HAGIWARA Solutions

Trellix Embedded Control(Windows)
VaccineUSB3 Use Permission Procedure Manual

1 Overview

This procedure manual describes the setup method for allowing the use of vaccine USBs in environments where Trellix Embedded Control (hereinafter referred to as TEC) has been introduced.

There are multiple options for permission methods, but please select a method that suits your organization's policy, considering security risks and operational burden.

- **Target File:**
  - **File Name:**Startup.exe
  - **Save Location:** Root of the vaccine USB's CD-ROM drive

2 Selection of Permission Method

There are three methods to allow the execution file (Startup.exe) of the vaccine USB:

Method	Advantages	Disadvantages/Notes
Method 1: Digital Signature	・ No re-registration required even if the file is updated if the signature is the same ・ High security	Re-registration is required if the signature expires (2-3 years)
Method 2: Checksum	・ Can guarantee that the file has not been tampered with ・ Highest security	Re-registration is required if the file is even slightly updated
Method 3: File Name	・ Easy to set up	Risk of executing malware with the same name

3 Preparation

Please prepare a vaccine USB and a TEC-equipped PC that will allow the vaccine USB.

4 Setup Procedure

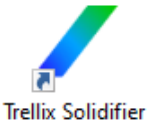
Method 1: Permission by Digital Signature

Register the digital signature attached to Startup.exe as trusted and allow execution and updates (Updater privilege).

Procedure 1: Extracting the Certificate

Use the scgetcerts.exe tool to extract the certificate file (.cer) from Startup.exe.

1. Connect the vaccine USB to the PC and launch the Trellix Solidifier command line.



2. Execute the following command. (The dot at the end specifies output to the current folder)
    - *Example*: If the vaccine USB's CD-ROM drive is D drive

3. ***scgetcerts.exe D:\Startup.exe .*** ***Don't forget the last dot**

The certificate file is usually saved under C:\Program Files\McAfee\Solidcore.
The certificate file is a 40-digit alphanumeric file (e.g., e12b34c56d...cer).

Procedure 2: Registering the Certificate

Register the extracted certificate file with TEC, granting Updater privilege.

1. Confirm the certificate file name generated in Procedure 1.
2. Execute the following command.
   sadmin cert add -u \<Certificate file name generated in Procedure 1\>.cer

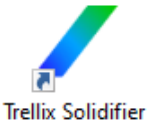
Method 2: Permission by Checksum

Register the unique checksum (hash value) of the Startup.exe file and allow only that file to execute and update (Updater privilege).

Procedure 1: Obtaining the Checksum

Obtain the checksum value (SHA-256) of the Startup.exe you want to allow in advance.

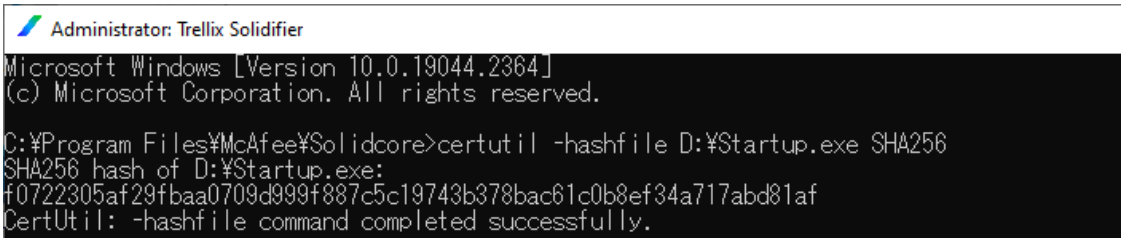
1. Connect the vaccine USB to the PC and launch the Trellix Solidifier command line.



2. Execute the following command.
    - *Example*: If the vaccine USB's CD-ROM drive is D drive

    certutil -hashfile d:\Startup.exe SHA256

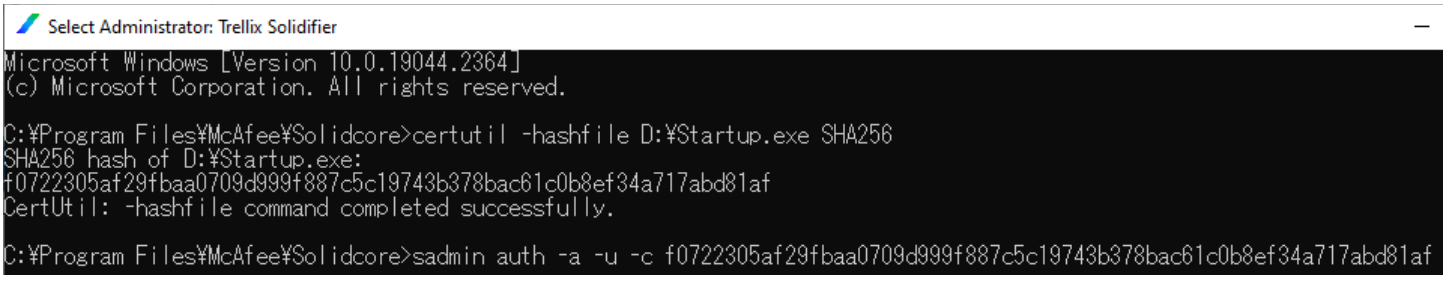
If successful, the hash value (f0722..) will be displayed on the screen.



Procedure 2: Registering the Checksum

Specify the obtained checksum value and grant execution privilege (-a) and Updater privilege (-u).

1. Execute the following command.
    sadmin auth -a -u -c \<Checksum value of Startup.exe obtained in Procedure 1\>



Registration is now complete.

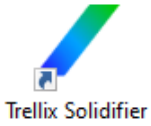
Method 3: Permission by Checksum

Allow files with the file name Startup.exe to be updated (Updater privilege).

Procedure 1: Registering the File Name

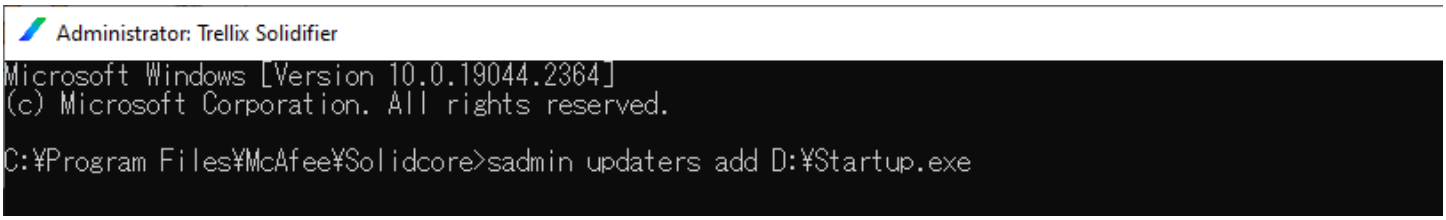
Specify the file name with the sadmin updaters add command.

1. Connect the vaccine USB to the PC and launch the Trellix Solidifier command line.



2. Execute the following command.
   - *Example: If the vaccine USB is the D drive*

   sadmin updaters add D:\Startup.exe



Registration is now complete.

For any questions or details regarding Trellix Embedded Control, please contact Trellix or a Trellix authorized reseller.

Trellix Embedded Control
Vaccine USB Use Permission Procedure Manual
Issued October 2025
Issued by Hagiwara Solutions Co., Ltd.