Secure File Access

Admin Guide

SFA

Secure File Access

Table of Contents

About

Secure File Access is an application meant for protecting data from unauthorized access and distribution. It allows protecting any types of data (text, graphics, multimedia, etc.), created in any types of applications (AutoCAD, Adobe Photoshop, MS Office, etc.).

System Requirements

The **Secure File Access Admin application** (SFA Admin):

- **Operating System**: Windows XP/Vista/7/8.
- **USB port** for USB flash drives.

The **Secure File Access User application** (SFA Decryptor):

- **Operating System**: Windows XP/Vista/7/8.
- **USB port** for USB flash drives.

How it Works

About

Secure File Access (SFA) protects files with encrypting them and allows the user to view and work with the protected data only if the corresponding USB flash drive is plugged into the USB port of the user computer. Only SFA administrators can define USB flash drives with which the user will be able to view protected files and work with them.

How SFA Admin Protects Data

As soon as the administrator selects the needed data for protection and defines parameters of protection**,** the Secure File Access application does the following operations:

1. Copies files to the location defined by the administrator and encrypts them.
2. Creates <File name>**.sfa** files with SFA metadata near each protected file.

During data protection the administrator can create file exceptions to define files, which will not be read-only when working with the protected data.

The user can work with the protected files only when he plugs an allowed USB drive into his computer.

How SFA User Works with Protected Data

When the allowed USB drive is plugged by the user to the USB port of the computer, all protected files are opened by corresponding applications in the so-called sandboxed session.

WARNING! Before the user starting to work with the protected files, the user has to close all instances of application in which these protected files will be opened, and only after that he can launch the SFADecryptor.exe application.

Sandboxed Session Restrictions

Below there is a table, which illustrates user possibilities when working with files in the sandboxed session.

User Action	Response
The operation of opening is performed for the protected files	
The user is trying to open the encrypted file without launching the SFADecryptor.exe file and without plugging the corresponding USB drive into the USB port of the computer.	The file is opened in the encrypted state.

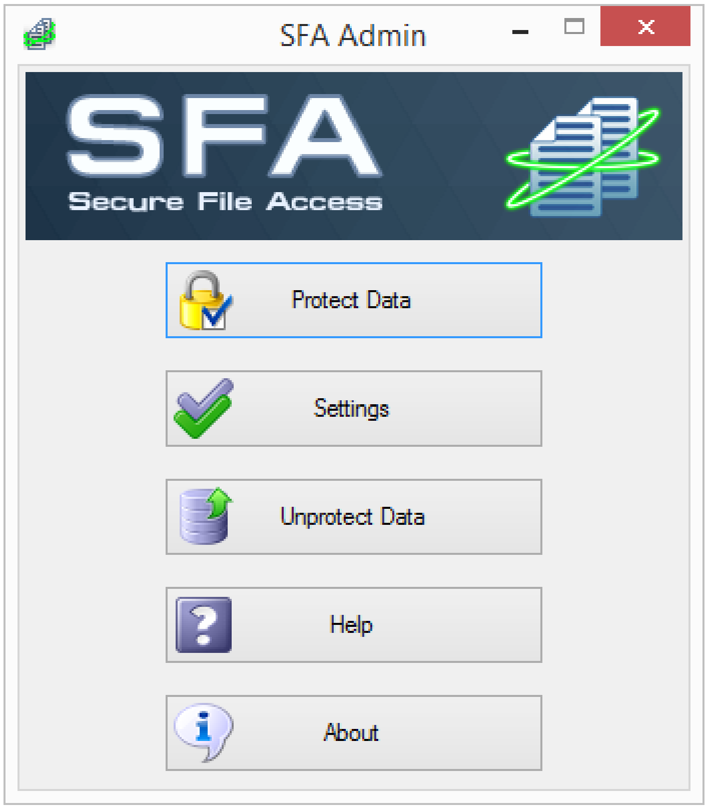
The user is trying to open the encrypted file after launching the SFADecryptor.exe file but without plugging the corresponding USB drive into the USB port of the PC.	The file is opened in the encrypted state.
The user is trying to open the encrypted file after launching the SFADecryptor.exe file and after plugging the corresponding USB drive into the USB port of the PC.	The file is opened and can be edited.
The user opens the encrypted file after launching the SFADecryptor.exe file and after plugging the corresponding USB drive into the USB port of the PC. But the digital signature of the application with which the user opens the file is not allowed by the SFA administrator.	The file is not opened.
The user opens the file using the application, which has been already opened before running the SFADecryptor.exe file.	The file is not opened.
Working with protected files (file operations)	
The user performs the Save As… operation.	The new file will be created in the current version of Secure File Access. This file will be protected.
The application that opens the current protected file creates a temporary file, for example, *.tmp.	In the current version of Secure File Access, the new temporary file will be protected.
The user works with the protected file and tries to open another protected file in the same application.	In the current version of Secure File Access, it is possible to work only with one opened protected file using the same application. The second file is not opened, an error message is displayed.
The user creates a new file while working with the current file.	The new file is encrypted in flight and remains encrypted after the user closes this file.
The user is working with protected files and opens the already existing not protected file not added to the exceptions list (or the file is opened by a sandboxed application).	The file is opened in read-only mode, it cannot be edited.
The user is working with protected files and opens the already existing not protected file added to the exceptions list (or the file is opened by a sandboxed application).	The file is opened, it can be edited and it will not be encrypted.

Other actions	
The user is trying to print the protected file while working with protected files.	Printing does not start.
The user is trying to send the protected file via email/ftp while working with protected data.	In the current version of Secure File Access, the file will be sent via email/ftp but the user won’t be able to open it.
The user is trying to make a screenshot while working with protected data.	A screenshot of the protected data is not made.
The user is working with the protected files and performs the Copy-Paste operation in the protected file.	The operation is performed correctly.
The user is copying and pasting the information from the protected file to the unprotected one.	Data is copied in the encrypted form. The user won’t be able to decrypt the copied data in the unprotected file.
The user is copying and pasting the information from unprotected file to the protected one.	The operation is performed correctly.

Secure File Access User Interface

The starting page of the Secure File Access application consists of the following parts:

- The **Protect Data** button: Evokes the **SFA Admin Data Protection** wizard, where the administrator can protect data and define its location for the user who will be working with protected data.
- The **Settings** button: Evokes the **SFA Admin Settings** wizard, where the administrator can define the flash drives that can be used for extracting protected data via the SFA Decryptor application by the user.
- The **Unprotect Data** button: Evokes the **SFA Admin Data Unprotector** page, where the administrator can unprotect the previously protected data and define the location for it.
- The **Help** button: Opens the help guide for administrator.
- The **About** button: Evokes the **About** page, in which information about the Secure File Access application is displayed.



How to Use Secure File Access Settings

About

Before starting protecting data with the Secure File Access application, the administrator has to define the following settings in the Secure File Access application:

- Admin flash drives: Flash drives with which it will be possible to unprotect data via the **SFAAdmin.exe** application.
- User flashes drives: Flash drives with which it is possible to work with the protected data on the user side using the **SFADecryptor.exe** application.
- File exceptions (optionally): File masks that will define which files will be not read-only when working with the protected data.

Managing Admin/User Flash Drives

Only the Secure File Access administrator can add/delete/rename Admin/User Flash Drives. USB flash drives must be added via the Secure File Access Admin application on the computer, on which files will be protected.

It is possible to add the same USB flash drive only once and into one list: either Admin flash drives or User flash drives.

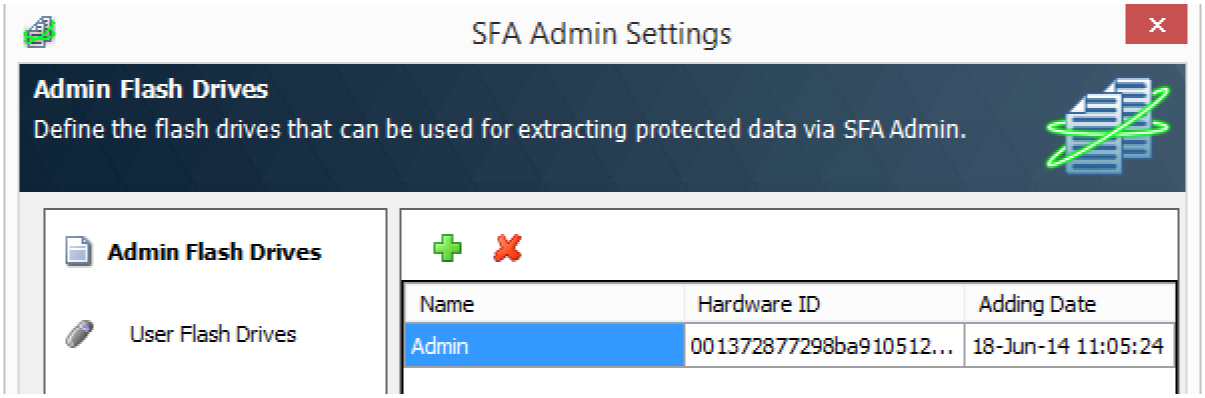
How to Add Admin/User Flash Drives

To add Admin/User Flash Drives, do the following**:**

1. Plug the flash drive into USB port of your computer.

NOTE: It is possible to use only USB flash drives and no other USB storage devices.

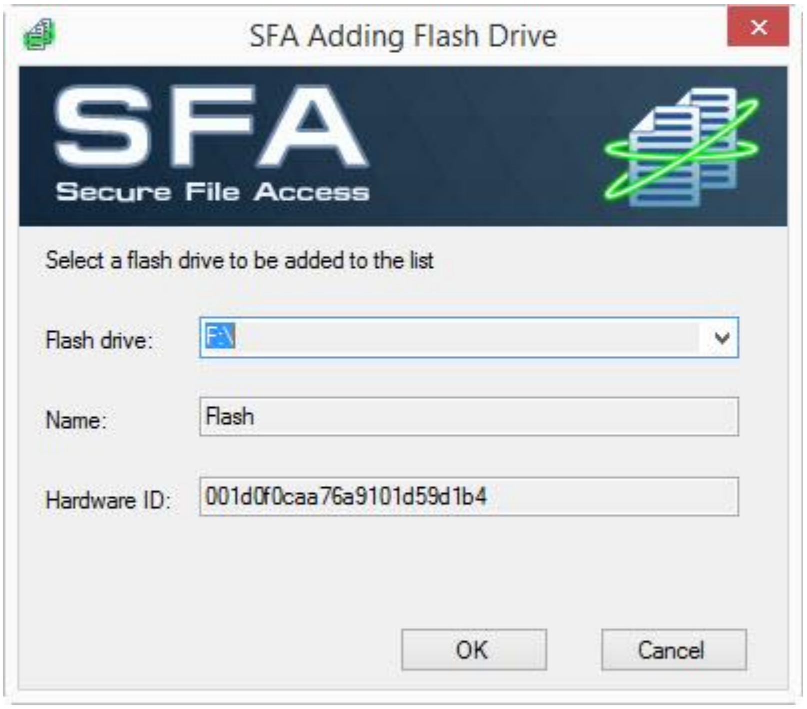
2. Run the **SFAAdmin.exe** file and in the **SFA Admin** main page, click **Settings**.
3. The **SFA Admin Settings** wizard opens.



Define the flash drives that can be used for extracting protected data via SFA Admin.

Name	Hardware ID	Adding Date
Admin	001372877298ba910512...	18-Jun-14 11:05:24

4. Open the **Admin Flash Drives/User Flash Drives** page.
5. Click the green plus sign ✚ to add the needed flash drives.
6. The **SFA Adding Flash Drive** page opens.



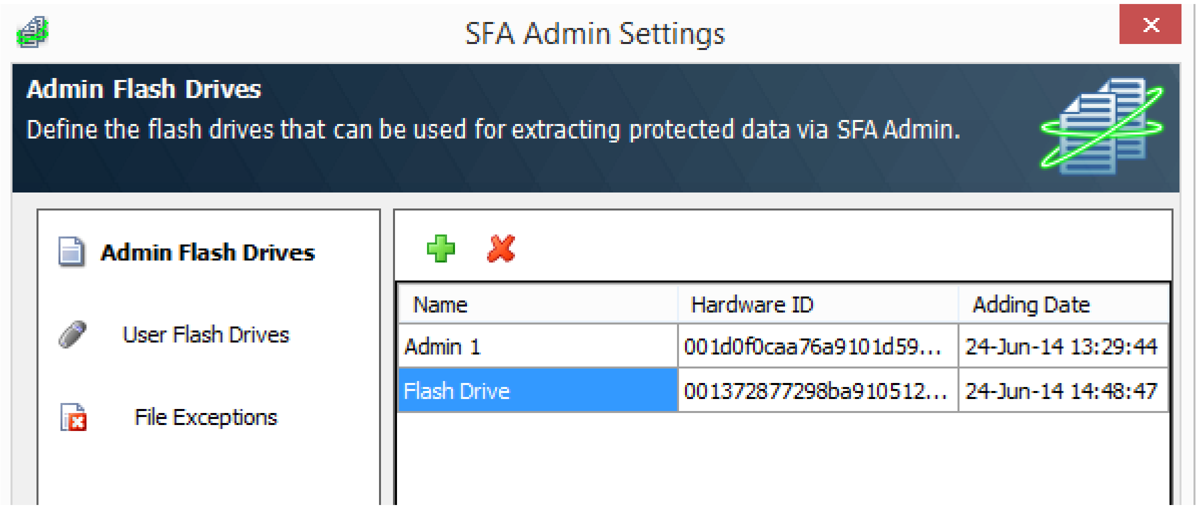
Select a flash drive to be added to the list

Flash drive: F:\

Name: Flash

Hardware ID: 001d0f0caa76a9101d59d1b4

7. In the **Flash drive** drop-down list, select the needed flash drive and click **OK.**
8. The added USB flash drive appears in the list.



Admin Flash Drives

Define the flash drives that can be used for extracting protected data via SFA Admin.

Name	Hardware ID	Adding Date
Admin 1	001d0f0caa76a9101d59...	24-Jun-14 13:29:44
Flash Drive	001372877298ba910512...	24-Jun-14 14:48:47

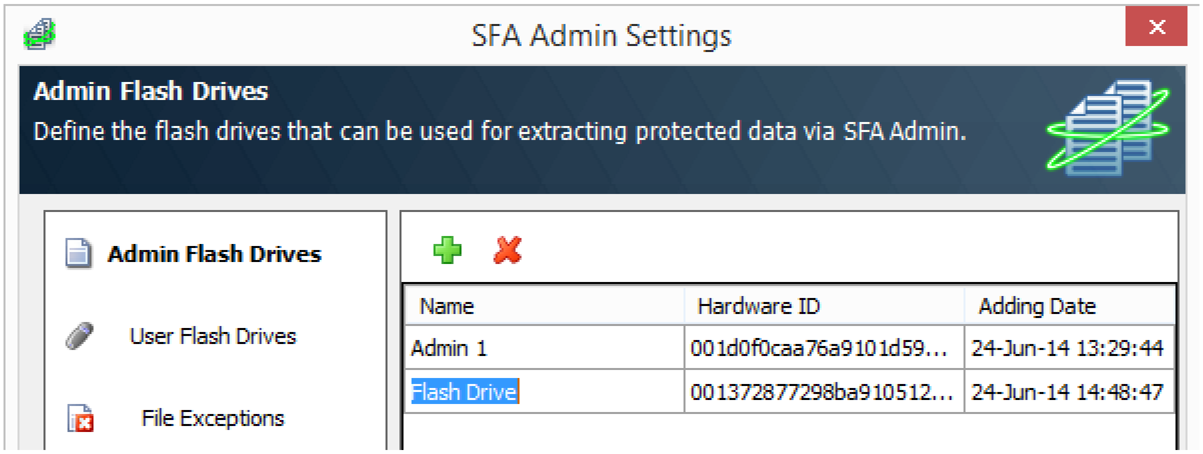
9. To change the name of the flash drive, edit it.
10. Click **Save** in the **SFA Admin Settings** wizard.
11. Unplug the flash drive. Having added the flash drive into the **Admin Flash Drives** list, you won't need this flash drive for further work. You need it for unprotection of files, which were protected when this flash drive was in the **Admin Flash Drives** list. Having added the flash drive into the **User Flash Drives** list, you won't need this flash drive for further data protection. Please give it to the user, so that he can work with the protected data on his computer.

How to Edit Admin/User Flash Drives

It is possible to edit only the name of the flash drive.

To edit the name of the Admin/User Flash Drive, do the following:

1. Run the **SFAAdmin.exe** file and in the **SFA Admin** main page, click **Settings**.
2. The **SFA Admin Settings** wizard opens.
3. Open the **Admin Flash Drives/User Flash Drives** page.
4. Double-click the needed name of the flash drive and start editing it.



Admin Flash Drives

Define the flash drives that can be used for extracting protected data via SFA Admin.

Admin Flash Drives

Name	Hardware ID	Adding Date
Admin 1	001d0f0caa76a9101d59...	24-Jun-14 13:29:44
Flash Drive	00137287729 8ba910512...	24-Jun-14 14:48:47

5. In the **SFA Admin Settings** wizard, click **Save** to apply changes.

How to Delete Admin/User Flash Drives

If you delete the Admin Flash Drive, you won't be able to unprotect data, which was protected when this flash drive was in the **Admin Flash Drives** list.

If you delete the User Flash Drive, it will be possible to open files, which were allowed to work with when this flash drive was in the **User Flash Drives** list. You won't be able to open new protected files with this flash drive.

To delete the Admin/User Flash Drive, do the following:

1. Run the **SFAAdmin.exe** file and in the **SFA Admin** main page, click **Settings**.
2. The **SFA Admin Settings** wizard opens.
3. Open the **Admin Flash Drives/User Flash Drives** page.
4. Select the needed flash drive and click the red ✖ sign to delete it.
5. If you delete an Admin flash drive, a warning message appears: "You might be unable to unprotect files that were protected when this flash drive was in the Administrator flash drives list. Do you really want to remove it from the list?". Click **Yes** to continue.
6. Click **Save** to apply changes.

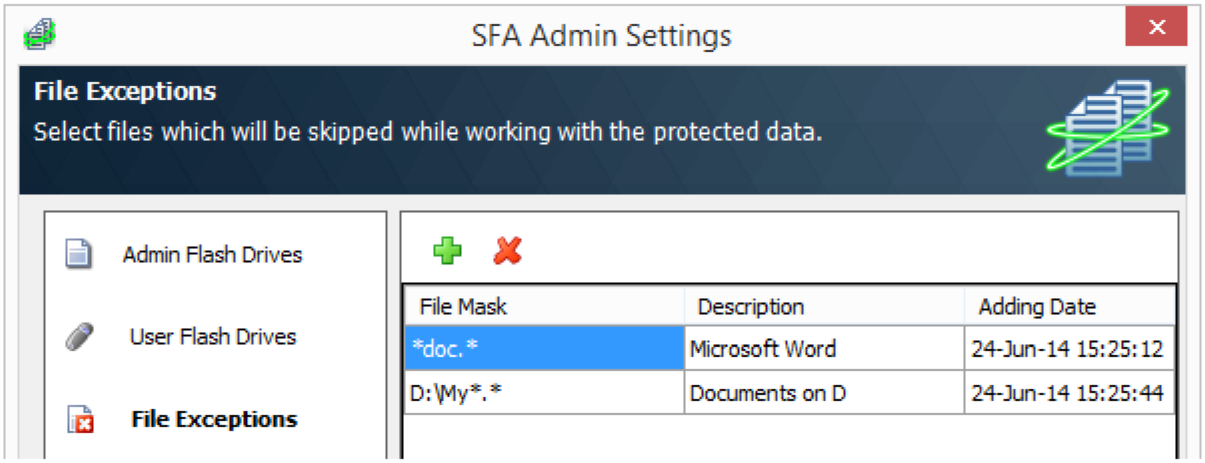
Defining File Exceptions

It is possible to define file exceptions by entering the full path to the file or simply the name of the file. For this purposes, you can use file masks.

To define file exceptions, do the following:

1. Run the **SFAAdmin.exe** file and in the **SFA Admin** main page, click **Settings**.
2. The **SFA Admin Settings** wizard opens.

3. Open the **File Exceptions** page.

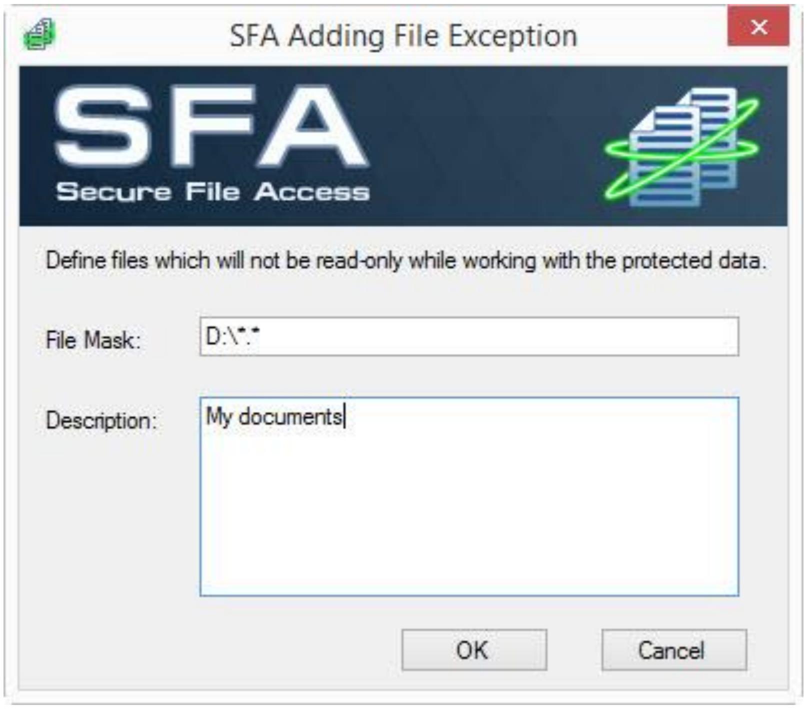


File Exceptions

Select files which will be skipped while working with the protected data.

File Mask	Description	Adding Date
doc.	Microsoft Word	24-Jun-14 15:25:12
D:\My*.*	Documents on D	24-Jun-14 15:25:44

4. Click the green plus sign ✚ to add a new file exception.
5. The **SFA Adding File Exception** page opens.



Define files which will not be read-only while working with the protected data.

File Mask: D:\*.*

Description: My documents

6. Enter the needed parameters in the **File Mask** and **Description** boxes.
7. Click **OK** to close the page.
8. Click **Save** in the **SFA Admin Settings** wizard to apply changes.

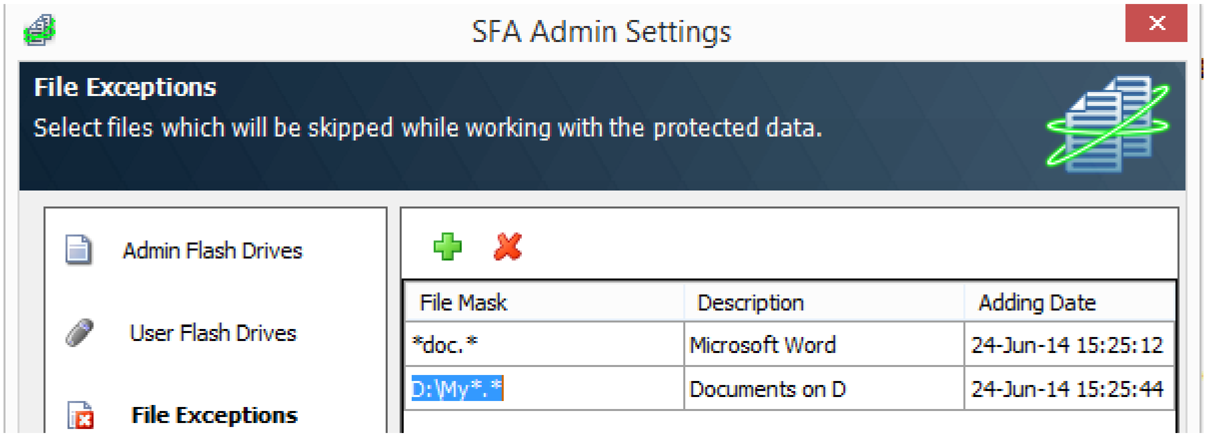
Editing File Exceptions

It is possible to change the **File Mask** and **Description** in the **File Exceptions**.

When you edit file exceptions, the new configuration will be applied only to those files, which will be protected after applying new parameters for the file exceptions.

To edit file exceptions, do the following:

1. Run the **SFAAdmin.exe** file and in the **SFA Admin** main page, click **Settings**.
2. The **SFA Admin Settings** wizard opens.
3. Open the **File Exceptions** page.
4. Double-click the needed column of the file exception and start to edit it.



File Mask	Description	Adding Date
doc.	Microsoft Word	24-Jun-14 15:25:12
D:\My*.*	Documents on D	24-Jun-14 15:25:44

5. In the **SFA Admin Settings** wizard, click **Save** to apply changes.

Deleting File Exceptions

If you delete file exceptions, the new configuration will be applied only to those files, which will be protected after deletion of file exceptions.

To delete file exceptions, do the following:

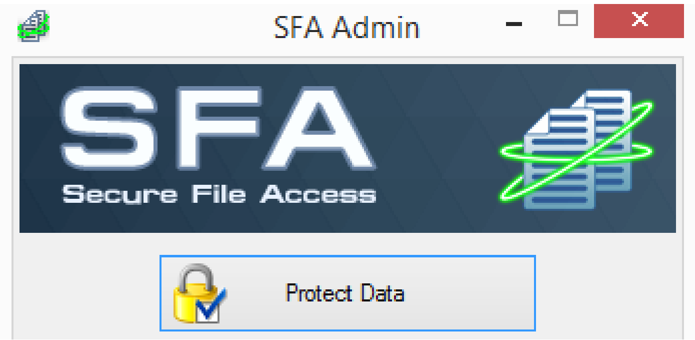
1. Run the **SFAAdmin.exe** file and in the **SFA Admin** main page, click **Settings**.
2. The **SFA Admin Settings** wizard opens.
3. Open the **File Exceptions** page.
4. Select the needed file exception and click the red ✖ sign to delete it.
5. Click **Save** to apply changes.
6. The file exception is successfully deleted.

Protecting Data with Secure File Access

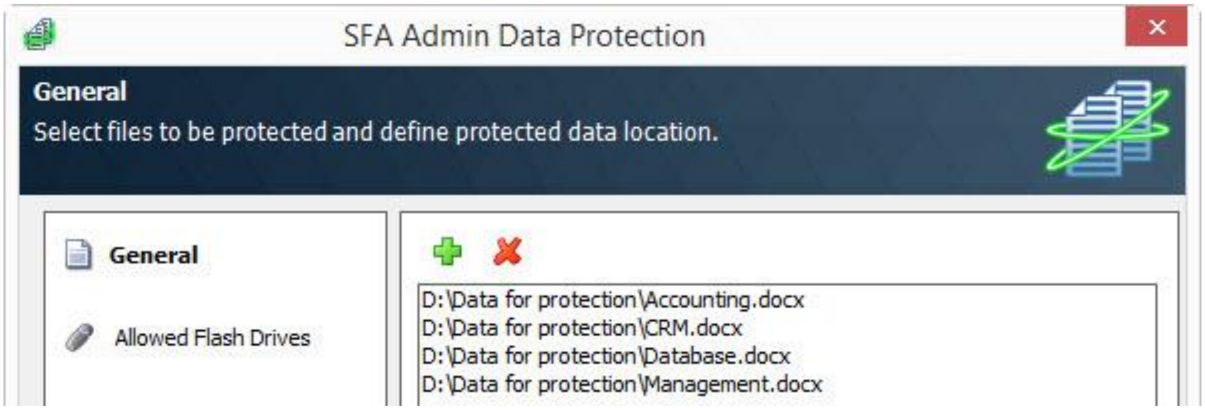
Data protection is performed via the **SFA Admin Data Protection** wizard. Before starting protecting data, the administrator has to define settings in the Secure File Access application.

To open the SFA Admin Data Protection wizard, do the following:

1. Run the **SFAAdmin.exe** file and in the **SFA Admin** main page, click **Protect Data**.



2. The **SFA Admin Data Protection** wizard opens.
3. On the **General** page, do the following:
   - To add files for protection, click the green plus sign ✚ .
   - If you need to remove data from the protection list, select the needed file and click the red ✖ sign to remove it.

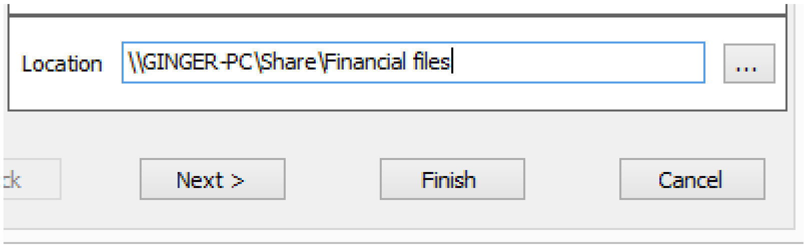


Select files to be protected and define protected data location.

D:\Data for protection\Accounting.docx
D:\Data for protection\CRM.docx
D:\Data for protection\Database.docx
D:\Data for protection\Management.docx

   - In the **Location** box, define destination folder to which the protected files will be copied and click **Next**.

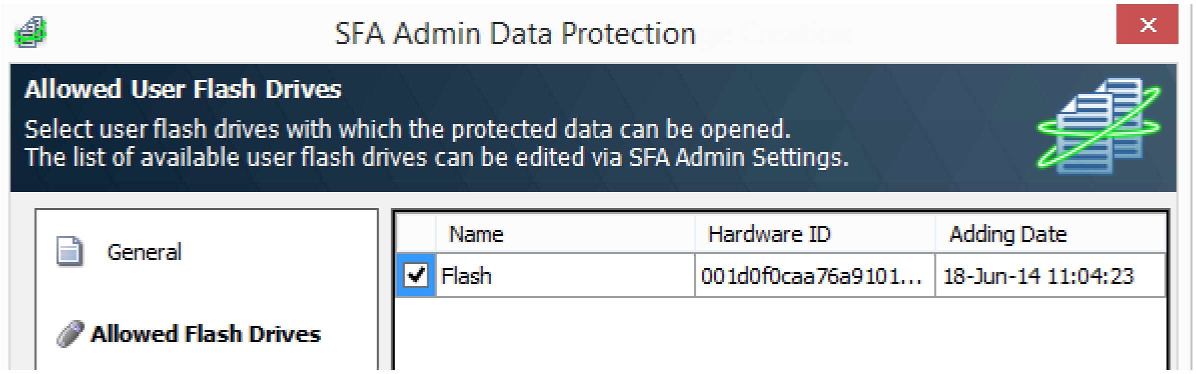
WARNING! If you define the original destination of the files for protection, the files will be rewritten and you won't have unprotected copies of files.



Location \\GINGER-PC\Share\Financial files

4. On the **Allowed Flash Drives** page, select those flash drives with which the user will be able to open protected data and click **Next**. If there is no needed flash drive in the list, add it via the **SFA Admin Settings** wizard.

NOTE: Secure File Access will automatically add all User Flash Drives to the Allowed Flash Drives list. By default, all User Flash Drives are selected in the SFA Admin Data Protection wizard.



SFA Admin Data Protection

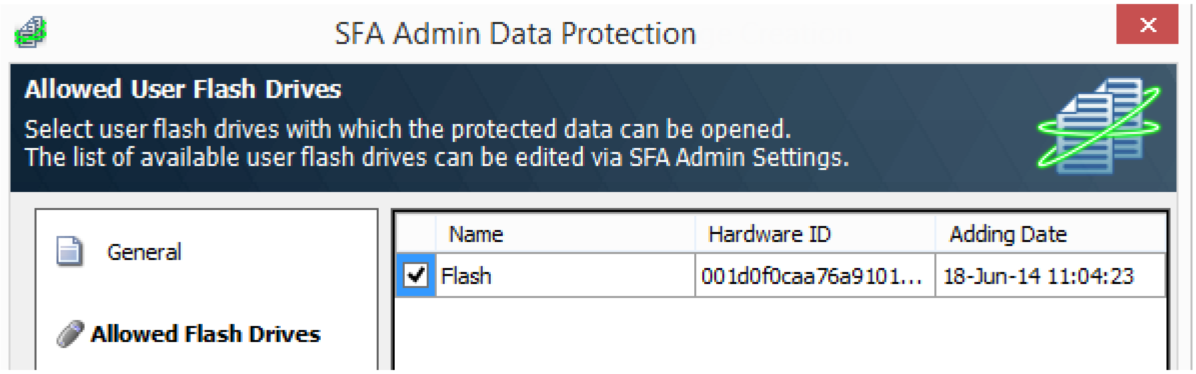
Allowed User Flash Drives

Select user flash drives with which the protected data can be opened.
The list of available user flash drives can be edited via SFA Admin Settings.

	Name	Hardware ID	Adding Date
☑	Flash	001d0f0caa76a9101...	18-Jun-14 11:04:23

5. If needed, on the **File Exceptions** page, select external files which will not be read-only while working with the protected data and click **Next.**

NOTE: By default, all File exceptions are selected in the SFA Admin Data Protection wizard.



SFA Admin Data Protection

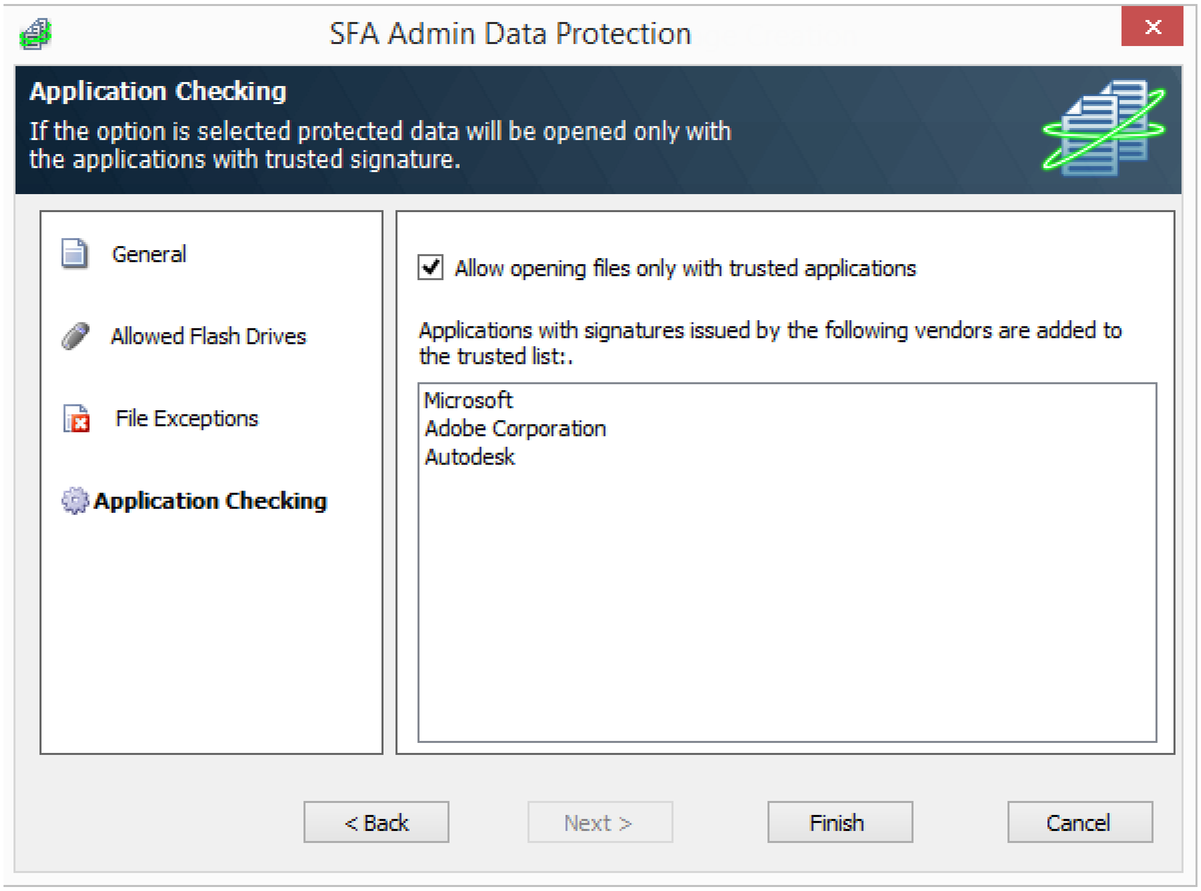
Allowed User Flash Drives

Select user flash drives with which the protected data can be opened.
The list of available user flash drives can be edited via SFA Admin Settings.

	Name	Hardware ID	Adding Date
☑	Flash	001d0f0caa76a9101...	18-Jun-14 11:04:23

6. If needed, on the **Application Checking** page, do one of the following:
   - Select **Allow opening files only with trusted applications**. In this case, the user is able to open protected files only with the following applications:
     - Microsoft Word.
     - Microsoft Outlook.

    - Microsoft Excel.
    - Microsoft Access.
    - Microsoft InfoPath.
    - Microsoft OneNote.
    - Microsoft PowerPoint.
    - Microsoft Project.
    - Microsoft Publisher.
    - Microsoft Share Point.
    - Adobe Acrobat.
    - Adobe Reader.
    - Autodesk Autocad.
    - Autodesk Maya.
- Unselect **Allow opening files only with only trusted applications**. In this case, the user will be able to open protected files with all types of programs.



Application Checking

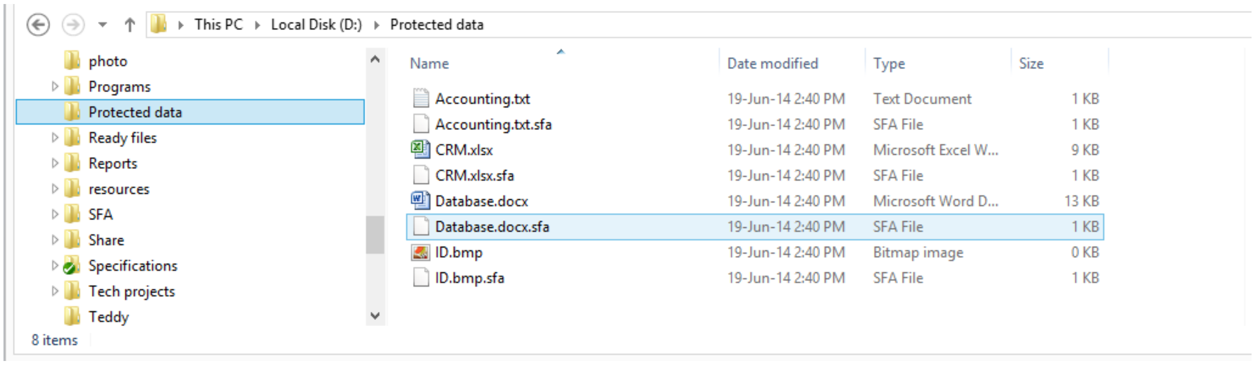
If the option is selected protected data will be opened only with the applications with trusted signature.

☑ Allow opening files only with trusted applications

Applications with signatures issued by the following vendors are added to the trusted list:.

Microsoft
Adobe Corporation
Autodesk

7. Click **Finish.**
8. The Secure File Access application copies files to the defined location and encrypts them. <File name>**.sfa** files with SFA metadata appear near each protected file. Do not delete/edit these files, otherwise the user won't be able to work with them.



Name	Date modified	Type	Size
Accounting.txt	19-Jun-14 2:40 PM	Text Document	1 KB
Accounting.txt.sfa	19-Jun-14 2:40 PM	SFA File	1 KB
CRM.xlsx	19-Jun-14 2:40 PM	Microsoft Excel W...	9 KB
CRM.xlsx.sfa	19-Jun-14 2:40 PM	SFA File	1 KB
Database.docx	19-Jun-14 2:40 PM	Microsoft Word D...	13 KB
Database.docx.sfa	19-Jun-14 2:40 PM	SFA File	1 KB
ID.bmp	19-Jun-14 2:40 PM	Bitmap image	0 KB
ID.bmp.sfa	19-Jun-14 2:40 PM	SFA File	1 KB

Unprotecting Protected Data with Secure File Access

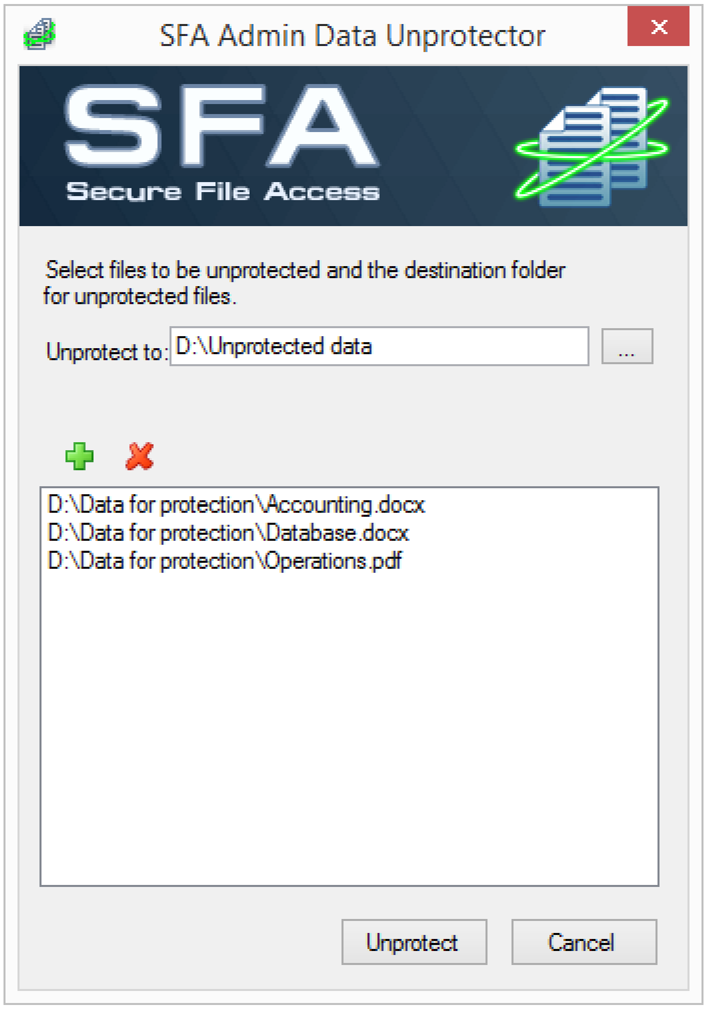
About

Only the Secure File Access administrator can unprotect the previously protected data by the Secure File Access application. During the process of unprotection, Secure File Access decrypts the selected files and as a result, the files become unprotected.

How to Unprotect Data

To unprotect data, do the following:

1. Run the **SFAAdmin.exe** file and in the **SFA Admin** main page, click **Unprotect Data**.
2. The **SFA Admin Data Unprotector** page opens.



Select files to be unprotected and the destination folder for unprotected files.

Unprotect to: D:\Unprotected data

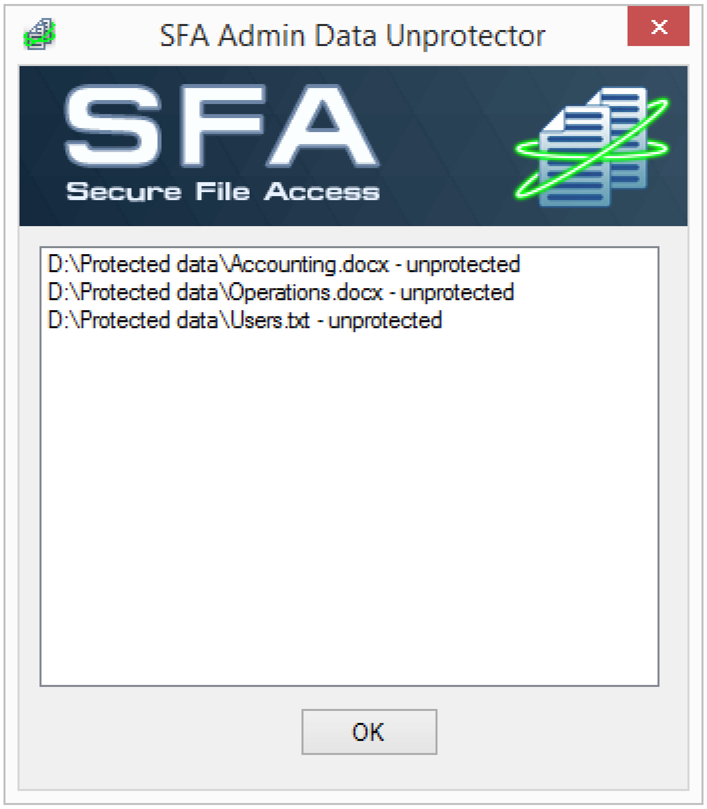
D:\Data for protection\Accounting.docx
D:\Data for protection\Database.docx
D:\Data for protection\Operations.pdf

3. In the **SFA Admin Data Unprotector** page, do the following:
    - In the **Unprotect to** box, browse the location to which the data will be unprotected.

NOTE: If you unprotect data to the same location with the protected copy of this data, such data will be unprotected but the metadata file (the file with the .sfa extension) won't be deleted.

- To add the needed data for unprotection, click the green plus sign ✚ .
- If you need to delete files from the list, select the needed file and click the red ✖ sign.

4. Click **Unprotect.**
5. The data is successfully unprotected. The process of files unprotection is displayed in the **SFA Admin Data Unprotector** page.



```
D:\Protected data\Accounting.docx - unprotected
D:\Protected data\Operations.docx - unprotected
D:\Protected data\Users.txt - unprotected
```

Working with Protected Data

About

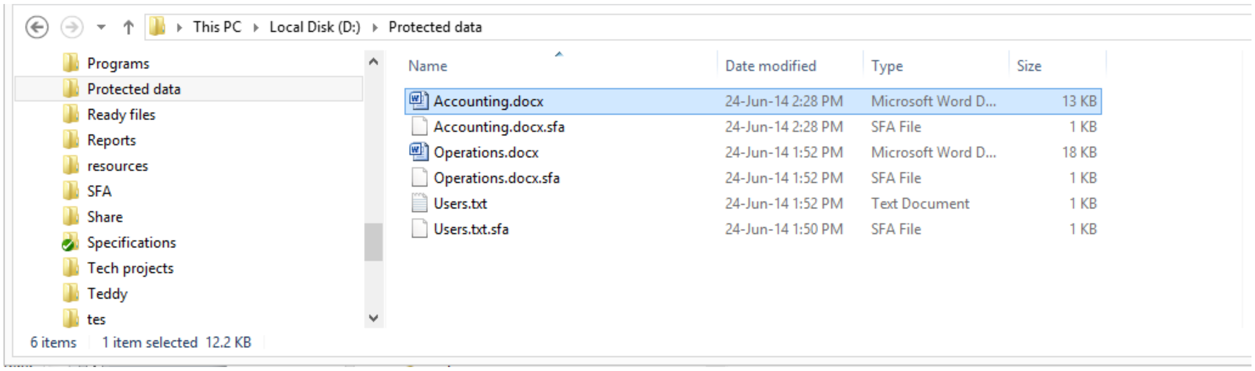
The user is able to decrypt and after that work with the protected data only after he launches the **SFADecryptor.exe** application and plugs the allowed USB flash drive into his computer.

Pay attention! To unprotect data, the user must have the protected file and a corresponding file with the .sfa extension, which was created during the file protection. These two files must be in the same location, otherwise the user won't be able to open the protected file.

Decrypting Protected Data

To decrypt protected data, do the following:

1. Plug the allowed USB flash drive into your computer.
2. Close applications in which protected files will be opened.
3. Run the **SFADecryptor.exe** file.
4. Double-click the protected file to open it.



Name	Date modified	Type	Size
Accounting.docx	24-Jun-14 2:28 PM	Microsoft Word D...	13 KB
Accounting.docx.sfa	24-Jun-14 2:28 PM	SFA File	1 KB
Operations.docx	24-Jun-14 1:52 PM	Microsoft Word D...	18 KB
Operations.docx.sfa	24-Jun-14 1:52 PM	SFA File	1 KB
Users.txt	24-Jun-14 1:52 PM	Text Document	1 KB
Users.txt.sfa	24-Jun-14 1:50 PM	SFA File	1 KB

5. Start working with the protected file in the sandboxed session.

Restrictions of the sandboxed session can be found here.