

McAfee Cloud Data Protection Beta Release 21-Mar-2017



Product Guide

McAfee File and Removable Media
Protection 6.0.0

McAfee Cloud Data Protection Beta Release 21-Mar-2017

COPYRIGHT

© 2017 Intel Corporation

TRADEMARK ATTRIBUTIONS

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. 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

	Preface	5
	About this guide	5
	Audience	5
	Conventions	5
1	Introduction	7
	Features	7
2	Installing the FRP client	9
	Requirements	9
	Install the FRP and Help extensions	10
	Check in the FRP software package	11
	Key Management Service	11
	Permissions required for Key Admins and Tenant Admins	11
	Add KMS as a registered server and provision a tenant on McAfee ePO.	12
	Deploy FRP to managed systems	12
	Deployment and activation - best practices	13
	Send an agent wake-up call	14
	Install FRP from the command line	15
3	Configuring FRP policies	17
	FRP policy settings	17
	Authentication	17
	Encryption Options	20
	General	20
	Create a policy	20
	Edit the FRP policy settings	21
	Assign a policy to a managed system	21
	Assign a policy to a system group	22
	Enforce FRP policies on a system	22
	Enforce FRP policies on a system group	23
A	Additional information	25
	FRP key management	25
	FRP integration with Endpoint Health Check	25
	Endpoint Health Check Failure Events	25
	Index	27

McAfee Cloud Data Protection Beta Release 21-Mar-2017

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.

<i>Italic</i>	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

McAfee Cloud Data Protection Beta Release 21-Mar-2017

1 Introduction

McAfee® File and Removable Media Protection (FRP) 6.0.0 is enhanced to support workflows within the Cloud Data Protection (CDP) solution. FRP helps secure files and folders that are synced to cloud storage services by encrypting them before they leave the endpoint based on the configured Cloud Data Protection rules.

Cloud Data Protection rules configured on McAfee® ePolicy Orchestrator® (McAfee® ePO™) Cloud management console are automatically synced to on-premise McAfee ePO, and enforced as an equivalent Data Loss Prevention (DLP) Endpoint Cloud Protection policies. DLP Endpoint agent relies on FRP to perform the encryption action associated with Cloud Data Protection rules.

FRP relies on Key Management Service (KMS) to fetch the required keys for encryption operations. Unlike in previous versions of FRP where encryption keys are stored within McAfee ePO, FRP 6.0 requires that a Key Management Service be provisioned, and encryption keys are stored and access controlled using Key Management Service.

FRP 6.0 also integrates with Endpoint Health Check (EHC) to restrict availability of encryption keys based on the state of the endpoint if the health check is enabled for Cloud Data Protection rules.

The `Common UI Policy:Cloud Sync` extension installed on on-premise McAfee ePO synchronizes policy data from McAfee ePO Cloud. This ensures that Cloud Data Protection rules configured on McAfee ePO Cloud are translated into appropriate DLP Endpoint Cloud Protection and FRP Endpoint Health policies. Access Control lists for encryption keys are also set up within Key Management Service in line with the configured Cloud Data Protection rules.

Deployment of FRP endpoint agents and policy management is still through on-premise McAfee ePO.



FRP 6.0.0 is a Windows only release that is restricted in comparison to its earlier releases. Upgrade from previous versions of FRP is also not supported with this release. FRP 6.0.0 is available for new installations only.

Features

These are the key features of FRP 6.0.0.

- **KMS registration and tenant provisioning** — Facilitates in adding KMS as a registered server and provisioning a KMS tenant using McAfee ePO.
- **Encryption of files and folders synced to cloud storage services** — Enables encryption action for DLP Endpoint Cloud Data Protection Rules. Also allows for a transparent end user experience on encrypted content access.

McAfee Cloud Data Protection Beta Release 21-Mar-2017

2

Installing the FRP client

The FRP software packages and extensions must be checked into the on-premise 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*
- ▶ *Install the FRP and Help extensions*
- ▶ *Check in the FRP software package*
- ▶ *Key Management Service*
- ▶ *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

Systems	Requirements
McAfee ePO server systems	See the McAfee ePO product documentation.
Client systems	<ul style="list-style-type: none"> • CPU: 1 GHz or faster • RAM: 1 GB RAM (32-bit) or 2 GB RAM (64-bit) • Hard disk: 200 MB minimum free disk space • TCP/IP network connection


Table 2-2 Software requirements

Software (or package name)	Requirements
McAfee management software	McAfee ePolicy Orchestrator 5.3.1 or above
McAfee® Agent	<ul style="list-style-type: none"> • McAfee Agent for Windows 4.8 Patch 3 or above

Table 2-2 Software requirements (continued)

Software (or package name)	Requirements
File and Removable Media Protection	Extensions <ul style="list-style-type: none"> • FRP-extension-6.0.0.xxx.ZIP • help_eeff_600.ZIP • Common UI Policy:Cloud Sync
	Software packages <ul style="list-style-type: none"> • MfeFRP_Client_6.0.0.xxx.ZIP for Windows systems

Table 2-3 Operating system requirements

Systems	Software
McAfee ePO server systems	See the McAfee ePO product documentation.
Windows client systems	<ul style="list-style-type: none"> • 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) <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  For the latest information on supported platforms, environments, and operating systems, refer to the KnowledgeBase article KB81149. </div>
Virtual Desktop Infrastructure (VDI)	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.

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-6.0.0.xxx.ZIP
 - b help_eeff_600.ZIP
 - c Common UI Policy:Cloud Sync

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

- 4 Click **OK**.

McAfee Cloud Data Protection Beta Release 21-Mar-2017

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_6.0.0.xxx.ZIP` software package for Windows 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.

Key Management Service

This section explains how to add Key Management Service (KMS) as a registered server and provision a KMS tenant using McAfee ePO.

Permissions required for Key Admins and Tenant Admins

The administrators require permission to manage the key server and access the registered server. Perform this task to provide administrators the required permissions.

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 | User Management | Permission Sets**.
- 3 On the left pane, click **KeyAdmins**, then click **Edit** corresponding to **FRP Manage Keys**.
- 4 Select the **Manage Key Server** option and click **Save**.
- 5 Click **Edit** corresponding to **Registered servers**.
- 6 Next to **Key Management Service**, enable the **View, create and edit registered servers** option, then click **Save**.
- 7 Click **Edit** corresponding to **Name and users**.
- 8 Next to **Active Directory groups mapped to this permission set**, select `adsrv` as **Server name**, add **Administrators**, **Domain Admin Users**, and **KeyAdmins** groups by clicking **Add**, then click **Save**.

Add KMS as a registered server and provision a tenant on McAfee ePO.

Perform this task to add KMS as a registered server and provision the KMS tenant on McAfee ePO.

Before you begin

You need to download the KMS certificate and import it to the key store on McAfee ePO. For more information, please refer to the *Key Management Service 1.0.0 Installation Guide*.



If you do not perform this task, the connection to KMS fails and the message "Unable to establish connection with key management service, please try again." appears.

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 | Registered Servers | New Server**.
- 3 Next to **Server type**, select **Key Management Service** from the drop-down list.
- 4 Type the required **Name** for the server and any **Notes**, then click **Next**.
- 5 Next to **Host Name**, type the KMS IP address where the KMS server is installed.



The **Port Number** and **Admin Port Number** are set to 8443 and 9003 respectively by default.

- 6 Click **Verify Connection**.
The message "Successfully connected to key management service" appears.
- 7 Click **Save**.
- 8 Select the created KMS server, click **Actions | Key Management Service: Provision**.
- 9 Type the **Username** and **Password** that were set up while installing KMS.
- 10 Type the tenant **Administrator Email** address, then click **Send Verification Email**.
A verification email will be received on the provided email address.
- 11 Type the **Email Verification Code** that you received.
- 12 Choose the required **ePO Cloud License File** in .json format.
- 13 Click **Save**.

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**.

McAfee Cloud Data Protection Beta Release 21-Mar-2017

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**.
 - 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.
 - 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.

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](#).

McAfee Cloud Data Protection Beta Release 21-Mar-2017

- **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.

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.

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**.
- 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**.

McAfee Cloud Data Protection Beta Release 21-Mar-2017

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.

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

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](#).

3

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*


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.


Authentication

You can define the policy settings for authentication to all FRP modules on the **Authentication** policy page.

OS Token



Option	Definition
Initialization Method	<p>Require authentication using Active Directory credentials at first logon — Select this option to require users to authenticate using Active Directory domain credentials at first logon on a client system for access to encryption keys assigned to OS Authentication. This option is disabled by default.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  Users will always be required to authenticate using Active Directory credentials with McAfee Endpoint Assistant. </div>

McAfee Endpoint Assistant

Option	Definition
Passcode Definition	<p>Select one of the following options to set a PIN or password to authenticate to the McAfee Endpoint Assistant app:</p> <ul style="list-style-type: none"> • PIN, exactly 4 digits — Enforces a PIN with exactly 4 digits. • PIN, exactly 6 digits — Enforces a PIN with exactly 6 digits. • PIN, exactly 8 digits — Enforces a PIN with exactly 8 digits. • Password: Minimum 6 characters with 1 numeric, 1 alphabetical characters — Enforces a password with minimum 6 characters containing 1 numeric and 1 alphabetic characters. • Password: Minimum 6 characters with 1 numeric, 1 uppercase and 1 lowercase characters — Enforces a password with minimum 6 characters containing 1 numeric, 1 uppercase, and 1 lowercase characters. • Password: Minimum 8 characters with 1 numeric, 1 uppercase, 1 lowercase and 1 symbol characters — Enforces a password with minimum 8 characters containing 1 numeric, 1 uppercase, 1 lowercase, and 1 symbol characters.
Client-to-Server Sync	<p>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.</p> <p>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.</p> <p>Every __ days (1-365) — Enter the number of days.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  This option is enabled only if the Require periodic authentication using domain (AD) credentials option is enabled. </div>
Connection Timeout	<p>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.</p>

McAfee Cloud Data Protection Beta Release 21-Mar-2017

Encryption Key Options

Option	Definition
Unlock Triggers	<p>Specifies the conditions at which users are prompted to authenticate (if required) and encryption keys are loaded.</p> <ul style="list-style-type: none"> • Windows logon — Encryption keys get loaded (if available) immediately following a successful OS logon. It is recommended that this unlock trigger is selected. • Encryption key access — Encryption keys are loaded whenever a user-initiated action requires access to an encryption key (authentication against domain credentials will be required at first logon if the relevant policy option is selected). • McAfee tray — Enables the user to manually logon/logoff to FRP using the McAfee tray Quick Settings menu.
Lock Triggers	<p>Specifies the conditions that trigger the unloading of encrypted keys.</p> <ul style="list-style-type: none"> • Windows screen lock — Controls encryption key access on a Windows screen lock operation. <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p> This option can either be disabled or enabled with a timeout. If disabled, the keys are always dropped as soon as Windows is locked. Being disabled is same as enabled with timeout as 0.</p> </div> <ul style="list-style-type: none"> • Key use inactivity — Requires that the user reauthenticate if encryption keys have not been used for the configured time period (5-720 minutes). Default value is 60.
Client-to-Server Sync	<p>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.</p>
Key Cache (this option is applicable only to keys that are assigned to systems and not users)	<p>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.</p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p> Status XML does not contain key information if the keys have been unloaded due to key cache expiry.</p> </div> <p>Key Cache expiry period — 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.</p>

Custom Messages

Option	Definition
OS Token Initialization Prompt (Windows)	The text displayed to prompt end users to authenticate using the Active Directory domain credentials to provide the OS token on a particular system.
OS Token Initialization Prompt (McAfee Endpoint Assistant app)	The text displayed to prompt end users to authenticate using the Active Directory domain credentials to allow provisioning of the McAfee Endpoint Assistant application.

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.

Option	Definition
Advanced File Handling Options	<ul style="list-style-type: none"> • 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.
Blocked Processes	<p>Blocks the specified processes from opening encrypted files. FRP blocks a process by withholding the keys required to decrypt the files.</p> <ul style="list-style-type: none"> • Add — Adds the process to the block list. • Remove — Removes the process from the block list. • Edit — Edits the process in the block list.
Key Request Exclusions	<p>Enables the process (such as anti-virus) to exclude encrypted files if required encryption keys are not already loaded.</p> <ul style="list-style-type: none"> • Add — Adds the process to the exclusion list. • Remove — Removes the process from the exclusion list. • Edit — Edits the process in the exclusion list.
File Extension Exclusions	<p>Excludes the specified file extensions from encryption.</p> <ul style="list-style-type: none"> • Add — Adds the file extension to the exclusion list. • Remove — Removes the file extension from the exclusion list. • Edit — Edits file extension in the exclusion list.
Advanced Debug Options	<p>Specify the elements to exempt the device inserted by the user for better security.</p>

General

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

Option	Definition
Windows Explorer integration	<p>Specifies the Windows Explorer context menu options available to a user on the client system.</p> <ul style="list-style-type: none"> • Enable padlock icon visibility — Displays a padlock icon on encrypted objects. Default value is enabled. • Enable search encrypted — Enables Search encrypted option for client system users. Default value is disabled.

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.

McAfee Cloud Data Protection Beta Release 21-Mar-2017

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.

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**.

McAfee Cloud Data Protection Beta Release 21-Mar-2017

- 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.

A

Additional information

This additional information includes guidelines on FRP key management, FRP integration with Endpoint Health Check, and Endpoint Health Check failure events.

Contents

- ▶ *FRP key management*
- ▶ *FRP integration with Endpoint Health Check*
- ▶ *Endpoint Health Check Failure Events*

FRP key management

Information on encryption keys used for Cloud Data Protection rules are available through the **FRP Key Management** page.

This page can be accessed by clicking **Menu | Data Protection | FRP Key Management**. The default columns included in this page provides details on Key ID and associated classification factors.

FRP integration with Endpoint Health Check

If an Endpoint Health Check is associated with a Cloud Data Protection rule with an encryption action, FRP checks the status of the endpoint and verifies whether the endpoint is deemed safe at every client sync interval (key update requests). In the case where the endpoint does not satisfy the required health check criteria, no new keys are made available and existing keys that are cached on the endpoint are purged and made unavailable. Encryption keys are again made available whenever the endpoint next satisfies the required health check criteria (the check is carried out every single time the client requests for encryption key updates).

Endpoint Health Check Failure Events

The **Endpoint Health Check Failure Events** page can be accessed by clicking **Menu | Reporting | Queries and Reports | McAfee Groups | FRP Queries | FRP: Endpoint Health Check Failure Events**.

If an administrator needs to override this action and enable access to encryption keys even when the system does not satisfy the configured health check criteria, which can be performed through **Actions | Override Endpoint Health Check**. The override interval is for 48 hours.

Endpoints for which override action is selected is recorded as part of this query: **Menu | Reporting | Queries and Reports | McAfee Groups | FRP Queries | FRP: Endpoints with Endpoint Health Check Override enabled**.

A

Additional information
Endpoint Health Check Failure Events

McAfee Cloud Data Protection Beta Release 21-Mar-2017

Index

- A**
 - [about this guide 5](#)
 - [agent wake-up call, sending 14](#)
- C**
 - [conventions and icons used in this guide 5](#)
- D**
 - [deployment 13](#)
 - [deployment, installing products 12](#)
 - [documentation
 - \[audience for this guide 5\]\(#\)
 - \[typographical conventions and icons 5\]\(#\)](#)
 - [drives, encryption 13](#)
- E**
 - [encryption keys, deployment 13](#)
 - [enforcement, *See* policy enforcement](#)
 - [extension, FRP
 - \[installing 10\]\(#\)](#)
- F**
 - [features 7](#)
 - [FRP policies
 - \[assign to managed system 21\]\(#\)
 - \[creating from Policy Catalog 20\]\(#\)
 - \[editing, from Policy Catalog 21\]\(#\)
 - \[enforcing on a system 22\]\(#\)
 - \[enforcing on a system group 23\]\(#\)](#)
- G**
 - [groups
 - \[policy enforcement for a product 23\]\(#\)](#)
- I**
 - [installation, FRP
 - \[checking in software package 11\]\(#\)
 - \[deploying to managed systems 12\]\(#\)
 - \[product extension 10\]\(#\)
 - \[requirements 9\]\(#\)](#)
- K**
 - [keys
 - \[encryption 13\]\(#\)](#)
- M**
 - [managed systems
 - \[assigning FRP policy 21\]\(#\)
 - \[assigning policy to 22\]\(#\)
 - \[deploying FRP on 12\]\(#\)
 - \[policy management on 17\]\(#\)](#)
 - [master repository
 - \[checking in software package 11\]\(#\)](#)
- O**
 - [operating system requirements 9](#)
 - [operating systems 13](#)
- P**
 - [password rule settings 17](#)
 - [policies
 - \[about 17\]\(#\)
 - \[assigning to system groups 22\]\(#\)
 - \[assigning to systems 21\]\(#\)
 - \[configuring 17\]\(#\)
 - \[create on Policy Catalog page 20\]\(#\)
 - \[editing, from Policy Catalog 21\]\(#\)
 - \[enforcement 17\]\(#\)
 - \[viewing 17\]\(#\)](#)
 - [Policy Catalog
 - \[creating FRP policies 20\]\(#\)
 - \[editing FRP policies 21\]\(#\)
 - \[page, viewing 17\]\(#\)](#)
 - [policy categories
 - \[encryption options 20\]\(#\)
 - \[exclusions 20\]\(#\)
 - \[password rules 17\]\(#\)](#)
 - [policy enforcement
 - \[enabling and disabling 23\]\(#\)
 - \[for a product 22, 23\]\(#\)
 - \[on a system group 23\]\(#\)](#)
 - [policy inheritance
 - \[lock 21\]\(#\)](#)

McAfee Cloud Data Protection Beta Release 21-Mar-2017

policy settings

 general [20](#)

 integration [20](#)

product installation

 configuring deployment tasks [12](#)

R

requirements [9](#)

S

servers

 requirements [9](#)

software packages

 checking in [11](#)

software requirements [9](#)

system groups, policy enforcement [23](#)

system requirements [9](#)

systems

 assigning policies to [21](#), [22](#)

 policy enforcement for a product [22](#)

