Product Guide

McAfee Endpoint Encryption for Files and Folders 4.2
For use with ePolicy Orchestrator 4.6 Software
COPYRIGHT
Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee CleanBoot, 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 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

Preface 5
About this guide .................................. 5
Audience .................................. 5
Conventions ................................. 5
Find product documentation .................. 6

1 Introduction 7
EEFF and data protection ......................... 7
How EEFF works .................................. 7
Features ...................................... 8

2 Installing the EEFF client 9
Requirements .................................... 9
Check in the EEFF software package ............... 10
Install the EEFF extension ...................... 11
Install the Help extension ...................... 11
Register Windows Active Directory .............. 11
Deploy EEFF to managed systems ................. 12

3 Configuring EEFF policies 15
EEFF policy settings ............................. 16
General .................................. 16
Folder encryption ................................ 16
File encryption ................................ 16
Removable media ............................... 18
CD/DVD encryption ............................ 20
Encryption options .............................. 21
Grant keys ................................. 22
Network .................................. 22
User local keys ............................... 23
Password rules ................................ 23
Create a policy ................. 24
Edit the EEFF policy settings .......... 24
Assign a policy to a managed system .......... 25
Assign a policy to a system group .......... 25
Enforce EEFF policies on a system .......... 26
Enforce EEFF policies on a system group ...... 26
How policy assignment rules work .......... 27
Policy assignment rule priority .......... 27
Working with policy assignment rules ...... 28
How multi-slot policies work .......... 28
Assign multiple instances of Grant Key policy through the System Tree ........ 28
Assigning Grant Key policy through policy assignment rules ...... 29
View the policies assigned to systems ...... 30
View the policies assigned to users .......... 30
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


2  Under Self Service, access the type of information you need:

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User documentation</td>
<td>1  Click Product Documentation.</td>
</tr>
<tr>
<td></td>
<td>2  Select a product, then select a version.</td>
</tr>
<tr>
<td></td>
<td>3  Select a product document.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>•  Click Search the KnowledgeBase for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>•  Click Browse the KnowledgeBase for articles listed by product and version.</td>
</tr>
</tbody>
</table>
EEFF and data protection

EEFF enables you to 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, it remains encrypted even when:
- The file is moved or copied to another location
- The file is moved out of an encrypted directory

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, so 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.

When the EEFF client is installed on the managed system, the system synchronizes with the McAfee ePO server and fetches the encryption keys and product policies. 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.
When a file that is encrypted with key A is moved to a folder where the files are encrypted with key B, 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.
- **Windows authentication-based policy enforcement** — Assigns encryption policies and keys to Windows user accounts.
- **User Personal Key** — Allows users to have unique encryption keys that are generated from the McAfee ePO server, which the administrator can assign to policies to enable encryption.
- **Delegated administration through role-based key management** — Enables the logical separation of key management between multiple administrators. This capability is critical for separation across business functions and subsidiaries. This functionality is available only to users of EEFF 4.2 with McAfee ePO 4.6, Patch 6.
- **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 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.
- **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 EEFF 4.2.0** — 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 EEFF client makes use of the McAfee Core Cryptographic Module (MCCM) User and Kernel FIPS 140-2 cryptographic modules. These cryptographic modules are being validated at FIPS 140-2 Level 1, and EEFF now 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.
Installing the EEFF client

The EEFF software packages and extensions must be checked into the McAfee ePO server before you can deploy the software and configure the policies.

The McAfee ePO server provides a scalable platform for centralized policy management and enforcement on the managed systems. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

This guide does not provide detailed information about installing or using McAfee ePO. For more details, refer to the ePolicy Orchestrator product documentation.

Contents

- Requirements
- Check in the EEFF software package
- Install the EEFF extension
- Install the Help extension
- Register Windows Active Directory
- Deploy EEFF to managed systems

Requirements

Make sure that your client and server systems meet these requirements.

Table 2-1 System requirements

<table>
<thead>
<tr>
<th>Systems</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO server systems</td>
<td>See the McAfee ePO product documentation.</td>
</tr>
<tr>
<td>Client systems</td>
<td>• CPU: 1 GHz or faster</td>
</tr>
<tr>
<td></td>
<td>• RAM: 1 GB RAM (32-bit) or 2 GB RAM (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Hard disk: 50 MB minimum free disk space</td>
</tr>
<tr>
<td></td>
<td>• TCP/IP network connection</td>
</tr>
</tbody>
</table>
### Table 2-2 Software requirements

<table>
<thead>
<tr>
<th>Software (or package name)</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| McAfee management software | - McAfee ePolicy Orchestrator 4.6 (minimum Patch 2) for EEFF  
                            - McAfee ePolicy Orchestrator 4.6 (minimum Patch 6) for EEFF Role Based Key Management functionality  
                            - McAfee® Agent for Windows 4.6  
                            - Windows 8 systems require McAfee® Agent 4.6 Patch 1 or later.  
                            - McAfee® Agent for Windows 4.8 (minimum Patch 1) for EEFF Key Cache Expiry functionality |
| McAfee Endpoint Encryption for Files and Folders | - EEFF extension  
                                         - EEFF-extension-4.2.0_xxx.ZIP  
                                         - help_eeff_4.2.0.ZIP  
                                         - MfeEEFF_Client_4.2.0.x.ZIP |
| Microsoft Windows Installer 3.0  
Redistributable package (for McAfee ePO) | See the McAfee ePO product documentation. |
| Microsoft .NET Framework 2.0  
Redistributable package (for McAfee ePO) | See the McAfee ePO product documentation. |
| Microsoft MSXML 6 (for McAfee ePO) | See the McAfee ePO product documentation. |

### Table 2-3 Operating system requirements

<table>
<thead>
<tr>
<th>Systems</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO server systems</td>
<td>See the McAfee ePO product documentation.</td>
</tr>
</tbody>
</table>
| Client systems | - Microsoft Windows 8 (32-bit and 64-bit)  
                      - Microsoft Windows 7 (Professional, Ultimate, or Enterprise), SP 1 (32-bit and 64-bit)  
                      - Microsoft Windows Vista (Business, Ultimate, or Enterprise) SP 2 (32-bit only)  
                      - Microsoft Windows XP Professional, SP 3 (32-bit only) |

---

### Check in the EEFF software package

The software package must be checked in to the master repository on the McAfee ePO server so that you can deploy the software to the client system.

**Task**

For option definitions, click ? in the interface.

1. Copy the `MfeEEFF_Client_4.2.0.x.zip` file to a temporary location.
2. Log on to the McAfee ePO server as an administrator.
3  Click Menu | Software | Master Repository | Actions | Check In Package.

4  On the Package page, select the Package type as Product or Update (ZIP), click Browse to locate the MfeEEFF _Client_4.2.0.x.zip file, then click Next.

5  On the Package Options page, click Save.

## Install the EEFF extension

You must install the EEFF extension into the repository on the McAfee ePO server before you can define and enforce product policies.

**Task**

1. Copy the EEFF-extension-4.2.0_xxx.zip file to a temporary location.

2. Log on to the McAfee ePO server as an administrator.

3. Click Menu | Software | Extensions | Install Extension.

4. Click Browse to locate the EEFF-extension-4.2.0_xxx file, then click OK. The Install Extension page displays the extension name and version details.

5. Click OK.

## Install the Help extension

You can install the Help extension on the McAfee ePO server using the Software tab. The Help extension is a .ZIP file.

**Task**

For option definitions, click ? in the interface.

1. Log on to the McAfee ePO server as an administrator.

2. Click Menu | Software | Extensions | Install Extension.

3. Click Browse to locate the help_eeff_4.2.0.zip file, then click OK.

4. Click OK.

## Register Windows Active Directory

You must register Windows Active Directory with your ePolicy Orchestrator server to permit dynamically assigned permission sets for Windows users.

Dynamically assigned permission sets are assigned to users based on their Active Directory group memberships.

You must have a registered LDAP server to use Policy Assignment Rules and to enable dynamically assigned permission sets.
Task
For option definitions, click ? in the interface.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Configuration | Registered Servers | New Server.

3 On the Description page, from the Server type drop-down list, select LDAP Server, specify a unique user-friendly name and any details, then click Next to open the Details page.

4 Select Active Directory from LDAP server type, then enter the Domain name or the Server name.

   Use a DNS-style domain name. Make sure that the McAfee ePO system is configured with the appropriate DNS setting and can resolve the DNS-style domain name of the Active Directory. The server name is the name or IP address of the system where the Windows Active Directory is present.

5 Enter the User name.

   The user name should be in the format: domain\Username for Active Directory accounts.

6 Enter the Password and confirm it.

7 Click Test Connection to verify that the connection to the server works, then click Save.

Deploy EEFF to managed systems
You can use McAfee ePO to create tasks to deploy EEFF to a single system, or to groups in the System Tree.

Task
For option definitions, click ? in the interface.

1 Click Menu | Policy | Client Task Catalog | Client Task Types | McAfee Agent | Product Deployment | Actions | New Task.

2 Set these options for the new task:
   a Make sure that Product Deployment is selected, then click OK.
   b In the Name field, enter the name for the task.
   c From the Target Platforms drop-down list, select Windows.
   d From the Products and components drop-down list, select McAfee Endpoint Encryption for Files and Folders.
   e As the Action, select Install.
   f Select an appropriate Language.
   g (Optional) To deploy EEFF in FIPS mode, in the Command line field, enter FIPS.
   h Next to Options, specify if you want to run this task for every policy enforcement process (Windows only).

3 Click Save.

4 Click Menu | Systems | System Tree | Assigned Client Tasks, then select the required group in the System Tree.
5 Select the Preset filter as Product Deployment (McAfee Agent). Each assigned client task per selected category appears in the details pane.

6 Click Actions | New Client Task Assignment.

7 Set these options:
   a On the Select Task page, select McAfee Agent as Product and Product Deployment as Task Type, then select the task you created for deploying the product.
   b Next to Tags, select the appropriate option, then click Next:
      • Send this task to all computers
      • Send this task to only computers that have the following criteria — Use one of the edit links to configure the criteria.
   c On the Schedule page, select whether the schedule is enabled, specify the schedule details, then click Next.

8 Review the summary, then click Save.

At the next agent-server communication, the task runs and EEFF is deployed on the managed systems.
Configuring EEFF policies

A policy is a collection of settings that you create, configure, and enforce. Policies make sure that the managed security software products are configured and perform correctly.

The McAfee ePO console enables you to configure policy settings for all products and systems from a central location.

- For each managed product or component, you can choose whether the agent enforces all or none of its policy selections.
- You can view policy assignments, where they are applied, and if they are enforced.
- You can also lock policy enforcement to prevent changes to enforcement.

Refer to the McAfee ePolicy Orchestrator product documentation for details on policy management.

Contents
- EEFF policy settings
  - Create a policy
  - Edit the EEFF policy settings
  - Assign a policy to a managed system
  - Assign a policy to a system group
  - Enforce EEFF policies on a system
  - Enforce EEFF policies on a system group
  - How policy assignment rules work
  - How multi-slot policies work
EEFF policy settings

Policy settings for EEFF are grouped under different categories. Each policy category refers to a specific subset of policy settings. Policies are created and displayed by product and category.

**General**

You can configure the general integration options for encrypting file and folders on the General EEFF policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explorer Integration</td>
<td>Specifies the Windows Explorer context menu options available to a user on the client system.</td>
</tr>
<tr>
<td></td>
<td>• Allow Explicit Encrypt — Enables the Encrypt option for client system users. Default value is disabled.</td>
</tr>
<tr>
<td></td>
<td>• Allow Explicit Decrypt — Enables the Decrypt option for client system users. Default value is disabled.</td>
</tr>
<tr>
<td></td>
<td>• Enable padlock icon visibility — Displays a padlock icon on encrypted objects. Default value is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Enable search encrypted – Enables Search encrypted option for client system users. Default value is disabled.</td>
</tr>
<tr>
<td></td>
<td>• Allow creation of Self-Extractors – Enables users to manually create encrypted self-extractors for files and folders. Self-extractors are password-protected executable files that can be decrypted on any Windows system. Default value is enabled. This policy also enables sending Self-Extractors as CAB file attachments from the context menu.</td>
</tr>
<tr>
<td>Email Integration</td>
<td>Specifies the Windows Explorer context menu options available to a user on the client system.</td>
</tr>
<tr>
<td></td>
<td>• Enable sending of encrypted email attachments – Enables managed system users to send encrypted email attachments to recipients in the form of SBA files. Default value is disabled.</td>
</tr>
</tbody>
</table>

**Folder encryption**

You can configure the folder encryption policy settings on the Folder Encryption policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Click Add to specify the folders to be encrypted.</td>
</tr>
<tr>
<td>Path</td>
<td>Specifies the path of the folder to be encrypted.</td>
</tr>
<tr>
<td></td>
<td>Specify the path of the folder by selecting from the list or typing it in the text box.</td>
</tr>
<tr>
<td></td>
<td>The folder can be local or on a network share.</td>
</tr>
<tr>
<td>Key</td>
<td>Specifies the encryption key to be assigned to the policy. Browse to select the key.</td>
</tr>
</tbody>
</table>

**File encryption**

You can configure the file encryption policy settings on the File Encryption policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Click Add to specify the process and the file extensions to be encrypted.</td>
</tr>
<tr>
<td>Process Name</td>
<td>Specifies the process name of the application that creates the files to be encrypted.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Extensions</td>
<td>Specifies the file extensions to be encrypted that are supported by the process. Multiple file extensions can be specified using a space, semi-colon, or colon as separators.</td>
</tr>
<tr>
<td>Key</td>
<td>Specifies the encryption key to be assigned to the policy. Browse to select the key.</td>
</tr>
</tbody>
</table>
Removable media
You can configure the policy settings for USB devices and floppy disks on the **Removable Media** policy page. The policy settings for removable media are organized according to media type.

**USB Media settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| USB Media Protection Level Enforce Encryption (onsite access only) | Specifies the methods used to encrypt a removable media.  
- **Allow Unprotected Access** — Does not encrypt files on removable media. Default value is disabled. When selected, context menu options are enabled on the client system.  
- **Allow Encryption (with offsite access)** — Allows securely encrypted data to be written to USB devices. Although part of the device may be left unencrypted, no further unencrypted data can be written to the device.  
This option allows the creation of media that can be securely authenticated and accessed by any system with a supported Windows operating system, without having to install the EEFF client. Individual files up to 4 GB in size can be placed on the removable media. |
| USB Media Protection Level Options | Specifies the options for the encryption of USB devices. The **All** tab displays the complete set of media protection options. To filter the list to view specific settings, select the corresponding tab.  
- **Protected Area** — Specifies options to configure the encrypted area on a removable media. (Applicable for **Allow Encryption (with offsite access)** and **Enforce Encryption (with offsite access)** protection levels only.)  
- **Entire device** — Encrypts the entire removable media.  
This option can be restricted based on device size by selecting **Except when device is greater than**, setting the maximum device size (in GB; default value is 64 GB), then specifying the required action:  
- **Do not encrypt** — Prevents encryption of a device that exceeds the specified size.  
- **User Managed** — Allows the user to determine the size of the encrypted container.  
- **User Managed** — Allows the user to determine the size of the encrypted container.  
- **Authentication Methods** — Specifies methods for user authentication (applicable for **Allow Encryption (with offsite access)** and **Enforce Encryption (with offsite access)** protection levels only):  
- **Password** — Enables the user to authenticate using a password. If you select this option, you are prompted to set the password.  

The availability of this section and the options it contains depends on the protection level.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>Enables the user to authenticate using a Windows certificate. If you select this option, you are prompted to attach a Windows certificate.</td>
</tr>
<tr>
<td>Either</td>
<td>Enables the user to authenticate using a password or a Windows certificate.</td>
</tr>
<tr>
<td>Recovery Methods</td>
<td>Specifies the methods used to recover the encrypted removable media. (Applicable for Allow Encryption (with offline access) and Enforce Encryption (with offline access) protection levels only.)</td>
</tr>
<tr>
<td>Recovery Key</td>
<td>Specifies the Regular or User Personal key that can be used to recover the encrypted removable media.</td>
</tr>
<tr>
<td>Recovery Password</td>
<td>Enables the user to specify a password during initialization that can be used to recover the encrypted removable media. Select Mandatory to require the user to specify a recovery password during initialization.</td>
</tr>
<tr>
<td>Recovery Certificate</td>
<td>Enables the user to attach a Windows certificate during initialization that can be used to recover the encrypted removable media. Select Mandatory to require the user to attach a certificate during initialization.</td>
</tr>
<tr>
<td>Customize UI Text displayed on Inserting Media</td>
<td>Specifies the message to be displayed to an end user upon inserting a removable media into an EEFF client with removal media encryption enabled. This text is customizable, and limited to 300 characters. If left blank, the default message is shown. (Applicable for Allow Encryption (with offline access) and Enforce Encryption (with offline access) protection levels only.)</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>The key to use to decrypt the removable media. This option is applicable only when Enforce Encryption (onsite access only) is selected.</td>
</tr>
<tr>
<td>Ignore existing content</td>
<td>Enter the encryption key or browse to and select the encryption key.</td>
</tr>
<tr>
<td>Exempted Device IDs</td>
<td>Specifies devices that should not be updated with changes in encryption policies. Exempted devices also exempted from explicit encryption and decryption.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds the ID of the device that will not be updated with the changes in encryption policies.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the device ID from the exemption list.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the ID of the device that will not be updated with the changes in encryption policies.</td>
</tr>
</tbody>
</table>

**Floppy Disk Media settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Floppy Disk Protection Level</td>
<td>Specifies the options for the protection of floppy disks.</td>
</tr>
<tr>
<td>Allow Unprotected Access</td>
<td>Does not encrypt files on floppy disks. Default value is enabled.</td>
</tr>
<tr>
<td>Block Write Operations</td>
<td>Prevents the copying of data onto a floppy disk.</td>
</tr>
</tbody>
</table>
CD/DVD encryption

You can configure the CD/DVD encryption settings on the CD/DVD Encryption options EEFF policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD/DVD Protection Level</td>
<td>• <strong>Allow Unprotected Access</strong> — Does not encrypt while burning files and folders to a CD or DVD.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Allow Encryption (with offsite access)</strong> — Allows securely encrypted data to be written to optical media or to ISO images. Individual files up to 4 GB in size can be placed on an encrypted CD/DVD.</td>
</tr>
<tr>
<td></td>
<td>This option allows the creation of media that can be securely authenticated and accessed by any system with a supported Windows operating system, without having to install the EEFF client.</td>
</tr>
<tr>
<td></td>
<td>The type of the optical media determines its capacity (ISO can be any size up to DVD-DL). Supported optical media: CD, DVD, and DVD-DL.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enforce Encryption (with offsite access)</strong> — Enforces the secure encryption of data written to optical media or to ISO images. Individual files up to 4 GB in size can be placed on an encrypted CD/DVD.</td>
</tr>
<tr>
<td></td>
<td>This option allows the creation of media that can be securely authenticated and accessed by any system with a supported Windows operating system, without having to install the EEFF client. At the same time, it disables the writing of files and folders to a CD or DVD using third-party software. Only McAfee Endpoint Encryption for CD/DVD/ISO can be used to write files and folders to CD/DVDs when this option is selected.</td>
</tr>
<tr>
<td></td>
<td>The type of the optical media determines its capacity (ISO can be any size up to DVD-DL). Supported optical media: CD, DVD, and DVD-DL.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enforce Encryption (onsite access only)</strong> — Encrypts files and folders while burning them to a CD or DVD with the selected key. The encrypted data is accessible only on systems with EEFF.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block Write Operations</strong> — Prevents the writing of any data to a CD or DVD.</td>
</tr>
<tr>
<td>CD/DVD Protection Options</td>
<td><strong>Encryption Key</strong> — Enter the encryption key or browse to and select the encryption key. This option is applicable only when <strong>Enforce Encryption (onsite access only)</strong> is selected.</td>
</tr>
</tbody>
</table>
## Encryption options

You can configure the options for encrypting file and folders on the Encryption Options policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encryption Options</strong></td>
<td></td>
</tr>
<tr>
<td>• Preserve file times</td>
<td>Does not change the file modified and accessed time on encryption or decryption. This is the default encryption option.</td>
</tr>
<tr>
<td>• Require authentication for listing of encrypted folders</td>
<td>Blocks unauthorized users from browsing encrypted folders. In an EEFF installed system, if the key used to encrypt a folder is not assigned to the user, then the user cannot view the content of that folder. If the key is assigned to the user, then the user can view the content of folders that is encrypted with that key.</td>
</tr>
<tr>
<td>• Use wiping when encrypting and deleting files</td>
<td>Uses a secure delete algorithm when encrypting files to ensure that no trace of the plaintext data remains on the client system. File wiping might slow down encrypted file operations due to the additional disk operations required.</td>
</tr>
<tr>
<td>• Enable limiting of the file size that will be encrypted</td>
<td>Encrypts only if the file size is less than the specified limit. Default value is 20 MB. This is applicable only if the folder is encrypted using Folder Encryption policy.</td>
</tr>
</tbody>
</table>

| Key Cache               |                                                                                                                                             |
| • Enable Key Cache expiry | When selected, enables the automatic removal of keys from the key cache if the client system fails to connect to the McAfee ePO server within the configured Key Cache expiry period. Status XML does not contain key information if the keys have been unloaded due to key cache expiry. |
| • Key Cache expiry period | Specifies the number of days after which a key is removed from the key cache when Enable Key Cache expiry is selected and the client system has not connected to the McAfee ePO server. Default value is 90 days. |

| I/O Utilization         |                                                                                                                                             |
| • Maximum I/O utilization | Specifies the percentage of I/O usage that EEFF processes can utilize during encryption. Default value is 50%. |

| Blocked Processes       |                                                                                                                                             |
| • Add                   | Adds the process to the block list to prevent the user running it to open or edit encrypted files.                                           |
| • Remove                | Removes the process from the block list to allow the user accessing edit encrypted files.                                                   |
| • Edit                  | Edits the process in the block list that is already an added process.                                                                       |
### Key Request Exclusions

Enables the process (such as anti-virus) to exclude encrypted files if it does not have access to the required encryption key.

- **Add** — Adds the process that is to be excluded.
- **Remove** — Removes the process from the exclusion list.
- **Edit** — Edits the process that is to be excluded.

All the keys assigned to the user through policy are unloaded every time the user logs off.

### File Extension Exclusions

Excludes the specified file extensions from encryption.

- **Add** — Adds the file extension that is to be excluded.
- **Remove** — Removes the file extension from the exclusion list.
- **Edit** — Edits file extension that is to be excluded.

### Grant keys

You can configure the keys that are granted on the Grant Keys policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Keys</td>
<td>Lists all active keys, including regular and user personal keys. If role-based key management is implemented, only keys assigned to the corresponding role are available.</td>
</tr>
<tr>
<td>Selected Keys</td>
<td>Specifies the keys that the policy grants when assigned to users.</td>
</tr>
</tbody>
</table>

### Network

You can configure the network encryption settings on the Network policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable network encryption</td>
<td>Enables encryption of files on network locations.</td>
</tr>
<tr>
<td>Enable network bandwidth limit</td>
<td>Limits the network bandwidth used by EEFF when encrypting files on network locations. Default value is 50 KB/sec.</td>
</tr>
<tr>
<td>Disable encryption on slow connections</td>
<td>Does not encrypt files on network locations if the network latency is above the specified limit. Default value is 500 msec.</td>
</tr>
<tr>
<td>Maximum clients allowed to encrypt folders</td>
<td>Specifies the maximum number of users who can simultaneously encrypt folders on a network.</td>
</tr>
</tbody>
</table>

This option is applicable only if the file is encrypted through policy enforcement.
User local keys

You can configure user local key settings on the User Local Keys Options policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user local keys</td>
<td>Allows users to create local keys on a client system using the EEFF client. These user local keys can be shared among users using the Export and Import options in the EEFF client.</td>
</tr>
<tr>
<td>Recovery Key</td>
<td>Specifies a Regular or a User Personal Key that can be used to recover user local keys.</td>
</tr>
<tr>
<td>Allow user local key generation</td>
<td>Allows users to create local keys on a client system using the EEFF client.</td>
</tr>
<tr>
<td>Allow export of user local keys</td>
<td>Allows users to export local keys from a client system using the EEFF client.</td>
</tr>
<tr>
<td>Allow import of user local keys</td>
<td>Allows users to import local keys to a client system using the EEFF client.</td>
</tr>
<tr>
<td>Allow deletion of user local keys</td>
<td>Allows users to delete local keys from a client system using the EEFF client.</td>
</tr>
<tr>
<td>Automatically create a user local key</td>
<td>Creates a default user local key when a new user logs on to the client system.</td>
</tr>
</tbody>
</table>

Password rules

You can define the required password length and complexity on the Password Rules policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Password complexity configuration for removable media, CD/DVD/ISO, self-extractors & User local keys | Defines the password policy rules for self-extractors, user local keys, CD/DVD/ISO and removable media in the EEFF client. If the password does not conform to a policy, an error message is displayed in the EEFF client detailing the reason and prompting the user to try again. In addition to the password complexity checks, when a password is changed for removable media and User Local Keys, the new password is checked against the user’s last password to prevent duplication.  
  • Minimum Password Length — Specifies the minimum number of characters that must be included in a password (from 4–40). Default value is 7.  
  • Minimum Lowercase Characters — Specifies the minimum number of lowercase letters that must be included in a password (from 0–15). Default value is 0.  
  • Minimum Uppercase Characters — Specifies the minimum number of uppercase (capital) letters that must be included in a password (from 0–15). Default value is 0.  
  • Minimum Alphabetical Characters — Specifies the minimum number of letters that must be included in a password (from 0–15). Default value is 5.  
  • Minimum Numeric Characters — Specifies the minimum number of numeric characters (digits) that must be included in a password (from 0–15). Default value is 1.  
  • Minimum Special Characters — Specifies the minimum number of special characters that must be included in a password (from 0–15). Default value is 1.  
  All password policies are system-based. In addition to the above complexity checks, internal checks are performed on all passwords to verify that they do not contain more than two consecutive characters of the user name, do not match the full account name, and do not contain any spaces. |
Create a policy

You can create a new policy from the Policy Catalog. By default, policies that are created using the Policy Catalog are not assigned to any groups or systems.

You can create policies before or after deploying the EEFF software.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog, then select Endpoint Encryption for Files and Folders 4.2.0 from the Product drop-down list.
2. Select the category from the drop-down list.
   
   All created policies for the selected category appear in the details pane.
3. Click Actions | New Policy.
4. Select the policy you want to duplicate from the Create a policy based on this existing policy drop-down list.
5. Enter a name for the new policy and click OK to open the Policy Settings wizard.
6. Edit the policy settings on each tab as needed.
7. Click Save.

Edit the EEFF policy settings

You can modify the EEFF policy settings from the Policy Catalog.

**Before you begin**

Your user account must have appropriate permissions to edit McAfee EEFF policy settings. If role-based key management is implemented, you can view and edit only those policies with keys associated with your specific role.

A Global Key Administrator can access only policies that have default keys. All administrators can access default keys provided that they have been assigned View/Manage permissions for the EEFF Key Server.

For option definitions, click ? in the interface.

**Task**

1. Click Menu | Policy | Policy Catalog, then select Endpoint Encryption for Files and Folders from the Product drop-down list.
2. Select the category from the drop-down list.
   
   All created policies for the selected category appear in the details pane.
3. Click the policy name.
4. Edit the settings as needed, then click Save.

The policy settings are updated.
Assign a policy to a managed system

You can assign a policy to a specific managed system before or after deploying the EEFF software.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Systems | System Tree | Systems**, then select the group under the **System Tree**. All the systems within this group (but not its subgroups) appear in the details pane.

2. Select the system, then click **Actions | Agent | Modify Policies on a Single System** to open the **Policy Assignment** page for that system.

3. Select **Endpoint Encryption for Files and Folders** from the drop-down list. The policy categories under **Endpoint Encryption for Files and Folders** are listed with the system’s assigned policy.

4. Locate the required policy category, then click **Edit Assignment**.

5. If the policy is inherited, select **Break inheritance and assign the policy and settings below next to Inherit from**.

6. Select the policy from the drop-down list.
   - The available policies depend on your role and permissions.
   - From this location, you can edit the selected policy or create a new policy.

7. Select whether to lock policy inheritance.
   - Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.

The policy is assigned to the selected managed system.

Assign a policy to a system group

You can assign a policy to multiple managed systems within a group before or after deploying the EEFF software.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Systems | System Tree | Systems**, then select the system group under the **System Tree**. All the systems within this group (but not its subgroups) appear in the details pane.

2. Select the relevant systems, then click **Actions | Agent | Set Policy & Inheritance** to open the **Assign Policies** page.

3. Select **Endpoint Encryption for Files and Folders** from the drop-down list.

4. Select the category and policy from the respective drop-down lists, then click **Save**.
   - The available policies depend on your role and permissions.

The policy is assigned to the selected system group.
Enforce EEFF policies on a system

You can enable or disable policy enforcement for EEFF on a system. Policy enforcement is enabled by default, and is inherited in the System Tree.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Systems | System Tree | Systems, then select the group under the System Tree where the system belongs. The list of systems belonging to this group appears in the details pane.
2. Select the system, then click Actions | Agent | Modify Policies on a Single System.
3. Select Endpoint Encryption for Files and Folders from the drop-down list, then click Enforcing next to Enforcement status.
4. To change the enforcement status, select Break inheritance and assign the policy and settings below.
5. Set the enforcement status to Enforcing or Not enforcing as needed.
6. Click Save.

The enforcement status is applied to the selected managed systems.

Enforce EEFF policies on a system group

You can enable or disable policy enforcement for a product on a System Tree group. Policy enforcement is enabled by default, and is inherited in the System Tree.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Systems | System Tree | Assigned Policies, then select the group in the System Tree.
2. Select Endpoint Encryption for Files and Folders from the drop-down list, then click Enforcing next to Enforcement Status.
3. To change the enforcement status, select Break inheritance and assign the policy and settings below.
4. Select Enforcing or Not enforcing accordingly as Enforcement status.
5. Select whether to lock policy inheritance.
   - Locking inheritance for policy enforcement prevents breaking enforcement for groups and systems that inherit this policy.
6. Click Save.

The selected enforcement status is applied to the product.
How policy assignment rules work

Policy assignment rules enable you to create system-specific and user-specific policy assignments. These assignments are enforced on the target system when a user logs on. The agent on the managed system keeps a record of the users who log on to the network. The policy assignments you create for each user are pushed down to the system they log on to, and are cached during each agent-server communication. The agent applies the policies that you have assigned to each user.

When a user logs on to a managed system for the first time, there can be a slight delay while the agent contacts its assigned server for the policy assignments specific to this user. During this time, the user has access only to that functionality allowed by the default machine policy, which typically is your most secure policy.

Policy assignment rules reduce the overhead of managing numerous policies for individual users, while maintaining generic policies across your System Tree. For example, you can create a policy assignment rule that is enforced for all users in your engineering group. You can then create another policy assignment rule for members of your IT department so they can log on to any computer in the engineering network with the access rights they need to troubleshoot problems on a specific system in that network. This level of granularity in policy assignment limits the instances of broken inheritance in the System Tree.

Policy assignment rule priority

You can prioritize rules for policy assignment to simplify policy assignment management. When you assign priority to a rule, it is enforced before assignments with a lower priority. In some cases, the outcome can be that some rule settings are overridden.

For example, consider a user who is included in two policy assignment rules, rules A and B. Rule A has priority level 1, and allows included users unrestricted access to Internet content. Rule B has priority level 2, and heavily restricts the same user’s access to Internet content. In this scenario, rule A is enforced because it has higher priority. As a result, the user has unrestricted access to Internet content.

How multi-slot policies work with policy assignment rule priority

Multi-slot policies are used when a policy setting needs to be shared among users or system groups. Rule priority is not considered for multi-slot policies. A Grant Key policy is a multi-slot policy.

- If a single rule containing multi-slot policies of the same product category is applied to a user, all settings of the multi-slot policies are combined.
- If multiple rules applied to a user contain multi-slot policy settings, all settings from each multi-slot policy are combined.

As a result, the user gets a policy that combines the settings of each rule.

For example, when these rules consist of multi-slot policy assignments, the settings for both policies are applied without regard to priority.

You can prevent application of combined settings from multi-slot policies across multiple policy assignment rules by excluding a user (or other Active Directory objects) when creating the policy assignment rule.
Working with policy assignment rules

You can set up, create, and manage policy assignment rules in your network. You can perform common management tasks when working with policy assignment rules in the McAfee ePO server. For details, see the McAfee ePO product documentation.

You can perform common management tasks when working with policy assignment rules in the McAfee ePO server. For details, see the McAfee ePO product documentation.

Tasks

- Create policy assignment rules on page 28

Policy assignment rules enable you to enforce permissions and criteria-based policies for individual users accessing your network.

Create policy assignment rules

Policy assignment rules enable you to enforce permissions and criteria-based policies for individual users accessing your network.

Task

For option definitions, click ? in the interface.


2. On the Details page, enter the name and description in the designated fields, then click Next.

3. On the Selection Criteria page, select the users by selecting the relevant criteria, then click Next.


You can add more than one Grant Key policy.

5. Select Endpoint Encryption for Files for Folders, select the Grant Keys category, then select the policy from the drop-down list.

6. Click OK.

7. On the Summary page, click Save.

How multi-slot policies work

The McAfee ePO administrator can add multiple Grant Key policies to users or system groups restricting the assignment of keys to authorized users only. The policy instances are automatically combined into an effective policy.

Multi-slot policies obey the ePolicy Orchestrator laws of inheritance within the System Tree (see ePolicy Orchestrator Product Guide for details).

Assign multiple instances of Grant Key policy through the System Tree

You can use the System Tree to assign multiple instances of a Grant Key policy to a system.
**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Systems | System Tree | Assigned Policies | Product | Endpoint Encryption for Files and Folders.** Each assigned policy per category appears in the details pane.

2. Locate the Grant Key policy category, then click **Edit Assignment.**

3. Click **New Policy Instance.** The new policy instance is added to the **Policy Assignment** page.

4. If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherited from.**

5. Select the **Grant Key** policy from the drop-down list.

   From this location, you can also edit the selected policy’s settings, or create a new policy.

6. Select whether to lock policy inheritance.

   Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.

7. Click **Save.**

**Assigning Grant Key policy through policy assignment rules**
You can assign multiple instances of Grant Key policy to a user or a system through Policy Assignment Rules.

**Tasks**

- **Assign multiple instances of Grant Key policy to systems on page 29**
  You can assign system-based policies to the tags you applied using McAfee ePO. You can assign multiple instances of a Grant Key policy to systems based on the tags applied to them.

- **Assign multiple instances of Grant Key policy to users on page 30**
  You can assign multiple instances of Grant Key policy to users based on the tags applied to them using McAfee ePO 4.6.

**Assign multiple instances of Grant Key policy to systems**
You can assign system-based policies to the tags you applied using McAfee ePO. You can assign multiple instances of a Grant Key policy to systems based on the tags applied to them.

When assigning a Grant Key policy using McAfee ePO 4.6, the policy assigned to a system (based on the tags applied) does not merge with Grant Key policy assigned through the System Tree.

**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Policy | Policy Assignment Rules | Actions | New Assignment Rule** to open the **Policy Assignment Builder** wizard.

2. On the **Details** page, enter the name and description in the designated fields.

3. Select **System Based** as the **Rule Type**, then click **Next.** The **Assigned Policies** page appears.

4. Click **Add Policy** to select the policies that you want to enforce using this policy assignment rule.

5. Select **Endpoint Encryption for Files for Folders**, select the **Grant Keys** category, then select the policy from the drop-down list.
6 Click Next.

7 On the Selection Criteria page, select the users by selecting the relevant criteria, then click Next.

8 On the Summary page, click Save.

Assign multiple instances of Grant Key policy to users
You can assign multiple instances of Grant Key policy to users based on the tags applied to them using McAfee ePO 4.6.

The Grant Key policy assigned to a user through a policy assignment rule is merged with the grant key policy assigned to the system through the System Tree.

Task
For option definitions, click ? in the interface.

1 Click Menu | Policy | Policy Assignment Rules | Actions | New Assignment Rule to open the Policy Assignment Builder wizard.

2 On the Details page, enter the name and description in the designated fields.

3 Select the Rule Type as User Based, then click Next. The Assigned Policies page appears.

4 Click Add Policy to select the policies that you want to be enforced by this policy assignment rule.

5 Select Endpoint Encryption for Files for Folders, select the Grant Keys category, then select the policy from the drop-down list.

6 Click Next.

7 On the Selection Criteria page, select the users by selecting the relevant criteria, then click Next.

8 On the Summary page, click Save.

View the policies assigned to systems
You can view the policies assigned to systems, including the available keys.

Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Assigned Policies | Product | Endpoint Encryption for Files and Folders 4.2.0. Each assigned policy per category appears in the details pane.

2 Locate the Grant Key policy category, then click View Effective Policy. The View Effective Grant Keys Policy page lists of keys available to the system and the associated policies.

Only keys contained in the permission set for the logged on user’s role are displayed.

View the policies assigned to users
You can view the policies assigned to users, including the available keys.

Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Systems, then select the required system.

2 Click Actions | Direct Management | View Effective Policy (by user).
3. Select **Endpoint Encryption for Files and Folders**, then click **Select User** next to **Effective Policy for User**.

4. Select the required user, then click **OK**. The policies assigned to the selected user appear in the details pane.

5. Locate the **Grant Key** policy category, then click **View Effective Policy**. The **View Effective Grant Keys Policy** page lists keys available to the user and the associated policies.

Only keys contained in the permission set for the logged on user's role are displayed.
Configuring EEFF policies
How multi-slot policies work
Managing EEFF keys

EEFF uses encryption keys to protect files and folders on networks, removable media (USB devices and floppy disks), CDs, DVDs, and users' hard disks. Encryption keys are generated and stored in an internal encryption key repository within the McAfee ePO environment.

Contents
- Encryption keys
- Create an encryption key
- Activate or deactivate the encryption keys
- Assign the encryption keys to a policy
- Edit an encryption key
- Delete an encryption key
- Export encryption keys
- Import keys
- How user personal keys work
- Role-based key management
- View key usage

Encryption keys

The EEFF client requests an encryption key when a user accesses an encrypted file or a folder. If a policy is assigned to the user with the requested encryption key, EEFF decrypts the data.

An administrator can create and manage encryption keys from McAfee ePO on the EEFF keys page. These keys are assigned to policies that are later assigned to users or systems.

Key types

EEFF supports three types of encryption keys:

- **Regular keys** — Created by McAfee ePO administrators and can be used in any policy.

- **User personal keys** — Generated in McAfee ePO when a key is granted to a user through the Grant Key policy. When this policy is assigned, the user can use this unique key across all the client systems in the same domain.

- **User local keys** — Created using EEFF client software on a client system. The user can use these keys to encrypt or decrypt data on the same network using the context menu. A local key is limited to the user and client system where it was created.

Create an encryption key

You can create a regular encryption key, with or without an expiry date.
**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Data Protection | EEFF keys**.
2. Click **Actions | Create a New Key**.
3. Enter a name and description for the key.
4. Select **Never expire key** or set an expiration date as needed.
5. If you are using Role-Based Key Management, select the checkboxes for the relevant roles.
   - Only roles assigned to the logged on user are available for selection. The key is accessible only to users assigned a selected role.
6. Click **OK**.

The new key is available for inclusion in EEFF policies.

---

**Activate or deactivate the encryption keys**
Activating or deactivating an encryption key determines the key's availability on the client systems.

**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Data Protection | EEFF keys**.
2. Select the keys to activate, then click **Actions | Activate Key(s)**.
   - To deactivate keys, select the keys, click **Actions | Deactivate Key(s)**, then click **OK**.

When an encryption key is activated, it is added to the client systems during the next policy update. When an encryption key is deactivated, it is removed from the client systems during the next policy update.

---

**Assign the encryption keys to a policy**
Encryption keys are assigned to users or systems through a Grant Key policy, which is a multiple instance policy.

- You can assign only active keys to a Grant Key policy.

**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Policy | Policy Catalog | Product | Endpoint Encryption for Files and Folders 4.2.0 | Category | Grant Keys (UBP)**. All Grant Key policies appear in the details pane.
2. Click the Grant Key policy name. The selected Grant Key policy page lists the active keys in the **Available Keys** pane, including all DEFAULT keys.
3. Select and move the required keys to the **Selected Keys** pane, then click **Save**.
4. Send an agent wake-up call.
Edit an encryption key

You can edit properties of an existing encryption key.

Task
For option definitions, click ? in the interface.

1 Click Menu | Data Protection | EEFF keys.
2 Select the key to edit, then click Actions | Edit key.
3 Edit the name, description, and expiry date of the key.
   If role-based key management is implemented, you can also edit the role settings.
4 Click OK.

Delete an encryption key

You can delete an encryption key as long as it no longer active.

Before you begin
You must deactivate an encryption key before you can delete it.

Files remain encrypted on client systems or removable media even if a key has been removed from all policies. Files encrypted with a deleted key are inaccessible and cannot be recovered.

Task
For option definitions, click ? in the interface.

1 Click Menu | Data Protection | EEFF keys.
2 Select the keys to delete, then click Actions | Delete Key(s).
3 Click OK.

The keys are deleted and any files encrypted with those keys are no longer accessible.

Export encryption keys

You can export encryption keys into a password-protected .bin file. If role-based key management is implemented, the exported key data includes role information.

Task
For option definitions, click ? in the interface.

1 Click Menu | Data Protection | EEFF keys.
2 Select the keys to export, then click Actions | Export Key(s).
3 Enter and confirm the password to be used to protect the exported file, then click OK to open the Export Keys for EEFF page.
4 Click the .bin or .xml file, and save it to the required location.
5 Click Close.
The selected keys are saved in a password-protected .bin file in the specified location.

**Import keys**

You can import encryption keys that have been exported from EEM or EEFF. The ability to import information related to role-based key management depends on the version of EEM or EEFF, and how the key data is exported.

**Import keys from EEFF**

You can import encryption keys from a password-protected .bin file that was created in a different instance of EEFF.

Key data exported from EEFF 4.x does not include roles or permission sets, so the imported keys are automatically assigned the Default role.

Key data exported from EEFF 4.2 includes role information. If a role exists with the same name, the imported keys are assigned to that role. If a role with the same name is not found, the key is skipped.

Key data exported from EEFF 3.x does not include roles or permission sets. However, the keys can be associated with roles and permission sets if the data is exported with level information from EEM. See Import keys from EEM for details.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Data Protection | EEFF keys**.
2. Click **Actions | Import Keys**.
3. Browse and select the .bin file, then enter the password if prompted.
4. Click **Import Keys**.

The **Import Keys** page lists the number of encryption keys successfully imported.

**Import keys from EEM**

You can import encryption keys from EEM 5.2 or later.

By default, the key data exported from EEM does not include key level (role) information. To include all key level information, install the SbAdmDLL.dll update (patch), which is shipped with EEM 5.2.13 before exporting the data.

When importing keys from EEM, the McAfee ePO EEFF extension checks for roles defined in McAfee ePO that correspond with the EEM level.

- If the XML file does not contain key level information, the imported keys are automatically associated with the Default role.
- If the key level already exists, EEFF imports the key and associates it with that role.
If the key level does not exist, EEFF creates a role with the prefix EEM_LEVEL, followed by the level number (for example, EEM_LEVEL_24. EEFF then imports the key and associates the key with the newly defined role, and create a permission set named accordingly (for example, EEM_LEVEL_24_PS). If a permission set with that name already exists, a new permission is not created and the role is associated with the existing permission set.

When multiple roles are imported using the same XML file, EEFF associates the keys to multiple roles based on the key levels. A higher key level is assigned the keys of any lower levels. For example, if the imported XML includes levels 24, 30, and 32, the EEM_LEVEL_30_PS would be assigned the EEM_LEVEL_30, EEM_LEVEL_24 and Default roles.

We recommend importing all of the files from EEM using a single file. If multiple files are imported, the administrator needs to set up the permissions sets manually.

**Task**

1. In EEM, run this command to export the key data into an XML file: `Sbadmcl.exe -AdminUser:Admin -AdminPwd:epo -command:ExportFfKeys`  
   
   `Sbadmcl.exe -AdminUser:Admin -AdminPwd:epo -command:ExportFfKeys`

2. In McAfee ePO, click **Menu | Data Protection | EEFF keys**.

3. Click **Actions | Import Keys**.

4. Browse and select the `.xml` file, then enter the password if prompted.

5. Click **Import Keys**.

The McAfee ePO EEFF extension checks for roles defined in McAfee ePO that correspond with the EEM level and imports the keys accordingly.

---

### How user personal keys work

User personal keys give you the ability to create user-specific encryption keys. These keys are created on the McAfee ePO server when the user logs on to the client system for the first time after the policy is enforced.

User personal keys are assigned to the Grant Key policy as a single key, but create individual user personal keys when assigned. If the policy is assigned at the system level, users on that system will have individual user personal keys. When assigned at the user level, these keys can be used on any system within the same domain.

The user personal key is enabled and assigned to the Grant Key policy using McAfee ePO. The Grant Key policy can be assigned to specific users with Policy Assignment Rules. The Grant Key policy can be assigned to specific systems or system groups from the **Assigned Policies** page. Enforcing the Grant Key policy on the managed system creates a user personal key at the first logon of the user. User personal keys can be used as recovery keys for user local keys and removable media encryption.

**Best practice**

By assigning a user personal key as a recovery key for removable media encryption, the administrator can make sure that the removable media can be recovered only by the assigned user on any system in the same domain.

**Assign a user personal key**

You can assign a user personal key with a Grant Key policy.
**Task**
For option definitions, click ? in the interface.

1. Enable the creation and assignment of user personal keys in EEFF:
   a. Click **Menu | Data Protection | EEFF keys**.
   b. Click **Edit next to User Personal Keys**.
   c. Select **Enable User Personal Keys**, then click **Save**.

2. Edit the EEFF policy settings to include user personal keys:
   a. Click **Menu | Policy | Policy Catalog | Product | Endpoint Encryption for Files and Folders**.
   b. Select the **Grant Keys (UBP)** policy category, then click the policy name.
   c. Select and move the **User Personal Key** to the **Selected Keys** table, then click **Save**.
   The keys available for selection depend on your permission set and roles.

3. Click **Menu | Policy | Policy Assignment Rules | New Assignment Rule** to open the **Policy Assignment Builder** wizard.

4. Enter the name and description in the designated fields, then click **Next** to open the **Selection Criteria** page.

5. Select the user by selecting the relevant criteria, then click **Next** to open the **Assigned Policies** page.

6. Click **Add**. The **Choose a policy to assign** dialog box appears.

7. Select **Endpoint Encryption for Files for Folders** from the drop-down list.

8. Select **Grant Keys**, select the necessary policy from the drop-down list, then click **OK**.

9. On the **Summary** page, click **Save**.
   After assigning the Grant Key policy to the user, a user personal key is generated when the user logs on to the client system.

**Recover a user personal key**
Displaying the user personal keys as regular keys enables the administrator to recover files encrypted with a user key belonging to another user.

**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Data Protection | EEFF keys**.

2. Select the user personal key, then click **Actions | Edit Key**.

3. Select **Display as regular**, then click **OK**.

---

**Role-based key management**
Role-based key management enables you to compartmentalize the administration of keys and permission sets for enhanced security by allowing you to define multiple key administrators based on permission sets defined by the Global Key Administrator. Each key administrator can manage only the
keys for the roles contained in the respective permission set. This functionality is available only to users of EEFF 4.2 with ePolicy Orchestrator 4.6, Patch 6.

How role-based key management works

Role-based key management enables a Global Key Administrator to define roles and assign them to permission sets. Users can manage only the keys for the roles contained in the respective permission set.

Role of the Global Key Administrator

In addition to creating users and permission sets, the Global Key Administrator (GKA) is responsible for creating roles and assigning the roles to user's permission sets appropriately. The GKA is assigned the Default role.

The Default role is created automatically and cannot be deleted. It enables the GKA to manage roles throughout the system. The GKA can manage only keys for the Default role. Keys associated with other roles are not accessible to the GKA. Those keys are managed by McAfee ePO admin users based on their role assignments, meaning that they can manage only the keys associated with their roles.

Roles and permission sets

A permission set can contain any number of roles. A user or administrator can manage only the keys for the roles contained in the respective permission set.

If a user has more than one assigned permission set, that user receives the roles assigned in all of the permission sets upon log in with their respective Key Server settings. If the user has View Key Server permissions for a role in one permission set, and Manage Key Server permissions for the same role in a different permission set, the Manage Key Server permission setting is applied for that role.

Add a role

If you are a Global Key Administrator, you can add roles.

Task

For option definitions, click ? in the interface.

1 Click Menu | Configuration | Server Settings | EEFF Role Settings.

2 Click Edit.

The Add New Role section appears below the list of roles.

3 Enter the name and description of the role, then click OK.

The role appears on the EEFF Role Settings page.

Edit a role

If you are a Global Key Administrator, you can edit the properties of a role that you created. (The Default role cannot be edited.)
Task
For option definitions, click ? in the interface.

1. Click Menu | Configuration | Server Settings | EEFF Role Settings.
2. In the row for the role, click Change.
   The properties of the selected role appear below the list of roles.
3. Edit the name and description of the role, then click OK.
   The role properties are updated.

Delete a role
If you are a Global Key Administrator, you can delete a role that you created. (The Default role cannot be deleted.)
You cannot delete a role if it contains keys. Delete the keys or reassign them to a different role before attempting to delete a role.

Task
For option definitions, click ? in the interface.

1. Click Menu | Configuration | Server Settings | EEFF Role Settings.
2. In the row for the role, click Delete.
   If keys are assigned to the role, you are prompted to reassign them before deleting the role.
3. When prompted for confirmation, click OK.
   The role is deleted.

Assign a role to a permission set
You can assign roles to a permission set, enabling the respective users to manage or view only the keys for the roles included in that permission set.

If a user has more than one assigned permission set, that user receives the roles assigned in all of the permission sets upon log in with their respective Key Server settings. If the user has View Key Server permissions for a role in one permission set, and Manage Key Server permissions for the same role in a different permission set, the Manage Key Server permission setting is applied for that role.

Task
For option definitions, click ? in the interface.

1. Click Menu | User Management | Permission Sets, then click Edit next to EEFF Policy Permissions.
2. In the Key Server section, select one of these options:
   - View Key Server — Enables the user to view the state of keys, without the ability to perform related actions.
   - Manage Key Server — Enables the user to manage the keys, including the ability to edit, activate, or delete keys.
3. Select the roles you want to include in this permission set by selecting or deselecting the corresponding checkboxes.
4. Click Save.
Users assigned to this permission set can manage or view the keys for the selected roles accordingly.

### View key usage

You can view summary information on EEFF key usage on the EEFF Key Management page, and easily access and edit the policies where they are used.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Data Protection | EEFF keys**.
   
   The number of policy objects where the key is a link in the **Usage** column.

2. To view a list of the policies where a specific key is used, click the number link.
   
   The policy names and categories are listed on the EEFF Key Usage page.

3. (Optional) To view or edit a policy, click its name.
   
   The policy details appear in the **Policy Editor**.
Managing EEFF keys
View key usage
Defining EEFF permission sets for McAfee ePO users

In the McAfee ePO server, administrator rights management determines the actions that McAfee ePO users can perform while administrating EEFF.

A permission set is a group of permissions that can be granted to users or Active Directory (AD) groups by assigning it to those users’ accounts. One or more permission sets can be assigned to users who are not global administrators. (Global administrators have all permissions to all products and features.)

User accounts and their associated permission sets define the tasks that the users can perform. This allows you to restrict specific users or groups from misusing EEFF features.

Contents
- Create permission sets for user accounts
- Edit the EEFF policy permissions
- Edit the EEFF key server permissions

Create permission sets for user accounts
If you are a global administrator, you can create permission sets for user accounts.

Task
For option definitions, click ? in the interface.

1. Click Menu | User Management | Permission Sets.
2. Click Actions | New permission Set.
3. Enter a unique name for the permission set.
4. To immediately assign specific users to this permission set, select their user names in the Users section.
5. To map all users in a specific Active Directory group to this permission set, select the server from the drop-down list, then click Add.
6. Click Save to create the permission set.

Edit the EEFF policy permissions
You can define the permissions for configuring EEFF policy settings.
Task
For option definitions, click ? in the interface.

1 Click Menu | User Management | Permission Sets.

2 Click Edit next to EEFF Policy Permissions.

3 Set the appropriate permissions, then click Save.

The updated permissions are applied to users and Active Directory groups assigned to this permission set.

Edit the EEFF key server permissions

You can define permission sets for creating and managing EEFF keys.

Task
For option definitions, click ? in the interface.

1 Click Menu | User Management | Permission Sets.

2 Click Edit next to EEFF Key Server.

3 In the Key Server section, select one of these options:
   - No Permission — Restricts users from viewing or modifying the keys.
   - View Key Server — Enables the user to view the state of keys, without the ability to perform related actions.
   - Manage Key Server — Enables the user to manage the keys, including the ability to edit, activate, and delete keys.

4 (Optional) If role-based key management is implemented, select the roles you want to include in this permission set by selecting or deselecting the corresponding checkboxes.

5 Click Save.
Managing EEFF reports

The McAfee ePO server ships with its own querying and reporting capabilities. These are highly customizable, flexible, and easy to use. EEFF reports are based on configurable EEFF queries, and can be displayed and exported in several formats.

Contents
- EEFF queries and query results
- Create EEFF custom queries
- View standard EEFF queries
- EEFF client events
- View audit log

EEFF queries and query results

EEFF queries are configurable objects that retrieve and display data from the database. These queries can be displayed in charts and tables. Any query results can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can be used as dashboard monitors.

EEFF queries are configurable objects that retrieve and display data from the database. These queries can be displayed in charts and tables. Any query results can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can be used as dashboard monitors.

Query results are actionable

Query results displayed in tables (and drill-down tables) have a variety of actions available for selected items in the table. For example, you can deploy agents to systems in a table of query results. Actions are available at the bottom of the results page.

Queries as dashboard monitors

Most queries can be used as a dashboard monitor (except those using a table to display the initial results). Dashboard monitors are refreshed automatically on a user-configured interval (five minutes by default).

Exported results

Query results can be exported in four different formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Unlike query results in the console, data in exported reports is not actionable.
Reports are available in these formats:

- **CSV** — Use the data in a spreadsheet application (for example, Microsoft Excel).
- **XML** — Transform the data for other purposes.
- **HTML** — View the exported results as a web page.
- **PDF** — Print the results.

## Create EEFF custom queries

You can create EEFF custom queries with the Query Builder wizard.

### Task

For option definitions, click ? in the interface.

1. Click **Menu** | **Reporting** | **Queries** | **Actions** | **New Query**. The Query Builder wizard opens.

2. On the **Result Type** page, select **Others** from the **Feature Group** pane and **Endpoint Encryption Result Type** for the query, then click **Next** to open the **Chart** page.

   For option definitions, click ? in the interface.

   This choice determines the options available on subsequent pages of the wizard.

3. Select the type of chart or table to display the primary results of the query, then click **Next** to open the **Columns** page.

   If you select **Boolean Pie Chart**, you must configure the criteria to include in the query.

4. Select the columns to be included in the query, then click **Next** to open the **Filter** page.

   *If you select **Table** on the **Chart** page, the columns you select here are the columns of that table. Otherwise, these are the columns that make up the query details table.*

5. Select properties to narrow the search results, then click **Run**. The **Unsaved Query** page displays the results of the query, which is actionable, so you can take any available actions on items in any tables or drill-down tables.

   Selected properties appear in the content pane with operators that can specify criteria used to narrow the data that is returned for that property.

   - If the query does not appear to return the expected results, click **Edit Query** to go back to the **Query Builder** and edit the details of this query.

   - If you do not need to save the query, click **Close**.

   - If this is a query you want to use again, click **Save** and continue to the next step.

6. On the **Save Query** page, enter a name for the query, add any notes, and select one of these options:

   - **New Group** — Enter the new group name and select either:
     - **Private group (My Groups)**
     - **Public group (Shared Groups)**
   
   - **Existing Group** — Select the group from the list of **Shared Groups**.

7. Click **Save**.
View standard EEFF queries

You can run and view the standard EEFF reports from the Queries page.

Task
For option definitions, click ? in the interface.

1. Click Menu | Reporting | Queries & Reports.

2. In the Groups pane, select EEFF Queries from the Shared Groups drop-down list. The standard EEFF query list appears.

<table>
<thead>
<tr>
<th>Query</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD/DVD/ISO Events</td>
<td>Lists all events related to CDs, DVDs, and ISOs.</td>
</tr>
<tr>
<td>EEFF Active Keys</td>
<td>Displays the number of active and inactive keys. (This information is also available on the Manage Keys page.)</td>
</tr>
<tr>
<td>EEFF Key Usage</td>
<td>Displays the available keys, their policy category, and the policy in which they are used. (This information is also available on the Manage Keys page.)</td>
</tr>
<tr>
<td>Protection Status:</td>
<td>Displays the protection status of removable media.</td>
</tr>
<tr>
<td>Removable Media</td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td>Lists all events related to removable media.</td>
</tr>
</tbody>
</table>

3. Select a query from the Queries list.

4. Click Actions | Run to display the query results.

5. Drill down into the report and take actions on items as needed. Available actions depend on the permissions of the user.

6. Optionally, you can edit the query and view its details.

6. Click Close when finished.
EEFF client events

Enforcement of EEFF policies generates client events, which include the Event ID, system information initialization details, and device information.

Removable media events

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>20500</td>
<td>Removable Media Device Insertion Event</td>
<td>This event is reported whenever any type of removable media is inserted in the client. Event severity: 4</td>
</tr>
<tr>
<td>20501</td>
<td>Removable Media User Response Event</td>
<td>This event is reported whenever the user clicks Yes or No in the Removable Media Format Message window. Event severity: 4</td>
</tr>
<tr>
<td>20502</td>
<td>Removable Media Initialization Start Event</td>
<td>This event is reported whenever the user clicks Initialize or Cancel in the Removable Media Initialization window. Event severity: 4</td>
</tr>
<tr>
<td>20503</td>
<td>Removable Media Initialization End Event</td>
<td>This event is reported when initialization is complete. Event severity: 4</td>
</tr>
<tr>
<td>20504</td>
<td>Removable Media Device Ejection Event</td>
<td>This event is reported whenever any type of removable media is ejected from the client. Event severity: 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event ID</td>
<td>Event ID number</td>
</tr>
<tr>
<td>System</td>
<td>• User information (DomainName, UserName)</td>
</tr>
<tr>
<td></td>
<td>• Timestamp</td>
</tr>
<tr>
<td></td>
<td>• Agent GUID</td>
</tr>
<tr>
<td>Initialization</td>
<td>• Initialization state (Failed, Cancelled, Successful)</td>
</tr>
<tr>
<td></td>
<td>• Backup state (None, Failed, Cancelled, Successful)</td>
</tr>
<tr>
<td></td>
<td>• Time taken for initialization (in msec)</td>
</tr>
<tr>
<td></td>
<td>• Time taken for backup (in msec)</td>
</tr>
<tr>
<td></td>
<td>• Backup size (in Bytes)</td>
</tr>
<tr>
<td></td>
<td>• Size of protected part (only when initialization has completed successfully, in bytes)</td>
</tr>
</tbody>
</table>
Table 6-2  Event details (continued)

<table>
<thead>
<tr>
<th>Information type</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Device**       | • Size (in bytes)  
|                   | • File system of device (FAT, NTFS, EERM)  
|                   | • Vendor name  
|                   | • Product name  
|                   | • Exempted (Yes, No, Unknown)  
|                   | • Protected (Yes, No, Unknown) (only removable media drives are considered protected) |
| **Event specific fields** | **User response — Valid for events 20501 and 20502 only** |

CD/DVD/ISO client events

Table 6-3  Event types

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 20505    | Encrypted CD/DVD/ISO Initialization Start Event | This event is reported whenever the user clicks **Initialize** or **Cancel** in the **Initialization** window.  
|          |       | Event severity: 4 |
| 20506    | Encrypted CD/DVD/ISO Initialization End Event | This event is reported when initialization is complete.  
|          |       | Event severity: 4 |
| 20507    | CD/DVD/ISO Insertion Event | This event is reported whenever a CD or DVD is inserted in the client.  
|          |       | Event severity: 4 |
| 20508    | CD/DVD/ISO Ejection Event | This event is reported whenever a CD or DVD is ejected from the client.  
|          |       | Event severity: 4 |

Table 6-4  Event details

<table>
<thead>
<tr>
<th>Information type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Event ID</strong></td>
<td>Event ID number</td>
</tr>
</tbody>
</table>
| **Computer**     | • Name of the computer  
|                   | • User name  
|                   | • IP address  
|                   | • Operating system type |
| **Media type**   | • For Encrypted CD/DVD/ISO Initialization Start Events, the smallest disk type that can hold archived data (ISO, CD, DVD or DVD-DL)  
|                   | • For Encrypted CD/DVD/ISO Initialization End Events, the physical media detected (for example, CD-ROM)  
|                   | • For CD/DVD/ISO Insertion and Ejection Events, "Optical" |
### Table 6-4  Event details (continued)

<table>
<thead>
<tr>
<th>Information type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>• Disk globally unique identifier (GUID)</td>
</tr>
<tr>
<td></td>
<td>• Protected (Yes, No, Unknown) (only EERM drives are considered protected)</td>
</tr>
<tr>
<td></td>
<td>• Protected size (GB)</td>
</tr>
<tr>
<td></td>
<td>• For Encrypted CD/DVD/ISO Initialization Start Events, the value is 0</td>
</tr>
<tr>
<td></td>
<td>• For Encrypted CD/DVD/ISO Initialization End Events, the size of the encrypted archive</td>
</tr>
<tr>
<td></td>
<td>• For CD/DVD/ISO Insertion and Ejection Events, the size of the encrypted archive if the media is EEFF-encrypted</td>
</tr>
<tr>
<td>Event description</td>
<td>• Description of the event</td>
</tr>
<tr>
<td></td>
<td>• Event generation time</td>
</tr>
<tr>
<td>Event specific fields</td>
<td>Initialization state (Failed, Cancelled, Successful) (CD/DVD/ISO Insertion and Ejection Events only)</td>
</tr>
</tbody>
</table>

Only relevant information is captured in each event. For example, a Device Insert Event does not contain Initialization State.

### View audit log

The actions performed by an EEFF administrator are recorded in the McAfee ePO audit log.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | User Management | Audit Log**.
2. For easier viewing, filter or sort the log entries. For more details, see the ePolicy Orchestrator documentation.

The **Audit Log** page lists the actions performed in the system.
Additional information

This additional information includes guidelines on FIPS certification, instructions for uninstalling EEFF, the use of registry controls to define removable media and exclude local drives and network drives from encryption, and best practices for large-scale deployments.

Contents

- FIPS certification
- Uninstall EEFF
- Removable media registry controls
- Best practices for large-scale deployment

FIPS certification

The 140 series of Federal Information Processing Standards (FIPS) is a set of U.S. government computer security standards that specify requirements for cryptography modules.

The EEFF client makes use of the McAfee Core Cryptographic Module (MCCM) User and Kernel FIPS 140-2 cryptographic modules. These cryptographic modules are being validated at FIPS 140-2 Level 1.

The current status of this certification is available on the NIST website.

Prerequisites

For EEFF 4.2 to be in compliance with FIPS 140-2, the software should meet these conditions:

- McAfee ePO must be installed in FIPS mode

  If McAfee ePO is not installed in FIPS mode, the EEFF client cannot operate in FIPS mode because all EEFF keys are generated in the EEFF extension.

- The Microsoft Windows operating system on the client where EEFF is installed must be running in FIPS mode.

  This is necessary to ensure that the key cache and policy cache files on the client system are protected using keys generated in FIPS mode.

If you don't install both McAfee ePO and EEFF in FIPS mode, the configuration does not operate in a FIPS-certified manner.

Impact of FIPS mode

In FIPS mode, certain self-tests are performed on start-up of the client system when the MCCM is loaded.

If FIPS self-tests fail, the system responds in one of these ways:
• If the MCCM FIPS component fails the self-test, the system doesn't activate or enforce policies.
• If the EEFF driver fails the self-test, the driver performs a bug-check (BSOD).

**FIPS 140-2** defines minimum requirements for entropy during key generation. This might lead to key generation errors in EERM initialization, EERM/CD/DVD/ISO creation, self-extractor creation, user local key creation, and when changing authentication methods for removable media where insufficient entropy (randomness) is available at the point of key generation. To avoid this, ensure that you connect to a network with sufficient network activity to allow entropy generation.

### Installing the client package in FIPS mode

The EEFF client need to be deployed in FIPS mode to operate in a FIPS-certified manner. Deploy EEFF on the client in one of these ways:

- Using an EEFF deployment task — make sure to add the keyword `FIPS` on the task command line in McAfee ePO.
- Using third-party deployment software — make sure to pass the parameter `FIPS_MODE=1` when you install the EEFF client package, as per the following command:
  - 32-bit system — `msiexec.exe/q/i eeff32.msi FIPS_MODE=1`
  - 64-bit system — `msiexec.exe/q/i eeff64.msi FIPS_MODE=1`

The above guidelines apply only to a clean installation of EEFF in FIPS mode. If EEFF is already installed and you want to upgrade to this version of EEFF and install in FIPS mode, see McAfee KnowledgeBase article 78872.

For details on uninstalling client packages, see *Uninstalling EEFF*.

### Uninstall EEFF

If you need to uninstall EEFF, you must uninstall the client from managed systems, using McAfee ePO or a command, and remove the extension and software package from the McAfee ePO server.

#### Use McAfee ePO to uninstall EEFF from managed systems

You can create a task in McAfee ePO to uninstall EEFF from managed systems in the System Tree.

Any encrypted files should be decrypted prior to uninstallation. Encrypted files remain encrypted following uninstallation.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu** | **Policy** | **Client Task Catalog**, select **McAfee Agent** | **Product Deployment** as Client Task Types, then click **Actions** | **New Task**.
2. Set these options for the new task:
   a. Make sure that **Product Deployment** is selected, then click **OK**
   b. In the **Name** field, enter the name for the task.
   c. From the **Target Platforms** drop-down list, select **Windows**.
   d. From the **Products and components** drop-down list, select **McAfee Endpoint Encryption for Files and Folders**.
e As the **Action**, select **Remove**.

f Select an appropriate **Language**.

g Next to **Options**, specify if you want to run this task for every policy enforcement process (Windows only).

3 Click **Save**.

4 Click **Menu**: Systems | System Tree | Assigned Client Tasks, then select the required group in the **System Tree**.

5 Select the **Preset** filter as **Product Deployment (McAfee Agent)**. Each assigned client task per selected category appears in the details pane.

6 Click **Actions**: New Client Task Assignment to open the **Client Task Assignment Builder** wizard.

7 Set these options:
   a On the **Select Task** page, select as **McAfee Agent** as **Product** and **Product Deployment** as **Task Type**, then select the task you created for deploying the product.

   b Next to **Tags**, select the appropriate option, then click **Next**:
      - **Send this task to all computers**
      - **Send this task to only computers that have the following criteria** — Use one of the edit links to configure the criteria.

   c On the **Schedule** page, select whether the schedule is enabled, specify the schedule details, then click **Next**.

8 Review the summary, then click **Save**.

### Remove the EEFF extension
Remove the EEFF extension from the McAfee ePO server. For option definitions, click ? in the interface.

#### Task
1 Log on to the McAfee ePO server as an administrator.

2 Click **Menu**: Software | Extensions. The **Extension** page displays the extension name and version details.

3 Select the **Endpoint Encryption for Files and Folders** extension file, then click **Remove**. The **Remove extension** confirmation page appears.

4 Select **Force removal, bypassing any checks or errors** to force product extension removal, then click **OK**.

### Remove the EEFF software package
Remove the EEFF software package from the McAfee ePO server. For option definitions, click ? in the interface.

#### Task
1 Log on to the McAfee ePO server as an administrator.

2 Click **Menu**: Software | Master Repository. The **Packages in Master Repository** page displays the list of software packages and their details.
3. Click **Delete** next to the EEFF package.

4. When prompted to confirm, click **OK**.

**Use Shell command to uninstall EEFF from managed systems**

You can uninstall EEFF from a managed system using the **MfeFfShell** command.

**Task**

1. At the command prompt, navigate to the folder where EEFF was installed. The default location is:

   \[SYSDRIVE\]:\Program Files\McAfee\Endpoint Encryption for Files and Folders

2. Run the following command:

   ```shell
   MfeFfShell.com -force_uninstall
   ```

   You are prompted to restart the system after uninstallation.

**Use MSI to uninstall EEFF from managed systems**

You can uninstall EEFF from a managed system using MSI.

**Task**

1. At the command prompt, navigate to the folder where EEFF MSI is available. The default location is:

   ```shell
   [LOCAL APPDATA]\McAfee\Common Framework\Current\EEFF_4000\Install\0000
   ```

   [LOCAL APPDATA] depends on your operating system:
   
   - Windows XP and Windows 2003 -- C:\Document and Settings\All Users
   - Windows Vista, Windows 2008, and Windows 7 -- C:\ProgramData

2. Run the following commands to uninstall EEFF:

   ```shell
   msiexec /q /norestart /I eeff[XX].msi
   msiexec /q /x eeff[XX].msi
   ```

   [XX] — 32 for 32-bit operating systems and 64 for 64-bit operating systems

   You are prompted to restart the system after uninstalling the software.

---

**Removable media registry controls**

EEFF defines removable media as a drive, with the exception of boot drive and remote drives. This might be a concern for client systems having built-in extra drives, for example, an extra hard drive with a .zip drive. These drives are subject to removable media encryption.

**Broaden the removable media definition**

EEFF allows you to broaden the removable media definition to include USB drives and FireWire drives, or drives that report themselves as removable to the operating system. The removable media
definition is broadened by adding a registry value on the client computer. In EEFF, the value is configured by default to 1.

**Task**

1. On the client system, create a DWORD registry value in `HKLM\System\CurrentControlSet\Services\MfeEEFF` called `RelaxedRemovableMediaDefinition`.

2. Set the registry value as needed.
   - 0 — Default definition (same as not having this registry value)
   - 1 — Only disks reported as Removable or located on the USB or IEEE 1394 (FireWire) port
   - 2 — Only disks reported as Removable

   Restart the system to save the changes.

**Exempt local drives and network shares from encryption**

You can exclude local drives and network drives from encryption by adding a registry value on the client. Setting this registry value makes the EEFF driver not attach to local and network drives, but only to removable media drives and CD/DVD drives.

**Task**

1. On the client system, create a DWORD value in `HKLM\System\CCS\Service\MfeEEFF` called `ExemptNonRemovable` and set its value to 1.

2. Restart the system to save the changes.

It fails to encrypt the file on the local drive, but encrypts the same file on a removable drive.

- This registry value must be manually set on each client system. It can also be remotely distributed with a systems management tool.
- When enabled, it is not possible to read (decrypt) any existing encrypted files on local drives or network shares.

**Best practices for large-scale deployment**

A large-scale deployment is any deployment with 1,000 or more users.

Consult your McAfee Endpoint Encryption support representative if you have special considerations for your environment.

**Key caching**

We recommend that you make use of the encryption key caching feature whenever possible. Key caching helps reduce the communication payload on the McAfee Agent to McAfee ePO.

- In some cases, key caching might not be possible based on security policy or other restrictions.

**Tuning encryption intensity for network**

When encrypting large folders on a network share through a policy, we recommend that you tune the network encryption intensity.

Configure these values to tune the network encryption intensity:
Additional information
Best practices for large-scale deployment

- I/O Utilization: 30% (Set in the Encryption options policy)
- Bandwidth limit: 100 KB/sec. (Set in the Network policy)
- Network latency: 600 ms. (Set in the Network policy)
- Maximum number of clients to encrypt folders: 10

You can limit the size of the files to be encrypted (Set in the Encryption options policy).

**Explicitly encrypting large shares in advance**

Use a manual (explicit) encryption method for large network folders encryption, rather than encrypting them through a folder encryption policy.

Initiate the encryption from a single machine, after logging on with an appropriate EEFF user, then let the encryption run (maybe overnight).

The reason is to avoid extreme payload on the file servers from many clients seeking to enumerate, fetch, encrypt, and upload files to/from the servers. This reduces the risk of network failure and file server payload overflow is minimized.

**Excluding the EEFF client program directory**

No matter which anti-virus solution is used on the clients, we recommend that you exclude the EEFF program directory from real-time anti-virus scanning.

By default, the EEFF program directory is [SYSDRIVE]\Program Files\McAfee\Endpoint Encryption for Files&Folders.

Typically, most anti-virus solutions can be policy controlled to exclude certain directories from real-time scanning. Consult the operating manuals for your anti-virus solution for further details.
Index

A
about this guide 5
audit log 50

B
best practices
  exclusion of EEFF client program directory 56
  explicit encryption of large shares 56
  key caching 55
tune encryption intensity 55

C
CD/DVD encryption 20
client program directory 56
conventions and icons used in this guide 5
custom queries 46

D
deployment, installing products 12
DNS settings 11
documentation
  audience for this guide 5
  product-specific, finding 6
typographical conventions and icons 5

E
EEFF client 7
EEFF policies
  assign to managed system 25
  creating from Policy Catalog 24
  editing, from Policy Catalog 24
  enforcing on a system 26
  enforcing on a system group 26
encryption keys 33
  about 33
  activating and deactivating 34
  creating 33
  deleting 35
  editing 35
  exporting 35
  importing 36
  importing from EEFF 36

F
encryption keys 33 (continued)
  importing from EEM 36
encryption, persistent 7
enforcement, See policy enforcement
exclusion of EEFF client program directory 56
explicit encryption of large shares 56
extension, EEFF
  FIPS mode 51
  help 11
  installing 11
  removing from ePO 53
features 8
file encryption 16
FIPS certification 51
FIPS mode
  client package deployment 52
  impact 51
  prerequisites 51
floppy disks, policy settings 18
folder encryption 16

G
Grant Key
  multi-slot policy 28–30
  viewing effective 30
Grant Key policy
  assigning keys 34
  assigning multiple instances 30
  assigning multiple instances to systems 29
  assigning personal key to user 37
  assigning to systems 28
  multi-slot 27
  personal keys 37
  settings 22
  viewing effective policy 30
groups
  policy enforcement for a product 26

H
Help extension 11
I
installation, EEFF
  checking in software package 10
  deploying to managed systems 12
  product extension 11
  requirements 9

K
key caching 55
key server permissions 44
keys
  activating 34
  assigning to policy 34
  assigning user personal 37
  creating 33
  deactivating 34
  deleting 35
  editing 35
  exporting 35
  importing 36
  importing from EEFF 36
  importing from EEM 36
  regular 33
  role-based management 39
  usage 41
  user local 33
  user personal 33

L
LDAP servers, registering 11
local keys 33
  policy settings 23

M
managed systems
  assigning EEFF policy 25
  assigning policy to 25
  deploying EEFF on 12
  policy management on 16
  uninstalling EEFF 52
  uninstalling EEFF with Shell command 54
  uninstalling EEFF, with MSI 54
master repository
  checking in software package 10
McAfee ServicePortal, accessing 6
MSI, using to uninstall EEFF 54
multi-slot policy 27
  assigning 28
  Grant Key 28
multiple instance policy
  assigning to systems 28, 29
  assigning to users 30

N
network settings 22

O
operating system requirements 9

P
password rule settings 23
permission sets, EEFF
  about 43
  creating 43
  key management 44
  policy settings 43
  role assignment 40
persistent encryption 7
personal keys 33
policies
  about 16
  assigning to system groups 25
  assigning to systems 25
  configuring 15
  create on Policy Catalog page 24
  editing, from Policy Catalog 24
  enforcement 15
  key usage 41
  multi-slot 28
  viewing 16
policy assignment rules
  about 27
  create 28
  multi-slot policy 27
  priority 27
Policy Catalog
  creating EEFF policies 24
  editing EEFF policies 24
  page, viewing 16
policy categories
  encryption options 21
  exclusions 21
  network 22
  password rules 23
policy enforcement
  enabling and disabling 26
  for a product 26
  on a system group 26
policy inheritance
  break inheritance 28
  lock 25
policy settings
  CD/DVD encryption 20
  file encryption 16
  folder encryption 16
  general 16
  grant keys 22
Index

policy settings (continued)
integration 16
removable media 18
user local keys 23
product installation
configuring deployment tasks 12

Q
queries
about 45
custom, creating 46
exported results 45
Query Builder wizard 46
viewing results 47

R
recovery of user personal keys 38
registered servers
LDAP servers, adding 11
regular keys 33
creating 33
removable media
broaden the definition 54
exempt local drives from encryption 55
policy settings 18
registry controls 54, 55
reports
about 45
formats 45
viewing 47
requirements 9
role-based key management
about 39
adding roles 39
deleting roles 40
editing roles 39
roles
adding 39
assigning to permission set 40
deleting 40
editing 39
global administrator 39
rules
policy assignment, creating 28
rules (continued)
priority 27
S
self-tests, FIPS mode 51
servers
LDAP servers, registering 11
McAfee ePO 11
requirements 9
ServicePortal, finding product documentation 6
Shell command, using to uninstall EEFF 54
software package
removing 53
software packages
checking in 10
software requirements 9
system groups, policy enforcement 26
system requirements 9
systems
assigning policies to 25
effective policies 30
policy enforcement for a product 26
T
Technical Support, finding product information 6
tune encryption intensity 55
U
USB devices, policy settings 18
user accounts
effective policy 30
permission sets 43
user personal keys
about 37
best practices 37
creating 37
enabling 37
Grant Key 37
recovering 38
W
Windows Active Directory 11