



User Guide

# McAfee File and Removable Media Protection (FRP) 4.3.0

For use with ePolicy Orchestrator 4.6.6, 4.6.7, 5.0.1, 5.1 Software

## **COPYRIGHT**

Copyright © 2014 McAfee, Inc. Do not copy without permission.

## **TRADEMARK ATTRIBUTIONS**

McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit [mcafee.com](http://mcafee.com) for the most current products and features.

## **LICENSE INFORMATION**

### **License Agreement**

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents

<b>Preface</b>	<b>5</b>
About this guide . . . . .	5
Audience . . . . .	5
Conventions . . . . .	5
Find product documentation . . . . .	6
<b>1 Introduction</b>	<b>7</b>
How FRP works . . . . .	7
Features . . . . .	8
<b>2 Managing user local keys and removable media encryption</b>	<b>9</b>
The FRP console . . . . .	9
Manage user local keys . . . . .	10
User local keys . . . . .	11
Create a user local key . . . . .	11
Delete a user local key . . . . .	12
Rename a User Local key . . . . .	12
Export user local keys . . . . .	13
Import user local keys . . . . .	13
Recover user local keys . . . . .	14
Change user local key authentication method . . . . .	14
Manage removable media protection . . . . .	15
Initialize removable media . . . . .	15
Recover removable media . . . . .	16
Change the removable media authentication details . . . . .	17
Managing CD/DVD/ISO media . . . . .	17
Writing McAfee Encrypted CD/DVD/ISO . . . . .	18
Working with McAfee Encryption for CD/DVD/ISO projects . . . . .	18
Select files and folders to encrypt to a CD/DVD/ISO . . . . .	19
Create McAfee Encrypted CD/DVD . . . . .	19
Create McAfee Encrypted ISO image . . . . .	20
<b>3 Managing encryption and decryption of files and folders</b>	<b>21</b>
Encrypt a file or a folder . . . . .	21
Decrypt a file or a folder . . . . .	22
Search for encrypted files or folders . . . . .	22
Create a self-extractor . . . . .	22
Read a self-extractor . . . . .	23
Attach a self-extractor to an email . . . . .	23
Add files and folders to encrypt to a CD/DVD/ISO . . . . .	24
Attach an encrypted file to an email . . . . .	24
<b>Index</b>	<b>25</b>



# Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

## Contents

- ▶ [About this guide](#)
- ▶ [Find product documentation](#)

---

## About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

### Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

### Conventions

This guide uses these typographical conventions and icons.

<i>Book title, term, emphasis</i>	Title of a book, chapter, or topic; a new term; emphasis.
<b>Bold</b>	Text that is strongly emphasized.
User input, code, message	Commands and other text that the user types; a code sample; a displayed message.
<b>Interface text</b>	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	<b>Note:</b> Additional information, like an alternate method of accessing an option.
	<b>Tip:</b> Suggestions and recommendations.
	<b>Important/Caution:</b> Valuable advice to protect your computer system, software installation, network, business, or data.
	<b>Warning:</b> Critical advice to prevent bodily harm when using a hardware product.

---

## Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

### Task

- 1 Go to the McAfee ServicePortal at <http://support.mcafee.com> and click **Knowledge Center**.
- 2 Enter a product name, select a version, then click **Search** to display a list of documents.

# 1

## Introduction

McAfee® File and Removable Media Protection (FRP) 4.3.0 delivers policy-enforced, automatic, and transparent encryption of files and folders stored or shared on PCs, file servers, emails, and removable media such as USB drives, CD/DVDs, and ISO files.

FRP is managed by McAfee® ePolicy Orchestrator® (McAfee ePO™) by creating a central point of management that makes sure the data is safe wherever it goes.

Typical FRP use cases include encrypting files such as spreadsheets and sensitive documents, allowing access to a specific folder on a shared network, encrypting removable media or blocking the copying of non-encrypted files, and sending self-extracting files in email attachments to partners or clients.

### Contents

- ▶ *How FRP works*
- ▶ *Features*

---

## How FRP works

FRP encrypts files and folders on local drives, network shares, or removable media devices according to the policies enforced by the administrator using the McAfee ePO server.

FRP supports system and user based policies, and provides a single point of control to protect data in your environment by integrating with the McAfee ePO server. FRP relies on Microsoft Windows credentials, so registered domain users and local system users are assigned product policies and encryption keys.

When the FRP client is installed on a McAfee ePO managed system, the system synchronizes with the McAfee ePO server and fetches product policies and encryption keys. The FRP client acts like a filter between the application to create or edit files and removable media. When a file is saved, the FRP filter executes the assigned policies and encrypts the data, if applicable.

FRP acts as a persistent encryption engine. When a file is encrypted, it remains encrypted even when:

- The file is moved or copied to another location.
- The file is moved out of an encrypted directory.



This is applicable only when you are using supported media files.

---

## Features

These are the key features of FRP.

- **Centralized management** — Provides support for deploying and managing FRP using McAfee ePO software.
- **Windows authentication-based policy enforcement** — FRP depends on leverages Microsoft Windows AD credentials for authentication, so registered domain users and local system users are assigned product policies and encryption keys.
- **User Personal Key** — An unique encryption key is created for each user; administrators can reference “User Personal Key” generically in policies.
- **Delegated administration through Role Based Key Management** — Enables the logical separation of management between multiple administrators. This capability is critical for separation across business functions and subsidiaries.
- **Auditing of key management and policy assignments** — The key management and policy assignment-related actions performed by McAfee ePO administrators are recorded in the audit log. This is critical to ensure compliance and prevent abuse by privileged administrators.
- **Protection of data on removable media** — Provides the ability to encrypt removable media and access encrypted content even on systems where FRP is not installed.
- **Network encryption** — Enables secure sharing and collaboration on network shares.
- **User-initiated encryption of files and email attachments** — Allows users to create and attach password-encrypted executable files that can be decrypted on systems where FRP is not installed.
- **Auditing and reporting for USB removable media and CD/DVD/ISO events** — Captures all end user actions related to USB removable media and CD/DVD/ISO events, with an auditing capability that provides an effective feedback loop for use by administrators in making policy decisions.
- **Configurable key cache expiry** — Enables the administrator to configure how long a key is cached on the client before it is removed due to non-connectivity to the McAfee ePO server.
- **Integration with the McAfee tray icon** — Consolidates the tray icons into one common McAfee icon.
- **Migration from EEFF v3.2.x to FRP 4.3.0** — Enables customers to migrate keys from legacy versions of the product to McAfee ePO-managed versions, with or without level information, with minimal effort.
- **Use of McAfee Common Cryptographic Module (MCCM)** — The FRP client makes use of the McAfee Core Cryptographic Module (MCCM) User and Kernel FIPS 140-2 cryptographic modules. FRP provides an option to install the product in FIPS mode. MCCM also provides performance benefits and, in particular, leverages Intel® Advanced Encryption Standard Instructions (AES NI), resulting in additional performance improvements on systems with AES NI support.

# 2

## Managing user local keys and removable media encryption

The FRP console enables you to view information on assigned policies and encryption keys, manage your user local keys, and secure removable media devices.

### Contents

- ▶ *The FRP console*
- ▶ *Manage user local keys*
- ▶ *Manage removable media protection*
- ▶ *Managing CD/DVD/ISO media*

---

## The FRP console

You can launch the FRP console by clicking the McAfee icon  on your taskbar and selecting **Manage Features | File and Removable Media Protection**.

From the left pane of the console, you can view a status report, create and manage User Local keys, and initialize, recover, and change the authentication method for USB and CD/DVD/ISO media devices.

### Status Report

The **Status Report** automatically appears when you launch the FRP console. It displays this information:

- Operating system running on the client system
- FRP installation files
- Encryption keys available to the system or the user
- General policies enforced on the system or the user
- Removable media policy enforced on the system or the user
- CD/DVD policy enforced on the system or the user
- Folder policies enforced on the system or the user
- File extension policies enforced on the system or the user
- List of exempted devices
- List of blocked processes
- List of file extensions excluded from encryption
- Key request exclusions
- Password policy rules enforced on the system

In the right pane of the console, click **Write to File** to export the status report to an XML file.

### Local keys

User local keys can be created and managed from the FRP console. Your administrator controls the availability of these options, according to your company's security policies.

See *Manage user local keys* for details.

### Removable media protection

FRP can be used to encrypt USB removable devices to protect data stored on the device. This feature provides the flexibility to create USB media that can be securely authenticated and accessed by any system with a supported Windows or Mac OS X operating system, without the need to install any McAfee encryption software.

Your administrator controls the availability of this solution on the console, according to your company's security policies.

See *Manage removable media protection* for details.

### CD/DVD/ISO media encryption

Using FRP, securely encrypted data can be written to optical media or ISO images. This feature provides the flexibility to create CD/DVD/ISO media that can be securely authenticated and accessed by any system with a supported Windows operating system, without the need to install any McAfee encryption software.

Your administrator controls the availability of this solution on the console, according to your company's security policies.

See *Managing CD/DVD/ISO Media* for details.

---

## Manage user local keys

User local keys are created by the user using the FRP client software on a client system. The user can use these keys to encrypt or decrypt data using the context menu. Access to the local key is limited to the user who created it. Your administrator controls your ability to create and manage user local keys, according to your company's security policies.



If you have a roaming profile, your user local keys travel with your profile.

## Tasks

- [Create a user local key on page 11](#)  
You can create a user local key and save it on your hard disk or removable storage device.
- [Delete a user local key on page 12](#)  
You can delete encryption keys that are not used. A deleted encryption key cannot be recovered. Consequently, documents encrypted with a deleted key cannot be opened.
- [Rename a User Local key on page 12](#)  
You can rename a user local key.
- [Export user local keys on page 13](#)  
To share encrypted files with other users, you must share the encryption keys they are encrypted with. When exported, the encryption key is packaged into a file with SKS as its extension. To export the file, the users must know the key store password. The SKS file can be sent as an e-mail attachment.
- [Import user local keys on page 13](#)  
To import an encryption key, you need to create a key store where you can save the imported key.
- [Recover user local keys on page 14](#)  
You can recover a user local key if the recovery key set in the user local key policy is available on the system.
- [Change user local key authentication method on page 14](#)  
You can change the protection mechanism for your key stores.

## User local keys

User local keys enable you to encrypt or decrypt data using the context menu. The use of a user local key is limited to the user who created it.

### Key storage

User local keys are stored in key stores. Each key store is protected with a password that you select (password token), or with your digital certificate (PKI token). You select the proper token when you create the key store. Your key store can be stored on your computer's hard disk, or on a removable storage media like a USB drive. It is possible to have one key store on the hard disk and another on removable storage, where each key store holds different keys.

## Create a user local key

You can create a user local key and save it on your hard disk or removable storage device.



If you want to save the local key on a USB drive, make sure the drive is inserted before you start the wizard.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.
- 2 In the left pane, click **Create new key** to open the **Welcome to Create Local Key** wizard, then click **Next**.
- 3 Select the location where you want to save the local key from the drop-down menu, then click **Next**. The **Data** page appears.

- 4 Enter a name for the local key, then select the inactivity timeout for the key from the drop-down menu.



The inactivity timeout defines how long a key can remain unused in memory. When the timeout is reached, you need to authenticate to FRP again before you can access encrypted files or folders.



Make sure that you provide unique names for the encryption keys, ideally reflecting the purpose of the key.

- 5 Click **Next**.

The **Tasks** page summarizes the key details configured in the wizard.

- 6 Click **Next**.

You might be prompted to authenticate to FRP before completing the wizard to ensure access to the corporate recovery key that will be used when you create your key store.

- 7 Click **Finish**.

## Delete a user local key

You can delete encryption keys that are not used. A deleted encryption key cannot be recovered. Consequently, documents encrypted with a deleted key cannot be opened.



Before deleting the key, make sure that you search for files that are encrypted with the key. For more information, see the **Search for encrypted files or folders** section.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.

- 2 In the left pane, click **Delete key** to open the **Welcome to the Delete Key wizard**, then click **Next**.

- 3 From the **Key name** drop-down list, select the required key, then click **Next**.

The **Tasks** page summarizes the key details configured in the wizard.

- 4 Click **Next**.

You might be prompted to authenticate to FRP before completing the wizard to ensure access to the key store.

- 5 Click **Finish**.

## Rename a User Local key

You can rename a user local key.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.

- 2 In the left pane, click **Rename key** to open the **Welcome to the Rename Key Wizard**, then click **Next**.

- 3 From the **Key name** drop-down list, select the required key, then click **Next**. The **Data** page appears.

- 4 Type a new name for the key, then click **Next**.

The **Tasks** page summarizes the key details configured in the wizard.

- 5 Click **Next**.

You might be prompted to authenticate to FRP before completing the wizard to ensure access to the key store.

- 6 Click **Finish**.

## Export user local keys

To share encrypted files with other users, you must share the encryption keys they are encrypted with. When exported, the encryption key is packaged into a file with SKS as its extension. To export the file, the users must know the key store password. The SKS file can be sent as an e-mail attachment.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.
- 2 In the left pane, click **Export keys** to open the **Welcome to the Export Key wizard**, then click **Next**.
- 3 Select the key, then browse to and select the destination file name and path where the key is to be exported.
- 4 Provide the password to be used to protect the exported key, then click **Next**.
- 5 When prompted, enter valid authentication information for the key store.
- 6 Click **Finish**.

## Import user local keys

To import an encryption key, you need to create a key store where you can save the imported key.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.
- 2 In the left pane, click **Import keys** to open the **Welcome to the Import Key wizard** page, then click **Next**.
- 3 Browse to and select the exported keys (\*.sks file), then click **Next**.
- 4 Select the volume and location where you want to insert the keys, then click **Next**.
- 5 When prompted for authentication for exported keys, enter a valid password, then click **OK**.
- 6 When prompted, enter valid authentication information for the key store, then click **OK**.
- 7 Click **Finish**.

## Recover user local keys

You can recover a user local key if the recovery key set in the user local key policy is available on the system.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.
- 2 On the left pane, click **Recover keys** to open the **Welcome to the Recover Key wizard**, then click **Next**.
- 3 From the drop-down menu, select the location where you saved the local key that needs to be recovered, then click **Next**.
- 4 Enter and confirm a new password for the key store, then click **Next**.

The **Tasks** page summarizes the key details configured in the wizard.

- 5 Click **Next**.

You might be prompted to authenticate to FRP before completing the wizard to ensure access to the key store.

- 6 Click **Finish**.

## Change user local key authentication method

You can change the protection mechanism for your key stores.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.
- 2 In the left pane, under the **Local Keys** section, click **Change authentication** to open the **Change Token wizard**, then click **Next**.
- 3 Select the location where you saved the local key, then click **Next**.

- 4 Select the token type you want to authenticate the device with. The authentication method selected determines the page that appears:

- If you select **Password Protection**, the **Password** page appears. Enter and confirm the new password, then click **Next**.
- If you select **Certificate Protection**, the **Certificate** page appears. Select a certificate from the list of available certificates, then click **Next**.

The **Tasks** page summarizes the key details configured in the wizard.

- 5 Click **Next**.

You might be prompted to authenticate to FRP before completing the wizard to ensure access to the key store.

- 6 Click **Finish**.

## Manage removable media protection

FRP enables you to encrypt removable USB devices to protect the data stored in the device.

You can view the contents of a removable media device on any supported Windows or Mac OS X client, without requiring to have any McAfee encryption software installed (otherwise, referred to as "offsite" access). In addition to enabling secure sharing of data with partners and vendors, this feature also enables users to carry data securely on USB drives and access it on other computers.

When the removable media device is inserted into the offsite client system, you will be prompted to enter authentication credentials. After successful authentication, you will be able to access the files on the device using the **McAfee Removable Media Protection** application that is available on the device.



An offsite application is now available for Mac OS X systems for FRP 4.3.

### Tasks

- [Initialize removable media on page 15](#)  
When you insert a non-protected removable device on a client with FRP installed and the policy for removable media is set to the **Allow Encryption (with offsite access)** or **Enforce Encryption (with offsite access)** protection level, you are prompted to initialize the device. You can also initiate initialization of the removable media from the FRP client console.
- [Recover removable media on page 16](#)  
You can recover access to the information on removable media using a recovery key, recovery password, or recovery certificate.
- [Change the removable media authentication details on page 17](#)  
You can change the protection mechanism for removable media from password to certificate, or vice versa.

## Initialize removable media

When you insert a non-protected removable device on a client with FRP installed and the policy for removable media is set to the **Allow Encryption (with offsite access)** or **Enforce Encryption (with offsite access)** protection level, you are prompted to initialize the device. You can also initiate initialization of the removable media from the FRP client console.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.
- 2 In the left pane, click **Initialize device**.
- 3 In the **Initialize Removable Media** dialog box, if the **Protected area** section is enabled, set the amount of space (in GB) on the device that you want to protect.

The ability to decide on the size of the protected area depends on the removable media encryption policy settings configured by the administrator.

4 In the **Authentication** section, select the required authentication method.

- If you select **Authentication password**, enter a password that conforms to the password complexity rules in your organization. If the password provided does not meet the required complexity, a message displaying the password complexity is displayed.
- If you select **Authentication certificate**, select a digital certificate from the drop-down menu.



The available authentication methods depend on the removable media encryption policy enforced on the system or the user.

5 In the **Recovery** section, select the required recovery method.



The available recovery methods depend on the removable media encryption policy enforced on the system or the user.

6 Click **Initialize**.



If the entire device policy is set for removable media encryption, you are prompted if the existing data should be moved to the protected area. If you choose to move existing data to the protected area, the amount of available space on the system root drive is calculated. If there is enough space, the initialization process is initiated. If there is not enough space, a pop-up message appears indicating the free and required amounts of space on the system root drive. Remove files from the system root drive to free up space, then click **Retry**. The message continues to appear until enough space is found on the system root drive. We recommend that you do not unplug the device during initialization or cancel the initialization process. This might result in a device in an unknown state.

## Recover removable media

You can recover access to the information on removable media using a recovery key, recovery password, or recovery certificate.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.
- 2 On the left pane, click **Recover media**.
- 3 Select one of these required recovery methods:
  - **Recovery key** — This method requires the recovery key used during initialization to be available on the system in order to configure the recovery of the device.
  - **Recovery password** — This recovery method requires the recovery password given during initialization in order to configure the recovery of the device. Also, you can perform this recovery from a non-FRP client.
  - **Recovery certificate** — This option requires the digital certificate key used during initialization to be available on the system in order to configure the recovery of the device.  
You can also perform this recovery from a non-FRP client, where the same certificate should be either available or imported.
- 4 Click **Recover**.

## Change the removable media authentication details

You can change the protection mechanism for removable media from password to certificate, or vice versa.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.
- 2 In the left pane under **Removable Media**, click **Change authentication**.
- 3 Click **Change**, then select the token type with which you want to authenticate the device.  
The available token types depend on the relevant policy configuration.
  - If the device is password-protected, authenticate the device using the existing password. When the device is successfully authenticated, enter and confirm the new authentication credentials.
  - If the device is protected by a certificate, the device is authenticated using the certificate installed on the client system. When the device is successfully authenticated, enter and confirm the new authentication credentials.
- 4 Click **OK**, then click **Close**.

---

## Managing CD/DVD/ISO media

The McAfee Encryption for CD/DVD/ISO feature enables securely encrypted data to be written to optical media or ISO images.



Individual files up to 4 GB in size can be placed on an encrypted CD/DVD or ISO image.

Although FRP allows the writing of encrypted files to optical media with the **Enforce Encryption (onsite access only)** protection level, subsequent use of these optical media is then restricted to FRP-enabled systems. Using the McAfee Encryption for CD/DVD/ISO feature allows the creation of media that can be securely authenticated and accessed by any system with a supported Windows OS, without the need for the FRP client to be present. This is allowed by both the **Allow Encryption (with offsite access)** and **Enforce Encryption (with offsite access)** protection levels, with the **Enforce Encryption (with offsite access)** protection level preventing writing to the optical media by an alternative method.

This feature can also be used to create secure encrypted ISO images of data, for subsequent burning to optical media or secure offsite back up. Once an ISO is created, it can be securely distributed and burned using any system that supports normal optical media burning.

For situations where a repeatable encrypted backup of a defined set of data that might change between backups is needed (for instance, source code folders, transaction records and so on), a project can be defined identifying the files/folders to be backed up, which can be saved to disk as an .emo file. The .emo file can then be loaded and run later to create the image, whenever required.

This project file mechanism allows you to create a sophisticated mapping between the source data and the eventual target media layout. This is flexible enough to allow reorganizing of the target file/ folder layout, addition of new folders, renaming of target files/folders, and so on, so that the eventual encrypted media image can be structured as required.

When the encrypted CD/DVD is inserted into a system or the encrypted ISO is mounted on a system where FRP is not installed, you are prompted for credentials to gain access to the CD/DVD/ISO media. Successful authentication enables access to the data using the offsite Explorer.

## Writing McAfee Encrypted CD/DVD/ISO

The process of writing an encrypted CD/DVD/ISO is performed in a number of stages, based on the selected parameters.

### Creating encrypted image

This stage creates a temporary encrypted image of the selected files and folders. This is done in the temporary directory of the system as defined by Windows. The availability of sufficient disc space is verified before image creation.

If files could not be added to the encrypted image, an informational dialog box appears after this stage, indicating how many files were added and skipped. These are the possible reasons for skipped files:

- Source files not available at time of image creation
- Source files not accessible due to wrong access rights
- Source files are FRP encrypted, but key not available at time of creation

### Writing out ISO image

This stage writes the temporary image to an ISO file at the selected location. If this location is a local disc, attempts are made to make sure that enough space is available. However, for mapped drive locations, this check is not performed and available space is assumed.

### Burning disc <x> of <y>

This stage appears for each physical copy requested. The sub-stages within this stage include:

- 1 Waiting for blank <media> or larger (<media> will be the **Media Type** specified earlier)
- 2 Burning encrypted image
- 3 Finalizing media
- 4 Verifying media (optional sub-stage depending on options selected)

At the end of the process (or after a cancellation from a user), an informational dialog box displays the status of the operation. At this point, all temporary files are deleted on the system and the user is returned to the main application.

## Working with McAfee Encryption for CD/DVD/ISO projects

When working with McAfee Encryption for CD/DVD/ISO, it is possible to create, save, and open project files with the .emo extension. These files contain the metadata detailing files and folders to be included in the encrypted media image to be created.

### Project rescan

When an .emo project file is opened (either from within the application or by double-clicking on the file itself to launch the application), a rescan operation is carried out.

If any of the files or folders specified in the project are not available at the defined source location, a dialog box prompts you to either delete the missing files/folders from the project, or keep them in the project, in which case they appear in red in the project view (and are not added to a subsequent encrypted media image unless available at media creation time).

If any new files or folders are found in source folders already included in the project, a dialog box prompts the user to either add the new files or folders to the project, or ignore them.

The rescan behavior can be instigated at any time by right-clicking the project file and selecting rescan from the context menu. The rescan occurs from the currently selected item of the tree view. To do a full rescan, select of the root of the tree view.

Once a project has been created or opened successfully, an estimate of the size of the resultant media is shown, along with a description of the physical media that can be burned to.

## Select files and folders to encrypt to a CD/DVD/ISO

You can select the required files and folders to encrypt to a CD/DVD/ISO using the **McAfee Removable Media Protection - CD/DVD/ISO** page.

### Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | File and Removable Media Protection** to open the client console.
- 2 In the left pane, click **Create CD/DVD/ISO Media** under **CD/DVD/ISO Media** to open the **McAfee Removable Media Protection - CD/DVD/ISO** page.



The **McAfee Removable Media Protection - CD/DVD/ISO** page can also be launched in two other ways:

- From the Windows Explorer pane, select the required files/folders, then right-click and select **McAfee File and Removable Media Protection | Add to Encrypted CD/DVD**.
- Locate a previously saved project file with the .emo extension, then double-click the file to open the **McAfee Removable Media Protection - CD/DVD/ISO** page.

- 3 Drag and drop the required files and folders from the **Folders** pane to the **Project File** pane. The **Image Properties** pane shows the appropriate total media size required for the selected files and folders.



You can delete the selected files and folders from the **Project File** pane using the delete option. You can save or load a project file describing the image contents from the **File** menu or the toolbar.

- 4 Click **Next** to open the **Create McAfee Encrypted CD/DVD/ISO** dialog box.

## Create McAfee Encrypted CD/DVD

You can burn the selected files and folders to the inserted CD or DVD for secure authentication and access to the data.

### Task

- 1 Open the **Create McAfee Encrypted CD/DVD/ISO** page.
- 2 In the **Disk Title** field, type the name to be assigned to the media, which is displayed when the media is inserted, following the ISO 9660 conventions:
  - Maximum 15 characters
  - Uppercase A to Z, numbers 0 to 9, and underscore symbol only
- 3 In the **Burn device** field, select the appropriate media device from the list. The available options include any suitable burner devices identified on the system as well as the **Create ISO image** option. For each device selected, a list of media sizes that is supported appears.

- 4 In the **Media Type** field, the smallest media to which the data should be written to is specified. This media must always be at least as large as the smallest suitable media type estimated.



This refers to the type of media, not the specific format of media. For instance, CD-RW and CD-R are considered to be of type CD.

- 5 In the **Copies** field, you can specify multiple (up to 10) copies of the same data.
- 6 Select the **Verify** checkbox to confirm the disc burning.
- 7 In the **Password** field, type the required password that will be used to authenticate to the resultant media.  
The password must conform to the rules defined in the FRP password policy applied to the system.
- 8 In the **Confirm** field, type the same password again.
- 9 Click **Burn CD/DVD** to write the required files and folders to the inserted disc.

The **Write McAfee Encrypted CD/DVD/ISO** page appears.

## Create McAfee Encrypted ISO image

You can create a securely encrypted ISO image that when burned to a disc or mounted using a third-party tool allows secure authentication and access to the data.

### Task

- 1 Open the **Create McAfee Encrypted CD/DVD/ISO** page.
- 2 In the **Disk Title** field, type the name to be used for the ISO image (.iso) file, following the ISO 9660 conventions:
  - Maximum 15 characters
  - Uppercase A to Z, numbers 0 to 9, and underscore symbol only
- 3 In the **Burn device** field, select **Create ISO Image**.
- 4 In the **Destination** field, enter the full path or click **Browse** to select the required destination folder for the ISO image, then click **OK**.
- 5 In the **Password** field, type the required password that will be used to authenticate to the resultant media.  
The password must conform to the rules defined in the FRP password policy applied to the system.
- 6 In the **Confirm** field, type the same password again.
- 7 Click **Create ISO** to create an .iso file of the selected files and folders to the local system.

The **Write McAfee Encrypted CD/DVD/ISO** page appears.

# 3

## Managing encryption and decryption of files and folders

The FRP context menu provides easy access to FRP options for files and folders.

When you right-click a file or folder, the context menu appears and displays the options enabled by your administrator, according to your company's security policies. The same options are available for files and folders.

### Contents

- ▶ *Encrypt a file or a folder*
- ▶ *Decrypt a file or a folder*
- ▶ *Search for encrypted files or folders*
- ▶ *Create a self-extractor*
- ▶ *Attach a self-extractor to an email*
- ▶ *Add files and folders to encrypt to a CD/DVD/ISO*
- ▶ *Attach an encrypted file to an email*

---

## Encrypt a file or a folder

You can manually encrypt a file or folder to prevent unauthorized access to its contents. This is particularly important for confidential information. You do this using the **Encrypt** option on the context menu, or from **Encryption** tab of the file or folder's **Properties** dialog box.

### Before you begin

Make sure that the file you want to encrypt is not being used by any application.

### Task

- 1 Right-click the file or the folder to be encrypted, then select **McAfee File and Removable Media Protection | Encrypt**. The **Select key** dialog box appears.



This option is not available if the folder has been encrypted by a policy defined by an administrator.

- 2 Select the key you want to use to encrypt the file, then click **OK**.



Click **Details** to view additional information about the selected key.

Depending on the policy settings, a padlock appears on the file or folder, indicating that it is encrypted with the selected key.

---

## Decrypt a file or a folder

You can decrypt an encrypted file using the **Decrypt** option on the context menu, or from the **Encryption** tab of the file or folder's **Properties** dialog box.

### Before you begin

Make sure that the file you want to decrypt is not being used by any application.

### Task

- To decrypt a file or a folder:
  - Right-click the file or the folder, then select **McAfee File and Removable Media Protection | Decrypt**.



This option is not available if the file or folder has been encrypted by a policy defined by an administrator.

- Right-click the file or the folder, then select **Properties**. On the **Encryption** tab, select **<plaintext>** as **Key name**, then click **Apply**.

File decryption and folder decryption might require authentication if the encryption key needed for the decryption is not available.

---

## Search for encrypted files or folders

The **Search encrypted** option on the context menu enables you to search for encrypted files and folders in a specified location.

### Task

- 1 Right-click on the folder, then select **McAfee File and Removable Media Protection | Search encrypted**. The **Search: encrypted files and folders** dialog box appears.
- 2 Select if you want to search for files and folders, and for the keys that are used to encrypt the files or folders.
- 3 Browse to specify the folder path, then select **Include sub-folders** to search subfolders for encrypted files or folders.
- 4 Click **Search**.

After the search is complete, objects that match the search criteria are listed. You can select objects and perform actions on them.

---

## Create a self-extractor

*Self-extractors* are password-encrypted executable files that can also be decrypted on systems that are not running FRP. The password used to create the self-extractor is required to read it.

You can change the name of the self-extractor. By default, its name is the same as the source file or folder with the `*.exe` extension.

### Task

- 1 Right-click the file or folder that you want to create a self-extractor for, then select **McAfee File and Removable Media Protection | Create Self-Extractor (<filename>.exe)**. The **Package and encrypt** dialog box appears.
- 2 Enter the password you want to use to encrypt the self-extractor, then click **OK**.
  - The source file or folder remains intact on disk; only a copy of the file or folder is converted into a self-extractor.
  - You can also specify where to save the self-extractor. The default location is the same as the source file or folder location.

## Read a self-extractor

You can read self-extractors on any client system running Windows XP SP3 or later. You can also read self-extractors on a non-FRP client, as long as you have the rights to run an executable file.

Make sure that you have the password that was used to create the file. (The creator of this file must share the password with the recipient of the file in a secure manner.)

### Task

- 1 Double-click the self-extractor and provide the password used to create the file.

The content of the self-extractor automatically opens in the associated application.



The content is not automatically saved to disk. When you close the application that opened the unpacked self-extractor content, the unpacked content is removed from the disk.

- 2 To save the self-extractor content to disk, click **Advanced**, then select **Extract** and specify the location.

---

## Attach a self-extractor to an email

You can attach a file or a folder as a self-extractor to an email.

The self-extractor is packaged into a \*.cab file, which can be attached to an email. You can attach a file or a folder as a self-extractor using any email program.



Email messages sent with a \*.cab self-extractor attachment might be blocked by a recipient's virus protection program.

### Task

- 1 Right-click the file or folder where you want to create a self-extractor, then select **McAfee File and Removable Media Protection | Attach as Self-Extractor to E-mail**. The **Package and encrypt** dialog box appears.
- 2 Enter the password you want to use to encrypt the self-extractor, then click **OK**.

The source file or folder remains intact on disk; only a copy is converted into a self-extractor and attached to an email.

---

## Add files and folders to encrypt to a CD/DVD/ISO

You can select the required files and folders to encrypt to a CD/DVD/ISO using the **Add to encrypted CD/DVD** option on the context menu. This option allows securely encrypted data to be written to optical media or ISO images.

For details on how to select files and folders to encrypt to a CD/DVD/ISO, see *Select files and folders to a CD/DVD/ISO*.

---

## Attach an encrypted file to an email

You can send a file (plain text or encrypted) in a protected way. The recipient must have FRP installed and must have access to the encryption key.

If you attach an encrypted file to an email without using **Attach encrypted to E-mail**, the file is attached as plain text even if the file is encrypted on disk. The source file is still encrypted, but the copy attached to the email is sent to the recipient in plaintext (unprotected).



You can attach self-extractor files up to 10 MB in size.

### Task

- 1 Right-click the file, then select **McAfee File and Removable Media Protection | Attach encrypted to E-mail**. The **Select protection keys** dialog box appears.
- 2 Select the key you want to encrypt the file with, then click **OK**. A \*.sba file is attached to the email.

# Index

## A

- about this guide [5](#)
- attachments [23](#)
- authentication method
  - user local keys [14](#)
- authentication recovery [16](#)

## C

- CD/DVD
  - burn [18](#)
  - create encrypted [19](#)
- CD/DVD/ISO
  - encryption [18](#)
  - managing [17](#)
  - select files for encryption [19](#)
- certificate, recovery [16](#)
- context menu options [21](#)
- conventions and icons used in this guide [5](#)

## D

- decryption, files or folders [22](#)
- documentation
  - audience for this guide [5](#)
  - product-specific, finding [6](#)
  - typographical conventions and icons [5](#)

## E

- encrypted files
  - attach [24](#)
- encryption
  - CD/DVD [19](#)
  - CD/DVD/ISO [18](#), [19](#)
  - files or folders [21](#)
  - ISO [20](#)
- encryption, persistent [7](#)

## F

- features [8](#)
- files
  - attach as self-extractor [23](#)
  - attach encrypted [24](#)
  - decrypt [22](#)

- files (*continued*)
  - encrypt [21](#)
  - encrypted, search for [22](#)
- folders
  - attach as self-extractor [23](#)
  - decrypt [22](#)
  - encrypt [21](#)
  - encrypted, search for [22](#)
- FRP
  - console, launching [9](#)
  - context menu options [21](#)
- FRP client [7](#)

## I

- image
  - create encrypted [18](#)
  - properties [19](#)
- initialization, removable media [15](#)
- ISO
  - create encrypted image [20](#)
- ISO image [18](#)

## K

- key storage [11](#)
- keys, user local
  - creating [11](#)
  - deleting [12](#)
  - exporting [13](#)
  - importing [13](#)

## M

- McAfee ServicePortal, accessing [6](#)

## P

- password protection [14](#)
- persistent encryption [7](#)
- project rescan [18](#)
- protection, change mechanism
  - removable media [17](#)
  - user local key [14](#)

**R**

- recovery methods [16](#)
- removable media
  - authentication details [17](#)
  - authentication method [15](#)
  - initialize [15](#)
  - protected area [15](#)
  - recover [16](#)
  - update protection mechanism [17](#)

**S**

- self-extractors
  - attach [23](#)
  - create [22](#)
  - read [23](#)
- ServicePortal, finding product documentation [6](#)
- status report [9](#)

**T**

- technical support, finding product information [6](#)

**U**

- user local keys
  - about [11](#)
  - changing authentication method [14](#)
  - creating [11](#)
  - deleting [12](#)
  - exporting [13](#)
  - importing [13](#)
  - password protection [14](#)
  - recovering [14](#)
  - renaming [12](#)
  - storage [11](#)

