Trellix

Method of Procedure

Version 24.05

Endpoint Product Removal Tool User Guide

Copyright

Contents

1. Introduction

The Endpoint Product Removal (EndpointProductRemoval.exe) tool allows you to remove the following Trellix products from endpoints in your environment:

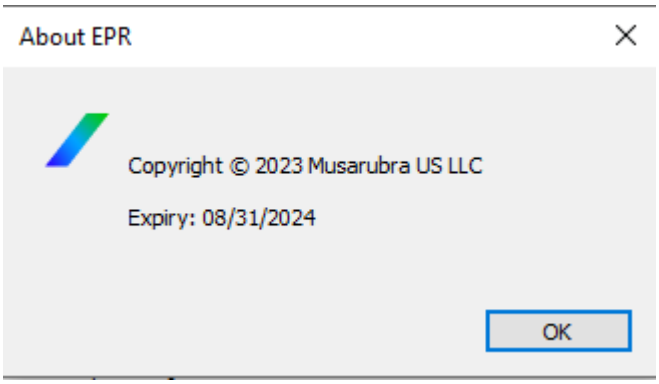
- DAT Reputation (DAT Rep)
- Data Exchange layer (DXL)
- Data Loss Prevention (DLP)
- Endpoint Intelligence Agent (EIA)
- Endpoint Security (ENS)
- Endpoint Security Storage Protection (ENS SP)
- ePO-MER
- Host Intrusion Prevention (HIPS)
- Trellix Active Response (MAR)
- Trellix Agent (MA)
- Trellix Application and Change Control (MACC)
- Client Proxy (MCP)
- Trellix Drive Encryption (MDE)
- Trellix File and Removable Media Protection (FRP)
- Trellix Management of Native Encryption (MNE)
- Trellix Product Improvement Program (not explicit: removed as part of Trellix Agent removal)
- Trellix Stinger
- MOVE multiplatform deployment
- Trellix Endpoint
- Trellix Endpoint Detection and Response (EDR)
- Policy Auditor (PA)
- Site Advisor Enterprise (SAE)
- Threat Intelligence Exchange Module for VSE (TIEm)
- Endpoint Security (HX) Agent
- VirusScan Enterprise (VSE)

For multi-platform Trellix products, note that this tool is for Windows versions only. The tool can be deployed via ePO or 3rd party deployment tools or can be executed as a standalone application.

1.1 Warnings and liability

This software:

- Should be tested in a pilot environment before you attempt to deploy it to your users.
- Expires and ceases to function after a specified date. To find the expiration date, click the icon in the top left corner of the tool, launch the About menu and the expiry date will be visible here.



- The tool expires so that customers are forced to update the EPR tool once a quarter to ensure the customer is running with the latest EPR Tool service level that picks up new bug fixes or new functionality that the customer should be using.
- Endpoint Upgrade Automation will not execute on an endpoint on which the EPR tool has been executed until that endpoint has been rebooted
- It is not recommended to remove Trellix Agent if there will be any other products remaining on the endpoint after it is removed (applies to both products supported and not supported by the EPR tool)
- If running from the command line, it is recommended to use the command line parameters for each individual product to be removed, instead of using the `-ALL` parameter.
- EPR may determine that Trellix Drive Encryption (MDE), Trellix Native Encryption (MNE) cannot be safely removed. In this scenario, MA will also not be removed, as this could affect the operation of MDE or MNE.
  - MDE will not be removed if it is active
  - MNE will not be removed if Network Unlock is enabled

    - In some versions of MNE, the flag stating that the product is safe to remove is incorrectly set, which leads to EPR unexpectedly not removing the product. In this case, refer to the command line parameter descriptions below for --BRUTEFORCE=REMOVE_ACTIVE_MNE.
- EPR may determine that Trellix Application and Change Control is active, in which case it will not be removed
- EPR does not operate in the presence of the following products:
    - VSE for Storage
    - VSE for SAP
    - OVI
    - Deep Defender
    - HIPS 7
    - VSE 8.5

The default and strongly recommended action is to reboot the endpoint after removing any products.

When the EPR tool removes products, it attempts to delete all files and registry keys associated with each product. For most products, there will be some files that cannot be deleted immediately, such as driver files that are loaded by the OS. When this happens, the EPR tool will mark the files for deletion on reboot instead.

If the machine is not rebooted, the following scenarios are possible:

- Certain kernel drivers will remain loaded, and users may observe unexpected behavior
- Installs may succeed, but because certain delete operations must be deferred until the first reboot, the product may be corrupted after the first reboot, when those operations are actioned.
- Product installs may fail until the machine is restarted.
- The operating system may not function as expected because there are hooks to the kernel, which may not have the appropriate instructions.

1.2 Best Practices

The EPR tool is designed to remediate endpoint that have a specific issue that cannot be fixed via the normal support channels. It should be used as a last resort and only after the issues have been properly analyzed and the details have been provided to the appropriate point product team via support.

It is not designed to be used as an ENS migration tool. If you are doing ENS migrations, you should use the Endpoint Upgrade Assistant for this purpose. If you're planning to use Endpoint Upgrade Automation, it will not execute on an endpoint on which EPR tool has been executed until that endpoint has been rebooted.

The following are requirements and best practices for ensuring a successful EPR run:

- Run with Administrator permissions
- Run locally from the system you're remediating. For example: don't execute from a network share
- When deploying from ePO, ensure you've supplied the mandatory command line arguments when creating your deployment task
- In most cases, `--ALL` removal should not be used. It's recommended that specific point product arguments are used to remove products. Example: `--accepteula --VSE`

1.3 System requirements

The following basic requirements are required on each machine:

- Windows 7 SP1 and later
- Windows Server 2008 R2 SP1 and above (Server Core versions are not supported)
- X86 or x64
- Administrator rights

2. Procedure

You can run the Endpoint Product Removal tool on your local machine by either running it from the command line or using the graphical user interface. If no command line is supplied the user interface is displayed.

2.1 Executing via the command line

Run the Endpoint Product Removal tool at the command line with the appropriate arguments. The Command line arguments are not case sensitive.

Argument	Removal order	Action
none	N/A	This will open the graphical user interface.
--accepteula	N/A	**Mandatory.** If not supplied EPR will not execute
--ALL	N/A	Remove all supported Trellix products
--VSE	1	Remove only VirusScan Enterprise
--TIEM	2	Remove only Threat Intelligence Exchange Module for VSE
--HIPS	3	Remove only Host Intrusion Prevention
--SAE	4	Remove only SiteAdvisor Enterprise
--DLP	5	Remove only Data Loss Prevention
--MAR	6	Removes only Trellix Active Response
--ENS	7	Remove only Trellix Endpoint Security
--DATRep	8	Remove only DAT Reputation
--MCP	9	Removes only Client Proxy
--MVISION_EP	10	Removes only Trellix Endpoint
--PA	11	Remove only Policy Auditor
--EIA	12	Remove only Endpoint Intelligence Agent
--FRP	13	Removes only Trellix File and Removable Media Protection. **Note:** Trellix Endpoint Encryption KeyStore files (*.sks) are preserved by default. These are local encryption keys created by FRP that do not exist in ePO.
--MNE	14	Removes only Trellix Management of Native Encryption **Note:** MNE and MA will not be removed if the Network Unlock authentication Feature is in effect
--MDE	15	Removes only Trellix Drive Encryption **Note:** If MDE is active MDE and MA will not be removed.

Argument	Removal order	Action
--MACC	16	Removes only Trellix Application and Change Control **Note:** If MACC is active, it will not be removed.
--MVISION_EDR	17	Removes only Trellix EDR
--DXL	18	Remove only Data Exchange Layer
--MA	19	Remove only Trellix Agent
--STINGER	20	Remove only Trellix Stinger
--EPOMER	21	Remove only ePO-MER
--MOVE	22	Remove only MOVE multiplatform deployment
--XAGENT	23	Remove only Endpoint Security (HX) Agent (v36.30 and earlier supported)
--BRUTEFORCE=REMOVE_ACTIVE_MNE	N/A	Force removal of MNE regardless of the status of the "CanRemove" flag value
--BRUTEFORCE= REMOVE_PROTECTED_MA	N/A	Force removal of MA regardless of the presence of MNE or MDE.
--BRUTEFORCE= REMOVE_ACTIVE_MNE_AND_MA	N/A	Force removal of MNE and MA regardless of the status of the "CanRemove" flag value
--DELETEFRPKEYS	N/A	If provided, Trellix Endpoint Encryption KeyStore files (*.sks) will be deleted.
--NOREBOOT	N/A	If provided, the Endpoint Product Removal tool will not restart the computer after removing the selected product(s) **Note:** EUA will not execute until a reboot has occurred.
--NOTELEMETRY	N/A	As part of product removal, EPR will send product removal telemetry to Trellix. If this switch is provided, no telemetry is sent.
--T=<*number of minutes to wait*>	N/A	Allows the user to set the amount of time to wait (in minutes) before restarting the client post product removal. (Note: This argument will be ignored if used in conjunction with "--noreboot")
--BRUTEFORCE= MFEDEEPREM_FOLDER_ATP_STOP	N/A	Used to work around issues where ENS ATP's $MfeDeepRem folder is not removed. This will cause EPR to stop the ATP service prior to deletion of the folder.

Argument	Removal order	Action
--INSTALLCERT=globalsign --INSTALLCERT=globalsign_r1 --INSTALLCERT=verisign_g5 --INSTALLCERT=usertrust_rsa --INSTALLCERT=sectigo_aaa --INSTALLCERT=digicert --INSTALLCERT=globalsign_r45 --INSTALLCERT=digicert_g4 --INSTALLCERT=MS_ID_Ver_2020 --INSTALLCERT=InstallAllCerts	N/A	Trellix endpoint products created after July 2019 are signed with a certificate issued by the Certificate Authority GlobalSign. If the GlogalSign root certificate is not installed on the endpoint, then Trellix products will not install, and the Endpoint Product Removal tool may not work correctly. To use this feature, the user must accept the EULA and use the command line parameter: --installcert=globalsign (SHA256) or –installcert=globalsign_r1 (SHA-1). If the certificate is present or disabled, it will reinstall an enabled certificate. No reboot is required after installing the certificate. Support for installing other potentially required root certificates is also provided via command line parameters. The verisign-g5, usertrust_rsa, sectigo_aaa and DigiCert root certificates are supported in addition to GlobalSign certificates and the Microsoft Identity Verification certificate for driver installs on certain operating systems. All certificates included can be installed using the InstallAllCerts option.
--REPAIR=ens_platform --REPAIR=fw --REPAIR=tp --REPAIR=atp --REPAIR=wc --REPAIR=dsp --REPAIR=ens	N/A	When used, EPR will invoke the ENS repair feature, which replaces the installed files from the ENS installer and sets some registry entries to default. This is potentially useful as a less invasive method of resolving issues. This is a comma separated list (no spaces). Examples: `--REPAIR=wc` - This will repair Web Control. `--REPAIR=ens`_platform,fw,tp,atp - this will repair ENS Platform, Firewall, Threat Prevention, Adaptive Threat Prevention - in the order that the options were supplied. `--REPAIR=ens` - this will repair all ENS modules. If modules can't be found and no unexpected failure occurs, the repair will still be deemed a success. `--REPAIR=,tp,fw,notaproduct,ens`, - this will repair Threat Prevention, Firewall and then all ENS, but will report a fail, because there are empty products (redundant commas) and 'notaproduct' is not a valid option.
--BRUTEFORCE= DELETE_LEGACY_SETTINGS	N/A	After migration from VirusScan Enterprise or Host IPS to Endpoint Security, migrated settings and exclusions are stored in `C:\ProgramData\McAfee\Endpoint Security\McAfeeSettingsBackup\`. Since this is a protected location, if removal of these files is desired, EPR is the recommended method of using this. The EULA must be accepted, so the full command line would be `--accepteula --noreboot --bruteforce=Delete_Legacy_Settings`.
--UPDATETRUST	N/A	This will update the Trellix inter-product trust system for older products, to ensure that product functionality is not impacted when this system changes, as happened in mid-2022. The EPR Tool and other products do this automatically, but a customer may use this option to update the trust system and avoid making any other change to the endpoint.

Argument	Removal order	Action
--ENABLEDEFENDER	N/A	The tool will attempt to install Microsoft Defender on Windows Server operating systems and restores a registry key set by VSE that disables Microsoft Defender. This operation requires a reboot to complete. Microsoft Windows 10 and Windows 11 are unaffected by this option as the functionality is controlled differently by Windows Security Center.
--BRUTEFORCE=MACC_Post_Reboot	N/A	The Tool will create “RunOnce” registry keys which will execute some cleanup steps for TACC after the first login, by an Admin User.
--BRUTEFORCE=ENS_Post_Reboot	N/A	The Tool will create “RunOnce” registry keys which will execute some cleanup steps for ENS after the first login, by an Admin User.

Example:

Scenario	Command line
Remove VSE, HIPs and DLP	`EndpointProductRemoval.exe --accepteula --VSE --HIPS --DLP`
Remove ENS with no reboot at the end of the process	`EndpointProductRemoval.exe --accepteula --ENS --noreboot`

2.2 Executing via the Graphical User Interface (GUI)

The Endpoint Product Removal tool has a simple, graphical user interface which informs the user about the installed Trellix products and allows you to select what product(s) to remove.

After launching the tool, the user needs to accept the EULA. This is always the first step, even if the tool was launched before.

Once the EULA is accepted, the Endpoint Product Removal tool scans for Trellix Products. It gets the list of the installed Trellix products from this registry key:

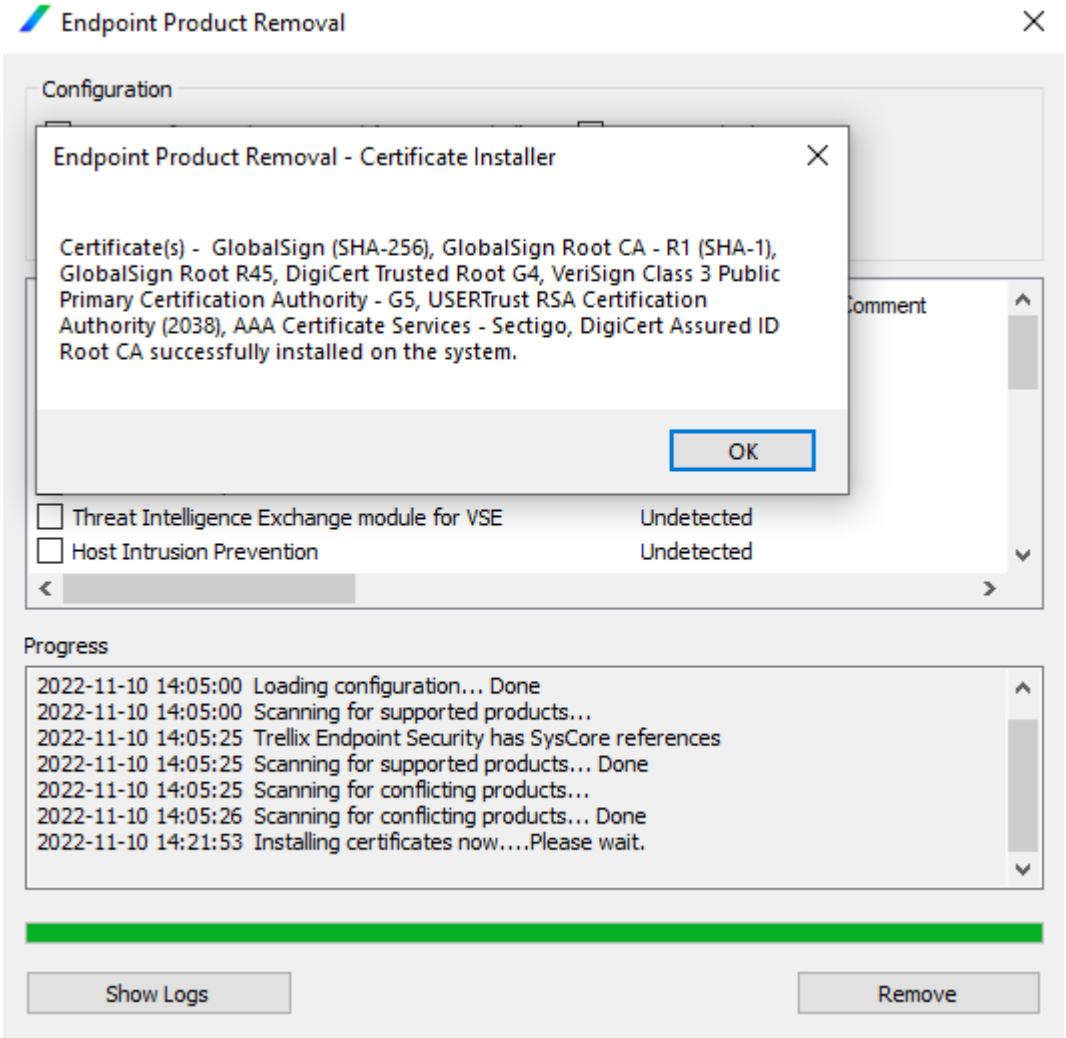
For x64 systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\NetworkAssociates\ePolicyOrchestrator\Application Plugins
```

Or for x86 Systems:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetworkAssociates\ePolicyOrchestrator\Application Plugins
```

There is one exception to this i.e., if a product that EPR supports is not found in the above registry location it will still appear in the list but will be identified as "**Undetected**". This is to allow for that fact that there may still be remnants of the products on the system due to a failed install/uninstall and by selecting the product, EPR will attempt to remove all remaining traces of the product.



After selecting the products to remove, click on **Remove** button. The default and recommended action is to reboot the endpoint after removing any products, but you can choose not to reboot by unselecting the “Restart after product removal” check box. Note: If you’re planning to use Endpoint Upgrade Automation, it will not execute on an endpoint on which EPR tool has been executed until that endpoint has been rebooted.

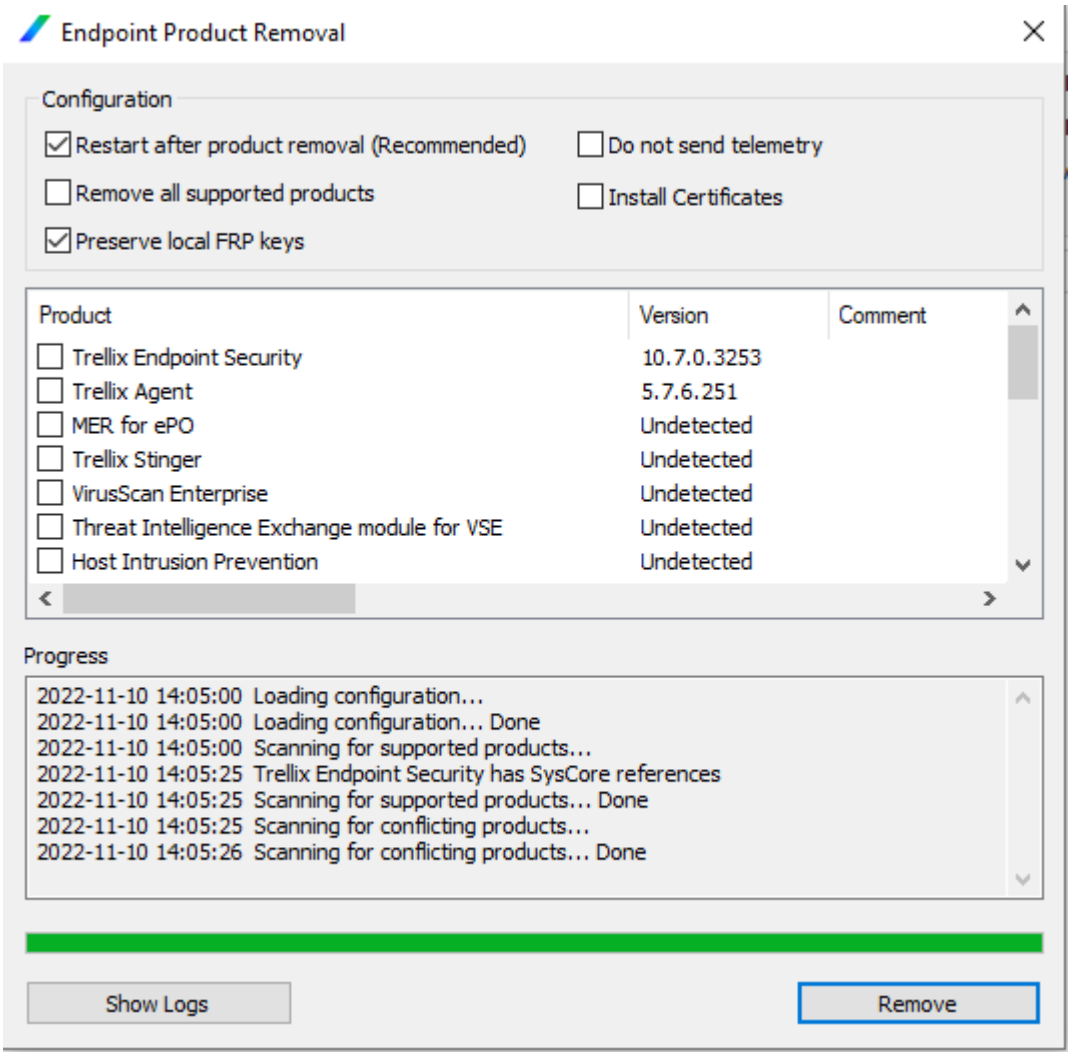
The progress of the removal is displayed in the Progress section. Logs can be opened by clicking on the **Show Logs** button.

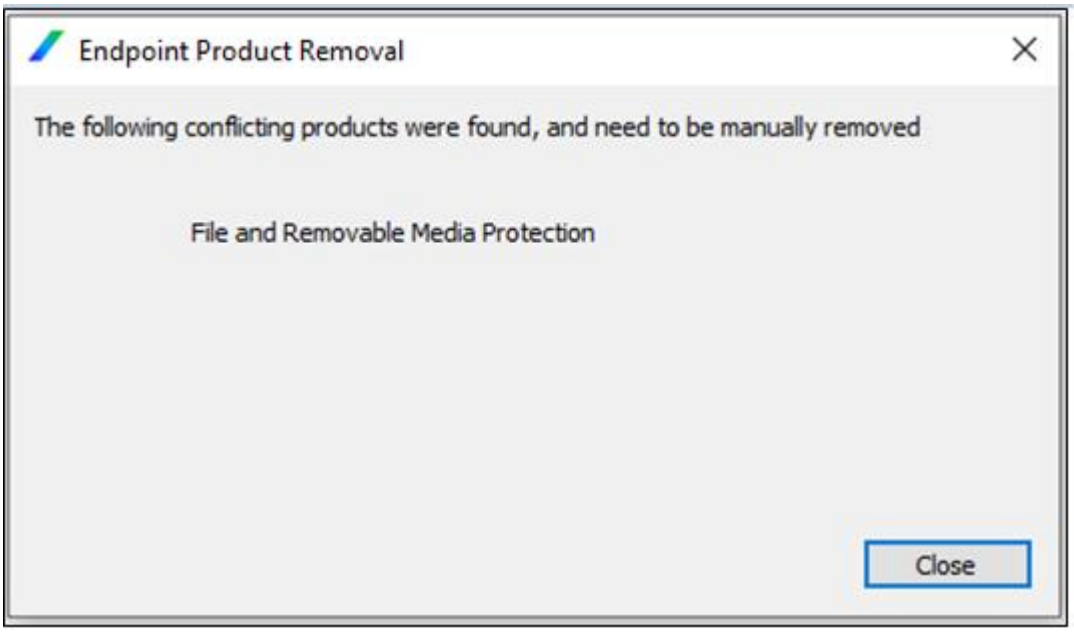
2.3 Conflicting products

When the EPR tool executes via the CMD line or UI it first checks for conflicting products and if any are found it will not execute.

2.3.1 Determining conflicting products via GUI execution

When a conflicting product is found a message will be displayed to the notify the user. Every time an attempt is made to remove a product the message will be displayed. You will not be able to execute the EPR tool until the conflicting product has been removed.





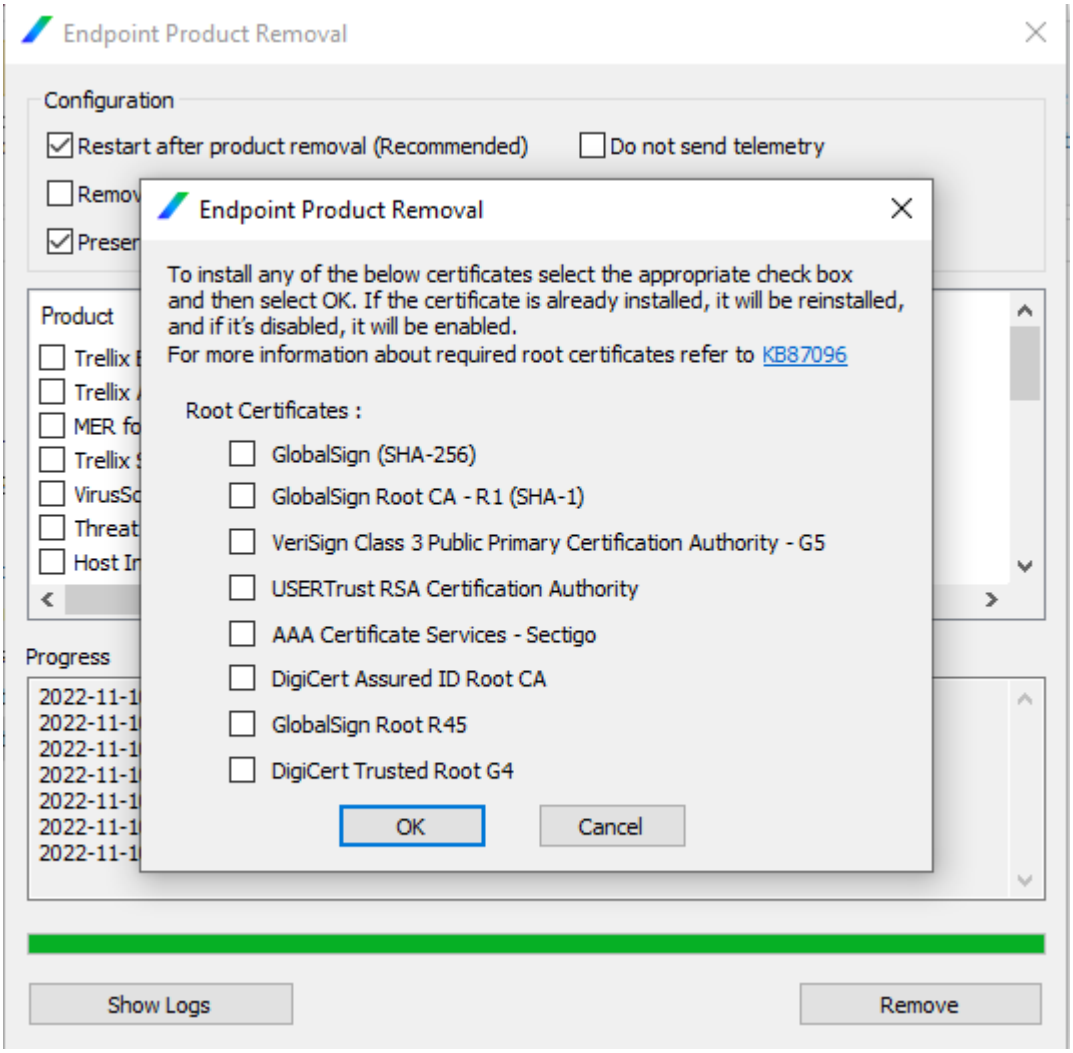
2.3.2 Determining conflicting products via CMD line execution

IF conflicting products are found to be present on the endpoint, an exit code of 5030 will be generated.
The following will be printed in the EPR logs:

Scanning for conflicting products...
EPR20 Conflicting product found on machine: File and Removable Media Protection/Endpoint Encryption for Files and Folders
Exit Code: 5030

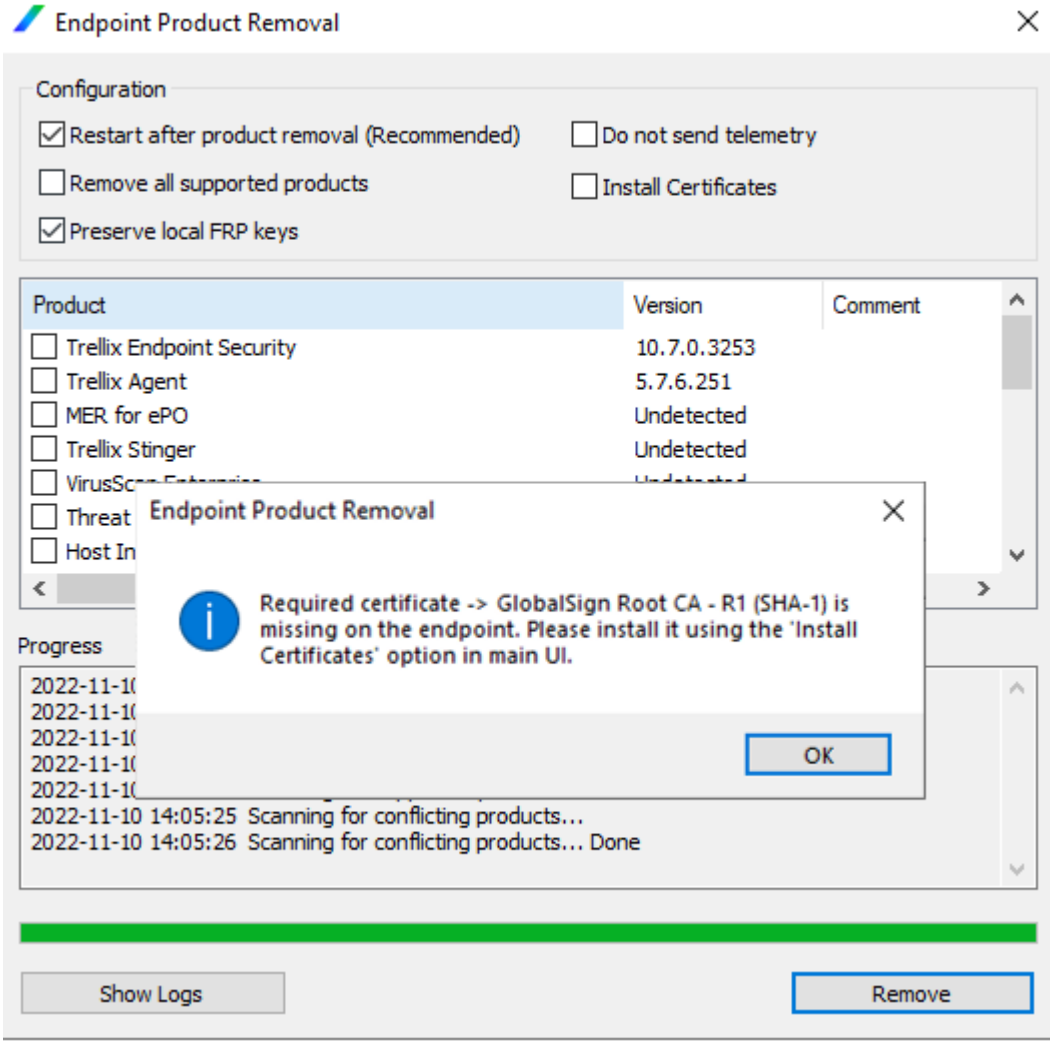
Root certificate Installation via User Interface

In some cases, root certificates required by Trellix for normal operation of its endpoint products can be missing or disabled. Removal of these products by EPR can be impacted as well. While this can be accomplished via command line execution, support for this feature is also provided in the user interface. Select “Install Certificates” to view the options. Select the root certificates you wish to install, then select OK. If the certificate already exists or is disabled, the certificate will be reinstalled as enabled.



When EPR is executed, it checks for these potentially required root certificates, and writes the scan results to the EPR log. If the GlobalSign Root CA – R1 root certificate is not found, a warning dialog will be displayed.

After execution of this feature, the results of the process will be displayed.


Endpoint Product Removal
Configuration
Restart after product removal (Recommended)
Do not send telemetry
Remove all supported products
Install Certificates
Preserve local FRP keys
Product
Version
Comment
Trellix Endpoint Security
10.7.0.3253
Trellix Agent
5.7.6.251
MER for ePO
Undetected
Trellix Stinger
Undetected
Endpoint Product Removal
Required certificate -> GlobalSign Root CA - R1 (SHA-1) is missing on the endpoint. Please install it using the 'Install Certificates' option in main UI.
OK
Progress
2022-11-10 14:05:25 Scanning for conflicting products...
2022-11-10 14:05:26 Scanning for conflicting products... Done
Show Logs
Remove

3. Mass deployments

You can execute the EPR tool on more than one computer at a time. How this is achieved is up to the end user. The EPR tool is provided both as an executable and a package which can be checked in and deployed from Trellix ePO.

3.1 ePO installation & deployments

To implement a mass ePO deployment, first check-in the EPR tool to the ePO Master repository. From there you can create a standard ePO deployment task and deploy the EPR tool to your environment. You must supply the appropriate command line options for the products you wish to remove, as well as the mandatory `--accepteula` argument while creating the deployment task.

3.2 Third-party deployments

The EPR tool can be deployed as a self-extractable executable or any other preferred deployment method.

4. Troubleshooting

4.1 Progress determination

The progress of the removal process is best tracked by viewing the EPR logs.

4.2 Exit codes

Exit Code	Explanation
0	Successful removal
1010	Invalid command line
5030	Conflicting product(s) found
-1	Error encountered while running EPR
1	Likely a successful removal. (It is difficult for the EPR tool to verify if it has been successful or that it has failed. Exit code 1 indicates that not all operations were successful, but in most cases, these failed operations are cosmetic and will not cause functional problems on the endpoint.)

4.3 Logging

To view logs, click the “Show Logs” button or the EPR log can be found here.

```
C:\Windows\Temp\McAfeeLogs\EPR_%TIMESTAMP%.log
```

When the EPR tool is executed and when it exits, an event is written to the Windows Event Log. This is done for traceability and visibility for administrators. “Source” is “Endpoint Product Removal Tool”.

When the EPR tool is executed and when it exits, an event is written to ePO with an ID of 1119. This is done for traceability and visibility for administrators. Note that if the EPR tool is executed with the `--ALL` command line argument, since Trellix Agent is removed, it will not report the final execution status to ePO.

4.4 If you encounter an issue

Please report any issues to Trellix Support with the following details provided:

- Steps to reproduce
- Expected results
- Actual results
- MER

4.5 Product documentation

- To access the product documentation for Trellix products, click here.
- To find supporting content on released products, including technical articles, click here.