

# FileSafe Agent Version 2.6

Installation and User's Guide

STOREWAY DPA





# STOREWAY DPA

## FileSafe Agent Version 2.6

### Installation and User's Guide

#### **Software**

March 2008

**BULL CEDOC  
357 AVENUE PATTON  
BP.20845  
49008 ANGERS CEDEX 01  
FRANCE**

**REFERENCE  
DPA\_FILES SAFE\_V2\_6\_EN**

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright © Bull SAS 2008

Printed in France

Suggestions and criticisms concerning the form, content, and presentation of this book are invited. A form is provided at the end of this book for this purpose.

To order additional copies of this book or other Bull Technical Publications, you are invited to use the Ordering Form also provided at the end of this book.

### **Trademarks and Acknowledgements**

We acknowledge the rights of the proprietors of the trademarks mentioned in this manual.

All brand names and software and hardware product names are subject to trademark and/or patent protection.

Quoting of brand and product names is for information purposes only and does not represent trademark misuse.

The information in this document is subject to change without notice. Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

---

# Table of Contents

<b>Chapter 1. Product overview .....</b>	<b>7</b>
How does the FileSafe agent work? .....	8
<b>Chapter 2. Installing and configuring the Agent .....</b>	<b>9</b>
Installation prerequisites .....	10
Installing the agent .....	11
Activate the FileSafe licence .....	12
Activate a licence using an internet connection .....	13
Activate a licence without an internet connection .....	14
Creating and configuring the Repository .....	15
<b>Chapter 3. Backup .....</b>	<b>18</b>
Express backup .....	19
Custom backup .....	22
Back up open files .....	25
<b>Chapter 4. Restoration .....</b>	<b>26</b>
Start a restoration .....	27
<b>Chapter 5. Repository backup and restoration: cross-restoration .....</b>	<b>30</b>
Repository backup and restoration .....	31
Cross restoration .....	32
Repository contents .....	32
Data retrieval on another system which does not have the FileSafe agent .....	33
Retrieving data on another system which has a FileSafe agent. ....	35
<b>Chapter 6. Managing file and directory versions .....</b>	<b>36</b>
Deleting a version of a backed up file .....	37
Deleting versions of a backed up directory .....	38
<b>Chapter 7. Reports and logs .....</b>	<b>39</b>
FileSafe logs .....	40
Generating an X-ray file .....	41
<b>Index .....</b>	<b>43</b>



---

## Chapter 1. Product overview

This document defines the integration and configuration process of the StoreWay DPA FileSafe agent on the system to protect. It also explains how to restore directory or file data.

StoreWay DPA FileSafe is a software application which protects your data by backing up directories and files to a different location. StoreWay DPA FileSafe is completely integrated into the Microsoft Windows Explorer environment.

You can protect and restore data simply by right-clicking on the required directory or file by selecting the option from the StoreWay DPA FileSafe menu.

When you protect a directory, indicate the place where the backup will take place. This space is called a Repository. It can be either local or remote.

- > The system where the agent is installed (local disk, USB, ...),
- > A shared network drive on a company server.

StoreWay DPA FileSafe includes a Repository manager which enables you to add, edit and remove storage areas.

A StoreWay DPA FileSafe agent is installed on the server or workstation to protect. This agent enables Windows directories and files to be backed up in programmed mode.

### The StoreWay DPA FileSafe agent has the following features:

- > Backup and restoration in block mode of file data and/or directories either locally or remotely.
- > Software versionning management.
- > Compression, encryption, data integrity.
- > File and directory inclusion and exclusion filters.
- > Detailed reports.

### Supported client agents

- > Microsoft Windows 2000 Professional, Server or Advanced Server (SP4).
- > Microsoft Windows Server 2003 Standard Edition or Enterprise Edition (Service Pack 1).
- > Microsoft Windows XP Home Edition and Professional (SP2 or later).
- > Microsoft Windows Vista

### Disk space requirements

- > 2.3 MB of free disk space.

**NOTE:** The StoreWay DPA FileSafe agent requires the installation of an Intelligent Management Agent (IMA), which is installed automatically if it is not present on the machine. IMA requires 5.8 MB of extra disk space.

- > Microsoft Internet Explorer 6.0 or later.

## How does the FileSafe agent work?

- > The backup performed by the StoreWay DPA agent has file-level granularity.
- > The configuration enables you to manage data inclusions and/or exclusions.
- > Backed up data are scanned on command or on schedule and the delta block is used to define the latest backup.
- > You can back up files independently. For example, you can back up a directory once a week but others more frequently.
- > If the backed up partitions or directories contain cookies, temporary internet files, offline web pages, temporary IIS files, Windows directories, file systems, pagefile.sys or the trashed items, these items will be filtered and not backed up.
- > In this version, open files are taken into account. In the **FileSafe Explorer**, open the menu **Tools/Options** and check the box **Backup open files**.
- > Backed up data is stored in a Repository which will in turn be backed up by the StoreWay DPA to be able to guarantee data externalisation.
- > This Repository can be located on a remote site.



---

## Chapter 2. Installing and configuring the Agent

See:

["Installation prerequisites" page 10](#)

["Installing the agent" page 11](#)

["Activate the FileSafe licence" page 12](#)

["Activate a licence using an internet connection" page 13](#)

["Activate a licence without an internet connection" page 14](#)

["Creating and configuring the Repository" page 15](#)

## Installation prerequisites

Before installing and configuring the agent, ensure you have:

- StoreWay DPA FileSafe Licence(s)
- The install CD-ROM **StoreWay DPA Initial Setup (Windows) – Agents (Windows, Linux, Netware) Graphical User Interface Setup – ASM & Disaster Recovery Agents**.

# Installing the agent

## FileSafeProduct License Key

If you install FileSafe and you have not yet received your product keys, you can use the 30-day evaluation key which is as follows:

**24R4TQQ545VMRB4G6L44E5TQF**

**NOTE:** You will still need to activate this key to be able to use FileSafe during the evaluation period.


## Install the StoreWay DPA FileSafe agent

- 1 Insert the **StoreWay® DPA Initial Setup (Windows), Agents (Windows, Linux, Netware, MAC OS), Graphical User Interface Setup, ASM & Disaster Recovery Agents Windows) Version X.X.XXX** CD-ROM into the Windows server you wish to protect. A web page opens :

**NOTE:** If the web page does not open, start the installation from the CD-ROM. Launch the **install.htm** page from the CD-ROM drive.

- 2 Click **FileSafe agent** and follow the set up wizard.
- 3 Click **Finish** to complete.

**NOTE:** If an older version of FileSafe is installed, you must first uninstall this agent.

- 4 Choose the installation directory, by default C:\Program Files\FileSafe.
- 5 Click **Next** to start the agent installation.
- 6 Wait for the **InstallShield Wizard Complete** Window to appear.
- 7 After the installation, the agent starts automatically: note its presence in the following screen and as an icon  in Window's lower right task bar (Systray).
- 8 To stop the agent, right-click the  icon and select **Exit**. The icon disappears from the task bar and becomes inactive.
- 9 To restart it from the Windows workstation: **Start/Programs/FileSafe**, and select the FileSafe Agent.
- 10 To add a licence, start the FileSafe explorer (right click the FileSafe icon  and select **Open FileSafe Explorer**). In the explorer, select **Help/Update License** and enter the licence key provided with the agent or contact your reseller. See also the following sections.

## Activate the FileSafe licence

During the installation, you will be asked to provide a licence key. You will need to activate this licence with Bull. (If you do not enter a licence key, you can still use FileSafe for a period of 5 days.) After entering the licence key, you can use the product for 30 days without activating the licence. Until you have entered and activated your licence key, you will be reminded to activate on starting up the product.

If your machine has an internet connection, the activation is automatic. If your machine is without an internet connection, the licence cannot be activated automatically and you need to follow the offline activation procedure.

["Activate a licence using an internet connection" page 13 \(« online activation »\)](#)

["Activate a licence without an internet connection" page 14 \(« offline activation »\)](#)

## Activate a licence using an internet connection

- 1 Enter (or copy/paste) the licence key into the **License Notification/Add license** dialogue box (in the menu **Help/Update Licence** in the FileSafe explorer). Click **OK**.
- 2 When you see the message confirming the activation, click **OK**. Your licence is activated and the FileSafe explorer opens.

## Activate a licence without an internet connection

If your machine does not have an internet connection, you can activate your licence offline:

- 1 Enter (or copy/paste) the licence key into the **License Notification/Add license**, select **Perform offline activation**. The **Activate offline** dialogue box displays the licence number you have entered.
- 2 Click on **Export License File**.
- 3 Save this file in a network share directory and send it from a machine with an internet connection to <http://support.bull/ols/online/keys>
- 4 When you receive the signature file from Bull, save this file and click on the button **Import Signature File...** to activate FileSafe.
- 5 Navigate to the signature file and select this file.
- 6 When the confirmation message appears, click **OK**.

You can now use FileSafe to back up and restore files and directories.

## Creating and configuring the Repository

To be able to perform backups, you first need to define a Repository. A Repository is a space where system data backups are stored on a system running a FileSafe agent.

**WARNING:** The Repositories created must always be backed up by a StoreWay DPA. In the event of a major incident, data will be retrieved from the StoreWay DPA.

A Repository can be one of these 3 types :

- > Local (USB included)
- > Network Share
- > FileSafe Server : currently unavailable.

**WARNING:** At present, only Local and Network Share type Repositories are supported by the StoreWay DPA.

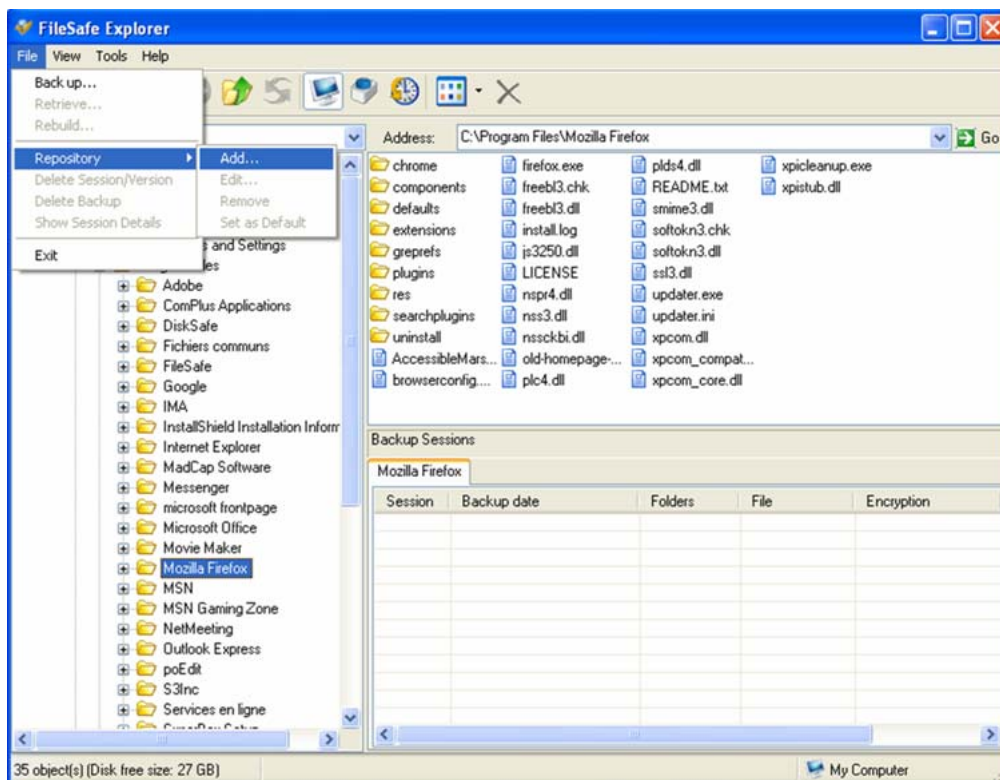
**NOTE:** A « Network Share » type Repository can be shared for several systems.

You can create the repository by using one of these two methods :

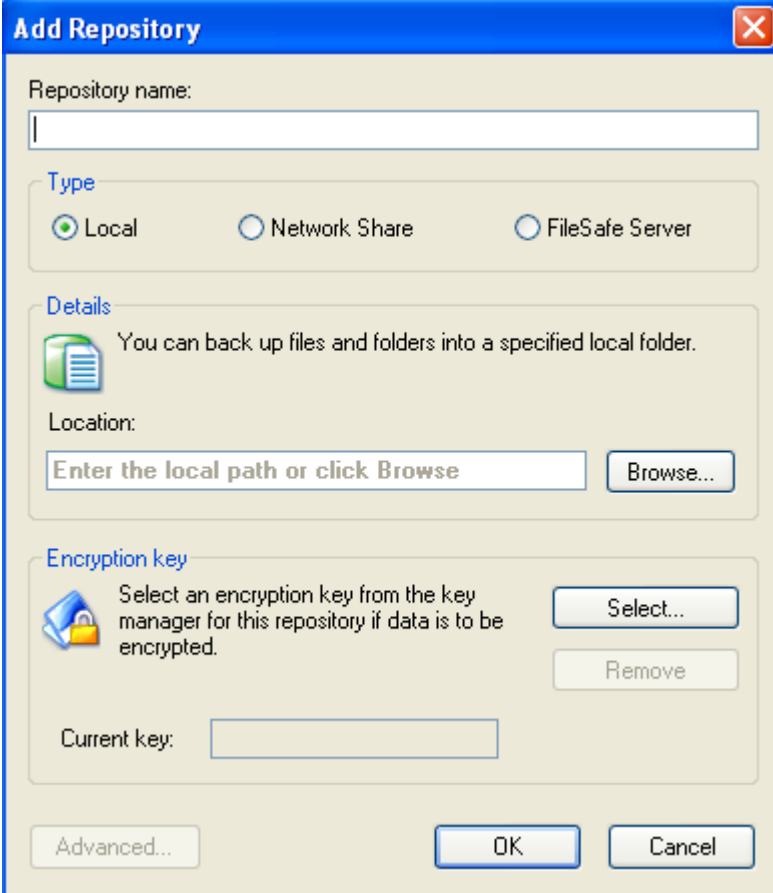
- > Click the FileSafe Agent icon and start the Repository Manager. This is the preferred method for creating the initial repository.
- > From the Windows Explorer, right-click the directory you wish to protect. Use this method when the repository has already been created.

## Method 1: Creating a Local or Network Share Repository

- 1 Open the FileSafe Explorer (right-click the FileSafe icon).
- 2 In the Explorer, select **File/Repository/Add....**



- 3** Choose the type of Repository: **Local** or **Network Share**.




**Add Repository**

Repository name:

Type


☒ Local ☐ Network Share ☐ FileSafe Server

Details

 You can back up files and folders into a specified local folder.

Location:

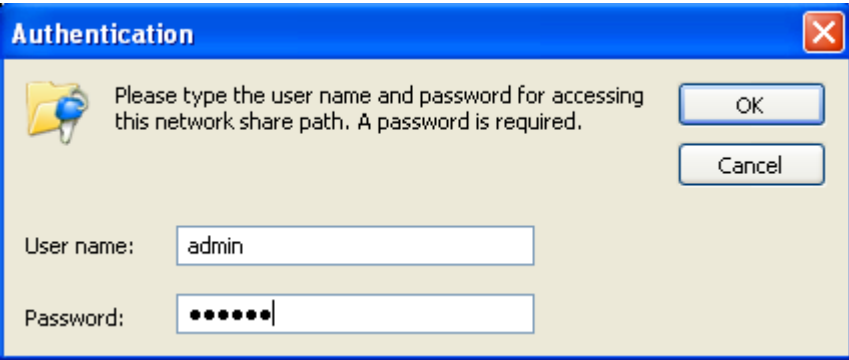
Encryption key

 Select an encryption key from the key manager for this repository if data is to be encrypted.


Current key:

- 4 Give the Repository a logical name in the **Repository Name** field.
- 5 Click **Browse...** to select the directory where data will be backed up or enter a local directory path or network share path in the **Location** or **Network Location** fields.
- 6 Click **OK**.

In the case of a network share Repository, the following authentication window opens:



**Authentication**

 Please type the user name and password for accessing this network share path. A password is required.

User name:

Password:

In the Explorer, the Repository you created is accessible by selecting **View/My Repositories**.



## Method 2 : Creating a Local or Network Share Repository

- 1 Once installed, the FileSafe agent is directly integrated into the Windows Explorer environment and therefore directly accessible from a Windows Explorer.
- 2 Right-click a directory or file which is applicable for data protection: **FileSafe/Backup** to open the FileSafe Backup Wizard.
- 3 Select **Custom backup** and click **Next**.
- 4 Create a new repository, or edit, remove or set as default any selected repository.  
To create a new repository, refer to the initial repository creation method.  
Once this repository has been created, you can define data protection procedures.

---

## Chapter 3. Backup

**WARNING:** The full directory path and file name must not exceed 252 characters. The repository cannot be backed up if this is the case.

See:

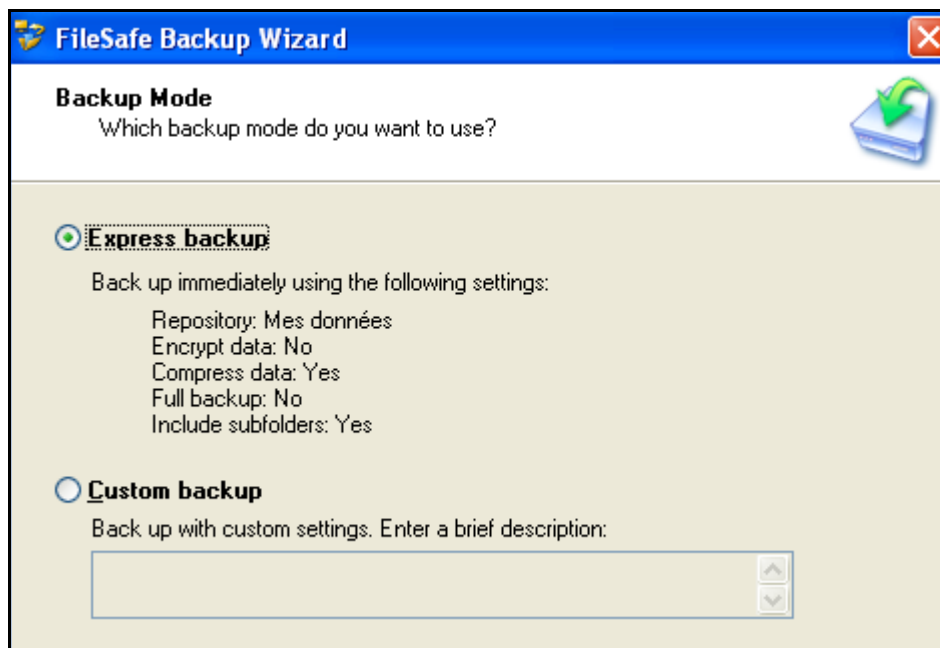
["Express backup" page 19](#)

["Custom backup" page 22](#)

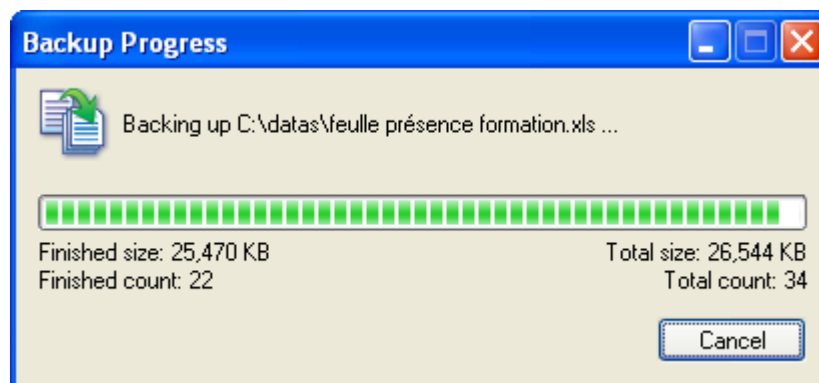
["Back up open files" page 25](#)

## Express backup

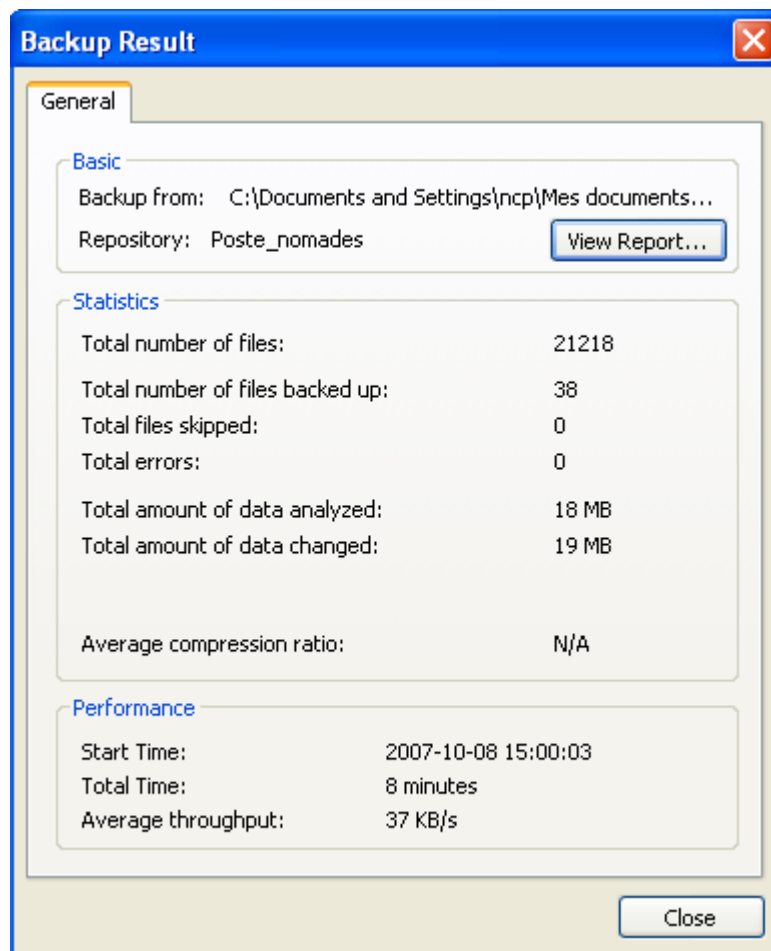
- 1 To perform an express backup, select the partition, the directory or the file to protect, then right-click **FileSafe/Back up to ...**
- 2 Select **Express backup** to start an express backup with the default options.



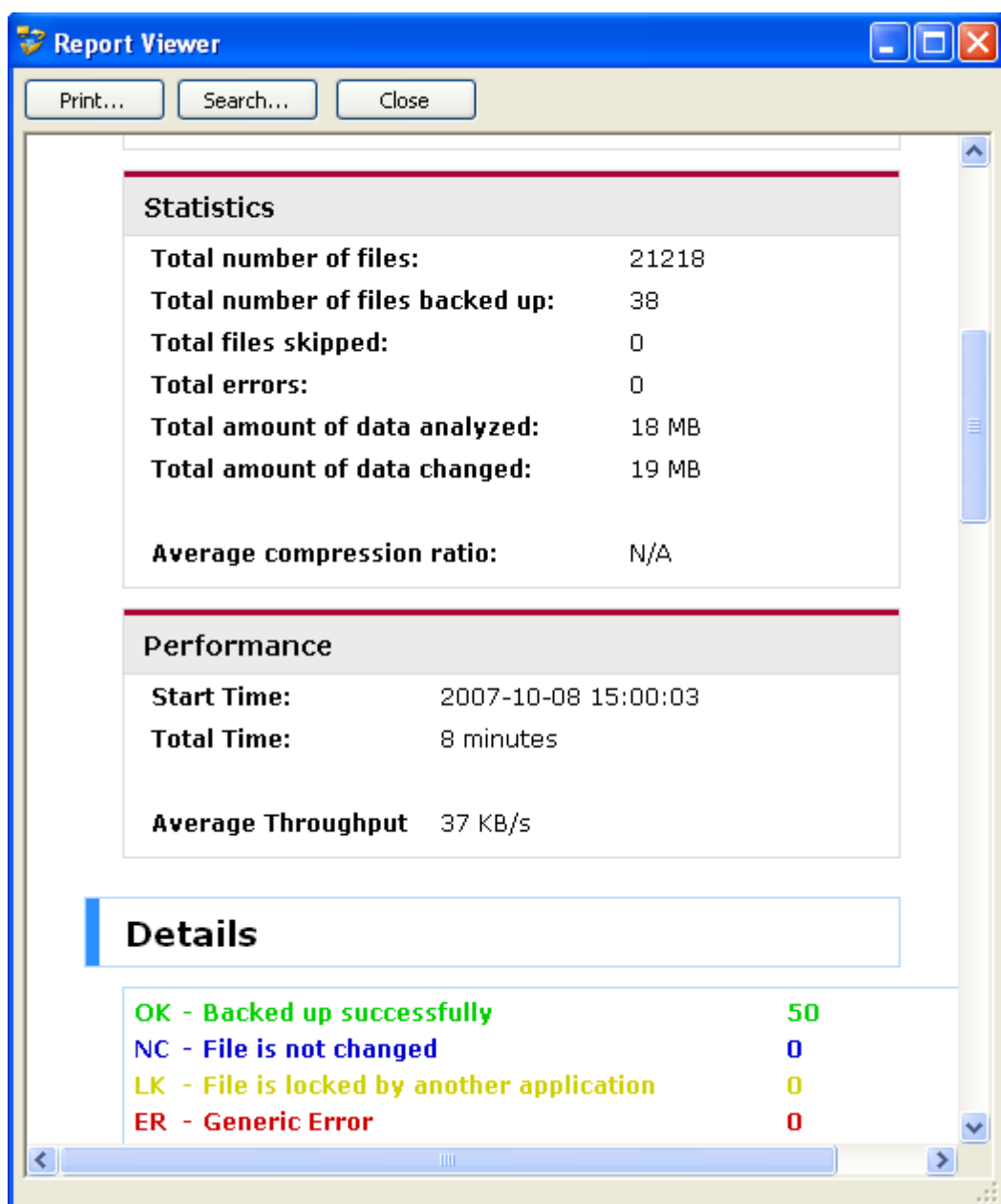
- 3 Click **Next**.  
The Completing FileSafe Backup Wizard opens.
- 4 Click **Finish** to start the backup immediately.  
The synchronization begins, file by file in block mode.



- 5 At the end of the backup, a report is displayed. Click **View Report** to display the detailed report.

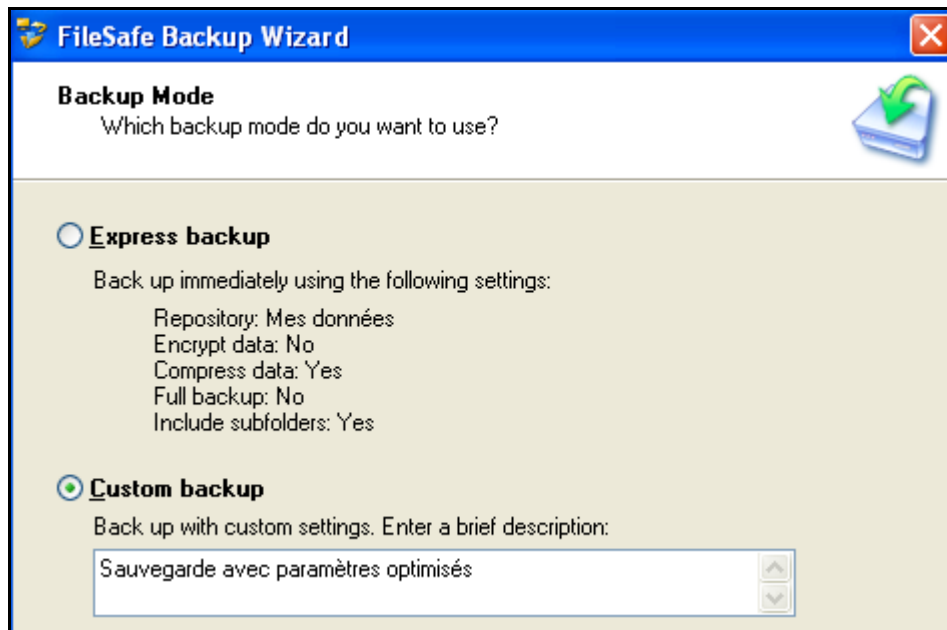


- 6 Consult the detailed report (click on the **View Report** button):

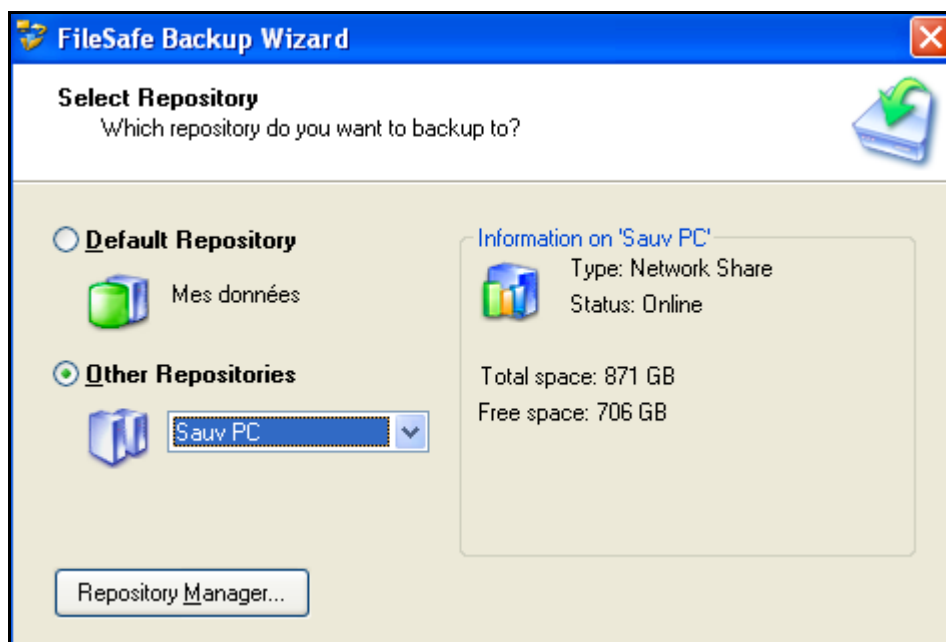


## Custom backup

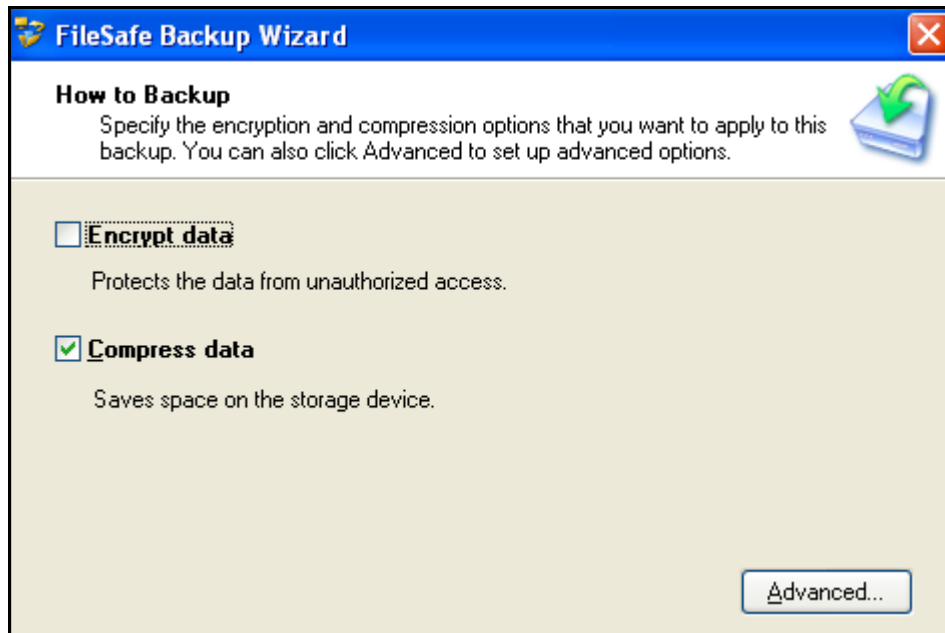
- 1 To perform a custom backup, select the partition, the directory or the file to protect, then right-click **FileSafe/Back up to...**



- 2 Select **Custom backup**.



- 3 Select Repository (default or other).
- 4 Select the data compression option.



5 Configure your advanced encryption and compression options.

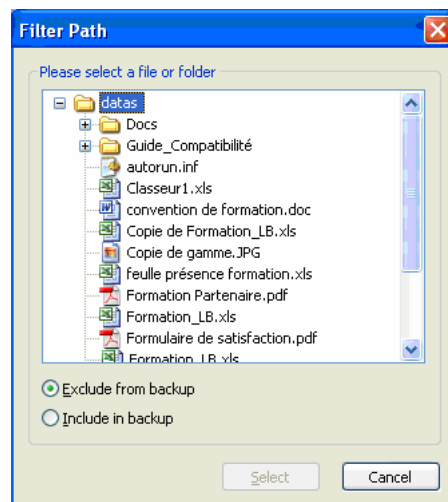
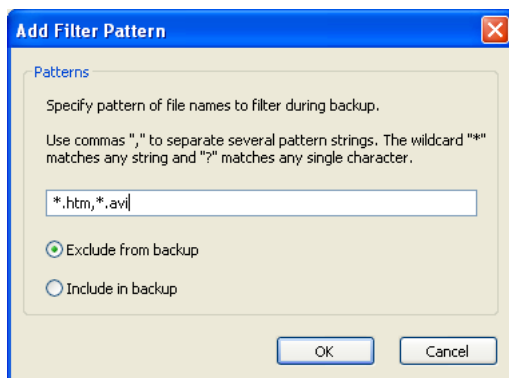
6 Configure your filter options:

#### General tab

**Add** → data type = file extensions, character strings to include or exclude.

#### Filter tab

**Add Path** → Data path to include or exclude.



7 Choose **Exclude from backup** or **Include in backup** depending on whether you wish to exclude or include these files and directories in the backup.

8 Start backup.

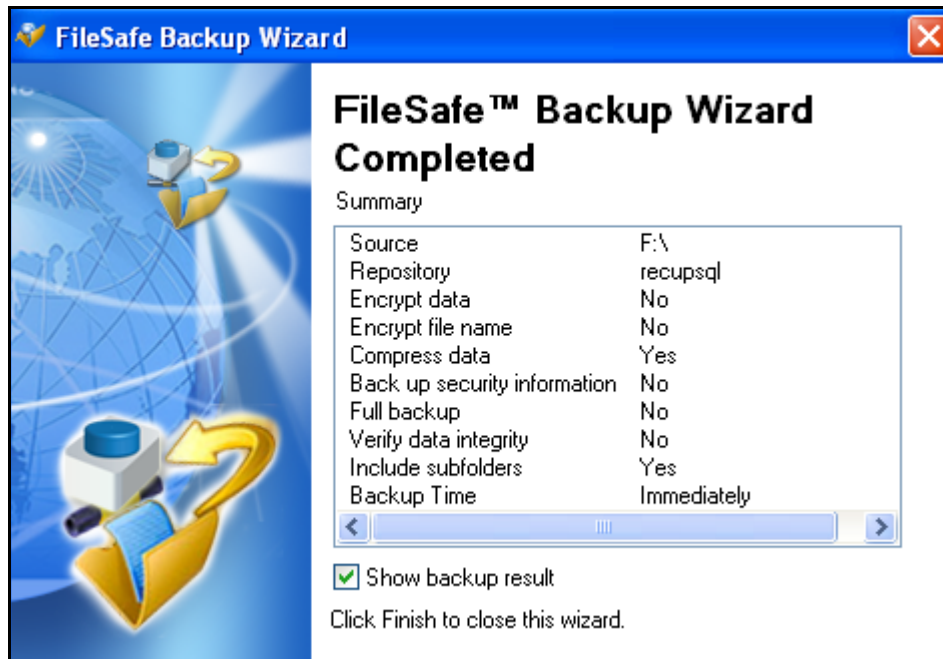
You can choose to start the backup using two methods :

- Back up immediately (select the option: **Back up immediately**).
- Schedule a backup (selecty the option **Schedule a backup** and click the **Set Schedule** button).

**NOTE:** For scheduled backups, you can configure the frequencies (hourly, daily etc) and also the periods to exclude from your backups (click on the **Advanced** button).

9 Click **OK** to save.

10 Click **Next** to display the final Wizard window.



11 Click **Finish** to finalize the backup.



## Back up open files

By default, open files are not backed up. However, you can configure FileSafe to back up open files. When you set this option, only the latest saved (manual or automatic save) version of the file is backed up by FileSafe.

**NOTE:** This option uses significant resources to create a static image of the drive before backing up. File activity is momentarily stopped during the backup.

### Configure the open file backup option:

- 1 In the FileSafe Explorer, select **Tools/Options**.
- 2 Using the **General** tab, specify if you want FileSafe to backup open files by selecting **Backup open files**.
- 3 If you select this option, you can also select the option **Invoke snapshot agents**. If you use SnapShots during backups, FileSafe can ensure a synchronisation of backups for files open in the databases.
- 4 Click **OK**.

---

## Chapter 4. Restoration

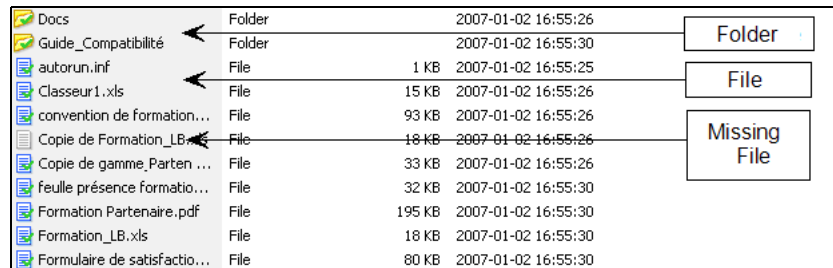
Restoration consists in retrieving data deleted by error or data which is present but unusable (file corruption etc....).

See:

["Start a restoration" page 27](#)

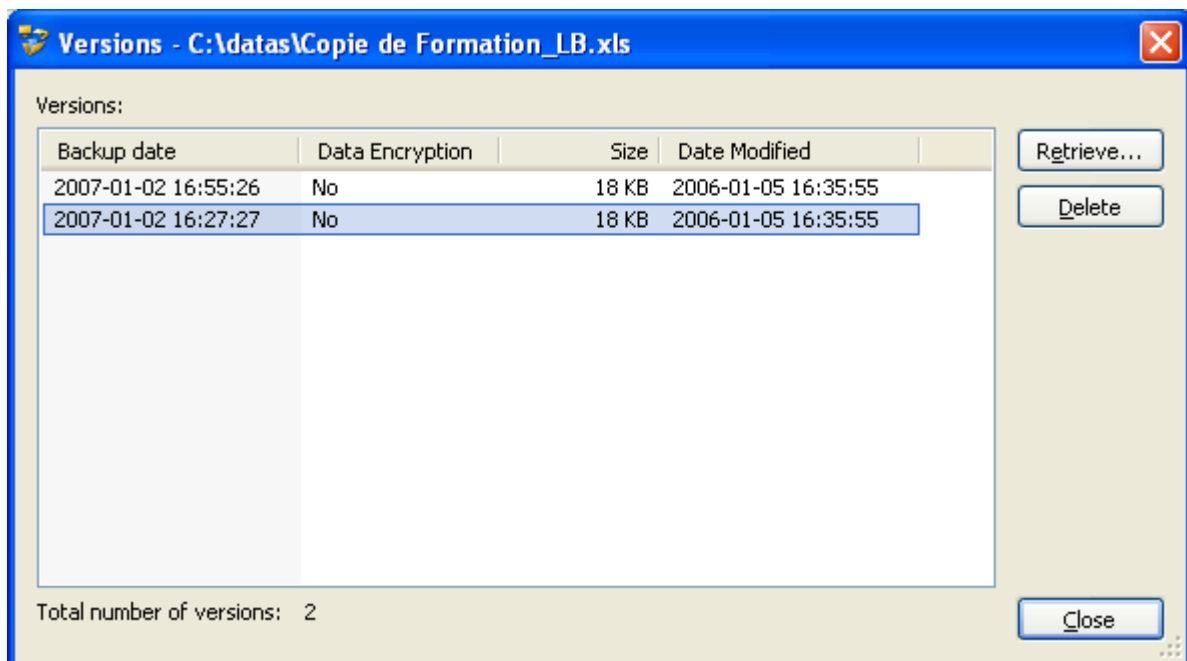
## Start a restoration

- 1 To perform a restoration, open a Windows Explorer on the machine you want to restore the data on.
- 2 Right-click the directory or file you wish to restore. Select **FileSafe/Retrieve backup...**
- 3 Select the target directory ; In this example, **datas** then display the contents:

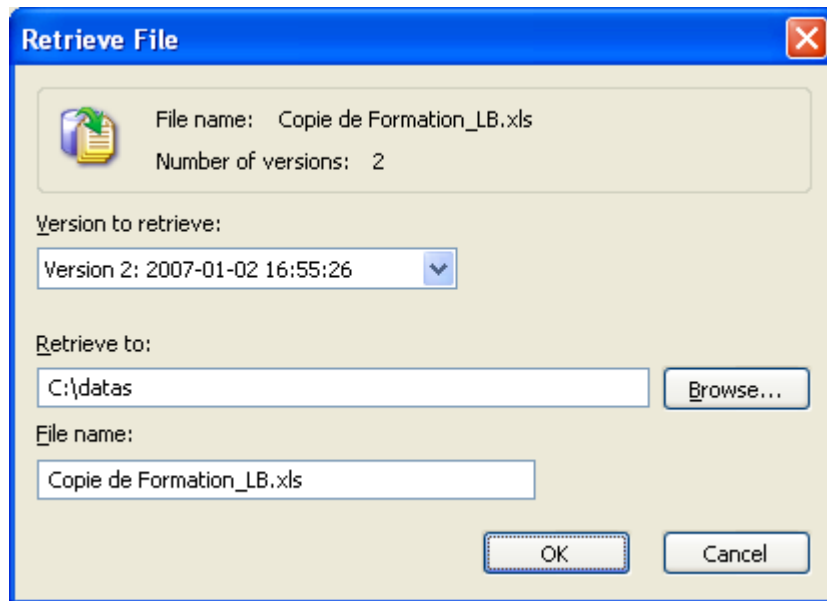


Docs	Folder		2007-01-02 16:55:26	Folder
Guide_Compatibilité	Folder		2007-01-02 16:55:30	
autorun.inf	File	1 KB	2007-01-02 16:55:25	File
Classeur1.xls	File	15 KB	2007-01-02 16:55:26	
convention de formation...	File	93 KB	2007-01-02 16:55:26	
Copie de Formation_LB.xls	File	18 KB	2007-01-02 16:55:26	Missing File
Copie de gamme, Parten ...	File	33 KB	2007-01-02 16:55:26	
feuille présence formatio...	File	32 KB	2007-01-02 16:55:30	
Formation Partenaire.pdf	File	195 KB	2007-01-02 16:55:30	
Formation_LB.xls	File	18 KB	2007-01-02 16:55:30	
Formulaire de satisfactio...	File	80 KB	2007-01-02 16:55:30	

- 4 Select the data to retrieve:
  - Right-click and select a version
  - Double click then click **Retrieve** or right-click **/Retrieve**
- 5 Choose the version to restore then click **Retrieve**. The following window opens.

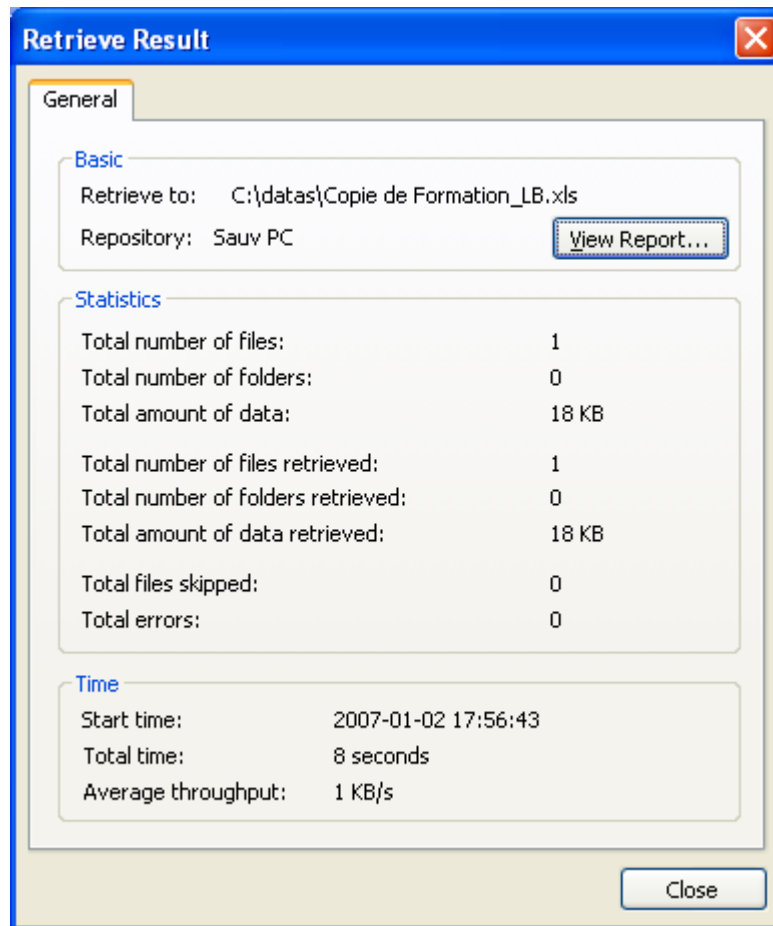


- 6 Choose the version to retrieve.



- 7 Choose the destination directory (**Browse...**). By default, the original directory name is used.  
**NOTE:** You can rename the file to restore (by default the original file name is used).
- 8 Click **OK** to start the recovery process.  
**NOTE:** If a file of this name already exists, you must confirm its replacement:
- 9 Wait for the retrieval to take place:
  - When the file is retrieved, you can consult a detailed report of the operation:

#### **Retrieve result after restoration**



### View Reports (summary)

Summary	
Retrieve Information	
Retrieve to:	C:\datas\Présentation.ppt
Repository:	Sauv PC
Statistics	
Total number of files:	1
Total number of folders:	0
Total number of files retrieved:	1
Total files skipped:	0
Total errors:	0
Total amount of data retrieved:	3.6 MB
Performance	
Start Time:	2007-01-02 18:00:36
Total Time:	59 seconds
Average Throughput	57 KB/s

---

## Chapter 5. Repository backup and restoration: cross-restoration

See:

["Repository backup and restoration" page 31](#)

["Cross restoration" page 32](#)

## Repository backup and restoration

The repository is an ordinary directory which needs to be backed up by the StoreWay DPA. The repository is either on a local machine (for example, C:\backup), or remote, accessible via a network share: for example \\exchange\Repository1.

You now need to apply a backup strategy on the directories which act as the Repository.

To back up the Repository, you must set up a standard data protection plan:

- 1** Install the StoreWay DPA agent on the machine which hosts the Repository
- 2** Verify the communication between the StoreWay DPA and client agent (browse)
- 3** Select the data to protect (the Repository).

**NOTE:** The Repository can be associated to a «global» profile, backing up « / » for example.

The Repository, once it is protected, can be restored at any time, using standard restoration procedures. Data can be retrieved from the original machine using the FileSafe agent.

## Cross restoration

It may be necessary to retrieve data immediately from a system which is down due to disk or system failure or any other problem which causes the original system to be unavailable.

See:

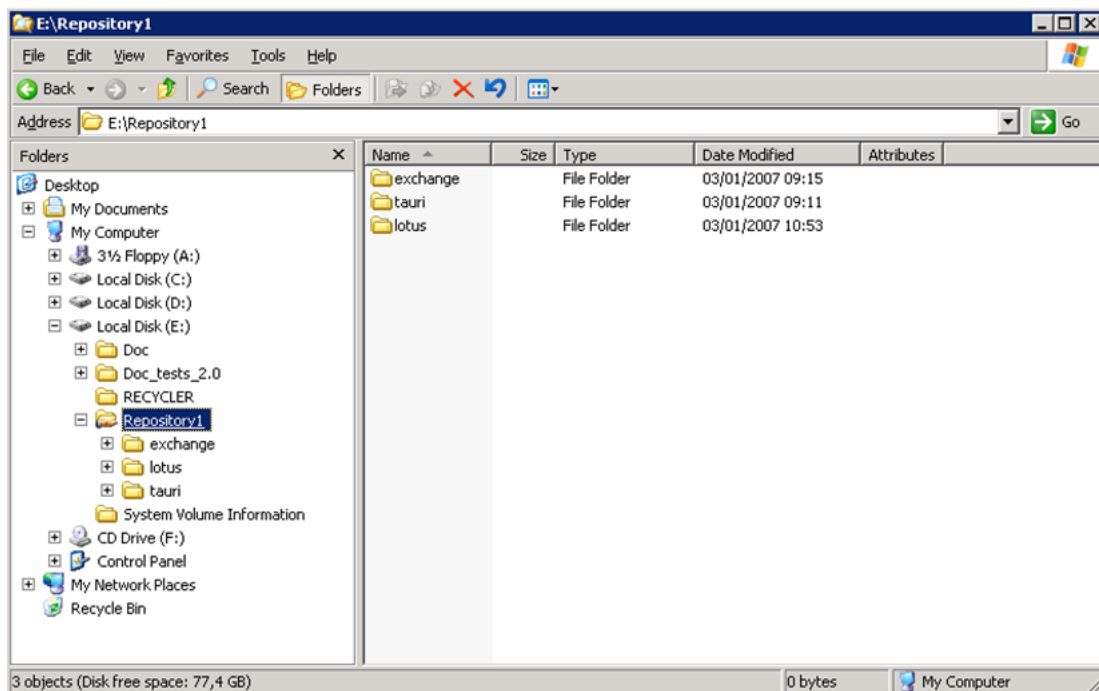
["Repository contents" page 32](#)

["Data retrieval on another system which does not have the FileSafe agent" page 33](#)

["Retrieving data on another system which has a FileSafe agent." page 35](#)

## Repository contents

For each time a system is backed up to a Repository, a directory with the name of the protected machine is created:



In the example above, 3 systems (**exchange**, **tauri** and **lotus**) are protected on the same Repository called Repository1. You will see on the server disk E:\ a directory Repository1 containing 3 "system" directories called **exchange**, **tauri** and **lotus**.

Each system directory contains 2 sub-directories 2c and backup\_id.

The directory 2c contains the list of backed up data (directories and files), preceded by the figure 2 for directories and 1 for files with the reference date of the latest synchronisation.

In this directory, you can therefore find the backed up data (initial version plus the 'delta blocks').

This data is not directly exploitable from the Repository (proprietary format = security and confidentiality).

The directory backup\_id contains the identifiers of the different backup sessions, ranked by ID number.

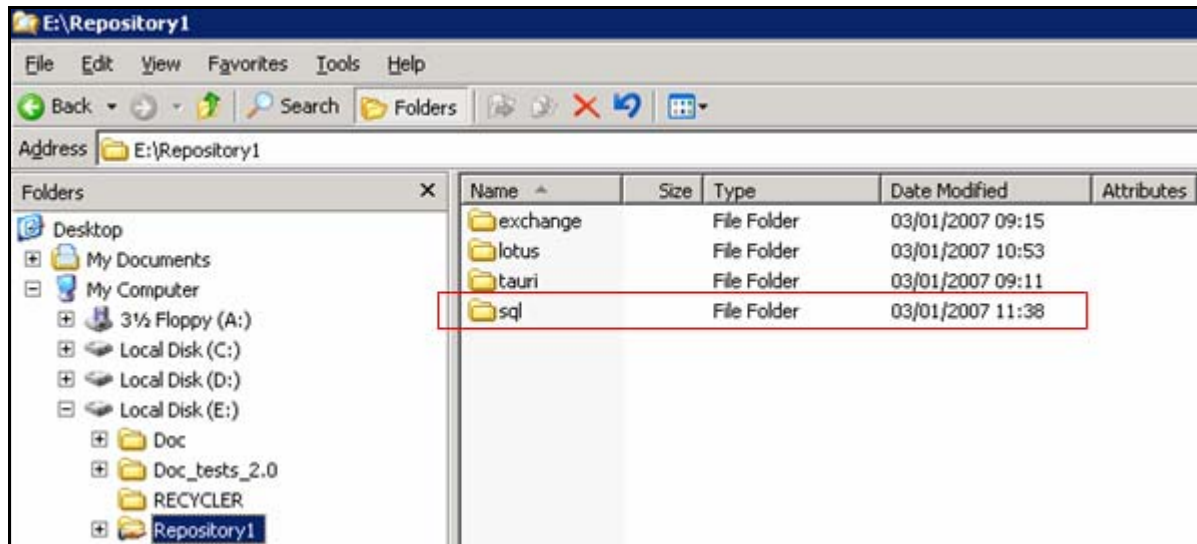


## Data retrieval on another system which does not have the File-Safe agent

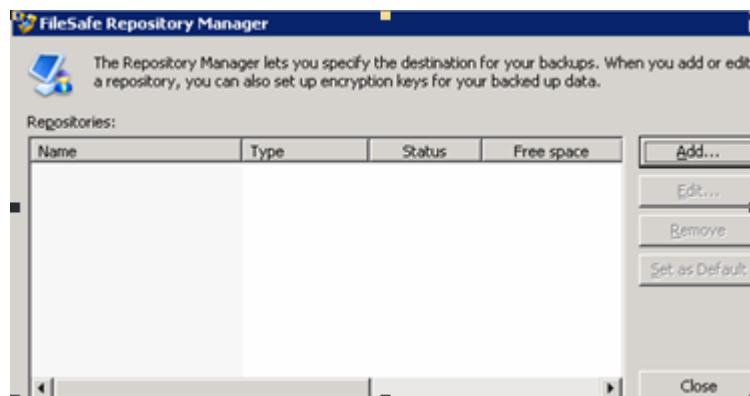
In the example used above, we will retrieve data from the system **tauri** to another system called **sql**.

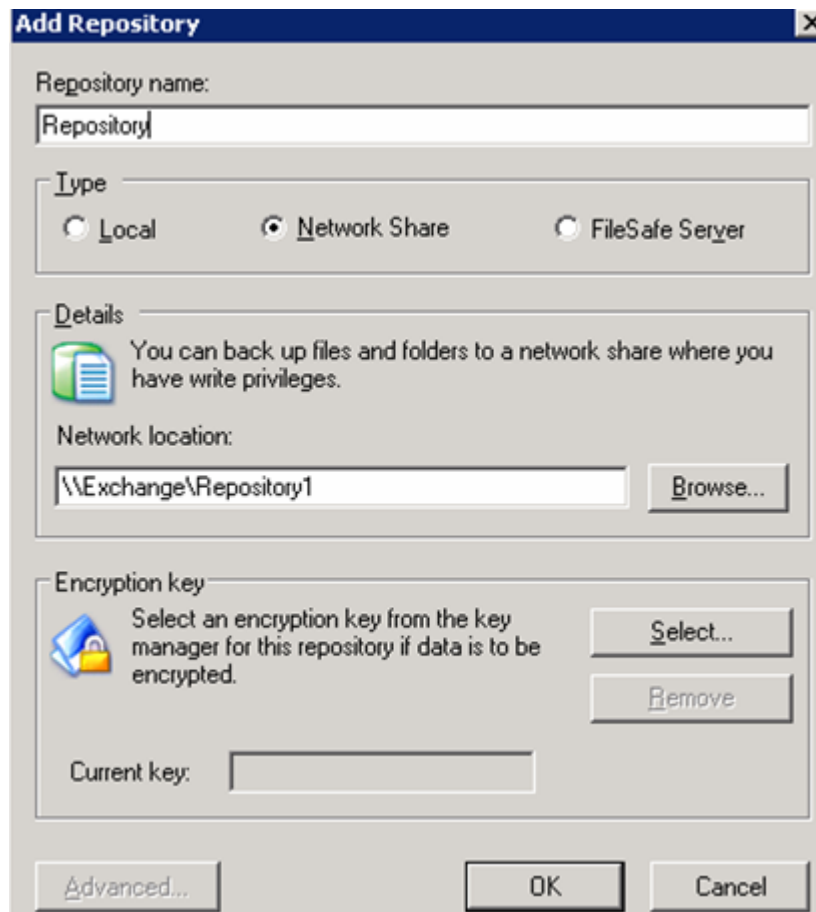
**NOTE:** The Windows versions can be different.

- 1 Install the FileSafe agent on the system **sql**.
- 2 Copy and/or rename the tauri directory in Repository1 to sql (name of the target system to be restored).

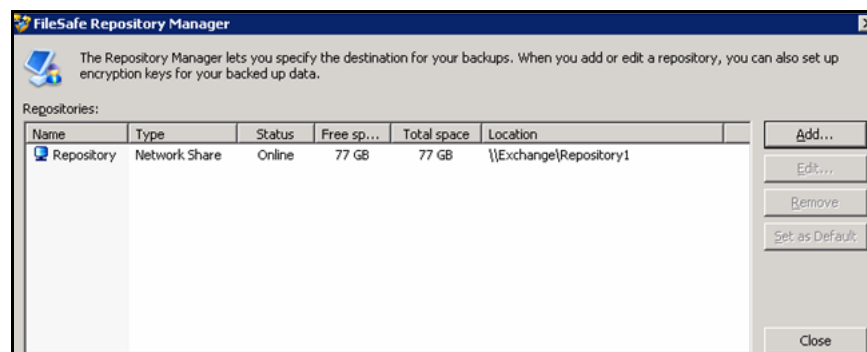


- 3 Configure the agent for it to access the sql Repository (ex. tauri). Right-click on the agent icon and select Repository Manager.
- 4 Add the Repository « Repository1 » where the «system\_ name » (sql) is located:





The new repository is visible in the FileSafe agent interface:



- 5 Restore data (access to the Repository declared) ;  
At this stage, FileSafe requests that backup data in the Repository is uploaded (data synchronization).
- 6 Click **Yes**: the data is visible, but greyed out (disappeared).
- 7 Retrieve the data.
  - Click **Retrieve** to start the retrieve process. A dialog box opens and requests the restoration path. By default, the path is « c:/ » because the agent is executed from the disk system root.
  - Click **Browse** to select a different location, then click **OK**.
  - Wait for data to be retrieved from the machine **tauri** to the **sql** system.
- 8 Display the retrieve results.

When it has been retrieved, the directory is displayed in yellow and no is longer greyed out. This change of colour means the directory is now available on the **sql** machine disk.

- 9 On the **sql** system, open the Windows Explorer and access the restored directory and data on **tauri**.

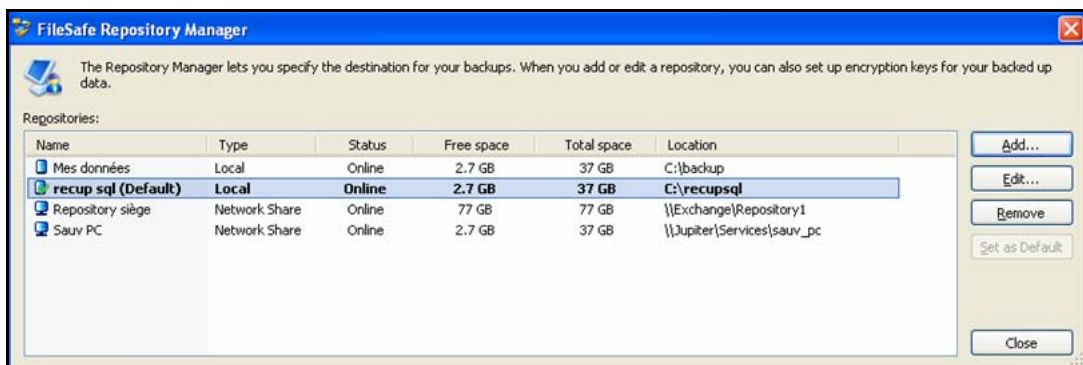
## Retrieving data on another system which has a FileSafe agent.

In this second case study, we will retrieve data on the **sql** system **sql** from the system called **tauri**. **Tauri** has a FileSafe agent and is also used as a Repository for **sql** under (c:\backup).

**Tauri** has several repositories declared, including one default.

- 1 Create a **tauri** directory Repository to retrieve sql data.
- 2 Copy and/or rename the sql backup directory (c:\backup) **tauri** (target system name where the restoration is performed).
- 3 Add the Repository which will be used by default.

In our example, we rename this Repository, « recupsql » under c:\.



- 4 Select the **c:\recupsql** Repository and click **Set as Default**.

**WARNING:** It is essential to define this Repository by default so that when FileSafe starts in the Explorer, data synchronization is possible.

- 5 Data restoration (access to the Repository declared).

At this stage, FileSafe requests the upload of backup data in the Repository (data synchronization) :

- 6 Click **Yes**: The data is visible but greyed out (missing).
- 7 **Effective data restoration.** Click **Retrieve** to launch the retrieval process. A dialog box opens to specify the restoration path. By default, this path is « c:/ » because the agent is executed from the disk system root.
- 8 Click **Browse** to choose a different location then click **OK**.
- 9 Wait for data to be restored from the **sql** machine to the **tauri** system.
- 10 Display the restoration report.

FileSafe provides a detailed report of the **sql** system data restoration in the **tauri** system « c:\test2 » directory.

- 11 The data are restored and accessible using the Explorer in the directory c:\test2.

---

## Chapter 6. Managing file and directory versions

Backed up data are not automatically purged; the product does not currently allow this. However, you simply need to monitor the volume or the repositories.

To free up space, you can delete data or backed up data versions which are no longer useful. If you apply this action to one file, all previous versions of the same file will be deleted from the Repository.

**EXAMPLE:** If you have backed up a file on January 1, 2, 3, 4 and 5, and you wish to delete the January 3 version, the versions of this file for January 1 and 2 will also be deleted.

- The removal of a file is managed by the FileSafe agent from the restoration (Retrieve...).
- The removal of the directory must be performed directly in the Repository by deleting one or more directories backed up and stored in the Repository.

## Deleting a version of a backed up file

We want to delete one or several intermediate file versions.

**NOTE:** To delete a version of a missing system file, see "Deleting a version of a backed up file" page 37.

- 1 Start a Windows Explorer
- 2 Select one or more versions of the file you want to delete then right-click to start FileSafe, then select **Retrieve backup**.
- 3 If the default Repository does not contain these versions to delete, select the relevant Repository in the drop-down menu.

**NOTE:** The list of versions may be different depending on the contents of each Repository and the backup policy in place.

- 4 In the list of versions, select the version you wish to delete.
- 5 Click **Delete**.

**WARNING:** Deleting the most recent version will delete all previous versions.

- 6 Click **Yes** to confirm the deletion of the version(s), based on the version selected.

**WARNING:** This operation is irreversible.

## Deleting versions of a backed up directory

This operational mode enables you to remove an entire directory or a protected file including data deleted from the system.

- 1 Right-click any directory in the Windows Explorer.  
By clicking on the disk partition letter you can display all directories and protected files.
- 2 Select **FileSafe** then **Retrieve backup**.
- 3 If the default Repository does not contain the versions to delete, select the relevant Repository from the drop-down menu.
- 4 Right-click the directory to delete from the Repository and select **Backup sessions** to access the list of versions.
- 5 In the list of versions, select the version(s) you want to delete.
- 6 Click **Delete**.  
**WARNING:** Deleting the most recent version will delete all previous versions.
- 7 Confirm the deletion of the versions. Click **Yes** to confirm the deletion of the version(s), based on the version selected.

---

## Chapter 7. Reports and logs

See:

["FileSafe logs" page 40](#)

["Generating an X-ray file" page 41](#)

## FileSafe logs

Each time a FileSafe occurs (for example, backup or restoration of an object file or directory), information on this event are written to the Windows Event Application (The Event Viewer). This information relates to FileSafe (Source column). If problems occur, this information can help you find out exactly what has happened, when it happened and which objects are affected so you can take the necessary action (for example, reprotecting data).

**NOTE:** If Windows events are full, FileSafe information will not be available. You need to use Windows system tools to access this information, or even increase the size of the system log files.

### Display FileSafe logs is directly accessible using the FileSafe icon:

- 1 Open the FileSafe Explorer.
- 2 In the main menu, select **View/Event Log...**

The FileSafe Event Viewer window opens.

This window lists all FileSafe events (Information, Error and Warning), date, time and a short event description. Double-click the event to display it in a dedicated window.



## Generating an X-ray file

In some cases, you may need technical support for the FileSafe agent. To provide all necessary help and to help solve your problems as quickly as possible, the technical support team requests that you generate an agent log (X-ray = troubleshooting file).

### Create an X-ray file

- 1 Open the FileSafe Explorer.
- 2 In the main menu, select **Tools/Take X-ray**
- 3 Click **Save** to back up the .cab file to disk.
- 4 Send this file to the Technical Support team.



---

# Index

## A

- activation
  - offline 14
  - online 13

## B

- backup
  - custom 22
  - express 19
  - open files 25

## C

- create
  - Local or Network Share Repository 15
- cross restoration 30

## D

- delete
  - version of a directory 38
  - version of a file 37
- directory
  - delete version 38
  - manage versions 36
- disk space
  - requirements 7

## E

- express
  - backup 19

## F

- file
  - delete version 37
  - manage versions 36
- files
  - backup open 25

## I

- import
  - Signature File 14
- install
  - StoreWay DPA FileSafe Agent 9
- installation
  - prerequisites 10

## L

- licence
  - StoreWay DPA FileSafe Agent 12
- Local Share Repository
  - create 15
- logs 39

## N

- Network Share Repository
  - create 15

## O

- open files
  - backup 25

## P

- prerequisites
  - installation 10

## R

- reports 39
- repository
  - backup and restoration 31
  - contents 32
- restoration
  - cross-restoration 30
  - overview 26

## S

- Signature File
  - import 14
- StoreWay DPA FileSafe Agent
  - install 9
  - licence 12
  - overview 8

## V

- versions
  - manage for files and directories 36

## X

- X-ray file 41



## Technical publication remarks form

<b>Title:</b>	FileSafe Agent Version 2.6. Installation and User's Guide
---------------	---

<b>Reference:</b>	DPA_FILES SAFE_V2_6_EN
-------------------	------------------------

<b>Date:</b>	3/19/08
--------------	---------

### ERRORS IN PUBLICATION

### SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.

If you require a written reply, please include your complete mailing address below.

NAME:

DATE:

COMPANY:

ADRESS:

Please give this technical publication remarks form to your BULL representative or mail to:

Bull - Documentation D<sup>é</sup>pt.

1 Rue de Provence

BP 208

38432 ECHIROLLES CEDEX

FRANCE

[info@frec.bull.fr](mailto:info@frec.bull.fr)

# Technical publication ordering form

To order additional publications, please fill in a copy of this form and send it via mail to:

<b>BULL CEDOC</b> <b>357 AVENUE PATTON</b> <b>B.P.20845</b> <b>49008 ANGERS CEDEX 01</b> <b>FRANCE</b>	<b>Telephone:</b> +33 (0) 2 41 73 72 66 <b>FAX:</b> +33 (0) 2 41 73 70 66 <b>E-Mail:</b> <a href="mailto:srv.Duplicopy@bull.net">srv.Duplicopy@bull.net</a>
--	---

Reference:	Designation:	Qty
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
__ _ _ _ _ [ _ _ ]		
[ _ _ ] The latest revision will be provided if no revision number is given.		

NAME:                      DATE:

COMPANY:

ADRESS:

TELEPHONE:              FAX:

E-MAIL:

**For Bull Subsidiaries:**

Identification:

**For Bull Affiliated Customers:**

Customer Code:

**For Bull Internal Customers:**

Budgetary Section:

**For Others: Please ask your Bull representative.**

**BULL CEDOC**

**357 AVENUE PATTON**

**B.P.20845**

**49008 ANGERS CEDEX 01**

**FRANCE**

**REFERENCE**

**DPA\_FILES SAFE\_V2\_6\_EN**

