McAfee File and Removable Media Protection 5.0.8 Installation Guide

COPYRIGHT

Copyright © 2018 McAfee, LLC

TRADEMARK ATTRIBUTIONS

McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

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

Contents

Contents

1 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

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

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

Refer to KB81478 for the latest information on support for VDI environments, including installation details.

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

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® Agentwill 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 FRP, 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.x.xxx.ZIP`
   b. `help_eeff_50X.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

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.x.xxx.ZIP` software package for Windows systems and/or `MfeFRP_Client_OSX_5.0.x.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

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

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**.
7. Under **Force policy update**, select **Force complete policy and task update**.
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 FRP, 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 1-1 Installation command

Operating system	Command line
Supported 32-bit system	msiexec.exe /q /i eeff32.msi
Supported 64-bit system	msiexec.exe /q /i eeff64.msi

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.

2 Upgrading the FRP client

You can upgrade to the FRP 5.0.8 client from the FRP 4.3.x client using McAfee ePO.

When you upgrade to the FRP 5.0.8 client from 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 imported from the existing McAfee ePO server to the new McAfee ePO server and assigned appropriately.

FRP client deployment forces a restart on the client system. The existing FRP 4.3.x client is uninstalled and FRP 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 FRP 4.x to FRP 5.0.8 by following the documented McAfee ePO process for extension upgrade.

Task

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu** | **Configuration** | **Server Settings** | **FRP Key Authentication Settings**.
3. Click **Edit** and select **Enable FRP key authentication**, 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.

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	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. With FRP you can 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 supports recovering removable media devices through admin assisted recovery. This feature is enabled by default. This also means that older clients managed with FRP 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 5.0.8.	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 5.0.8.

Table 2-1 Phases of client upgrade from FRP 4.3.x to FRP 5.0.8

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 2-1 Phases of client upgrade from FRP 4.3.x to FRP 5.0.8 *(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 FRP 5.0.8 functionality.

3 FRP - Additional information

Contents

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.

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

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.

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.

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.

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:

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

2 Run the following command: .

```
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.

Index

McAfee™
Together is power.