Method of Procedure

Revision A

Using the McAfee Removal Tool

Contents

- *Confidentiality Notice*
- *Introduction*
- *Procedure*
- *Troubleshooting*
- *Mass deployments*

Confidentiality Notice

This document and its contents are confidential and proprietary to Intel Security, Inc. (Intel Security) and are intended only for the individual or entity specified herein or otherwise identified by Intel Security.

Unauthorized use, reproduction, or distribution of this document or any of its contents may result in legal and financial penalties.

Introduction

The McAfee Removal (MFERemoval) tool allows you to remove ePO products from computers in your network.

Warnings and liability

The MFERemoval tool is provided as a best effort by Intel Security support. This software:

- Has not been tested or approved by Intel Security.
- Should be tested in your local environment before you attempt to deploy it to your users.
- Expires and ceases to function after the date indicated. To find the expiration date:
    1. Extract the standalone executable.
    2. Right-click the executable file and click Properties | General | Description.

System requirements

The following basic requirements are required on each machine:

- Windows 5.x-10.x
- X86 or x64
- Administrative permissions

If you running the application manually with UAC enabled, elevation is also required. For more information:

http://msdn.microsoft.com/en-us/library/windows/desktop/aa511445.aspx

Other dependencies:

- Verisign Class 3 Public Primary Certification Authority – G5
  https://kc.mcafee.com/corporate/index?page=content&id=KB87096
- Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package (Version 10.0.40519.01)
  https://www.microsoft.com/en-us/download/details.aspx?id=26999

Procedure

You can run the MFERemoval tool on your local machine by running it from the command line.

Task

1 Run MFERemoval100.exe at the command line with the appropriate switches.
Switches are not case sensitive.

/noreboot	Will not call reboot, overwrites **/t** and **/forcereboot**
/forcereboot	Will call reboot upon completion
/t xx	Time in minutes to delay if reboot is needed or **/forcereboot** is used. Default is 10 minutes. For example, **/t 10**
/pass	HIPs client UI password. Does not work with HIPs 7. For example, **/pass abcde12345**
/q or **/quiet**	Prevents status message boxes. If deployed from ePO, this is automatically set. When specified, the process exits when it completes successfully.
Product switches: **/MA** – McAfee Agent **/DLP** – Host Data Loss Prevention **/HIP** – Host Intrusion Prevention **/VSE** – Virus Scan Enterprise **/ENS** – Endpoint Security **/DXL** – McAfee Data Exchange Layer **/EIA** – Endpoint Intelligence Agent **/TIEM** – McAfee Threat Intelligence Exchange Module for VSE **/MAR** – McAfee Active Response **/DATRep** – DATReputation **/All** – All products	One or more are required.

For example:

Scenario 1: Remove all products and reboot after 5 minutes	**MFERemoval100.exe /all /forceboot /t 5**
Scenario 2: Remove VSE and HIP. Include the HIP password.	**MFERemoval100.exe /vse /hip /pass abcde12345** or **MFERemoval100.exe /vse /hip /pass "abc 123"**

2 Reboot your computer.
A reboot is strongly recommended if you have removed products with the intention of reinstalling them.
Removing HDLP requires a reboot.
Removing individual products does not require a reboot.

Removing all products requires a reboot if you want to reinstall them later.

Required reboot	Occurs when removing HDLP using force option or files/registry key could not be removed. MFERemoval performs clean up. • Normal mode – Reboot option appears in status box. • Quiet mode – MFERemoval calls shutdown.exe with a time specified **`/t`** (default of 10 minutes). Valid time for **`/t`** are 0-99. • **`/noreboot`** can be used to prevent an automatic reboot.
Recommended reboot	Occurs when service/driver is pending a reboot. • Normal mode – Reboot option appears in status box. • Quiet mode – No action.

Troubleshooting

Use the status box and log files to troubleshoot errors.

Success and error determination

When the application completes successfully, a dialog box displays with the following information:

- The results
- The path to the log file
- Reboot recommendation (if any)

Also, the application writes a generic registry key that can be queried. The key is deleted at the start of each run, and then rewritten when the process is successful. If the registry key is missing, you know there was an error.

Logs and data

The MFERemoval tool writes data to the following logs:

- Runtime log – generates to **%SYSTEM ROOT%\TEMP\McAfeelogs\Applet - YYYY.MM.DD – HH.MM.SS-[MFERemoval100.exe].txt**
- Event log – after runtime, creates a Windows Application Event Log entry from source **MFERemoval100.exe**.

  Event IDs:

  - 666 – failure
  - 777 – success

Registry key

The registry key can be found in these locations, depending on your version of Windows:

X64	**HKEY_LOCAL_MACHINE\Software\Wow6432Node\MFERemoval**
X86	**HKEY_LOCAL_MACHINE\Software\MFERemoval**

Registry key values:

Value name	Finish
Value name for each product removed	• MA • VSE • HIP • DLP • ENS • DATRep • TIEM • DXL • EIA • MAR
Data	1

Activity icon

When the application runs, the Activity icon displays in the Windows Notification Area. This icon is a white Intel logo on a blue background. The purpose of the icon is to indicate that the application is

running.

For more information about the Windows Notification Area:

http://msdn.microsoft.com/en-us/library/windows/desktop/aa511448.aspx

To view the Windows Notification Area:

http://windows.microsoft.com/en-us/windows7/change-how-icons-appear-in-the-notification-area

Review the log file

When the process completes successfully, the log reads: **`Exit: Success`**

If this message is missing from the log, you will need to correct the error or contact your Intel Security Support representative.

Common errors

You can diagnose problems using error messages in the status box or in the log file.

Invalid Password. Please provide password as a switch. Example: MFERemoval.exe /pass abcde12345	• **`/pass`** switch was provided and it was incorrect • If there is a space in the HIP password, use quotes: **`/pass "abcde 12345"`**
HIPS Enabled. Please disable HIPs IPS and re-run.	• Open HIP client UI, unlock the GUI, and disable IPS. • In ePO, disable Host IPS via policy and push down to client. • Provide password via command line switch: **`/pass abcde12345`** or **`/pass "abcde 12345"`**
VSE AP Enabled. Please disable VSE AP and re-run.	• Open VSE Console and disable Access Protection. • In ePO, disable VSE AP via policy and push down to client.
Failed to install certificate: 4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5	• MFERemoval depends on Verisign Class 3 Public Primary Certification Authority – G5 to work. • MFERemoval attempted to install a certificate and failed. • For more information: https://kc.mcafee.com/corporate/index?page=content&id=KB87096
Unable to disable protection	• MFERemoval was unable to establish Trust with McAfee software. • Other reasons, including failed certificate install. Contact Intel Security support.

Work arounds

You can use the **`/force`** and **`/safemode`** switches to remove products when you encounter errors.

- Always use the **`/all`** switch with these options.
- Test these options before using them in a mass deployment

/force

Use **`/force`** to bypass all check and remove all products. Intel Security recommends this option.

```
/force /all
```

Requires a reboot.

/safemode

Use **`/safemode`** to boot a computer into safe mode, run, and then reboot back into normal mode.

```
/safemode /all
```

Safe mode troubleshooting

- Does not work with pre boot authentication. Reboot would leave at Preboot screen twice (once to go into safe mode and once to back into normal mode)
- GPO could interfere auto login – reboot would leave at safe mode log-in screen
  https://technet.microsoft.com/en-us/magazine/ee872306.aspx

  https://technet.microsoft.com/en-us/library/cc978776.aspx
- GPO could add back legal notice caption – would leave at safe mode waiting on a click
  https://technet.microsoft.com/en-us/library/cc939712.aspx
- Does not work properly on Domain Controllers.

Safe mode process

1. Create a temp user and add it to the local admin group.
2. Set the OS to boot into safe mode.
3. Reboot after one minute unless `/t` is set to another time.
4. Boot into safe mode.
5. Run MFERemoval, delete temp user, reset all settings
6. Reboot
7. In Normal mode, delete temp user profile.

Mass deployments

You can update more than one computer at a time. To implement a mass deployment process, create a custom ePO Endpoint Deployment Kit (EEDK) package and deploy it using ePO.

Before you begin

EEDK packages are not supported by Intel Security support. However, you can visit the McAfee Community site for information and support:

https://community.mcafee.com/docs/DOC-3401

The current version of EEDK is 9.6.1.

Task

1 Complete the initial setup.

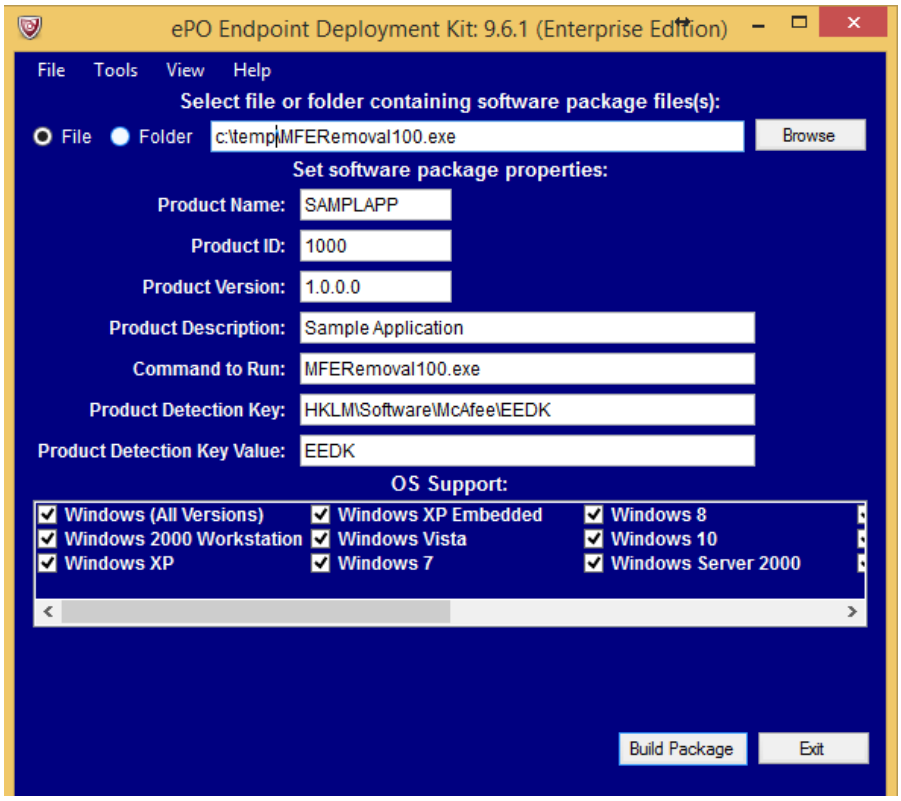
   a. Extract the zip file.

   b. Create a new folder called **Build.**

   c. Run **`EEDK.exe`**.

   d. Click Tools | Option and click Browse.

   e. Select your **Build** folder and click **Save**.



2 Create the EEDK for MFERemoval.

   a. Select File. Browse to **`MFERemoval100.exe`**.

   b. Specify the software package properties.

Product Name	Type a name. Limit to 8 alphanumeric characters.
Product ID	Type a 4 digit number.
Product Version	Type the version number. Use 4 digits separated by periods.
Product Description	Enter the description you want to appear when creating the ePO task.
Command to Run	Enter the name of the executable file: MFERemoval100.exe. **Note:** Intel Security recommends using command line switches in the ePO deployment task. Any switch that you use is automatically hard coded and always used when deployed through ePO. This method makes it easy to identify the products that are being removed by the task.
Product Detection Key	Specify the registry location that contains the **Product Detection Key Value**. In the EEDK, abbreviate the top-level key locations. For example, HKEY_LOCAL_MACHINE is abbreviated HKLM.
Product Detection Key Value	Specify the registry key value. If this key value exists on a machine the deployment task will *not* run. The field cannot be blank. **Scenario 1:** Use the product detection key **MFERemoval** and the non-existent key value **New.** Because, the key value does not exist, all computers are updated. **Scenario 2:** Use the product detection key **MFERemoval** and the non-existent key value **Finish.** Because, the key value is already present on computers that have updated successfully, only computers that are missing the key are updated.
OS Support	Select all of the Windows operating systems that you support.

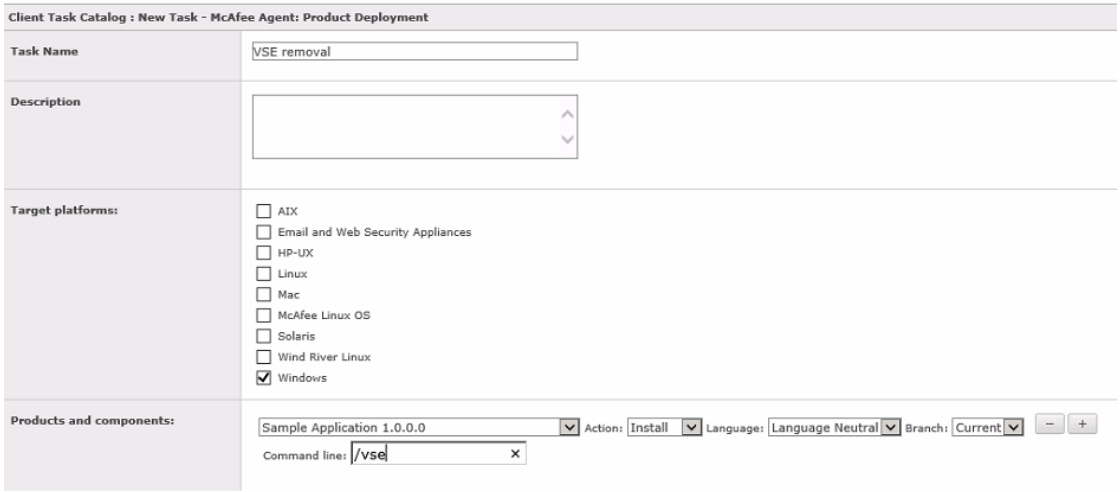
c. Click **Build Package**.
   A status box notifies you when the new zip is created.

3 Check the EEDK package into ePO.

   a. In ePO, open the **Master Repository**.
   b. Click Check in Package.
   c. Select the package type: **Product or Update (.ZIP)**
   d. Next to **File Path**, click **Browse** and locate the EEDK package.
   e. Click **Next**, choose the branch, click **Save**.

4 Create the client task in ePO.

   a. In ePO, open the Client Task Catalog.
   b. Select McAfee Agent.
   c. Click New Task.
   d. Select the task type: **Product Deployment**. Click **OK**.
   e. In the **Task Name** field, enter a name.
   f. Complete the options for **Products and Components**. For example, you can add a product switch: /vse.



5 Assign client tasks.

Caution	Incorrectly assigned tasks can cause the removal tool to make changes to your entire network. If McAfee Agent is removed, it means that your computers are not protected by ePO. Intel Security recommends assigning the task to just the nodes that need to run the removal process or using tag-based client task assignments.

Create EEDK with FramePkg

You can also create the EEDK using FramePkg.exe. Most of the steps are the same.

Using FramePkg allows you to reinstall McAfee Agent after successfully running a mass deployment.

Before you begin

- Each customer requires a unique copy of framepkg.exe
- You must use one of the following MFERemoval switches: /MA, /ALL, or /SAFEMODE

Task

1 Complete the initial setup.

   a. Create a new folder.

   b. Copy MFERemoval and Framepkg.exe to the new folder.

2 Setup EEDK.

   a. In EEDK, select **Folder.**

   b. Click **Browse** and locate your new folder.

   c. Specify the software package properties.

Product Name	Type a name. Limit to 8 alphanumeric characters.
Product ID	Type a 4 digit number.
Product Version	Type the version number. Use 4 digits separated by periods.
Product Description	Enter the description you want to appear when creating the ePO task. For example, MFERemoval with MA install 5.03
Command to Run	Enter the name of the executable file: MFERemoval100.exe. Use the FramePkg switches: • **`/framepkg`** • **`/framepkgcmd='cmdline switches'`** For example: **`MFERemoval.exe /framepkg /framepkgcmd='/install=agent /silent`**

	/customprops1="MFERemovalRanOn"'
Product Detection Key	Specify the registry location that contains the **Product Detection Key Value**. In the EEDK, abbreviate the top-level key locations. For example, HKEY_LOCAL_MACHINE is abbreviated HKLM.
Product Detection Key Value	Specify the registry key value. If this key value exists on a machine the deployment task will *not* run. The field cannot be blank. **Scenario 1:** Use the product detection key **MFERemoval** and the non-existent key value **New.** Because, the key value does not exist, all computers are updated. **Scenario 2:** Use the product detection key **MFERemoval** and the non-existent key value **Finish.** Because, the key value is already present on computers that have updated successfully, only computers that are missing the key are updated.
OS Support	Select all of the Windows operating systems that you support.

d. Click Build Package.

   A status box notifies you when the new zip is created.

3 Check in EEDK package.

4 Create the client task in ePO.

5 Assign client tasks.

After the task runs successfully, the computer reboots and FramePkg attempts to reinstall MA. If there is no reboot, FramePkg will run automatically.

Note	MFERemoval cannot guarantee the reinstallation of MA. For all issues, contact the appropriate Intel Security support team.

Copyright © 2016 McAfee, Inc. www.intelsecurity.com

Intel and the Intel logo are trademarks/registered trademarks of Intel Corporation. McAfee and the McAfee logo are trademarks/registered trademarks of McAfee, Inc. Other names and brands may be claimed as the property of others.