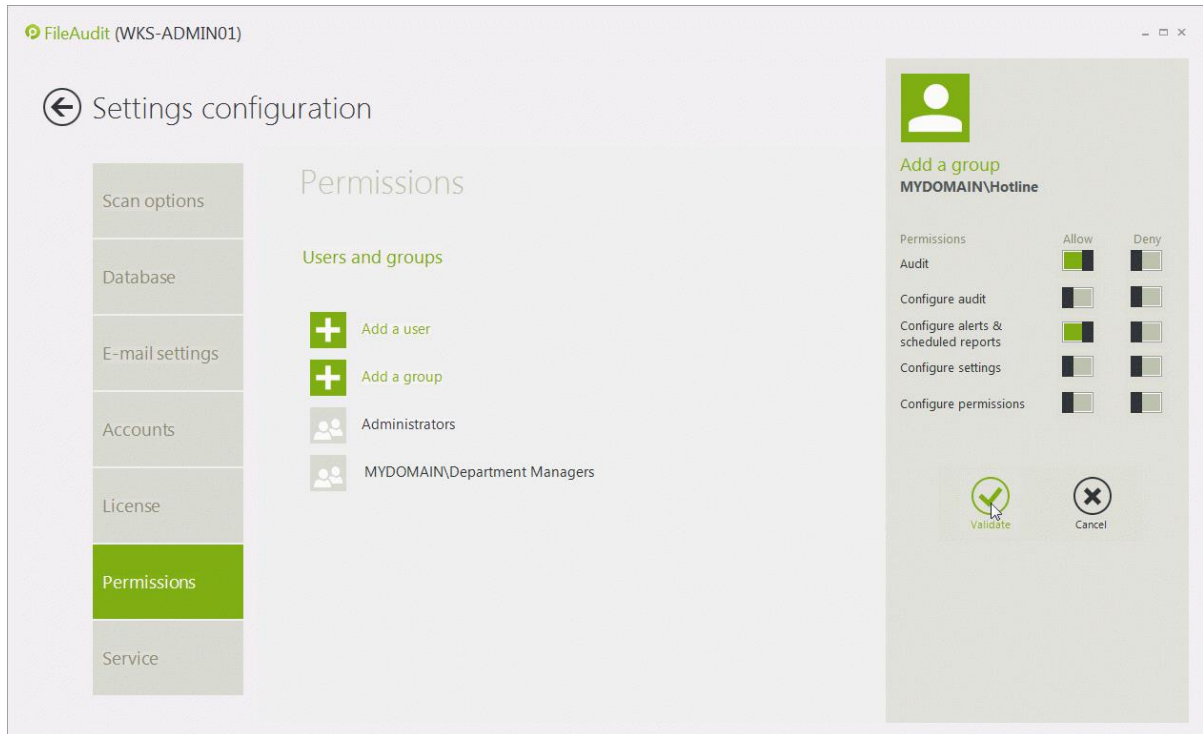
### 5.1. Exclude users, programs and extensions from the audit.

In the 'Settings configuration', the 'Scan options' section allows to exclude access events generated for specific user accounts, executables and extensions. This is particularly useful to exclude file accesses generated by backup software, an antivirus, etc.

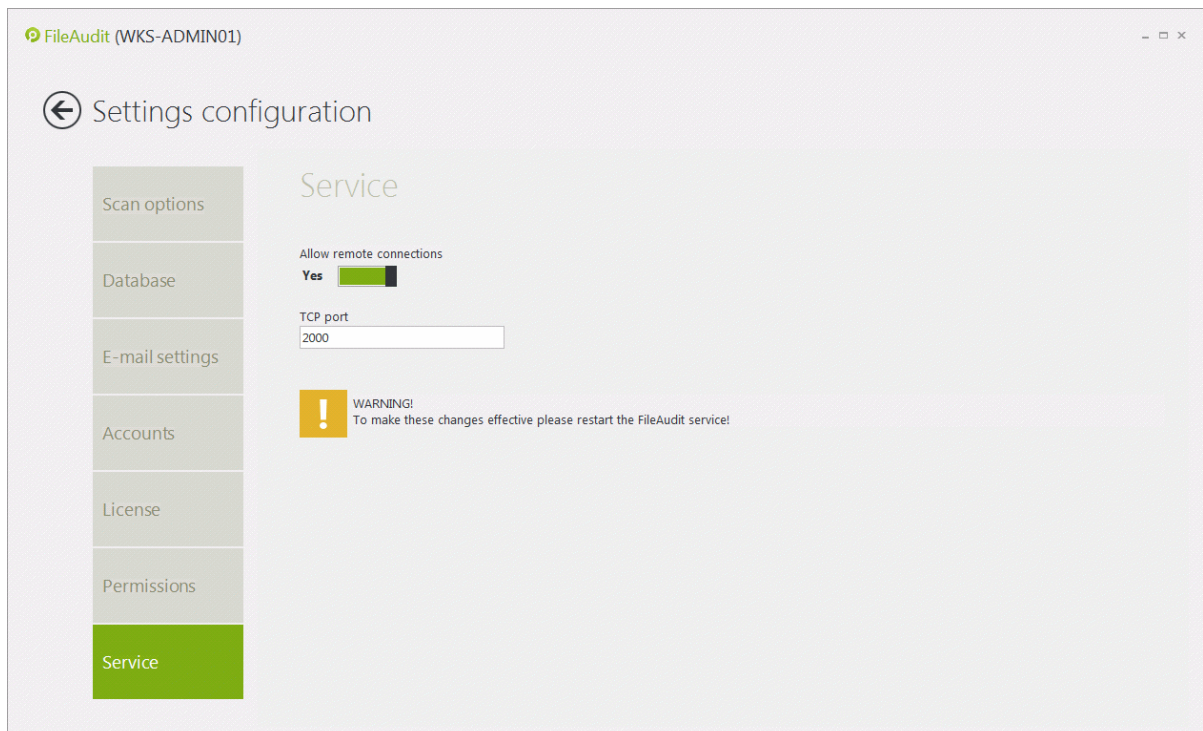


## 5.2. Granularly authorize FileAudit access for specific accounts.

You can set specific accounts for people without administrative rights and define which FileAudit features you wish to make available to them. To access to this feature, click on the 'Settings' Tile in the Tools area and go into the 'Permissions' section.



Then, you can allow the remote connection to the FileAudit auditing service. This avoids giving a direct access to the system where FileAudit is installed.



Perform a custom installation of FileAudit on the machine of non-IT auditors by selecting only the console component. Once done, open FileAudit and remotely connect to the auditing service using the 'Connect' button.

