Migration Guide

McAfee File and Removable Media Protection 5.0.0

Contents

Contents

Preface

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

Contents

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.

Conventions

This guide uses these typographical conventions and icons.

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

Find product documentation

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

Task

1 Go to the **Knowledge Center** tab of the McAfee ServicePortal at http://support.mcafee.com.

2 In the **Knowledge Base** pane, click a content source:

- **Product Documentation** to find user documentation
- **Technical Articles** to find KnowledgeBase articles

3 Select **Do not clear my filters**.

4 Enter a product, select a version, then click **Search** to display a list of documents.

1 Introduction

McAfee® File and Removable Media Protection (FRP) 5.0.0 offers data protection in the form of powerful encryption technology so that only authorized users can access information. FRP 5.0.0 integrates with McAfee® ePolicy Orchestrator® (McAfee ePO™) , and is managed through the McAfee ePO server, using a combination of user- and system-based policies.

McAfee® recommends that you migrate to FRP 5.0.0 to improve manageability and other supported features.

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 details, see *File and Removable Media Protection 5.0.0 Product Guide*.

Overview

File and Removable Media Protection legacy versions (prior to EEFF 4.0) use McAfee Endpoint Encryption Manager (EEM) as the management console. This utility allows privileged users to manage the enterprise from any workstation that can establish a TCP/IP link or file link to the Object Directory.

This guide describes the steps required to migrate EEFF 3.2.x clients managed by EEM to FRP 5.0.0 clients managed by McAfee ePO. For information about upgrading from EEFF 4.x.x to FRP 5.0.0, refer to the *Upgrading the FRP client* section.

The migration process from EEFF 3.2.x to FRP 5.0.0 consists of these steps:

1. Export keys from EEM. For more information, see the *Export keys* section.
2. Deploy the required versions of McAfee® Agent for your systems that need to migrate to FRP 5.0.0.

   Make sure that the client system communicates successfully with the McAfee ePO server.
3. Install the McAfee ePO client package on the McAfee ePO server.
4. Install the McAfee ePO extension on the McAfee ePO server.
5. Import the encryption keys into the McAfee ePO server.
6. Define policies and assign keys to policies.
7. Assign policies to systems and users through system based and user based policies.
8. Deploy FRP 5.0.0 to the client system.
9. Send an agent wake-up-call.

Policies are not exported as part of the 3.x export process and the client upgrade does not transfer any policy, policy assignments, or key assignments from the EEFF 3.x client to the FRP 5.0.0 client. These settings must be reconfigured on McAfee ePO, then enforced on the client.

2 Encryption keys

Migrating from EEFF 3.2.x to FRP 5.0.0 includes exporting the encryption keys from EEM, importing them to McAfee ePO server, and upgrading the EEFF client to FRP 5.0.0.

The encrypted files and folders on the client systems remain encrypted during the migration process. The client upgrade does not transfer any policy from the 3.x client to the 5.0.0 client.

A command line application is provided to enable the export of encryption keys from the EEM database (5.2 or later). Exporting keys from the EEM database reduces the amount of configuration required by the administrator.

Contents

Export keys from EEM

The process of exporting keys varies depending on your requirements as follows:

Exporting keys with Role Based Key Management support

- If you have EEM 5.2.13 installed, there are no pre-requisite steps.
- If you have EEM 5.2.12 or below installed, upgrade to EEM 5.2.13 to be able to export keys with key level related information.

Exporting keys without Role Based Key Management support

- If you have EEM 5.2.13 installed, keys are by default exported with level information. After running the export process, EEM 5.2.13 administrators need to manually edit the XML export file to be able to import the keys into McAfee ePO without any role information. Please remove all <level> tags from the exported XML as indicated in the below example.

  <?xml version="1.0"?>

  <Description>key temp</Description>

  <Status>active</Status>

  <AlgID>00000011</AlgID>

  <KeySize>32</KeySize>

  <KeyData

  Encryption="None">eEK3onS4wwb3HwNPO+GABzAKu5DIT5NBZCDXPlar6jg=</KeyData>

  <ValidUntil>00000000</ValidUntil>

  <Level>0</Level>

  </Key>

  </EeffKeys>

- If you have EEM v.5.2.12 or below installed, run `SetupEEFFMigration.exe` to perform the migration update.

Task

1 On the command prompt, navigate to the EEM install folder (default location is `Program Files \McAfee\Endpoint Encryption Manager`).

2 Run this command:

```
SbAdmCl -AdminUser:JohnSmith -AdminPwd:
123456 -Database:MyDatabase -Command:ExportFFKeys -Group:MyKeys -File:MyExportedKey
s.xml -Password:thepassword
```

Parameter	Description
`AdminUser:JohnSmith`	User name for EEM administrator logon.
`AdminPwd:123456`	Password for EEM administrator logon.
`Database:MyDatabase`	(Optional) EEM database server name. Include this parameter only if you want to export keys from an external database.
`Group:MyKeys`	(Optional) Key group name in EEM. If no key group is specified, all key groups in EEM are exported.
`File:MyExportedKeys.xml`	(Optional) Default name of the file where key group should exported (default location is `Program Files\McAfee\Endpoint Encryption Manager`). If the file name is not specified, an XML file will be created in the EEM folder (`C:\Program Files\McAfee\EEM)`. The command line does not display an error if the file name is not specified in the command. Keys can also be exported into a .bin file if you edit this command parameter accordingly. For example: `File:MyExportedKeys.bin`
`Password:thepassword`	(Optional) Password to protect the exported file.

The exported file is saved in the default or specified location.

You can only export the keys that you have access to.

Import keys to McAfee ePO

You can import encryption keys that have been exported from EEM. The ability to import information related to Role Based Key Management depends on the version of EEM, and how the key data is exported.

If the McAfee ePO server is running in FIPS mode, only ALG 12 (FIPS AES) keys are imported from EEM. All other keys are discarded.

You can import encryption keys from EEM 5.2 or later.

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

- If the XML file does not contain key level information, the imported keys are automatically associated with the Default role.
- If the key level already exists, FRP imports the key and associates it with that role.

- If the key level does not exist, FRP creates a role with the prefix EEM_LEVEL, followed by the level number (for example, EEM_LEVEL_24). FRP then imports the key and associates the key with the newly defined role, and create a permission set named accordingly (for example, EEM_LEVEL_24). If a permission set with that name already exists, a new permission is not created and the role is associated with the existing permission set.
- When multiple roles are imported using the same XML file, FRP associates the keys to multiple roles based on the key levels. A higher key level is assigned the keys of any lower levels. For example, if the imported XML includes levels 24, 30, and 32, the EEM_LEVEL_30 would be assigned the EEM_LEVEL_30, EEM_LEVEL_24 and Default roles.

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

Task

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

2 Click **Actions** | **Import Keys**.

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

4 Click **Import Keys**.

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

3 Upgrading the FRP client

You can upgrade to the FRP 5.0.0 client from the EEFF 4.2.x or FRP 4.3.x client using McAfee ePO.

When you upgrade to the FRP 5.0.0 client from EEFF 4.2.x or FRP 4.3.x, the client retains all key and policy information. If using a different McAfee ePO server, the encryption keys and policies must be necessarily imported from the existing McAfee ePO server to the new McAfee ePO server and assigned appropriately.

FRP 5.0.0 client deployment forces a restart on the client system. The existing EEFF 4.2.x or FRP 4.3.x client is uninstalled and FRP 5.0.0 client is installed, taking effect upon restart. All encrypted files and folders on the client system remain encrypted.

Contents

Run the FRP Upgrade Task

FRP extension can be upgraded from EEFF 4.x / FRP 4.x to FRP 5.0.0 by following the documented McAfee ePO process for extension upgrade. However, with FRP 5.0.0 a lot of new features are made available especially relating to handling of encryption keys, which requires the FRP Upgrade Task to be run.

Task

For option definitions, click **?** or **Help** in the interface.

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

2 Click **Menu** | **Configuration** | **Server Settings** | **FRP Authentication Settings**.

3 Click **Edit** and select **Enable and run FRP Upgrade Task**, then click **Save**.

Please note that once this is done, you cannot undo this operation. On clicking **Save**, the FRP Upgrade Task is automatically run. Based on the amount of processing that is required, the time taken to run the task could vary. To check the status of the task, you can navigate to **Menu** | **Automation** | **Server Task Log** and check for the last run of FRP Upgrade Task.

Once the task has completed successfully, you now have the option to use the new FRP Authentication methods.

At this stage, you now have FRP 5.0.0 extension with the FRP Upgrade Task completed.

Different phases of FRP extension upgrade

This table highlights each phase of the upgrade process and the status before, and after running the FRP Upgrade Task.

Feature	Before running the FRP Upgrade Task	After running the FRP Upgrade Task
Key assignment	Grant Keys policies are still the mechanism to assign keys to system/users through the system tree or policy assignment rules.	Once the FRP upgrade task has been run you can now assign keys to systems and users directly from the **FRP Keys** page. It is strongly recommended to move away from Grant Key policies key assignment mechanism. You can, over a period of time, make assignments that are same as the Grant Key assignments using the new assignment workflows. FRPwill clean up and delete any unused Grant Key policy objects that either have no keys or no assignments automatically. Once all Grant Key policy objects are deleted by this task, you will no longer see this policy type in McAfee ePO. Existing Grant Key policies will work as they do before the upgrade, however no new keys can be added to these policies.
User Personal Keys	No change in functionality to older FRP versions	With FRP 5.0.0 we have ensured that User Personal Keys (UPKs) can only be assigned to user/user groups or organizational units. UPKs previously assigned and created for users that were part of the domain will be automatically upgraded into the corresponding user's OS token. Please note that for this to happen the AD server must have been registered with McAfee ePO and be available at the time of running the upgrade task. UPKs that were not upgraded to users OS token will now show up as "Deprecated User Keys". This will happen if either the AD server was not reachable at the time of running the task or if the UPK was not created for a domain user, for example WORKGRP1\User1. If the UPK was not upgraded because of AD connectivity issues, you can run the FRP Upgrade Task again and it will process all the deprecated user keys.

Feature	Before running the FRP Upgrade Task	After running the FRP Upgrade Task
Assignment methods	No change in functionality to older FRP versions	You can now assign keys to systems directly from the **FRP Keys** page. Additionally, we have now introduced a new feature with FRP 5.0.0 that will enable assignment of keys to users directly from the **FRP Keys** page. You can also assign UPKs to users directly from the **FRP Keys** page.
Policies	The removable media policy has now been enhanced for an improved end user authentication experience. You can setup removable media policies with a key as an authentication mechanism in addition to the existing password/ certificate authentication methods. FRP 5.0.0 supports recovering removable media devices through admin assisted recovery. This feature is enabled by default. This also means that older clients managed with FRP 5.0.0 extension will continue to function as they do now, but no policy updates are possible. The key cache expiry option has now been moved to the **Encryption Options** tab in the **Authentication** policy. Older clients will retain their existing settings until upgraded to FRP 5.0.0.	This behavior does not change after running the FRP Upgrade Task. New Grant key policy objects can no longer be created. Existing Grant key policies can be assigned / re-assigned using system tree or policy assignment rules as before. Grant keys policies can also now be edited only to remove keys; you can no longer add keys to it. To assign new keys to old clients, you can do it directly from the **FRP Keys** page.

Different phases of FRP client upgrade

This tables highlights each phase of the update process and the status before, during, and after the client upgrade to FRP 5.0.0.

Table 3-1 Phases of client upgrade from EEFF 4.2.x or FRP 4.3.x to FRP 5.0.0

Stage	Client status	Comments
Before running the FRP Upgrade Task	Pre FRP 5.x client	Removable media policy and key cache expiry policy settings cannot be updated; it will hold settings that were previously assigned.
Before running the FRP Upgrade Task	FRP 5.x client	No visible changes compared to pre FRP 5.x client. However, you can now avail below additional benefits: • Auto unlock feature in removable media and admin assisted recovery of media • Encrypt cloud storage SYNC folders However, you will not be able to use the new key assignment work flows nor will you be able to access encrypted files on mobile devices.

Table 3-1 Phases of client upgrade from EEFF 4.2.x or FRP 4.3.x to FRP 5.0.0 *(continued)*

Stage	Client status	Comments
After running the FRP Upgrade Task	Pre FRP 5.x client	Removable media policy and key cache expiry policy settings cannot be updated; it will hold settings that were previously assigned. If you had previously assigned UPKs to systems, requests from clients to already created UPKs will still be honoured. However, new UPKs will not be created as now UPKs can only be assigned to users.
After running the FRP Upgrade Task	FRP 5.x client	You should now have access to all new functionality of FRP 5.0.0.

Index