Upgrading Trusted Platform Module (TPM) firmware

For security reason, it is required to upgrade the Infineon TPM 2.0 SLB9670 firmware to version 7.85.

W082 WARNING

W082: These procedures are for advanced users only. Risk of system damage.

Prerequisites

- An USB key in FAT32 format, with a storage capacity of at least 1.4 MO
- A computer with a free USB port
- The TPM_version_7.85.zip package

1. Preparing the USB key using a computer

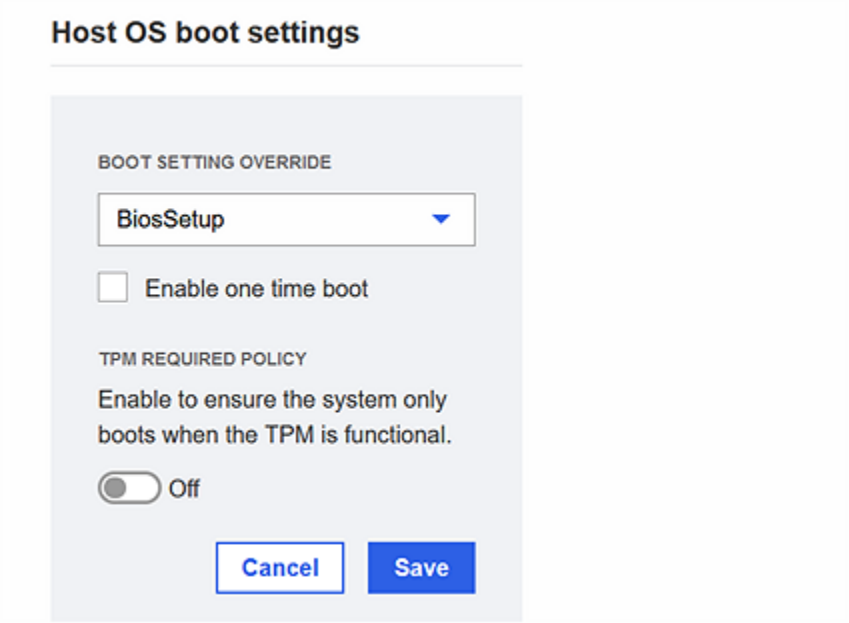
1. Unzip the TPM_version_7.85 package on Download folder.
2. Insert the USB key in the computer.
3. Copy all the files, except the PDF file, on the USB key.
4. Insert the USB key in the BullSequana Edge server.

2. Clearing the TPM

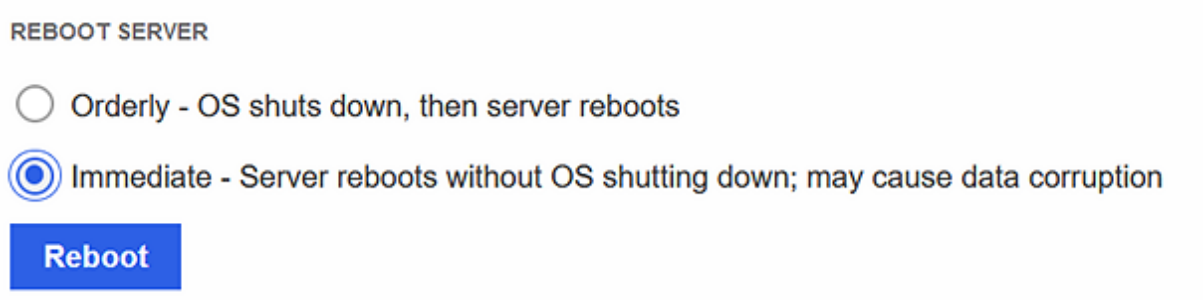
I. Start the BullSequana Edge Server Hardware Console (SHC)

II. Boot the server on BIOS settings

1. From the Control tab, select Server power operation.
2. Set BOOT SETTING OVERRIDE to BiosSetup and save.



3. Reboot as appropriate.



III. Clear the TPM

1. From the Control tab, select KVM.
The KVM page opens.
2. From the Security tab, use the navigation arrows to select Clear TPM and press [Enter].

IV. Save change and reboot the system

Select Exit > Exit Saving Changes and press [Enter]. The system reboots.

3. Upgrading the TPM

I. Open the internal EFI shell

1. When the logo appears, press the [Esc] key to display the BIOS interface.
2. Select Boot Manager using the navigation arrows and press [Enter].
3. Select Internal EFI shell and press [Enter].

Important The startup.nsh autoload script runs and may take a few seconds. It must not be interrupted.

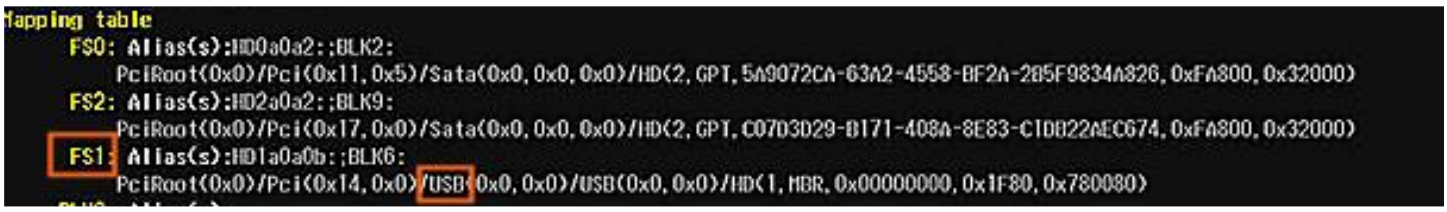
The UEFI shell windows opens.

II. Access to the USB key file system

1. List all the detected volumes. Run the command:

```
map
```

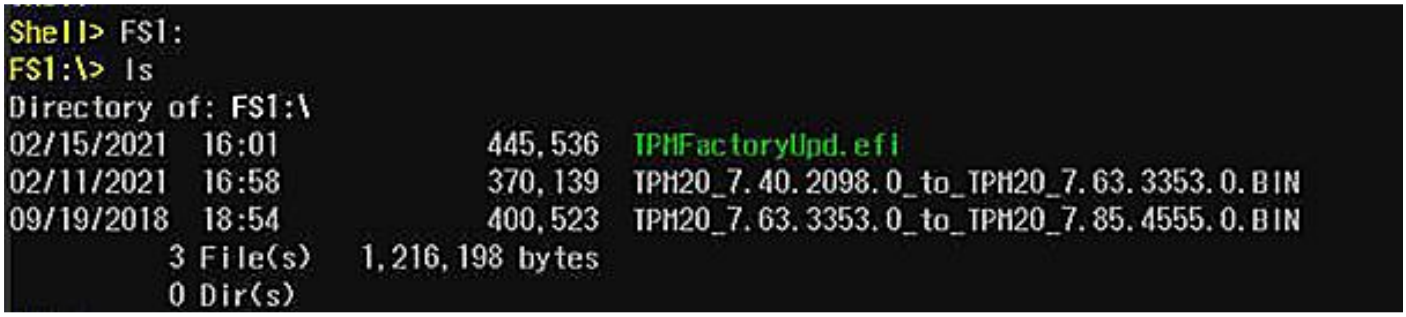
2. Find the volume named FSx for the USB key.



3. Enter into the volume.

```
Shell> FSx
```

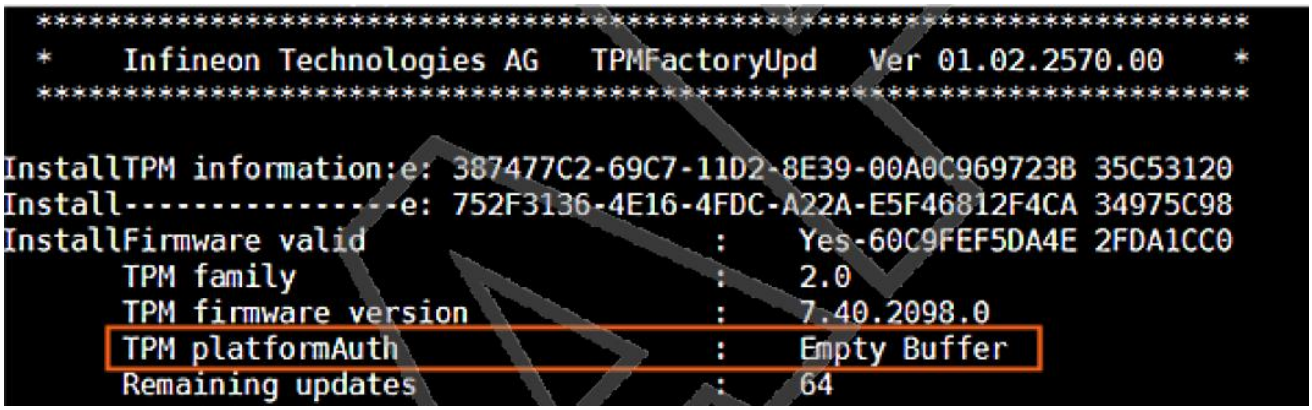
4. List the files (the screenshot is an example with 2 BIN files).



III. Check that the TPM is clean

1. Display TPM chip information.

2. Check that the TPM platformAuth value is Empty Buffer.



The current version in this screenshot is 7.40.2098.0

If the TPM platformAuth value is Not Empty Buffer, perform the previous clean-up step again to properly clean the TPM.

IV. Upgrade the TPM

1 If TPM version is earlier than 7.63

First step upgrade the TPM version to 7.63
Then upgrade to 7.85 in the following step 2.

TPMFactoryUpd.efi -update tpm20-emptyplatformauth -firmware TPM20_<version>.BIN

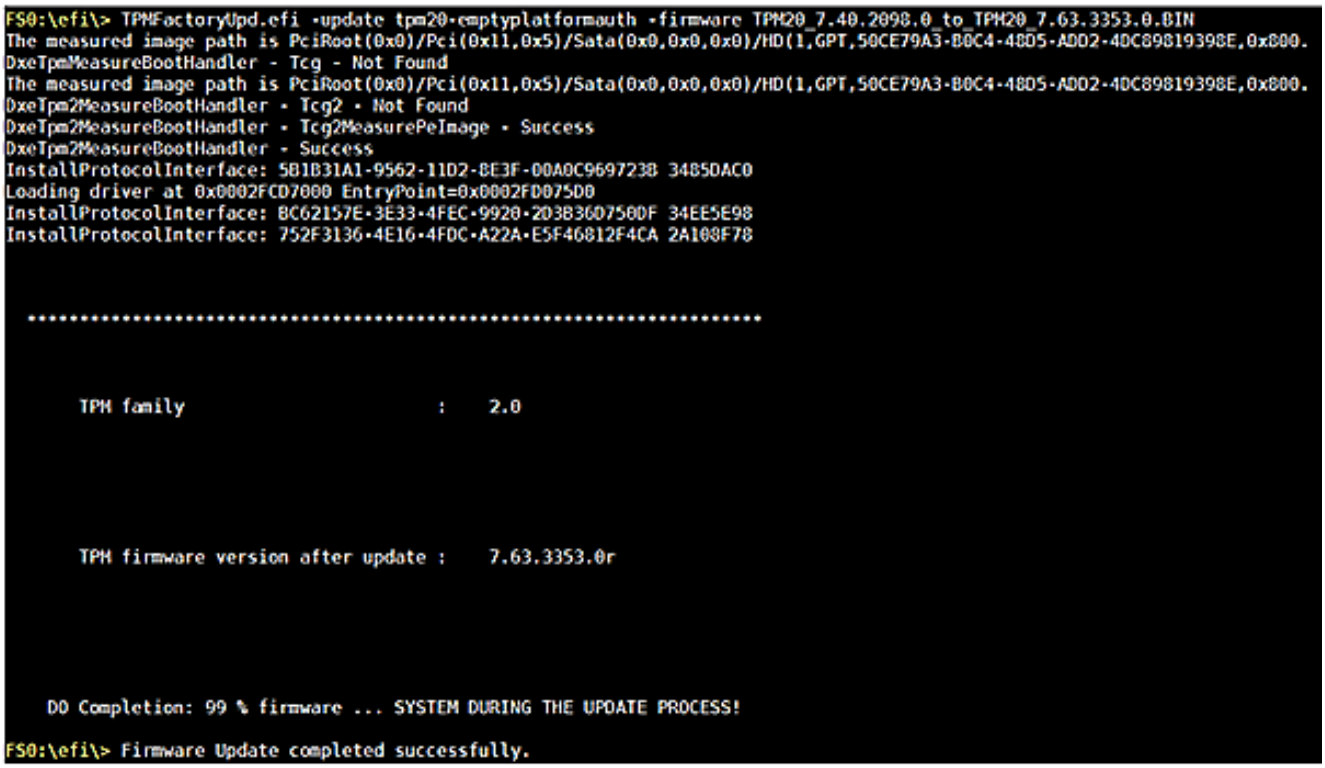
2 If TPM version is later or equal than 7.63 and earlier than 7.85

Upgrade the TPM version to 7.85.

TPMFactoryUpd.efi -update tpm20-emptyplatformauth -firmware TPM20_<version>.BIN

Important The script must not be stopped and the server must not be turned off during the operation.

Output



3. When the upgrade operation is completed, stop or reboot the server.