



User Guide

McAfee Endpoint Encryption for Files and Folders 4.1

For use with ePolicy Orchestrator 4.6 Software

COPYRIGHT

Copyright © 2012 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS

McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq 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.

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 MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

	Preface	5
	About this guide	5
	Audience	5
	Conventions	5
	Find product documentation	6
1	Introduction	7
	Purpose of EEFF	7
	How EEFF works	7
	Features	8
2	Using the EEFF console	9
	Launch the EEFF console	9
	Managing Endpoint Encryption for Removable Media	10
	Initialize Removable Media	10
	Recover Removable Media	11
	Update the EERM authentication details	12
	Managing User Local keys	12
	User Local keys	12
	Create a User Local key	13
	Delete a User Local key	13
	Rename a User Local key	14
	Export User Local keys	14
	Import User Local keys	15
	Recover User Local keys	15
	Change User Local key authentication method	15
3	Using the context menu	17
	Encrypt a file or a folder	17
	Decrypt a file or a folder	18
	Search for encrypted files or folders	18
	Create a self-extractor	18
	Read a self-extractor	19
	Attach a self-extractor to an email	19
	Attach an encrypted file	20
	Index	21

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.

*Book title, term,
emphasis*

Title of a book, chapter, or topic; a new term; emphasis.

Bold

Text that is strongly emphasized.

User input, code,
message

Commands and other text that the user types; a code sample; a displayed message.

Interface text

Words from the product interface like options, menus, buttons, and dialog boxes.

Hypertext blue

A link to a topic or to an external website.



Note: Additional information, like an alternate method of accessing an option.



Tip: Suggestions and recommendations.



Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.



Warning: Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

- 1 Go to the McAfee Technical Support ServicePortal at <http://mysupport.mcafee.com>.
- 2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	<ol style="list-style-type: none">1 Click Product Documentation.2 Select a product, then select a version.3 Select a product document.
KnowledgeBase	<ul style="list-style-type: none">• Click Search the KnowledgeBase for answers to your product questions.• Click Browse the KnowledgeBase for articles listed by product and version.

1

Introduction

McAfee® Endpoint Encryption for Files and Folders™ (EEFF) uses powerful encryption technology to allow you to protect information from access by unauthorized users. Your data is stored, managed, archived, and distributed as any other file is, however, it can be viewed only by those who have been granted access.

Contents

- *Purpose of EEFF*
- *How EEFF works*
- *Features*

Purpose of EEFF

EEFF enables you to define and protect your data so that only certain users can access it. This data is stored, managed, archived, and distributed, and can be viewed only by authorized users. This protection depends on Microsoft Windows user accounts and works in real-time to authenticate the user, to access the encryption keys, and to retrieve the correct policy in EEFF. A smart card implementation based on Windows logon provides for enhanced security.

How EEFF works

EEFF encrypts files and folders as per the policies assigned to users. These policies are enforced by the McAfee ePO server.

EEFF acts as a Persistent Encryption engine. When a file is encrypted and is moved or copied to another location, it remains encrypted. If it is moved out of an encrypted directory, it still remains encrypted.

Integrated with McAfee® ePolicy Orchestrator® (McAfee ePO™), EEFF provides a single point of control over the data on all systems, and supports both user and system-based policies. EEFF depends on Microsoft Windows credentials, thus both registered domain users and local system users can be assigned encryption policies and associated keys. Assigning these policies to users encrypts the data on the client. User-based policy assignments can be assigned only to registered domain users.

The EEFF client is installed on the managed system, then the system synchronizes with the McAfee ePO server and acquires the user data. EEFF then assigns encryption policies and keys to the user.

EEFF client acts like a filter between the application creating or editing the files and the storage media. When a file is saved, the EEFF filter executes the assigned encryption policies and encrypts the data, if applicable.

When a user attempts to deviate from the assigned encryption policy by stopping the main EEFF process (`MfeffCore.exe`) on the client system, the process is automatically regenerated. The automatic restart cannot be disabled. If the user manages to stop the main EEFF process on the client system, EEFF encrypts folders and files according to the policies assigned to the user. These policies are enforced by the McAfee ePO server.

When a file that is encrypted with key A is moved to a folder where the files encrypted with key B are available, the file that is encrypted with key A is instantly re-encrypted with key B. This process is known as *follow-target-encryption*; it requires that the user or process transferring the file have access to both key A and key B.

Features

These are the key features of EEFF.

- **Centralized management** — Provides support for deploying and managing EEFF using McAfee ePO software 4.6 (minimum Patch 2).
- **Windows authentication-based policy enforcement** — Assigns encryption policies and keys to Windows user accounts.
- **Integration with the McAfee tray icon** — Consolidates the tray icons into one common McAfee icon.
- **User Personal Key** — Allows users to have individual encryption keys that are generated from the McAfee ePO server, which the administrator can assign to policies to enable encryption.
- **Protect data on removable media** — Removable media encryption, including the ability to access encrypted content in systems where EEFF 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 EEFF is not installed.
- **Migration from EEFF v3.x to EEFF 4.1.0** — Migrating encryption keys from the previous version of the product to the current version, by importing them into the McAfee ePO server.

2


Using the EEFF console

The EEFF console enables you to manage your User Local Keys and the encryption of removable media.

Contents

- ▶ *Launch the EEFF console*
- ▶ *Managing Endpoint Encryption for Removable Media*
- ▶ *Managing User Local keys*

Launch the EEFF console

You can launch the EEFF console by clicking the McAfee icon  on your taskbar and selecting **Manage Features | Endpoint Encryption for Files and Folders**.

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 removable media.

Status Report

Status Report is the default screen that appears when you launch the EEFF console, and it displays this information:

- Operating system running on the client system
- EEFF installation files
- Encryption keys available to the user or the system
- General policies 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

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 EEFF console. Your administrator controls the availability of these options, according to your company's security policies.

See *Managing User Local Keys* for details.

Removable Media

McAfee Endpoint Encryption for Removable Media (EERM) is a software solution that encrypts removable devices to protect data stored in the device. Your administrator controls the availability of this solution on the console, according to your company's security policies.

See *Managing Endpoint Encryption for Removable Media* for details.

Managing Endpoint Encryption for Removable Media

McAfee Endpoint Encryption for Removable Media (EERM) is a software solution that encrypts removable devices to protect data stored in the device. Any attached removable storage can be protected with EERM, except for CDs/DVDs, and floppy disks.


Contents

- ▶ [Initialize Removable Media](#)
- ▶ [Recover Removable Media](#)
- ▶ [Update the EERM authentication details](#)

Initialize Removable Media

When you insert a non-protected removable device on a client with EEFF installed and the policy for removable media is enabled, you are prompted to initialize the device. You can also initiate initialization of the removable media using **McAfee Endpoint Encryption for Files and Folders** client console.

Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | Endpoint Encryption for Files and Folders**. The **Endpoint Encryption for Files and Folders** client console appears.
- 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 enforced on the system or user.

- 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.

- 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, meaning that it cannot be used on a machine with EEFF installed.

When the initialization is complete, an authentication dialog prompts you to authenticate to the device. Provide the authentication information to use the device.

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 | Endpoint Encryption for Files and Folders**. The **Endpoint Encryption for Files and Folders** client console appears.
- 2 On the left pane, click **Recover media**. The **Recover Authentication** window appears.
- 3 Select one of these required recovery methods:
 - **Recovery key** — This method uses a Recovery key from the central management system to configure the recovery of the device. You might be prompted to authenticate to EEFF to access this key and will not be able to change the Recovery key the administrator has selected.
 - **Recovery password** — This recovery method enables the user to select a Master Password (Recovery password). With this password you can recover the encrypted device without any interaction with the Helpdesk. Also, you can perform this recovery from a non-EEFF client.




The Recovery password must conform to the same password quality rules as your authentication password. The Recovery password cannot be set to the same password as the authentication password.

- **Recovery certificate** — This option enables the user to select a digital certificate to use for recovery. With the recovery certificate, you can recover the device without any interaction with the Helpdesk. You can also perform this recovery from a non-EEFF client, where the same certificate should be either available or imported.
- 4 Click **Recover**.

Update the EERM authentication details

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

Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | Endpoint Encryption for Files and Folders**. The **Endpoint Encryption for Files and Folders** client console appears.
- 2 In the left pane under **Removable Media**, click **Change authentication**.
- 3 Click **Change**.
- 4 Select the token type with which you want to authenticate the device.
 - If the device is password-protected, authenticate the device using the existing password. When the device is successfully authenticated, enter and confirm the new password, then click **OK**. A pop-up message indicates that the authentication method has been changed.
 - If the device is protected by a certificate, the device is authenticated using the certificate installed on the client system. Select the required certificate from the list of available certificates, then click **OK**. A pop-up message indicates that the authentication method has been changed.
- 5 Click **OK**, then click **Close**.

Managing User Local keys

User Local keys are the keys you create on your client for specific files and folders. User Local keys can be created and managed from the EEFF console. User Local keys are meant for the individual users and the system where they are created. Your administrator controls your ability to create and manage User Local keys, according to your company's security policies.

Contents

- [User Local keys](#)
- [Create a User Local key](#)
- [Delete a User Local key](#)
- [Rename a User Local key](#)
- [Export User Local keys](#)
- [Import User Local keys](#)
- [Recover User Local keys](#)
- [Change User Local key authentication method](#)

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 and client system where it is created.


Key storage

Encryption keys, including 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.

Task

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



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

- 5 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 Endpoint Encryption 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.

- 6 Click **Next**. The **Tasks** page appears, summarizing the key details configured in the wizard.
- 7 Click **Next**. You might be prompted to authenticate to Endpoint Encryption before completing the wizard to ensure access to the corporate recovery key that will be used when you create your key store.
- 8 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 | Endpoint Encryption for Files and Folders**. The EEFF client appears.
- 2 In the left pane, click **Delete key**. The **Welcome to the Delete Key** wizard appears.
- 3 Click **Next**. The **Select Key** page appears.
- 4 From the **Key name** drop-down list, select the required key, then click **Next**. The **Tasks** page appears summarizing the key details configured in the wizard.

- 5 Click **Next**.


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

- 6 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 | Endpoint Encryption for Files and Folders**. The EEFF client appears.
- 2 In the left pane, click **Rename key**. The **Welcome to the Rename Key Wizard** appears.
- 3 Click **Next**. The **Select Key** page appears.
- 4 From the **Key name** drop-down list, select the required key, then click **Next**. The **Data** page appears.
- 5 Type a new name for the key, then click **Next**. The **Tasks** page appears summarizing the key details configured in the wizard.
- 6 Click **Next**.


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

- 7 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 | Endpoint Encryption for Files and Folders**. The **Endpoint Encryption for Files and Folders** client console appears.
- 2 In the left pane, click **Export keys**. The **Welcome to the Export Key wizard** page appears.
- 3 Click **Next**. The **Select key** page appears.
- 4 Select the key, then browse to and select the destination file name and path where the key is to be exported.
- 5 Provide the password to be used to protect the exported key, then click **Next**.
- 6 When prompted, enter valid authentication information for the key store.
- 7 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 | Endpoint Encryption for Files and Folders**. The **Endpoint Encryption for Files and Folders** client console appears.
- 2 In the left pane, click **Import keys**. The **Welcome to the Import Key wizard** page appears.
- 3 Click **Next**. The **Path** page appears.
- 4 Browse to and select the exported keys (*.sks file), then click **Next**.
- 5 Select the volume and location where you want to insert the keys, then click **Next**.
- 6 When prompted for authentication for exported keys, enter a valid password, then click **OK**.
- 7 When prompted, enter valid authentication information for the key store, then click **OK**.
- 8 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 or your machine.


Task

- 1 Click the McAfee icon  on your taskbar, then select **Manage Features | Endpoint Encryption for Files and Folders**. The **Endpoint Encryption for Files and Folders** client console appears.
- 2 On the left pane, click **Recover keys**. The **Welcome to the Recover Key wizard** page appears.
- 3 Click **Next**. The **Volume** page appears.
- 4 From the drop-down menu, select the location where you saved the local key that needs to be recovered, then click **Next**. The **Password** page appears.
- 5 Enter and confirm a new password for the key store, then click **Next**. The **Tasks** page appears summarizing the key details configured in the wizard.
- 6 Click **Next**. You might be prompted to authenticate to Endpoint Encryption before completing the wizard to ensure access to the key store.
- 7 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 | Endpoint Encryption for Files and Folders**. The **Endpoint Encryption for Files and Folders** client console appears.
- 2 In the left pane, under the **Local Keys** section, click **Change authentication**. The **Change Token** wizard appears.
- 3 Click **Next**. The **Volume** page appears.

- 4 Select the location where you saved the local key, then click **Next**. The **Type** page appears.
- 5 Select the token type you want to authenticate the device with. The authentication method selected determines the page that appears:
 - If you selected **Password Protection**, the **Password** page appears. Enter and confirm the new password, then click **Next**. The **Tasks** page appears summarizing the key details configured in the wizard.
 - If you selected **Certificate Protection**, the **Certificate** page appears. Select a certificate from the list of available certificates, then click **Next**. The **Tasks** page appears summarizing the key details configured in the wizard.
- 6 Click **Next**. You might be prompted to authenticate to Endpoint Encryption before completing the wizard to ensure access to the key store.
- 7 Click **Finish**.

3

Using the context menu

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

When you right-click a file or a 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*
- ▶ *Attach an encrypted file*

Encrypt a file or a folder

You can manually encrypt a file or a 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.



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

Task

- 1 Right-click the file or the folder to be encrypted, then select **McAfee Endpoint Encryption | Encrypt**. The **Select key** dialog box appears.
- 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 to view its contents. You do this with 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.



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

Task

- To decrypt a file or a folder:
 - Right-click the file or the folder, then select **McAfee Endpoint Encryption | Decrypt**.
 - 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 Endpoint Encryption | 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 the files or folders are encrypted with.
- 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 EEEF. 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/folder with the *.exe extension.

Task

- 1 Right-click the file or the folder you want to create a self-extractor for, then select **McAfee Endpoint Encryption | 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/folder remains intact on disk; only a copy of the file/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/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-EEFF client, provided 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 Endpoint Encryption | Attach 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/folder remains intact on disk; only a copy of the file/folder is converted into a self-extractor and attached to an email.

Attach an encrypted file

You can send a file (plain text or encrypted) in a protected way. The recipient must have EEEF 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).



Email attachments of self-extractor files up to 10 MB in size are supported.

Task

- 1 Right-click the file, then select **McAfee Endpoint Encryption | 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 [19](#)
 - authentication method
 - User Local keys [15](#)
 - authentication recovery [11](#)
- C**
 - certificate, recovery [11](#)
 - context menu options [17](#)
 - conventions and icons used in this guide [5](#)
- D**
 - decryption, files or folders [18](#)
 - documentation
 - audience for this guide [5](#)
 - product-specific, finding [6](#)
 - typographical conventions and icons [5](#)
- E**
 - EEFF
 - client [7](#)
 - console, launching [9](#)
 - context menu options [17](#)
 - features [8](#)
 - how it works [7](#)
 - purpose [7](#)
 - encrypted files
 - attach [20](#)
 - encryption
 - files or folders [17](#)
 - encryption, persistent [7](#)
- F**
 - files
 - attach as self-extractor [19](#)
 - attach encrypted [20](#)
 - decrypt [18](#)
 - encrypt [17](#)
 - encrypted, search for [18](#)
 - folders
 - attach as self-extractor [19](#)
- folders (*continued*)
 - decrypt [18](#)
 - encrypt [17](#)
 - encrypted, search for [18](#)
- I**
 - initialization, removable media [10](#)
- K**
 - key storage [12](#)
 - keys, User Local
 - create [13](#)
 - export [14](#)
 - import [15](#)
 - keys, User Local,
 - delete [13](#)
- M**
 - McAfee ServicePortal, accessing [6](#)
- P**
 - password protection [15](#)
 - persistent encryption [7](#)
 - protection, change mechanism
 - EERM [12](#)
 - User Local key [15](#)
- R**
 - recovery methods [11](#)
 - removable media
 - authentication details [12](#)
 - authentication method [10](#)
 - initialize [10](#)
 - protected area [10](#)
 - recover [11](#)
 - update protection mechanism [12](#)
- S**
 - self-extractors
 - attach [19](#)
 - create [18](#)

self-extractors (*continued*)

read [19](#)

ServicePortal, finding product documentation [6](#)

status report [9](#)

T

Technical Support, finding product information [6](#)

U

User Local keys

about [12](#)

User Local keys (*continued*)

change authentication method [15](#)

create [13](#)

delete [13](#)

export [14](#)

import [15](#)

password protection [15](#)

recover [15](#)

rename [14](#)

storage [12](#)

