Product Guide

McAfee File and Removable Media Protection 5.0.2
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.
## Preface

About this guide .................................. 5
Audience .................................. 5
Conventions .................................. 5

## Introduction

How FRP works ................................... 7
Features ...................................... 8

## Installing the FRP client

Requirements .................................... 9
Deploy McAfee Agent for Mac through SSH ....................... 10
  Deployment and activation - best practices ........................ 11
Install the FRP and Help extensions .................... 12
Check in the FRP software package .................. 12
Deploy FRP to managed systems .................... 12
Send an agent wake-up call ......................... 13
Install FRP from the command line .................... 14

## FRP key authentication: Encryption key access

Enable the FRP key authentication server settings .................... 15
Configure FRP key authentication ........................... 16
User Token Recovery ................................ 18
Force credential change .................................. 18

## Managing FRP keys

Encryption keys .................................. 21
Create an encryption key ................................ 21
Activate or deactivate the encryption keys .................. 22
Edit an encryption key ................................ 22
Delete an encryption key ................................ 23
Export encryption keys ................................ 23
Import keys ..................................... 24
  Import keys from EEFF or FRP ......................... 24
  Import keys from EEM ................................ 24
Assign an encryption key ................................ 24
  Assign user personal keys to users or user groups ........... 25
  Assign regular keys to systems ....................... 25
  Assign regular keys to users or user groups ............. 26
View key usage .................................. 27
How user personal keys work ......................... 27
Convert a user personal key into a regular key ............ 27
Role Based Key Management ............................. 28
  How Role Based Key Management works ................. 28
  Add a role .................................... 28
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit a role</td>
<td>28</td>
</tr>
<tr>
<td>Delete a role</td>
<td>29</td>
</tr>
<tr>
<td>Assign a role to a permission set</td>
<td>29</td>
</tr>
<tr>
<td><strong>5 Configuring FRP policies</strong></td>
<td>31</td>
</tr>
<tr>
<td>FRP policy settings</td>
<td>31</td>
</tr>
<tr>
<td>Application-based Protection</td>
<td>31</td>
</tr>
<tr>
<td>Authentication</td>
<td>32</td>
</tr>
<tr>
<td>Encryption Options</td>
<td>36</td>
</tr>
<tr>
<td>General</td>
<td>37</td>
</tr>
<tr>
<td>Location-based Protection</td>
<td>37</td>
</tr>
<tr>
<td>Network</td>
<td>38</td>
</tr>
<tr>
<td>Optical Media</td>
<td>39</td>
</tr>
<tr>
<td>Removable Media</td>
<td>40</td>
</tr>
<tr>
<td>User Local Keys Options</td>
<td>43</td>
</tr>
<tr>
<td>Create a policy</td>
<td>44</td>
</tr>
<tr>
<td>Edit the FRP policy settings</td>
<td>44</td>
</tr>
<tr>
<td>Assign a policy to a managed system</td>
<td>45</td>
</tr>
<tr>
<td>Assign a policy to a system group</td>
<td>45</td>
</tr>
<tr>
<td>Enforce FRP policies on a system</td>
<td>46</td>
</tr>
<tr>
<td>Enforce FRP policies on a system group</td>
<td>46</td>
</tr>
<tr>
<td>How policy assignment rules work</td>
<td>47</td>
</tr>
<tr>
<td>Policy assignment rule priority</td>
<td>47</td>
</tr>
<tr>
<td>Working with policy assignment rules</td>
<td>48</td>
</tr>
<tr>
<td>Policy assignments - best practices</td>
<td>48</td>
</tr>
<tr>
<td><strong>6 Defining FRP permission sets for McAfee ePO users</strong></td>
<td>49</td>
</tr>
<tr>
<td>Create permission sets for user accounts</td>
<td>49</td>
</tr>
<tr>
<td>Edit the FRP policy permissions</td>
<td>49</td>
</tr>
<tr>
<td>Edit the FRP key server permissions</td>
<td>50</td>
</tr>
<tr>
<td>Edit recovery permission set</td>
<td>50</td>
</tr>
<tr>
<td><strong>7 Managing FRP reports</strong></td>
<td>51</td>
</tr>
<tr>
<td>FRP queries and query results</td>
<td>51</td>
</tr>
<tr>
<td>Create FRP custom queries</td>
<td>52</td>
</tr>
<tr>
<td>View standard FRP queries</td>
<td>53</td>
</tr>
<tr>
<td>FRP client events</td>
<td>54</td>
</tr>
<tr>
<td>View audit log</td>
<td>57</td>
</tr>
<tr>
<td><strong>A Additional information</strong></td>
<td>59</td>
</tr>
<tr>
<td>FIPS certification</td>
<td>59</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>59</td>
</tr>
<tr>
<td>Impact of FIPS mode</td>
<td>59</td>
</tr>
<tr>
<td>Installing the client package in FIPS mode</td>
<td>60</td>
</tr>
<tr>
<td>Uninstall FRP</td>
<td>60</td>
</tr>
<tr>
<td>Use McAfee ePO to uninstall FRP from managed systems</td>
<td>60</td>
</tr>
<tr>
<td>Remove the FRP extension</td>
<td>61</td>
</tr>
<tr>
<td>Remove the FRP software package</td>
<td>61</td>
</tr>
<tr>
<td>Use Shell command to uninstall FRP from managed systems</td>
<td>62</td>
</tr>
<tr>
<td>Use MSI to uninstall FRP from managed systems</td>
<td>62</td>
</tr>
<tr>
<td>Removable media registry controls</td>
<td>62</td>
</tr>
<tr>
<td>Broaden the removable media definition</td>
<td>62</td>
</tr>
<tr>
<td>Exempt local drives and network shares from encryption</td>
<td>63</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>65</td>
</tr>
</tbody>
</table>
Preface

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

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.

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

*Bold*  
Text that is emphasized

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

*Narrow Bold*  
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:* Extra information to emphasize a point, remind the reader of something, or provide an alternative method

*Tip:* Best practice information

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

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

McAfee® File and Removable Media Protection (FRP) delivers policy-enforced, automatic, and transparent encryption of files and folders stored or shared on PCs, file servers, cloud storage services, emails, and removable media such as USB drives, CD/DVDs, and ISO files. FRP provides support for Removable Media initialization for Mac client systems.

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

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

Contents

- How FRP works
- Features

How FRP works

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

FRP supports system and user-based policies, and provides a single point of control to protect data in your environment by integrating with the McAfee ePO server. Access to encryption keys is based on authentication mechanism that the administrator has configured.

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

FRP acts as a persistent encryption engine for operations performed through Windows File Explorer. 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.
Features

These are the key features of FRP.

- **Centralized management** — Provides support for deploying and managing FRP using McAfee ePO software.

- **User Personal Key** — A unique encryption key is created for each user; administrators can reference “user personal key” generically in policies.

- **Delegated administration through Role Based Key Management** — Enables the logical separation of management between multiple administrators. This capability is critical for separation across business functions and subsidiaries.

- **Auditing of key management and policy assignments** — The key management and policy assignment-related actions performed by McAfee ePO administrators are recorded in the Audit Log. This is critical to ensure compliance and prevent abuse by privileged administrators.

- **Protection of data on removable media** — Enables encryption of removable media and access to encrypted content even on systems where FRP is not installed.

- **Protection of data (including auditing and reporting) for cloud storage services** — Enables encryption of sync folders on PCs for Dropbox, Box, Google Drive, and OneDrive. It also provides secure access to encrypted files on mobile devices using McAfee Endpoint Assistant application.

- **Network encryption** — Enables secure sharing and collaboration on network shares.

- **User-initiated encryption of files and email attachments** — Allows users to create and attach password-encrypted executable files that can be decrypted on systems where FRP is not installed.

- **Auditing and reporting for USB removable media and CD/DVD/ISO events** — Captures all end-user actions related to USB removable media and CD/DVD/ISO events. The auditing capability provides an effective feedback loop for use by administrators in making policy decisions.

- **Integration with the McAfee tray icon** — Consolidates the tray icons into one common McAfee icon.

- **Use of McAfee Common Cryptographic Module (MCCM)** — The FRP client uses the McAfee Core Cryptographic Module (MCCM) User and Kernel FIPS 140-2 cryptographic modules. FRP provides an option to install the product in FIPS mode. MCCM also provides performance benefits and leverages Intel® Advanced Encryption Standard Instructions (AES NI), resulting in additional performance improvements on systems with AES NI support.
Installing the FRP client

The FRP 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
- Deploy McAfee Agent for Mac through SSH
- Install the FRP and Help extensions
- Check in the FRP software package
- Deploy FRP to managed systems
- Send an agent wake-up call
- Install FRP from the command line

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: 200 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>
<tbody>
<tr>
<td>McAfee management software</td>
<td>McAfee ePolicy Orchestrator 5.1.0 (and above) or 5.3.0</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>• McAfee Agent for Windows 4.8 Patch 1 or above</td>
</tr>
<tr>
<td></td>
<td>• McAfee Agent for Mac 4.8 Patch 3 or above</td>
</tr>
</tbody>
</table>
Table 2-2  Software requirements (continued)

<table>
<thead>
<tr>
<th>Software (or package name)</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| File and Removable Media Protection | Extensions
• FRP-extension-5.0.2.xxx.ZIP
• help_eeff_502.ZIP

Software packages
• MfeFRP_Client_5.0.2.xxx.ZIP for Windows systems
• MfeFRP_Client_O SX_5.0.2.xxx.ZIP for Mac systems

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>
| Windows client systems | • Microsoft Windows 10 (32-bit and 64-bit)
• Microsoft Windows 8.1 (32-bit and 64-bit)
• Microsoft Windows 8 (32-bit and 64-bit)
• Microsoft Windows 7 SP 1 (32-bit and 64-bit) |

For the latest information on supported platforms, environments, and operating systems, refer to the KnowledgeBase article KB81149.

| Mac OS X client systems | • El Capitan 10.11.0
• Yosemite 10.10.0 or above
• Mavericks 10.9.0 or above |

| Virtual Desktop Infrastructure (VDI) | • Citrix XenDesktop 5.6
• Citrix XenDesktop 7.1 |

Refer to KB81478 for the latest information on support for VDI environments, including installation details and constraints that apply such as supported modes of operation.

Deploy McAfee Agent for Mac through SSH

You can deploy McAfee Agent for Mac to client systems through Secure Shell (SSH).

**Before you begin**

To deploy McAfee Agent for Mac to your system, you must enable SSH (remote login). SSH can be enabled on your Mac system by enabling the Remote Login option under System Preferences | Sharing | Remote Login.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click Menu | Systems | System Tree | Actions | New Systems.
3 Select the required option from How to add systems.

4 Select Push agents and add systems to the current group (My Organization).

5 In the Target systems field, add the IP address of the system where you want to deploy the McAfee Agent.

6 In the Agent version field, select Non-Windows, then select McAfee Agent for Mac from the drop-down list.

7 In the Credentials for agent installation field, enter administrator credentials of the Mac.

8 Click OK to trigger the McAfee Agent deployment on the Mac system.

To view the deployment status, click Menu | Automation | Server Task Log.

**Deployment and activation - best practices**

This section provides general recommendations for the deployment of FRP.

**Client operating systems**

- **Verify operating system support** — Make sure that the client operating system, including service pack levels, is officially supported. For details, see KB81149.

- **Prevent deployment to non-supported client operating systems** — Use McAfee ePO to prevent deployments to unsupported operation systems such as Windows XP 64 bit and Windows Vista 64 bit. McAfee ePO together with McAfee® Agent will ensure that the FRP client is run only on endpoints with supported operating systems.

**VDI environments**

For the latest information on support for VDI environments, including installation details and applicable constraints, see KB81478.

**Deployment using third-party tools**

You can manually install FRP locally or in conjunction with a third-party deployment tool using the command line interface.

To upgrade from McAfee® Endpoint Encryption for Files and Folders, you must first uninstall the existing version. You must install a supported version of McAfee Agent before using the command line method.

The specific command depends on the operating system:

- **32-bit operating system**: msiexec.exe /q /i eeff32.msi
- **64-bit operating system**: msiexec.exe /q /i eeff64.msi

After executing the command line instruction, you must restart the client to complete the installation procedure. For details on installing FRP from the command line, see KB81433.

- Deployment through McAfee ePO is the recommended approach.

**Encryption key deployment**

Initial key delivery following deployment to a large number of client systems can subject the Tomcat process on the McAfee ePO server to high load, as it has to process secure data channel messages to and from the client. To reduce the risk of overloading the Tomcat process, adopt a phased deployment strategy so that the key delivery can be evenly distributed. Although the number of systems that can be supported consecutively depends on a number of factors (server performance, number of keys 


granted to each client, whether database is local to McAfee ePO server, and so on), we recommend starting at 100 systems per hour and monitoring the load. Alternatively, consult McAfee Professional Services to determine the optimal rate for your environment.

## Install the FRP and Help extensions

Install the product and Help extensions to the McAfee ePO server.

The FRP extension contains the product settings that must be enforced onto the client systems. The Help extension contains the Help content for the options in the user interface that appear when you click ? in the user interface.

**Task**

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu | Software | Extensions | Install Extension**.
3. For each extension file, click **Browse**, select it, then click **OK**.
   a. FRP-extension-5.0.2.xxx.ZIP
   b. help_eeff_502.ZIP

   The Install Extension page displays the extension name and version.
4. Click **OK**.

## Check in the FRP 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 your client systems.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu | Software | Master Repository**, then click **Actions | Check In Package**.
3. On the **Package** page, select the **Package type** as **Product or Update (.ZIP)**, click **Browse** to locate the MfeFRP_Client_5.0.2.xxx.ZIP software package for Windows systems and/or MfeFRP_Client_OSX_5.0.2.xxx.ZIP software package for Mac systems, then click **Next**.
4. On the **Package Options** page, click **Save**.

   The new package appears in the **Packages in Master Repository** page under the respective branch in the repository.

## Deploy FRP to managed systems

You can use McAfee ePO to create tasks to deploy FRP to a single system, or to groups in the **System Tree**.
Task
For details about product features, usage, and best practices, click ? or Help.

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 or Mac.
   d From the Products and components drop-down list, based on the target platform selected in the previous step, select File and Removable Media Protection for Windows systems or File and Removable Media Protection - OS X for Mac systems.
   e As the Action, select Install.
   f Select an appropriate Language.
   g (Optional) To deploy FRP 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 FRP is deployed on the managed systems.

Send an agent wake-up call
The client system gets the policy update whenever it connects to the McAfee ePO server during the agent-server communication. However, you can force an immediate update with an agent wake-up call.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Systems | System Tree, then select a system or a group of systems from the left pane.
3. Select the System Name of that group.
4. Click Actions | Agent | Wake Up Agents.
5. Select a Wake-up call type and a Randomization period (0-60 minutes) to define the length of time when all systems must respond to the wake-up call.
6. Under Options, select Get full product properties.
8. Click OK.

To view the status of the agent wake-up call, navigate to Menu | Automation | Server Task Log.

Install FRP from the command line

Use the following command line instruction to manually install FRP, either locally or in conjunction with a third-party deployment tool. To upgrade from an earlier version of EEFF, you must first uninstall the existing version by following the instructions in the Additional Information section.

You must install a supported version of McAfee Agent before using the command line method. For more information about supported versions, see KB81149.

Table 2-4 Installation command

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported 32-bit system</td>
<td>msiexec.exe /q /i eeff32.msi</td>
</tr>
<tr>
<td>Supported 64-bit system</td>
<td>msiexec.exe /q /i eeff64.msi</td>
</tr>
</tbody>
</table>

After executing the command line instruction, you must restart the client to complete the installation procedure.

For more information about installing FRP from the command line, see KB81433.
FRP key authentication: Encryption key access

Encryption keys can be assigned to either systems or users. User assigned keys can either be associated with OS token or FRP password token.

**OS authentication**

Keys associated with OS authentication are available for users who have successfully logged on to Windows client as a domain user. The user experience is similar to Windows logon authentication mechanism used in previous versions of EEFF/FRP 4.x for access to encryption keys.

McAfee ePO administrator has the flexibility to mandate that the user authenticates using the Active Directory user name and password for the first time the OS token is used on a given Windows system. This can be configured from the **OS Token** tab of the **Authentication** policy.

Customers upgrading from previous versions of EEFF/FRP 4.3 are advised to enable the Windows logon unlock trigger to preserve end user experience. This can be configured on the **Encryption Key Options** tab of the **Authentication** policy.

**FRP Password authentication**

Keys associated with Password authentication are available for users who authenticate with proprietary FRP password credentials.

**Contents**

- Enable the FRP key authentication server settings
- Configure FRP key authentication
- User Token Recovery
- Force credential change

---

Enable the FRP key authentication server settings

To enable FRP key authentication, navigate to the **Server Settings** page.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu | Configuration | Server Settings**.
3. In the **Setting Categories** pane, click **FRP Key Authentication Settings**, then click **Edit** to open the **Edit FRP Key Authentication Settings** page.
4 Select the **Enable FRP Key Authentication** option to enable upgrade to the FRP Key Authentication module.

Make appropriate selections on the authentication options available. For more information about these options, refer to the *Configure FRP key authentication* topic.

5 Click **Save**.

---

### Configure FRP key authentication

Options related to FRP key authentication are configured on the **Server Settings** page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable FRP Key</td>
<td>Select this option to enable upgrade to the FRP step-up authentication functionality.</td>
</tr>
<tr>
<td>Authentication</td>
<td>This is a configurable option that is available only for users upgrading from EEFF 4.x.x and FRP 4.3.x. For new installations, this option is enabled by default. Also, this option cannot be disabled after it has been enabled.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Password Token Initialization Method** | • Email (Custom Email message) — Sends the configured text to the user's email together with a random-generated password.  
  - The email server must be configured in the McAfee ePO server settings.  
  - Ensure that the Active Directory includes the email attribute. If the email attribute is not available and this setting is selected for password token initialization, users must be led through a token recovery process.  
  • Password (Default) — Assigns a default password when keys are assigned to the user's password token for the first time. The user will be forced to change this password on first logon. This is the default initialization method.  
  - Change default password — Select this option to change the default password with a more secure initialization password, then enter a new password in the Password and Confirm fields.  
  • No Password — Forces the user to setup a new password. |
| **Smart card** | • Certificate Revocation List  
  - Enable Certificate Revocation List processing — Select this option to maintain a list of certificates that have been revoked, and therefore, users presenting those (revoked) certificates will no longer be allowed to logon using their smart card.  
  - Certificate Revocation List URL — The URL where the Certificate Revocation List is maintained.  
  - Delta Certificate Revocation List URL — The URL where changes in the Certificate Revocation List are monitored.  
  - Note that smart card authentication is not supported out of the box. If you require smart card authentication, raise a PER with relevant details. |
| **Token Recovery** | • Generate random passwords — Generates random passwords for use in the recovery process.  
  - This option is automatically enabled and can't be disabled.  
  • Generate simple passwords — Generates simple random passwords, which are easier to read out to the end user. Default value is enabled.  
  - It is recommended to disable this option if you enable the Send recovery password by Email option.  
  • Send recovery password by Email — Sends the recovery password to the email address configured for the user.  
  - Recovery by email requires that the McAfee ePO email server settings be configured and that Active Directory contain the user's email address.  
  • Smart card recovery token settings  
  - Expire after __ logon attempts (1-60) — Sets the number of valid logon attempts after which the smart card recovery token expires.  
  - Expire after __ days (1-366) — Sets the time period (in days) after which the smart card recovery token expires.  
  - Warn after __ days (1-366) — Sets the time period (in days) after which a warning is displayed that the smart card recovery token is about to expire. |
### User Token Recovery

When users forget their FRP password authentication credential details, they are given a recovery code and instructed to contact the McAfee ePO administrator.

**Before you begin**

You must have administrator rights to perform this task, and your FRP Recovery permission set must be set to Manage Recovery.

The user can initiate the recovery process from the FRP client console under Authentication by selecting Recovery. A recovery code is displayed in the FRP client. The user is instructed to read out the recovery data to the administrator.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, click Menu | Data Protection | FRP Recovery.

2. On the User Token Recovery tab, in the Recovery Code field, enter the recovery data provided by the end user.

   The user's display name, email address, account details, and token type are displayed to enable verification of the caller's identity.

3. Click Recover to generate a new response code.

4. Instruct the user to click OK in the pop-up message on the client. Read out the temporary credential details to the end user, or the credentials will be mailed to the user automatically if configured. The user can then use those temporary credentials to log on and reset the authentication password.

### Force credential change

You can force users or groups to change the FRP password used for authentication.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Data Protection | FRP User Actions.

2. In the User Selection area, browse to locate and select specific users or groups.

3. From the User Action Types drop-down list, select Force Credential Change, then click OK.
4 In the User Selection area, browse to locate and select specific users or groups, then select the token type. The selected users or groups are prompted to change their passwords the next time they log on.

5 To cancel the Force Credential Change action, from the User Action Types drop-down list, select Remove all user actions, then click OK.
FRP key authentication: Encryption key access
Force credential change
Managing FRP keys

FRP uses encryption keys to protect files and folders on PCs, file servers, cloud storage services, emails, and removable media such as USB drives, CD/DVDs, and ISO files.

Contents
- Encryption keys
- Create an encryption key
- Activate or deactivate the encryption keys
- Edit an encryption key
- Delete an encryption key
- Export encryption keys
- Import keys
- Assign an encryption key
- View key usage
- How user personal keys work
- Convert a user personal key into a regular key
- Role Based Key Management

Encryption keys
An administrator can create and manage encryption keys from McAfee ePO on the FRP keys page. These keys can be assigned to users and/or systems.

Key types
FRP supports encryption using three types of keys:
- **Regular keys** — Created by McAfee ePO administrators and can be used in any policy.
- **User personal keys** — User personal keys is a per user unique encryption key generated in McAfee ePO when assigned to users. When a user is assigned a user personal key, the user can use this unique key on any FRP system managed by the same McAfee ePO.
- **User local keys** — Created by the user using the FRP client software on a client system. The user can use these keys to encrypt or decrypt data. These keys are never backed up in McAfee ePO.

Create an encryption key
You can create a regular encryption key, with or without an expiry date.
Task
For details about product features, usage, and best practices, click ? or Help.

1 Click Menu | Data Protection | FRP 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, choose an appropriate role from the Roles drop-down list. If you do not select a role or do not use Role Based Key Management, all McAfee ePO administrators will have access to the created key based on key server permission configuration. Only roles assigned to the logged on McAfee ePO user are available for selection. The key is accessible only to McAfee ePO users who are assigned a selected role.

6 Click OK.

The new key is available for inclusion in FRP policies.

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

Task
For details about product features, usage, and best practices, click ? or Help.

1 Click Menu | Data Protection | FRP keys.

2 Select the keys to activate, then click Actions | Activate Keys.

To deactivate keys, select the keys, click Actions | Deactivate Keys, then click OK.

When an encryption key is deactivated, it is removed from the client systems during the next policy update. When an encryption key is re-activated, it is made available on the client systems during the next policy update/key synchronization.

Edit an encryption key
You can edit properties of an existing encryption key.

Task
For details about product features, usage, and best practices, click ? or Help.

1 Click Menu | Data Protection | FRP 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 even if a key has been removed from all policies. Files that are already encrypted with a deleted key will be inaccessible and cannot be deleted from FRP systems.

**Task**

For details about product features, usage, and best practices, click ? or **Help**.

1. Click **Menu** | **Data Protection** | **FRP keys**.
2. Select the keys to delete, then click **Actions** | **Delete Keys**.
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 details about product features, usage, and best practices, click ? or **Help**.

1. Click **Menu** | **Data Protection** | **FRP keys**.
2. Select the keys to export, then click **Actions** | **Export Keys**.
3. Enter and confirm the password to be used to protect the exported file, then click **OK** to open the **Export Keys for FRP** page.
4. Click the .bin file and save it to the required location.
5. Click **Close**.

- It is recommended that this exported file be protected with a strong password that contains a combination of upper and lower case characters, digits, and special characters.

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 EEFF or FRP. The ability to import information related to Role Based Key Management depends on the version of EEFF or FRP, and how the key data is exported.

Import keys from EEFF or FRP

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

Key data exported from EEFF 4.0.x or 4.1.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.x or FRP 4.3.0 or later 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.

Task

For details about product features, usage, and best practices, click ? or Help.

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

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

Import keys from EEM

You can import keys from EEM 5.2 or later. For detailed instructions, refer to the McAfee File and Removable Media Protection 5.0.2 Migration Guide.

Assign an encryption key

You can assign a regular key to systems or users. However, you can assign a user personal key only to users or user groups.

On the FRP Keys page, under the Usage column, click Show for the required encryption key to view the user/system assignment, key type, and authentication method details.

Make sure to note that the lock trigger for Windows systems does not unload the system keys.
Assign user personal keys to users or user groups

You can assign a user personal key only to users, user groups, or organizational units.

Before you begin

Verify that the LDAP task is set up to register the Active Directory server.

Please note that the FRP Upgrade task fails to process user personal keys, on McAfee ePO versions other than 5.1.2 and 5.3, even though the Active Directory server is turned online after being offline. The workaround for this is to restart the services of McAfee ePO (any version) to process the user personal keys.

Task

For details about product features, usage, and best practices, click ? or Help.

1 Click Menu | Data Protection | FRP keys.

2 Actions | Key Assignments | Assign UPKs to assign a user personal key.

3 Assign the user personal key to the user, user group, or organizational unit by selecting from either Users, From the groups, or From the organizational units accordingly.

4 (Optional) Select Recursive to assign the key to subgroups of the selected groups (if applicable).

5 In the Authentication Type area, select either of the following:

- **OS authentication** — To enable users to access assigned keys through operating system authentication.

  McAfee ePO administrator has the flexibility to mandate that the user authenticates using the Active Directory user name and password for the first time that the OS token is used on a given Windows system. This can be configured from the OS Token tab of the Authentication policy.

- **Password authentication** — To enable users to access assigned keys through password authentication.

6 Click OK.

The key assignment is processed as a task. You can view the task progress in the McAfee server task log. This task is automated and runs immediately after key assignment. If this task is not successfully run immediately after key assignment, it is run as part of the daily FRP Process key assignments task or when the task is run manually.

When the key assignment task is complete, the key is available to users or user groups. The key assignment process can be in these states:

- **Pending Processing** — In the queue or being prepared for processing.

- **Processing in Progress** — Key assignment process is in progress.

- **Processing was Successful** — Keys are available to the assigned users and user groups.

Similar to the key assignment, the key unassignment process can be in these states: Pending Unassignment, Processing Unassignment, and Successfully Unassigned.

Assign regular keys to systems

You can assign a regular key to systems in order to allow users (who have access to that system) get access to the assigned key.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Data Protection | FRP Keys to open the FRP Keys page.
3. Select the key that you want to assign, then click Actions | Key Assignments | Assign to systems.
4. Select the required system or group, then click OK.

System assignment is completed successfully.

---

**Assign regular keys to users or user groups**
To assign regular keys to users, user groups, or organizational units, follow this procedure.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Data Protection | FRP Keys to open the FRP Keys page.
3. Select the key that you want to assign, then click Actions | Key Assignments | Assign to users.
4. Assign the key to the user, user group, or organizational unit by selecting from either Users, From the groups, or From the organizational units accordingly.
5. (Optional) Select Recursive to assign the key to subgroups of the selected groups (if applicable).
6. In the Authentication Type area, select either of the following:
   - **OS authentication** — To enable users to access assigned keys through operating system authentication.
   - **Password authentication** — To enable users to access assigned keys through password authentication.
7. Click OK.

The key assignment is processed as a task. You can view the task progress in the McAfee server task log. This task is automated and runs immediately after key assignment. If this task is not successfully run immediately after key assignment, it is run as part of the daily FRP Process key assignments task or when the task is run manually.

When the key assignment task is complete, the key is available to users or user groups. The key assignment process can be in these states:
• **Pending Processing** — In the queue or being prepared for processing.
• **Processing in Progress** — Key assignment process is in progress.
• **Processing was Successful** — Keys are available to the assigned users and user groups.

Similar to the key assignment, the key unassignment process can be in these states: **Pending Unassignment**, **Processing Unassignment**, and **Successfully Unassigned**.

The enrollment details for McAfee Endpoint Assistant (QR image) is not sent when a key is assigned to a user, who is part of an Organizational Unit (OU).

---

**View key usage**

You can view summary information on FRP key usage on the **FRP Key Management** page, and drill down to view the policies, users/groups, or systems/groups where they are used.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Click **Menu | Data Protection | FRP keys**.
2. Click the **Show** link to view a list of the policies, users/groups, or system/groups where a specific key is used.

The details are listed on the **FRP Key Usage** page.

---

**How user personal keys work**

User personal keys provide the ability to create unique keys for users.

User personal keys are generally used as recovery keys for user local keys and as auto unlock keys for removable media encryption. Assigning a user personal key as the auto unlock key for Removable Media encryption provides a transparent authentication experience to the user who encrypted the removable media.

User personal keys can't be assigned to systems.

---

**Convert a user personal key into a regular 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 details about product features, usage, and best practices, click ? or Help.

1. Click **Menu | Data Protection | FRP keys**.
2. Select the user personal key, then click **Actions | Edit Key**.
3. Select **Available as regular key**, 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.

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 permissions 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 details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Configuration | Server Settings | FRP 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 FRP 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 details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Configuration | Server Settings | FRP 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 details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Configuration | Server Settings | FRP 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.

Task
For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | User Management | Permission Sets, then click Edit next to FRP 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.
5

Configuring FRP 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.

Contents

- FRP policy settings
- Create a policy
- Edit the FRP policy settings
- Assign a policy to a managed system
- Assign a policy to a system group
- Enforce FRP policies on a system
- Enforce FRP policies on a system group
- How policy assignment rules work

FRP policy settings

Policy settings for FRP 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.

Application-based Protection

You can configure encryption policy settings for applications based on their process names on the Application-based Protection 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>Specify the process name of the application as seen in the Windows process explorer to encrypt files created by the application.</td>
</tr>
<tr>
<td>Extensions</td>
<td>Specify the file extensions to be encrypted without a dot such as 'txt', 'doc' and so on 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>Action</td>
<td>Specify the encryption key to be assigned to the policy. Browse to select the key.</td>
</tr>
</tbody>
</table>
**Authentication**
You can define the policy settings for authentication to all FRP modules on the Authentication policy page.

**Password**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Content Requirements</strong>&lt;br&gt;(applicable to both Windows and Mac systems)</td>
<td>Defines the password policy rules for FRP Password Authentication, self-extractors, user local keys, CD/DVD/ISO, and removable media in the FRP client. If the password does not conform to a policy, an error message is displayed in the FRP client detailing the reason and prompting the user to try again.</td>
</tr>
<tr>
<td>• <strong>Minimum Password Length</strong> — Specifies the minimum number of characters (7–40) that must be included in a password. Default value is 7.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Minimum Special Characters</strong> — Specifies the minimum number of special characters (0–15) that must be included in a password. Default value is 0.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Minimum Numeric Characters</strong> — Specifies the minimum number of numeric digits (0–15) that must be included in a password. Default value is 0.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Minimum Alphabetical Characters</strong> — Specifies the minimum number of letters (0–15) that must be included in a password. Default value is 0.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Minimum lowercase characters</strong> — Specifies the minimum number of lowercase letters (0–15) that must be included in a password. Default value is 0.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Minimum uppercase characters</strong> — Specifies the minimum number of uppercase letters (0–15) that must be included in a password. Default value is 0.</td>
<td></td>
</tr>
<tr>
<td><strong>Content Restrictions</strong>&lt;br&gt;(applicable to FRP Password Authentication only)</td>
<td>Defines the password content restrictions that apply to FRP Password Authentication only.</td>
</tr>
<tr>
<td>• <strong>No anagrams</strong> — The password must not contain a word or phrase formed by rearranging the letters of another word or phrase.</td>
<td></td>
</tr>
<tr>
<td>• <strong>No palindromes</strong> — The password must not comprise a string that reads the same backward as forward.</td>
<td></td>
</tr>
<tr>
<td>• <strong>No user name</strong>— The password must not contain the user name.</td>
<td></td>
</tr>
<tr>
<td>• <strong>No simple sequences</strong> — The password must not contain simple sequences (for example, 1234 or abcd) or a sequence based on the previous password.</td>
<td></td>
</tr>
<tr>
<td><strong>Client Display Options</strong>&lt;br&gt;(applicable to FRP Password Authentication only)</td>
<td></td>
</tr>
<tr>
<td>• <strong>Allow user to see typed password</strong> — Enables the user to view the password as it is being typed. This option is disabled by default.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Display list of password rules to user</strong> — Enables the use to view the password content requirements from the client. This option is enabled by default.</td>
<td></td>
</tr>
</tbody>
</table>
### Change Requirements
(only applicable to FRP Password Authentication only)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent change</td>
<td>Prevents the user from changing the password.</td>
</tr>
<tr>
<td>Require change after __ days (1-366)</td>
<td>Requires that the user change the password at predefined intervals.</td>
</tr>
<tr>
<td>Warn user before change required - days __ (1-30)</td>
<td>Notifies the user to change the password before it expires.</td>
</tr>
<tr>
<td>Enable password history - changes __ (1-10)</td>
<td>Prevents the user from reusing the last X number of passwords in the password history.</td>
</tr>
</tbody>
</table>

### Incorrect Password Behavior
(only applicable to FRP Password Authentication only)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalidate password after __ invalid attempts (1-100)</td>
<td>The number of failed logon attempts before the user password is invalidated and a recovery operation is required.</td>
</tr>
<tr>
<td>Initiate exponential backoff timeout after __ invalid attempts (1-20)</td>
<td>The number of times a user can enter an incorrect password before a timeout is enforced.</td>
</tr>
<tr>
<td>Maximum timeout - minutes __ (1-64)</td>
<td>The maximum time that the user is unable to enter password credentials after exceeding the allowed number of invalid attempts.</td>
</tr>
</tbody>
</table>

### Smart card PKI

Smart cards are not supported out of the box in this release. Raise a Product Enhancement if smart card based authentication that is independent of Windows logon is required for your environment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialization Method</td>
<td>Client-side Initialization</td>
</tr>
<tr>
<td>Use Windows user name if DN not available</td>
<td>Initializes the smart card with the Windows user name when a DN is not available. This option is enabled by default.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PIN Options</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow PIN change</td>
<td>Allows the user to change the PIN.</td>
</tr>
<tr>
<td>This option works only if the smart card allows a change PIN operation.</td>
<td></td>
</tr>
<tr>
<td>Allow user to see typed PIN</td>
<td>Allows the user to view the PIN in the user interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lock Triggers</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>On smart card removal</td>
<td>Unloads encryption keys when the smart card is removed making encrypted files inaccessible.</td>
</tr>
</tbody>
</table>

### OS Token

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialization Method</td>
<td>Require authentication using Active Directory credentials at first logon</td>
</tr>
<tr>
<td>Users will always be required to authenticate using Active Directory credentials with McAfee Endpoint Assistant.</td>
<td></td>
</tr>
</tbody>
</table>
## McAfee Endpoint Assistant

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passcode Definition</strong></td>
<td>Select one of the following options to set a PIN or password to authenticate to the McAfee Endpoint Assistant app:</td>
</tr>
<tr>
<td>• PIN, exactly 4 digits</td>
<td>— Enforces a PIN with exactly 4 digits.</td>
</tr>
<tr>
<td>• PIN, exactly 6 digits</td>
<td>— Enforces a PIN with exactly 6 digits.</td>
</tr>
<tr>
<td>• PIN, exactly 8 digits</td>
<td>— Enforces a PIN with exactly 8 digits.</td>
</tr>
<tr>
<td>• Password: Minimum 6 characters with 1 numeric, 1 alphabetical characters</td>
<td>— Enforces a password with minimum 6 characters containing 1 numeric and 1 alphabetic characters.</td>
</tr>
<tr>
<td>• Password: Minimum 6 characters with 1 numeric, 1 uppercase and 1 lowercase characters</td>
<td>— Enforces a password with minimum 6 characters containing 1 numeric, 1 uppercase, and 1 lowercase characters.</td>
</tr>
<tr>
<td>• Password: Minimum 8 characters with 1 numeric, 1 uppercase, 1 lowercase and 1 symbol characters</td>
<td>— Enforces a password with minimum 8 characters containing 1 numeric, 1 uppercase, 1 lowercase, and 1 symbol characters.</td>
</tr>
<tr>
<td><strong>Client-to-Server Sync</strong></td>
<td>Sync interval __ min (5-2880) — Enter the time in minutes to allow the McAfee Endpoint Assistant app on the client's mobile device to synchronize with the McAfee ePO server periodically.</td>
</tr>
<tr>
<td></td>
<td>Require periodic authentication using domain (AD) credentials — Enable this option to mandate periodic authentication on the McAfee Endpoint Assistant app using the Active Directory domain credentials.</td>
</tr>
<tr>
<td></td>
<td>Every __ days (1-365) — Enter the number of days.</td>
</tr>
<tr>
<td></td>
<td>This option is enabled only if the Require periodic authentication using domain (AD) credentials option is enabled.</td>
</tr>
<tr>
<td><strong>Connection Timeout</strong></td>
<td>After seconds __ (5-300) — Enter the time in seconds to configure timeout before the McAfee Endpoint Assistant application stops waiting for response from McAfee ePO. It is recommended to tune this value based on network latency in your specific environment.</td>
</tr>
</tbody>
</table>
### Encryption Key Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unlock Triggers</strong></td>
<td>Specifies the conditions at which users are prompted to authenticate (if required) and encryption keys are loaded.</td>
</tr>
<tr>
<td>• <strong>Windows logon</strong>— If there are any keys associated with Password token, an authentication prompt is shown to users immediately after Window logon. If there are any keys associated with OS token, those get loaded (if available) immediately following a successful OS logon.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Encryption key access</strong>— Prompts the user to authenticate whenever a user-initiated action requires access to an encryption key.</td>
<td></td>
</tr>
<tr>
<td>• <strong>McAfee tray</strong>— Enables the user to manually logon/logoff to FRP using the McAfee tray Quick Settings menu.</td>
<td></td>
</tr>
<tr>
<td><strong>Lock Triggers</strong></td>
<td>Specifies the conditions that trigger the unloading of encrypted keys.</td>
</tr>
<tr>
<td>• <strong>Windows screen lock</strong>— Requires that the user reauthenticate if Windows is not used for the configured time period (0-720 minutes). Default value is 0.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Key use inactivity</strong>— Requires that the user reauthenticate if encryption keys have not been used for the configured time period (5-720 minutes). Default value is 60.</td>
<td></td>
</tr>
<tr>
<td><strong>Client-to-Server Sync</strong></td>
<td>Sync interval __ min (5-2880) — Enter the time in minutes after which the client system synchronizes with the McAfee ePO server periodically. Default value is 120 minutes.</td>
</tr>
<tr>
<td><strong>Key Cache</strong> (this option is applicable only to keys that are assigned to systems and not users)</td>
<td>Enable Key Cache expiry — Enables the automatic removal of keys from the key cache if the client system fails to connect to the McAfee ePO server within the Key Cache expiry period. Status XML does not contain key information if the keys have been unloaded due to key cache expiry.</td>
</tr>
<tr>
<td><strong>Key Cache expiry period</strong> — Specifies the number of days after which all keys are removed from the key cache. This is applicable when Enable Key Cache expiry is selected and the client system has not connected to the McAfee ePO server. Default value is 90 days.</td>
<td></td>
</tr>
</tbody>
</table>

### Custom Messages

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OS Token Initialization Prompt (Windows)</strong></td>
<td>The text displayed to prompt end users to authenticate using the Active Directory domain credentials to provide the OS token on a particular system.</td>
</tr>
<tr>
<td><strong>OS Token Initialization Prompt (McAfee Endpoint Assistant app)</strong></td>
<td>The text displayed to prompt end users to authenticate using the Active Directory domain credentials to allow provisioning of the McAfee Endpoint Assistant application.</td>
</tr>
<tr>
<td><strong>Authentication Prompt (Windows)</strong></td>
<td>The text displayed to prompt end users to authenticate to FRP.</td>
</tr>
</tbody>
</table>
### Encryption Options

You can configure the options related to accessing encryption keys on the Encryption Options policy page. These options can't be used in user based PARs.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Advanced File Handling Options** | *
| Preserve file times                | Preserves the file time stamp while encrypting and decrypting.              |
| Require authentication for listing of encrypted folders | Mandates authentication for listing the encrypted folders. |
| Use wiping when encrypting and deleting files | Enables the wiping option to wipe redundant data when encrypting and deleting files. |
| Enable limiting of the file size that will be encrypted | Restricts the files to be encrypted according to the file size specified in the File size limit ___ MB field. |
| *File size limit ___ MB* | Enter the size of the files to be encrypted. |

| I/O Utilization                    | Maximum percentage of I/O utilization___ | Specifies the percentage of I/O usage that FRP processes can use during encryption. Default value is 50 percent. |

<table>
<thead>
<tr>
<th>Blocked Processes</th>
<th>Blocks the specified processes from opening encrypted files. FRP blocks a process by withholding the keys required to decrypt the files.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Adds the process to the block list.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the process from the block list.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the process in the block list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key Request Exclusions</th>
<th>Enables the process (such as anti-virus) to exclude encrypted files if required encryption keys are not already loaded.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Adds the process to the exclusion list.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the process from the exclusion list.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits the process in the exclusion list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Extension Exclusions</th>
<th>Excludes the specified file extensions from encryption.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Adds the file extension to the exclusion list.</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the file extension from the exclusion list.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edits file extension in the exclusion list.</td>
</tr>
</tbody>
</table>

| Advanced Debug Options             | Specify the elements to exempt the device inserted by the user for better security.                                        |
**General**

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Explorer integration</strong></td>
<td>Specifies the Windows Explorer context menu options available to a user on the client system.</td>
</tr>
<tr>
<td>• Allow Explicit Encrypt — Enables the <strong>Encrypt</strong> option for users. Default value is disabled.</td>
<td></td>
</tr>
<tr>
<td>• Allow Explicit Decrypt — Enables the <strong>Decrypt</strong> option for users. Default value is disabled.</td>
<td></td>
</tr>
<tr>
<td>• Enable padlock icon visibility — Displays a padlock icon on encrypted objects. Default value is enabled.</td>
<td></td>
</tr>
<tr>
<td>• Enable search encrypted — Enables <strong>Search encrypted</strong> option for client system users. Default value is disabled.</td>
<td></td>
</tr>
<tr>
<td>• Allow creation of Self-Extractor — 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>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email Integration</strong></td>
<td>Specifies the Windows Explorer context menu options available to a user on the client system.</td>
</tr>
<tr>
<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>
<td></td>
</tr>
</tbody>
</table>

**Location-based Protection**

You can configure the location-based policy settings on the **Location-based Protection** policy page.

**Local/Network Folders**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add</strong></td>
<td>Click <strong>Add+</strong> to specify the folders to be encrypted.</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>Specifies the path of the folder to be encrypted. 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. Make sure that you don't setup conflicting paths to prevent system and network abuse. For example, &quot;\abserver.com&quot; and &quot;P:&quot; are both resolving to the same location, but different keys are specified.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Specifies the encryption key to be assigned to the policy. Browse to select the key.</td>
</tr>
<tr>
<td></td>
<td>You can also configure this as Decrypt to maintain a plain text only folder.</td>
</tr>
</tbody>
</table>
### Cloud Sync Folder

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Click Add/+ to specify protection options for cloud sync folders. By default, all supported providers are in report mode and information collected from systems are accessible through the Cloud: Protection State FRP query.</td>
</tr>
<tr>
<td>Provider</td>
<td>Specifies the list of cloud providers namely Dropbox, Box, Google Drive, and OneDrive to be encrypted.</td>
</tr>
<tr>
<td>Protection Level</td>
<td>Specifies the protection level of the cloud providers as follows:</td>
</tr>
<tr>
<td></td>
<td>• Audit — Enabling this option allows capturing additional details related to cloud sync folder such as number of files and folder size.</td>
</tr>
<tr>
<td></td>
<td>• Allow Encryption — Creates an encrypted sub-folder named &quot;McAfee Protected Folder&quot; by default in the sync folders for cloud providers. The name of the sub-folder can be customized. Any data in this sub-folder will be synchronized in its encrypted form while still available transparently from the FRP client like other encrypted files.</td>
</tr>
<tr>
<td></td>
<td>• Enforce Encryption — Encrypts all the files and folders in the sync folder that will be synchronized in its encrypted form while still available transparently from the FRP client like other encrypted files.</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies the encryption key to be assigned to the policy. Browse to select the key. You can also configure this as Decrypt to maintain a plain text only folder.</td>
</tr>
<tr>
<td>Introductory Message</td>
<td>Displays the introductory message on the client system, if at least one policy protection level is set to Allow Encryption or Enforce Encryption. It is also displayed on the client system when a policy is changed and the related cloud provider is detected.</td>
</tr>
<tr>
<td>Allow-Level Message</td>
<td>If Allow Encryption protection level is selected for any of the Cloud providers, the text configured as part of this field is appended to the introductory message (followed by the Enforce-Level Message, if relevant), and a consolidated message is shown along with the details of the associated cloud provider.</td>
</tr>
<tr>
<td>Enforce-Level Message</td>
<td>If Enforce Encryption protection level is selected for any of the Cloud providers, the text configured as part of this field is appended to the introductory message (and Allow-Level Message, if relevant), and a consolidated message is shown along with the details of the associated cloud provider.</td>
</tr>
</tbody>
</table>

### Network

You can configure the network encryption settings on the Network policy page. Make sure to note that this policy cannot be used in user based PARs.

<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. This option is enabled by default.</td>
</tr>
<tr>
<td>Enable network bandwidth limit</td>
<td>Limits the network bandwidth used by FRP folder policies when encrypting files on network locations. Default value is 50 KB/sec.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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. This option is applicable only if the file is encrypted through location-based policy.</td>
</tr>
<tr>
<td>Maximum clients allowed to encrypt folders</td>
<td>Specifies the maximum number of FRP client systems that can simultaneously encrypt folders on a network. This option is applicable only if the file is encrypted through location-based policy.</td>
</tr>
</tbody>
</table>

### Optical Media

You can configure the optical media (CD and DVD) protection levels on the Optical Media FRP policy page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optical Media Protection Level</td>
<td>Provides the ability to specify protection level for CD/DVD. These methods are mutually exclusive and the Enforce Encryption (with onsite access) option is enabled by default.</td>
</tr>
<tr>
<td></td>
<td>• Allow Unprotected Access (report) — Does not encrypt while burning files and folders to a CD or DVD.</td>
</tr>
<tr>
<td></td>
<td>• Allow Encryption (with onsite access) — 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 FRP 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>• Enforce Encryption (with onsite access) — 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 FRP client. At the same time, it disables the writing of files and folders to a CD or DVD using third-party software. Only McAfee FRP 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>• Enforce Encryption (onsite access only) — Encrypts files and folders while burning them to a CD or DVD with the selected key. The encrypted data is accessible only on FRP systems with the availability of the required key.</td>
</tr>
<tr>
<td></td>
<td>• Block Write Operations — Prevents the writing of any data to a CD or DVD.</td>
</tr>
<tr>
<td>Optical Media Protection Options Encryption Key</td>
<td>Enter the encryption key or browse to and select the encryption key. This option is applicable only when Enforce Encryption (onsite access only) is selected.</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

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Media Protection Level</td>
<td>Provides the ability to specify protection level for removable media. These methods are mutually exclusive and the Enforce Encryption (with offsite access) option is enabled by default.</td>
</tr>
<tr>
<td></td>
<td>• Allow Unprotected Access (report) — Does not encrypt files on removable media.</td>
</tr>
<tr>
<td></td>
<td>- This protection level is available for both Windows and Mac OS X client systems.</td>
</tr>
<tr>
<td></td>
<td>• Allow Encryption (with offsite access) — Enables users to create an encrypted container on the USB device and copy data to the device in a secure manner.</td>
</tr>
<tr>
<td></td>
<td>- This protection level is available for both Windows and Mac OS X client systems.</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 or Mac OS X operating system, without having to install the FRP client. FRP supports files of size greater than 4 GB.</td>
</tr>
<tr>
<td></td>
<td>• Enforce Encryption (with offsite access) — Users must create an encrypted container on the USB device and copy data to the device in a secure manner. In addition, copying of data to the USB device is prevented if the user attempts to copy data to the unencrypted portion of the USB device.</td>
</tr>
<tr>
<td></td>
<td>- For Mac OS X systems, the fallback option for Enforce-Level protection is Allow-Level.</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 or Mac OS X operating system, without having to install the FRP client. FRP supports files of size greater than 4 GB.</td>
</tr>
<tr>
<td></td>
<td>• Enforce Encryption (onsite access only) — Encrypts files and folders with the selected key while copying them to a USB device. The encrypted data is accessible only on FRP systems with the availability of the required key.</td>
</tr>
<tr>
<td></td>
<td>- This protection level is available only for Windows client systems.</td>
</tr>
<tr>
<td></td>
<td>• Block Write Operations — Prevents the copying or writing of data onto a USB device.</td>
</tr>
<tr>
<td></td>
<td>- This protection level is available for both Windows and Mac OS X client systems.</td>
</tr>
<tr>
<td></td>
<td>- Copying of data from the USB device is permitted.</td>
</tr>
<tr>
<td>USB Media Protection Options</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- The availability of this section and the options it contains depends on the protection level.</td>
</tr>
<tr>
<td></td>
<td>• 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.)</td>
</tr>
<tr>
<td></td>
<td>• Full device — Creates an encrypted container that is equal to the size of the device.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>This option can be restricted based on device size by selecting <strong>Except when device is greater than</strong>, setting the maximum device size (in GB; default value is 64 GB), then specifying either <strong>Do not encrypt</strong> or <strong>User Managed</strong>.</td>
<td>For Mac systems, the user is not provided an option to backup the existing data. Any existing data will be deleted before a container is created.</td>
</tr>
<tr>
<td>• <strong>User Managed</strong> — Allows the user to determine the size of the encrypted container.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Allow large file support (&gt; 4GB)</strong> — Allows the user to encrypt files larger than 4 GB on the USB device.</td>
<td>This option is applicable only to Windows client systems. By default, the containers created on Mac OS X will support files of size larger than 4 GB.</td>
</tr>
<tr>
<td>When a device that is initialized with EEFF 4.2 and below is inserted on to a FRP 4.3 or later client (with the <strong>Allow large file support (&gt; 4GB)</strong> option enabled), the container format is automatically updated to support files of size greater than 4 GB. There is no need to reinitialize the device.</td>
<td>Any device &gt; 4 GB in size will use the new container format that was introduced with FRP 4.3 to support files of size &gt; 4 GB.</td>
</tr>
<tr>
<td>Clients running on EEFF 4.2 and below cannot recognize the new container format of FRP 4.3 or later. We recommend that you enable the <strong>Allow large file support (&gt; 4GB)</strong> option only when a critical mass of clients have been upgraded to FRP 4.3 or later to ensure a seamless upgrade experience.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Authentication</strong> — Specifies the methods used to authenticate the encrypted removable media. (Applicable for <strong>Allow Encryption (with offsite access)</strong> and <strong>Enforce Encryption (with offsite access)</strong> protection levels only.)</td>
<td></td>
</tr>
<tr>
<td>• <strong>Password</strong> — Enables the user to specify a password during initialization that can be used to recover the encrypted removable media. Select <strong>Mandatory</strong> to require the user to specify an authentication password during initialization.</td>
<td>For Mac OS X systems, <strong>Password</strong> is the only authentication mechanism and is mandatory.</td>
</tr>
<tr>
<td>• <strong>Certificate</strong> — Enables the user to attach a Windows certificate during initialization that can be used to authenticate to the encrypted removable media. Select <strong>Mandatory</strong> to require the user to attach a certificate during initialization.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Key</strong> — Specifies the Regular or User Personal key that can be used to authenticate to the encrypted removable media.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Customisable Recovery Message</strong> — Specifies the message that is displayed to the end user when a removable media recovery is initiated.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Customize UI Text displayed on inserting Media</strong> — Specifies the message to be displayed to an end user upon inserting a removable media into an FRP client with removal media encryption enabled. This text is customizable, and limited to 300 characters.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring FRP policies
FRP policy settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>blank, the default message is shown. (Applicable for Allow Encryption (with offsite access) and Enforce Encryption (with offsite access) protection levels only.)</td>
</tr>
<tr>
<td></td>
<td>• Encryption Key — The key to use to encrypt the USB device. This option is applicable only when Enforce Encryption (onsite access only) is selected.</td>
</tr>
<tr>
<td></td>
<td>• Ignore existing content — Existing content on the USB device is left untouched.</td>
</tr>
<tr>
<td></td>
<td>• Exempted Device IDs — Specifies devices for which the Removable Media policies are not applicable. Exempted devices are also exempted from explicit encryption and decryption.</td>
</tr>
<tr>
<td></td>
<td>This policy is applicable for Windows systems only.</td>
</tr>
<tr>
<td></td>
<td>• Add — Adds the ID of the device that will not be updated with the changes in encryption policies.</td>
</tr>
<tr>
<td></td>
<td>• Remove — Removes the device ID from the exemption list.</td>
</tr>
<tr>
<td></td>
<td>• Edit — Edits the ID of the device that will not be updated with the changes in encryption policies.</td>
</tr>
</tbody>
</table>

Floppy Disk Media

<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></td>
<td>• Allow Unprotected Access (report) — Does not encrypt files on floppy disks. Default value is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Block Write Operations — Prevents the copying of data onto a floppy disk.</td>
</tr>
</tbody>
</table>

Administrative helpdesk recovery for Removable and Optical media devices

In case of forgotten password scenarios, end users can use a helpdesk-assisted challenge and response mechanism to reset encrypted removable media and recover data from optical media. The recovery process can be used in both onsite and offsite scenarios (even on endpoints without the software installed). This feature is enabled by default.

- Helpdesk recovery for Removable Media devices is the only recovery option available for FRP OS X clients.
- Helpdesk recovery for Optical Media devices was introduced with FRP 5.0.1, and is only available for Windows platforms.

When end users forget their authentication credentials, to initiate recovery, perform either of the below options:

- Click Forgot Password on the Authentication window.
- Click Recover media under the Removable Media section on the FRP client console (Windows clients only).

A challenge code (with the phonetics) is displayed to the client user along with a recovery message that is customizable by the administrator. The user can now contact the helpdesk with the challenge code.

As a McAfee ePO user, your FRP Recovery permission set must be set to Manage Recovery to be able to generate a response code for end users.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu | Data Protection | FRP Recovery**
3. Select the **Removable Media Recovery** or **Optical Media Recovery** tab.
4. In the **Challenge Code** field, type the code provided by the user. The system starts to automatically match/filter with the known entries after 12 characters have been entered to quicken the recovery process. It is also possible to speed up the lookup by selecting vendor and product filters with the **Removable Media Recovery**.

For the recovery information to be available on McAfee ePO, events generated at the time of initialization of the removable media/optical media device on the FRP client need to have been sent and processed by McAfee ePO. This automatically occurs at the next client ASCI.

Once a match of the challenge code with the available database has been established, details such as user name (user who initialized the device), device size, and last access time are displayed to verify the caller’s identity.

5. Click **Recover** to generate a response code. Read out the response code to the user. Depending on the type of media and the applied policy, the user may be asked to reset the authentication credentials after entering the response code. For **Removable Media Recovery**, users will be asked to reset their authentication credentials to complete the recovery process. For **Optical Media Recovery**, the media will be unlocked to enable data recovery.

6. A McAfee ePO audit log is generated with details of the McAfee ePO user or administrator, who generated the response code along with the client user for whom the code was generated. An event is also generated for **Recovery/Credential Change** when the operation is performed on a FRP client.

The event for **Recovery/Credential Change** on the client was introduced in FRP 5.0.1, and is generated only for FRP Windows clients.

**User Local Keys Options**
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 FRP client. These user local keys can be shared among users using the Export and Import options in the FRP 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 FRP 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 FRP 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 FRP 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 FRP 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>
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 FRP software.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Policy | Policy Catalog, then select File and Removable Media Protection 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 FRP policy settings

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

**Before you begin**

Your user account must have appropriate permissions to edit McAfee FRP 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 FRP Key Server.

For details about product features, usage, and best practices, click ? or Help.

**Task**

1. Click Menu | Policy | Policy Catalog, then select File and Removable Media Protection 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 FRP software.

**Task**

For details about product features, usage, and best practices, click ? or Help.

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 **File and Removable Media Protection** from the drop-down list. The policy categories under **File and Removable Media Protection** 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 FRP software.

**Task**

For details about product features, usage, and best practices, click ? or Help.

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 **File and Removable Media Protection** 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 FRP policies on a system

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

**Task**

For details about product features, usage, and best practices, click ? or Help.

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 File and Removable Media Protection 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 FRP 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 details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Systems | System Tree | Assigned Policies, then select the group in the System Tree.
2. Select File and Removable Media Protection 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.

For FRP OS X clients, policy assignment rules can be used only for system-specific assignments. User-Based policies are not supported on FRP OS X 5.0 clients.

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.

- 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 48*
  
  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.

Policy assignment rules for an FRP user-based policy override the policy assigned to a system through the System Tree.

Task

For details about product features, usage, and best practices, click ? or Help.


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.


5. Select File and Removable Media Protection, select the policy category, then select the policy from the drop-down list.

6. Click OK.

7. On the Summary page, click Save.

Policy assignments - best practices

This section provides recommendations regarding the effective implementation of policy assignments.

Pragmatic policy assignment rules

We recommend that you simplify policy assignments by defining a baseline or default policy for your organization, and implementing it as a system-based policy. Then, for any exceptions to the policy, create a user-based policy assignment rule. This rule will always supersede system-based policies (both those assigned via the System Tree and those assigned by system-based policy assignment rules), making this the easiest way to implement complex policies. This also minimizes the amount of processing on the McAfee ePO server.

For further information on policy assignments, see KB81441 and KB72775.
Defining FRP 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 FRP.

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 FRP features.

Contents

- Create permission sets for user accounts
- Edit the FRP policy permissions
- Edit the FRP key server permissions
- Edit recovery permission set

Create permission sets for user accounts

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

Task

For details about product features, usage, and best practices, click ? or Help.

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 FRP policy permissions

You can define the permissions for configuring FRP policy settings.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | User Management | Permission Sets.
2. Click Edit next to FRP 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 FRP key server permissions
You can define permission sets for creating and managing FRP keys.

Task
For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | User Management | Permission Sets.
2. Click Edit next to FRP 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.

Edit recovery permission set
An administrator must have FRP Recovery permissions to recover end users' FRP key authentication and removable media credentials.

Task
For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Data Protection | FRP Recovery.
2. Click Edit next to FRP Recovery.
3. Select Manage Recovery to enable an administrator to recover the credentials of end users.
4. Click Save.
Managing FRP reports

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

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

FRP queries and query results

FRP 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.

FRP 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 FRP custom queries**

You can create FRP custom queries with the **Query Builder** wizard.

**Task**

For details about product features, usage, and best practices, click ? or Help.

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

2. On the Result Type page, select **File and Removable Media Protection** from the Feature Group pane and Result Type for the query required, then click Next to open the Chart page.
   
   For details about product features, usage, and best practices, click ? or Help.

   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 FRP queries**

You can run and view the inbuilt FRP queries from the Queries & Reports page.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Click **Menu | Reporting | Queries & Reports**.

2. In the **Groups** pane, select **FRP Queries** from the **McAfee Groups** drop-down list. The standard FRP query list appears.

<table>
<thead>
<tr>
<th>Query</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud: Number of Instances</td>
<td>Lists the total number of cloud storage system and user instances.</td>
</tr>
<tr>
<td>Cloud: Number of Users</td>
<td>Lists the unique cloud storage users across systems.</td>
</tr>
<tr>
<td>Cloud: Provider Audit Events</td>
<td>Lists the audit events related to cloud providers.</td>
</tr>
<tr>
<td>Cloud: Provider State</td>
<td>Lists the state of cloud providers across systems.</td>
</tr>
<tr>
<td>Cloud: Top 10 Users by Folder Size</td>
<td>Lists the top ten users with maximum cloud storage usage.</td>
</tr>
<tr>
<td>Cloud: Top 10 Users by Number of Files</td>
<td>Lists the top ten users with most number of files in cloud storage.</td>
</tr>
<tr>
<td>Cloud: Trend of Instances</td>
<td>Lists the total number of cloud storage instances detected over time.</td>
</tr>
<tr>
<td>Cloud: Trend of usage by folder size</td>
<td>Displays the total size of cloud storage folders over time.</td>
</tr>
<tr>
<td>Cloud: Trend of usage by number of files</td>
<td>Lists the total number of files in cloud storage over time.</td>
</tr>
<tr>
<td>Cloud: Trend of Users</td>
<td>Lists the total number of cloud storage users detected over time.</td>
</tr>
<tr>
<td>FRP: Advanced Debug Option Events</td>
<td>Lists all events related to advanced debugging.</td>
</tr>
<tr>
<td>FRP: Key Authentication Events</td>
<td>Lists all events related to FRP key authentication.</td>
</tr>
<tr>
<td>FRP: Client Versions</td>
<td>Lists all FRP client versions that are currently installed.</td>
</tr>
<tr>
<td>FRP User Key Mappings</td>
<td>Lists all users and their key usage within FRP.</td>
</tr>
<tr>
<td>FRP: Users by Operating System</td>
<td>Lists all users according to their operating system usage, who use encryption keys.</td>
</tr>
<tr>
<td>Mobile: Events</td>
<td>Lists all events related to the McAfee Endpoint Assistant application.</td>
</tr>
<tr>
<td>Optical Media: Device Events</td>
<td>Lists all events related to optical media like CDs, DVDs, and ISOs.</td>
</tr>
<tr>
<td>Removable Media: Activations</td>
<td>Displays all instances of removable media device initialization success events over the last 7 days.</td>
</tr>
<tr>
<td>Removable Media: Device Events</td>
<td>Lists all events related to removable media.</td>
</tr>
<tr>
<td>Removable Media: Protection Status</td>
<td>Displays the protection status of removable media.</td>
</tr>
<tr>
<td>Removable Media: Recent Usage</td>
<td>Displays all instances of removable media device insert events over the last 7 days.</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.

 optionally, you can edit the query and view its details.

6 Click Close when finished.

# FRP client events

Enforcement of FRP policies generates client events, which include the Event ID and appropriate information related to the event.

## Removable media events

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Types</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>20500</td>
<td>Removable Media Device Insert Event</td>
<td>This event is reported whenever any type of removable media is inserted in the client. Event severity: 0</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: 0</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: 0</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: 0</td>
</tr>
<tr>
<td>20509</td>
<td>Removable Media Device Upgrade Event</td>
<td>This event is reported whenever the removable media is being upgraded to support large file sizes (&gt; 4GB). Event severity: 0</td>
</tr>
<tr>
<td>20521</td>
<td>Removable Media Application Upgrade Event</td>
<td>This event is reported when the removable media application is upgraded.</td>
</tr>
<tr>
<td>20553</td>
<td>Removable Media Authorization Success Event</td>
<td>This event is reported when the user's removable media is authorized successfully.</td>
</tr>
<tr>
<td>20554</td>
<td>Removable Media Authorization Failure Event</td>
<td>This event is reported when the user's removable media authorization is failed.</td>
</tr>
<tr>
<td>20555</td>
<td>Removable Media Recovery Success Event</td>
<td>This event is reported when the user's removable media is recovered successfully.</td>
</tr>
<tr>
<td>20556</td>
<td>Removable Media Recovery Failure Event</td>
<td>This event is reported when the user's removable media recovery is failed.</td>
</tr>
<tr>
<td>20557</td>
<td>Removable Media Authentication Change Success Event</td>
<td>This event is reported when the user has changed the removable media authentication details successfully.</td>
</tr>
<tr>
<td>20558</td>
<td>Removable Media Authentication Change Failure Event</td>
<td>This event is reported when the user's request for changing the removable media authentication details is failed.</td>
</tr>
</tbody>
</table>
### Table 7-2  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>
| **System**       | • User information (DomainName\UserName)  
                   • Time-stamp |
| **Initialization** | • Initialization state (Failed, Canceled, Successful)  
                       • Backup state (None, Failed, Canceled, Successful)  
                       • Time taken for initialization (in sec)  
                       • Time taken for backup (in sec)  
                       • Backup size (in GB)  
                       • Size of protected part (only when initialization has completed successfully, in GB) |
| **Device**       | • Size (in GB)  
                   • File system of device (FAT32, NTFS, EERM)  
                   | ![File system for devices with new container format (support for files > 4 GB) are shown as FAT32; devices with legacy container are shown as EERM.](image) |
| **Event specific fields** | User response — Valid for events 20501 and 20502 only |

### Optical Media client events

#### Table 7-3  Event types

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 20505    | Optical Media Initialization Start Event | This event is reported whenever the user clicks Initialize or Cancel in the Initialization window.  
          Event severity: 0 |
| 20506    | Optical Media Initialization End Event | This event is reported when initialization is complete.  
          Event severity: 0 |
| 20507    | Optical Media Insertion Event | This event is reported whenever an optical media is inserted in the client.  
          Event severity: 0 |
| 20508    | Optical Media Ejection Event | This event is reported whenever a optical media is ejected from the client.  
          Event severity: 0 |
Table 7-4  Event details

<table>
<thead>
<tr>
<th>Information type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event ID</td>
<td>Event ID number</td>
</tr>
</tbody>
</table>
| Computer         | • Name of the computer  
                  |   • User name  
                  |   • IP address  
                  |   • Operating system type |
| Media type       | • For Optical Media Initialization Start Events, the smallest disk type that can hold archived data (ISO, CD, DVD, or DVD-DL)  
                  |   • For Optical Media Initialization End Events, the physical media detected (for example, CD-ROM)  
                  |   • For Optical Media Insertion and Ejection Events, "Optical" |
| Device           | • Disk globally unique identifier (GUID)  
                  |   • Protected (Yes, No, Unknown) (only CD/DVDs protected by the "offsite access" options are considered protected)  
                  |   • Protected size (GB)  
                  |     • For Optical Media Initialization Start Events, the value is 0  
                  |     • For Optical Media Initialization End Events, the size of the encrypted archive  
                  |     • For Optical Media Insertion and Ejection Events, the size of the encrypted archive if the media is FRP encrypted |
| Event description| • Description of the event  
                  |   • Event generation time |
| Event specific fields | Initialization state (Failed, Canceled, Successful) (Optical Media Insertion and Ejection Events only) |

Only relevant information is captured in each event. For example, a device insert event does not contain the initialization state.

FRP: Key Authentication events

Table 7-5  Event types

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 20510   | Token initialization success event | This event is reported when token initialization is complete.  
                  |   Event severity: 0 |
| 20511   | Token initialization failure event | This event is reported when token initialization fails.  
                  |   Event severity: 1 |
| 20512   | Authentication success event    | This event is reported when authentication successfully completes.  
                  |   Event severity: 0 |
| 20513   | Authentication failure event     | This event is reported when authentication fails.  
                  |   Event severity: 1 |
### Table 7-5  Event types (continued)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event</th>
<th>Definition</th>
</tr>
</thead>
</table>
| 20514    | Authentication token invalidation event | This event is reported when an authentication token has been invalidated by exceeding permitted incorrect attempts.  
            |                                | Event severity: 1                                                                                  |
| 20515    | Authentication change success event   | This event is reported when an authentication change successfully completes.                            |
|          |                                | Event severity: 0                                                                                  |
| 20516    | Authentication change failure event   | This event is reported when an authentication change fails.                                            |
|          |                                | Event severity: 1                                                                                  |
| 20517    | Authentication recovery success event | This event is reported when authentication recovery successfully completes.                             |
|          |                                | Event severity: 0                                                                                  |
| 20518    | Authentication recovery failure event | This event is reported when authentication recovery fails.                                             |
|          |                                | Event severity: 1                                                                                  |
| 20519    | Authentication recovery expired event | This event is reported when the authentication recovery password has expired based on FRP Key Authentication settings. |
|          |                                | Event severity: 1                                                                                  |
| 20520    | Authentication lockout event         | This event is reported when authentication locks out for the user.                                   |
| 20522    | Advance Debug Option event           | This event is reported when the device inserted by the user is exempted by the system for better security. |

### Cloud provider client events

### Table 7-6  Event types

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>20551</td>
<td>Cloud provider report event</td>
<td>This event is reported when the cloud provider sends a report to the McAfee ePO server, even if any protection level is not selected.</td>
</tr>
<tr>
<td>20552</td>
<td>Cloud provider audit event</td>
<td>This event is reported when the cloud provider sends an audit-level report to the McAfee ePO server, when the Audit protection level policy is selected.</td>
</tr>
</tbody>
</table>

### View audit log

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

**Task**

For details about product features, usage, and best practices, click ? or Help.

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 FRP, 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 FRP
- Removable media registry controls

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 FRP client makes use of the McAfee Core Cryptographic Module (MCCM) User and Kernel FIPS 140-2 cryptographic modules. These cryptographic modules have been validated at FIPS 140-2 Level 1. For more information, refer to the KnowledgeBase article KB83483.

Prerequisites

The FRP client package must be installed on the client in FIPS mode. Depending on compliance requirements mandated by your auditor, you might also have to meet certain conditions to run FRP in FIPS mode.

- McAfee ePO may have to be installed in FIPS mode.
- The operating system on the client where FRP is installed may have to run in FIPS mode. For more information, refer to the KnowledgeBase article KB83483.

Impact of FIPS mode

In FIPS mode, certain self-tests are performed on start-up of the client system when the MCCM module 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 FRP 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 during Removable Media device initialization when using offline access support, 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 FRP client need to be deployed in FIPS mode to operate in a FIPS-certified manner. This topic is applicable only to Windows systems and not Mac systems.

Deploy FRP on the client in one of these ways:

- Using an FRP 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 FRP 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 FRP in FIPS mode. If FRP is already installed and you want to upgrade to this version of FRP and install in FIPS mode, see McAfee KnowledgeBase article 78872.

Uninstall FRP

If you need to uninstall FRP, 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 FRP from managed systems

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

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

For details about product features, usage, and best practices, click ? or Help.

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 File and Removable Media Protection.
   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 FRP extension
Remove the FRP extension from the McAfee ePO server.
For details about product features, usage, and best practices, click ? or Help.

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 File and Removable Media Protection 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 FRP software package
Remove the FRP software package from the McAfee ePO server.
For details about product features, usage, and best practices, click ? or Help.

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 FRP package.

4 When prompted to confirm, click OK.
Use Shell command to uninstall FRP from managed systems

You can uninstall FRP from a managed system using the `MfeFfShell` command. This topic is applicable only to Windows systems and not Mac systems.

**Task**

1. At the command prompt, navigate to the folder where FRP was installed. The default location is:
   ```shell
   [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 FRP from managed systems

You can uninstall FRP from a managed system using MSI. This topic is applicable only to Windows systems and not Mac systems.

**Task**

- Run the following command to uninstall FRP:
  - On 32-bit systems — `msiexec /q /x eeff32.msi`
  - On 64-bit systems — `msiexec /q /x eeff64.msi`

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

Removable media registry controls

FRP 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**

FRP 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 FRP, 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 FRP 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.
Additional information

Removable media registry controls
Index

A
about this guide 5
agent wake-up call, sending 13
application-based protection 31
audit log 57

C
conventions and icons used in this guide 5
credential changes, forcing 18
credentials
  recovering 18
custom queries 52

D
deployment 11
deployment, installing products 12
documentation
  audience for this guide 5
typographical conventions and icons 5
drives, encryption 11

E
encryption keys 21
  about 21
  activating and deactivating 22
  creating 21
  deleting 23
  editing 22
  exporting 23
  importing 24
  importing from FRP 24
encryption keys, deployment 11
encryption, persistent 7
enforcement. See policy enforcement
extension, FRP
  FIPS mode 59
  installing 12
  removing from ePO 61

F
features 8
FIPS certification 59

FIPS mode
  client package deployment 60
  impact 59
  prerequisites 59
floppy disks, policy settings 40
FRP authentication
  configuring 16
  forcing credential change 18
  recovery 18
FRP client 7
frp key authentication 15
FRP key authentication
  recovery 50
FRP policies
  assign to managed system 45
  creating from Policy Catalog 44
  editing, from Policy Catalog 44
  enforcing on a system 46
  enforcing on a system group 46

G
groups
  key usage 27
  policy enforcement for a product 46

I
installation, FRP
  checking in software package 12
  deploying to managed systems 12
  product extension 12
  requirements 9

K
key server permissions 50
keys
  activating 22
  assigning 25
  creating 21
  deactivating 22
  deleting 23
  editing 22
  encryption 11
keys (continued)
  exporting 23
  importing 24
  importing from FRP 24
  regular 21
  role-based management 28
  usage 27
  user local 21
  user personal 21

L
local keys 21
  policy settings 43
location-based protection 37

M
managed systems
  assigning FRP policy 45
  assigning policy to 45
  deploying FRP on 12
  policy management on 31
  uninstalling FRP 60
  uninstalling FRP with Shell command 62
  uninstalling FRP, with MSI 62
master repository
  checking in software package 12
McAfee Agent for Mac, downloading and deploying 10
  MSI, using to uninstall FRP 62
  multi-slot policy 47

N
network settings 38

O
operating system requirements 9
  operating systems 11
  optical media 39

P
password rule settings 32
permission sets, FRP
  about 49
  creating 49
  key management 50
  policy settings 49
  role assignment 29
permission sets, FRP recovery
  key management 50
persistent encryption 7
personal keys 21
policies
  about 31
  assigning to system groups 45

Policies (continued)
  assigning to systems 45
  configuring 31
  create on Policy Catalog page 44
  editing, from Policy Catalog 44
  enforcement 31
  viewing 31
policy assignment rules 48
  about 47
  create 48
  multi-slot policy 47
  priority 47
Policy Catalog
  creating FRP policies 44
  editing FRP policies 44
  page, viewing 31
policy categories
  encryption options 36
  exclusions 36
  network 38
  password rules 32
policy enforcement
  enabling and disabling 46
  for a product 46
  on a system group 46
policy inheritance
  lock 45
policy settings
  file encryption 31
  general 37
  integration 37
  location-based protection 37
  optical media 39
  removable media 40
  user local keys 43
product installation
  configuring deployment tasks 12

Q
queries
  about 51
  custom, creating 52
  exported results 51
  Query Builder wizard 52
  viewing results 53

R
recovery
  credentials 18
  tokens 18
  user personal keys 27
regular keys 21
  assigning 25
  creating 21
removable media
   broaden the definition 62
   exempt local drives from encryption 63
   policy settings 40
   registry controls 62, 63
reports
   about 51
   formats 51
   viewing 53
requirements 9
role-based key management
   about 28
   adding roles 28
   deleting roles 29
   editing roles 28
roles
   adding 28
   assigning to permission set 29
   deleting 29
   editing 28
   global administrator 28
rules
   policy assignment, creating 48
   priority 47
S
self-tests, FIPS mode 59
servers
   requirements 9
Shell command, using to uninstall FRP 62
software package
   removing 61
software packages
   checking in 12
software requirements 9
step-up authentication 16
system groups, policy enforcement 46
system requirements 9
System Tree
   policy assignment rules 48
   systems
      assigning policies to 45
      policy enforcement for a product 46
U
USB devices, policy settings 40
user accounts
   permission sets 49
user personal keys
   about 27
   assigning 25
   best practices 27
   converting to regular keys 27
users
   key usage 27