TPM 1.2 Firmware Update Guidance

for Infineon SLB9655 and SLB9660

Rev. 05

Document Number: 3600_R7

1. Introduction

This guidance described about in-field firmware update method for Infineon Trusted Platform Module (TPM) version 1.2

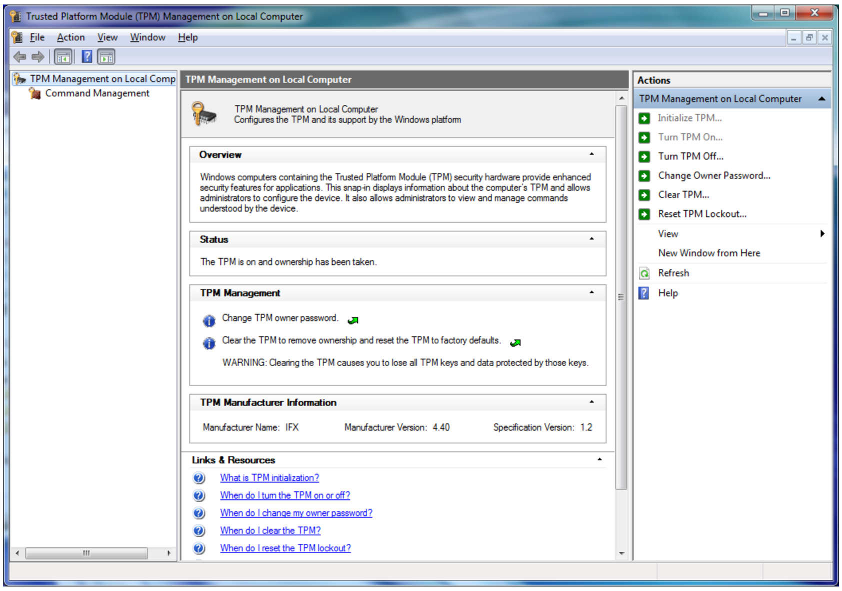
2. Target TPM Device and Firmware Update Tool

The following table shows target TPM device of this document, and related Firmware Update Tool.

Each Manufacturer Name, Manufacturer Version, and Specification Version column corresponds to text shown in Windows utility “Trusted Platform Module (TPM) Management”.

Table 1

Manufacturer Name	**Manufacturer Version**	**Specification Version**	**Firmware Update Tool**
IFX	4.32	1.2	IFXTPMUpdate_TPM12_v0434.exe
IFX	4.40	1.2	IFXTPMUpdate_TPM12_v0443.exe



TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status

The TPM is on and ownership has been taken.

TPM Management

Change TPM owner password.

Clear the TPM to remove ownership and reset the TPM to factory defaults.

WARNING: Clearing the TPM causes you to lose all TPM keys and data protected by those keys.

TPM Manufacturer Information

Manufacturer Name: IFX   Manufacturer Version: 4.40   Specification Version: 1.2

Links & Resources

- What is TPM initialization?
- When do I turn the TPM on or off?
- When do I change my owner password?
- When do I clear the TPM?
- When do I reset the TPM lockout?

3. Preconditions

To run the update tool, **administrative privilege** is required.

During the update tool executing, you may need the TPM Owner Password. If the operating system does not store the Owner Password or Owner Password Backup File, you may need to clear the TPM.

WARNING

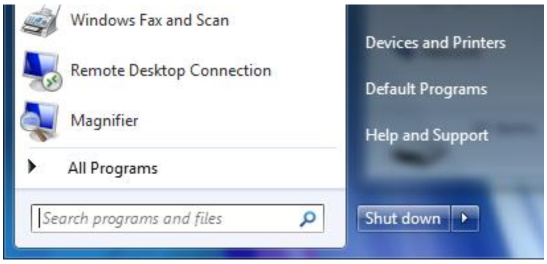
- Before starting update, it is strongly recommended to backup the computer.
- In case your drive was encrypted by BitLocker, it blocks the TPM firmware update. Before starting the firmware update, “Suspend protection” of BitLocker.
- In case clearing the TPM, it resets the TPM to factory defaults. It will lose every created keys and data protected by those keys. Clearing the TPM may cause you to be prompted for your BitLocker recovery key, or re-setting PIN, in case using these features.

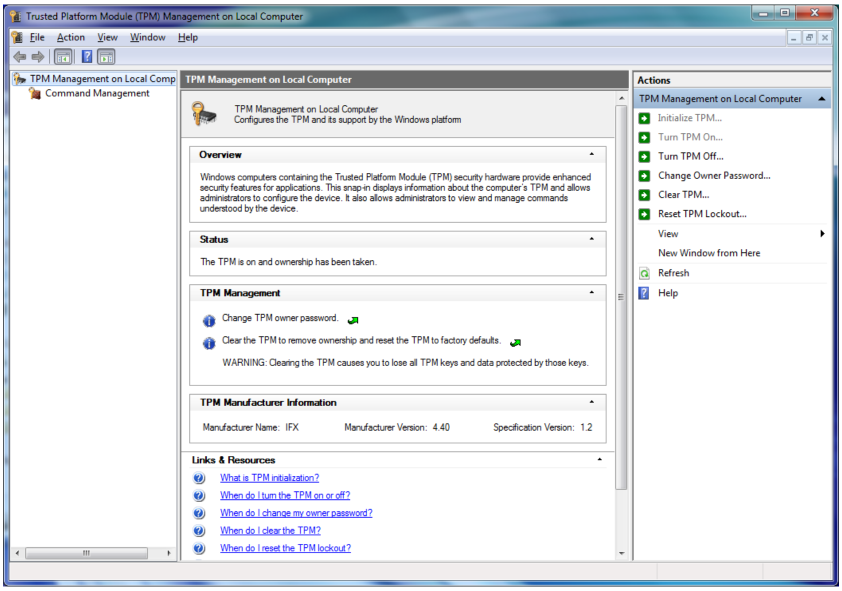
4. How to Update the TPM Firmware

To run the update tool, administrative privilege is required.

4.1. Windows 7

1. Run “tpm.msc” from Start Menu. (Type “tpm.msc” at “Search programs and files”.) “Trusted Platform Module (TPM) Management on Local Computer” appears.





TPM Management on Local Computer

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status

The TPM is on and ownership has been taken.

TPM Management

Change TPM owner password.

Clear the TPM to remove ownership and reset the TPM to factory defaults.

WARNING: Clearing the TPM causes you to lose all TPM keys and data protected by those keys.

TPM Manufacturer Information

Manufacturer Name: IFX Manufacturer Version: 4.40 Specification Version: 1.2

Links & Resources

What is TPM initialization?
When do I turn the TPM on or off?
When do I change my owner password?
When do I clear the TPM?
When do I reset the TPM lockout?

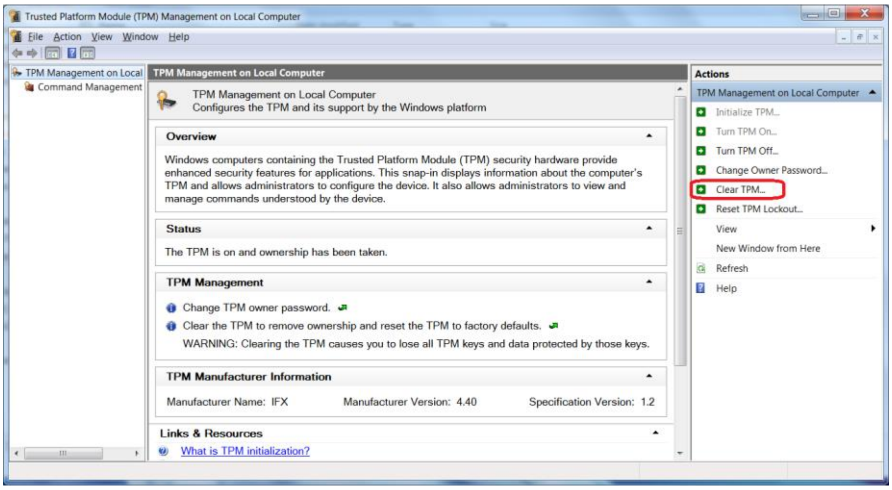
2. To confirm whether the TPM firmware is subject to update, clarify “Manufacturer Name” and “Specification Version” are “IFX” and “1.2”, and “Manufacturer Version” are shown in Table 1.

3. In case you have the TPM Owner Password or the TPM Owner Password Backup File, proceed to 10.
   In case both the TPM Owner Password and the TPM Owner Password Backup File are not found, you need to clear the TPM.

WARNING

- Before starting update, it is strongly recommended to backup the computer.
- In case your drive was encrypted by BitLocker, it blocks the TPM firmware update. Before starting the firmware update, “Suspend protection” of BitLocker.
- In case clearing the TPM, it resets the TPM to factory defaults. It will lose every created keys and data protected by those keys. Clearing the TPM may cause you to be prompted for your BitLocker recovery key, or re-setting PIN, in case using these features.

4. On“Trusted Platform Module (TPM) Management on Local Computer”, choose “Initialize TPM…” from “Actions”.



TPM Management on Local Computer

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status

The TPM is on and ownership has been taken.

TPM Management

- Change TPM owner password.
- Clear the TPM to remove ownership and reset the TPM to factory defaults.

WARNING: Clearing the TPM causes you to lose all TPM keys and data protected by those keys.

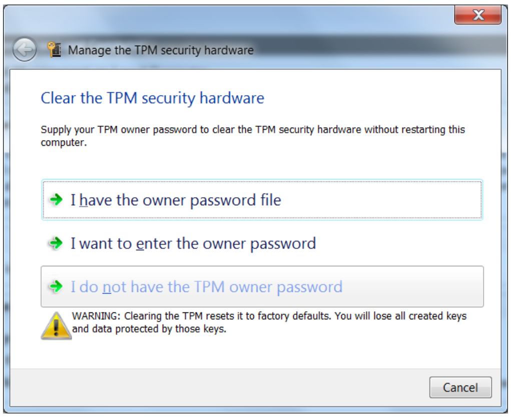
TPM Manufacturer Information

Manufacturer Name: IFX   Manufacturer Version: 4.40   Specification Version: 1.2

Links & Resources

What is TPM initialization?

The following screen appears. Choose “I do not have the TPM owner password”.

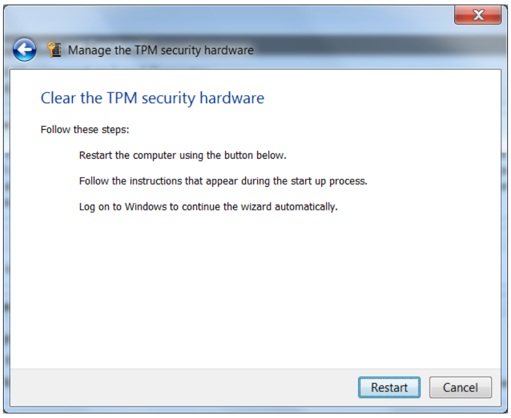

Manage the TPM security hardware
I have the owner password file
I want to enter the owner password
I do not have the TPM owner password
Cancel

Clear the TPM security hardware

Supply your TPM owner password to clear the TPM security hardware without restarting this computer.

WARNING: Clearing the TPM resets it to factory defaults. You will lose all created keys and data protected by those keys.

5. The following screen appears. Choose “Restart” to restart the computer.



Clear the TPM security hardware

Follow these steps:

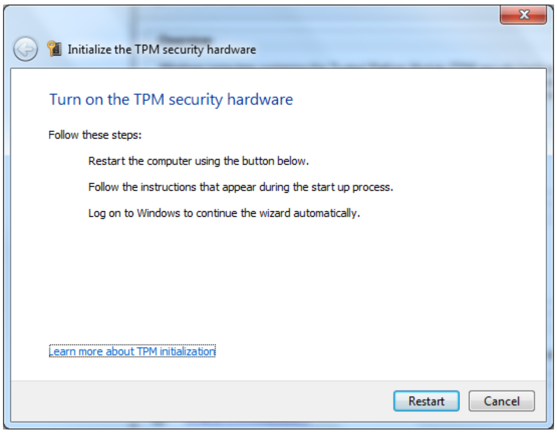
Restart the computer using the button below.

Follow the instructions that appear during the start up process.

Log on to Windows to continue the wizard automatically.

After restart, BIOS warning message may appear. Press [F11] to clear TPM and proceed.

After restart, the following screen appears. Choose “Restart” to restart the computer.



Initialize the TPM security hardware

Turn on the TPM security hardware

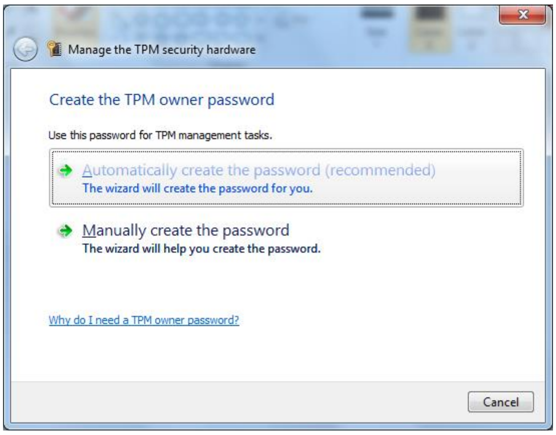
Follow these steps:

Restart the computer using the button below.

Follow the instructions that appear during the start up process.

Log on to Windows to continue the wizard automatically.

6. The following screen appears. Choose how to create the TPM Owner Password. Usually, choose “Automatically create the password (recommended)”.



Manage the TPM security hardware

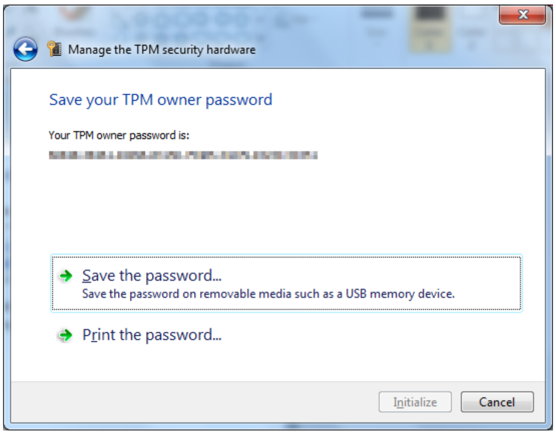
Create the TPM owner password

Use this password for TPM management tasks.

Automatically create the password (recommended)
The wizard will create the password for you.

Manually create the password
The wizard will help you create the password.

7. Choose “Save the password...” and choose location to save the TPM Owner Password. USB memory is recommended.



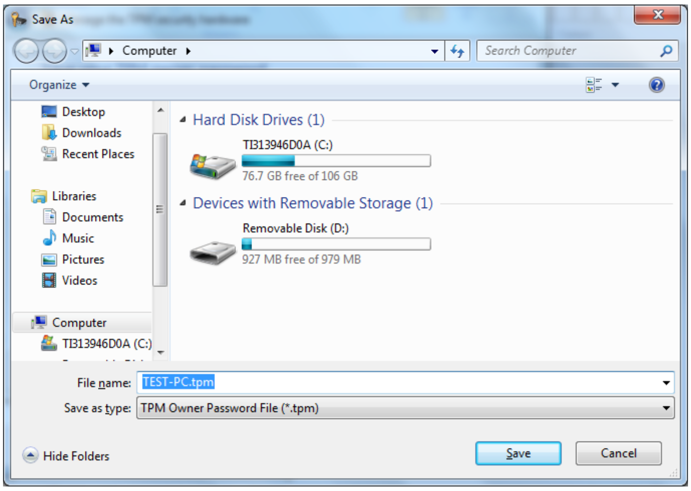
Manage the TPM security hardware

Save your TPM owner password

Your TPM owner password is:

Save the password...
Save the password on removable media such as a USB memory device.

Print the password...

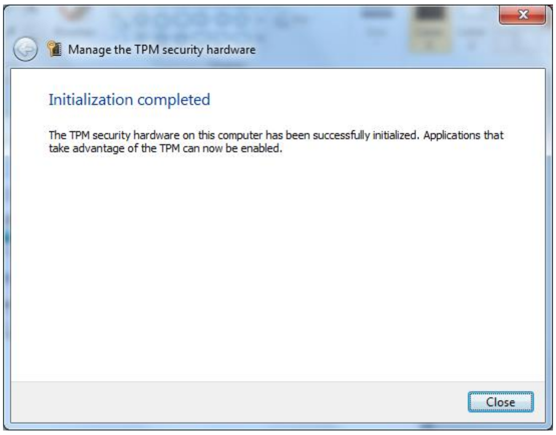


File name: TEST-PC.tpm

Save as type: TPM Owner Password File (*.tpm)

8. After saving or printing the password, “Initialize” button becomes active. Choose “Initialize” to start TPM initialization.

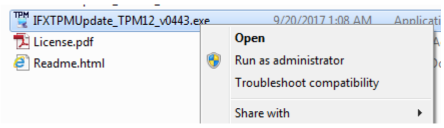
9. After initialization completed, the following screen appears.



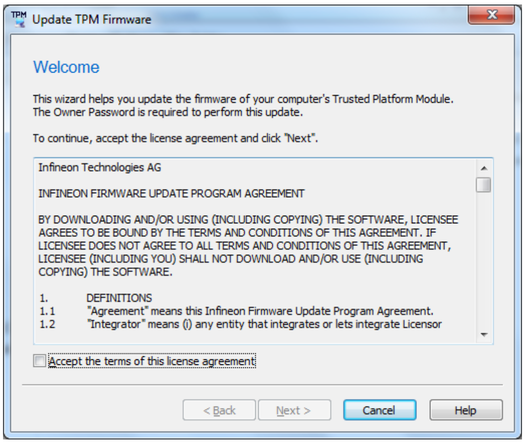
Initialization completed

The TPM security hardware on this computer has been successfully initialized. Applications that take advantage of the TPM can now be enabled.

10. Right click Firmware Update Tool in Table 1 corresponds to Manufacturer Version, choose “Run as administrator”.



The following screen appears.



Welcome

This wizard helps you update the firmware of your computer's Trusted Platform Module.
The Owner Password is required to perform this update.

To continue, accept the license agreement and click "Next".

Infineon Technologies AG

INFINEON FIRMWARE UPDATE PROGRAM AGREEMENT

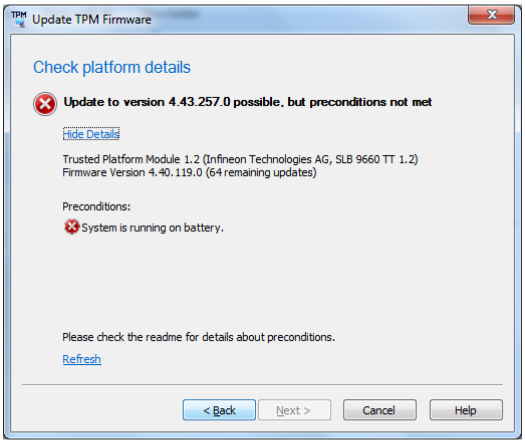
BY DOWNLOADING AND/OR USING (INCLUDING COPYING) THE SOFTWARE, LICENSEE AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF LICENSEE DOES NOT AGREE TO ALL TERMS AND CONDITIONS OF THIS AGREEMENT, LICENSEE (INCLUDING YOU) SHALL NOT DOWNLOAD AND/OR USE (INCLUDING COPYING) THE SOFTWARE.

1. DEFINITIONS
1.1 "Agreement" means this Infineon Firmware Update Program Agreement.
1.2 "Integrator" means (i) any entity that integrates or lets integrate Licensor

□ Accept the terms of this license agreement

11. Check “Accept the terms of this license agreement”, and choose “Next”.

In case AC adapter is not plugged, the following screen appears. Plug the AC adapter and choose “Back” to return previous screen once.



Check platform details

Update to version 4.43.257.0 possible, but preconditions not met

Hide Details

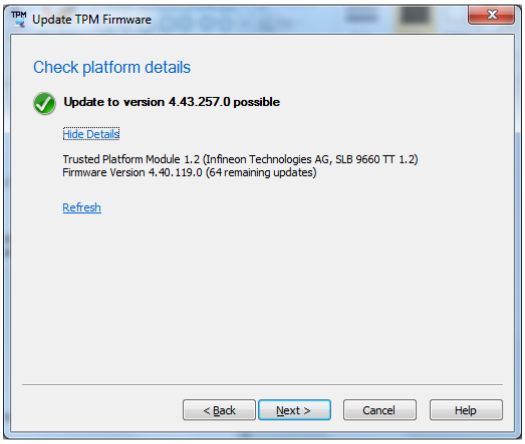
Trusted Platform Module 1.2 (Infineon Technologies AG, SLB 9660 TT 1.2)
Firmware Version 4.40.119.0 (64 remaining updates)

Preconditions:
System is running on battery.

Please check the readme for details about preconditions.

Refresh

12. The following screen appears. Check platform details and choose “Next”.



Update TPM Firmware

Check platform details

Update to version 4.43.257.0 possible

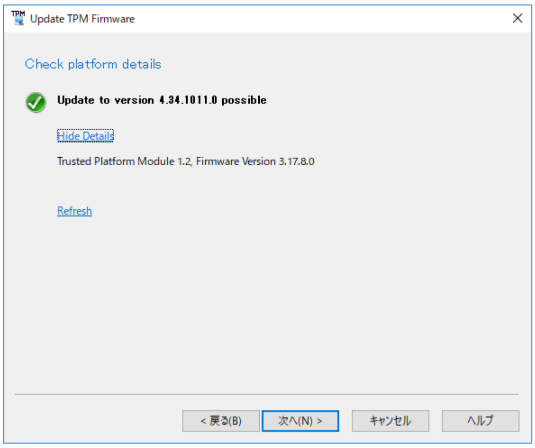
Hide Details

Trusted Platform Module 1.2 (Infineon Technologies AG, SLB 9660 TT 1.2)
Firmware Version 4.40.119.0 (64 remaining updates)

Refresh

WARNING

- In case Manufacturer Version is 3.17 or 3.19, it is not a subject to firmware update, the following screen can appear. In the case, choose “Cancel” to cancel firmware update. Even if you choose “Next”, firmware update is not executed.



Update TPM Firmware

Check platform details

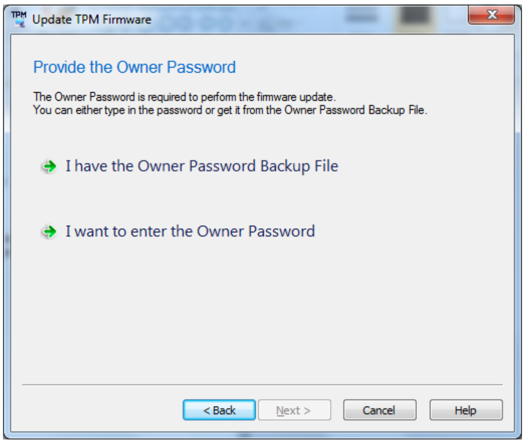
Update to version 4.34.1011.0 possible

Hide Details

Trusted Platform Module 1.2, Firmware Version 3.17.8.0

Refresh

13. Provide the Owner Password. In case having the Owner Password as the Owner Password Backup File, choose “I have the Owner Password Backup File” and specify the file location by pressing “Browse...”.



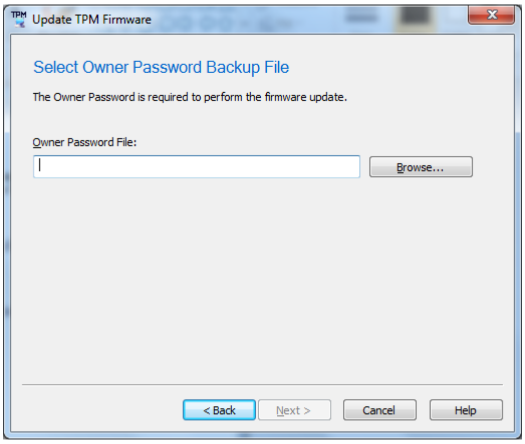
Update TPM Firmware

Provide the Owner Password

The Owner Password is required to perform the firmware update.
You can either type in the password or get it from the Owner Password Backup File.

I have the Owner Password Backup File

I want to enter the Owner Password



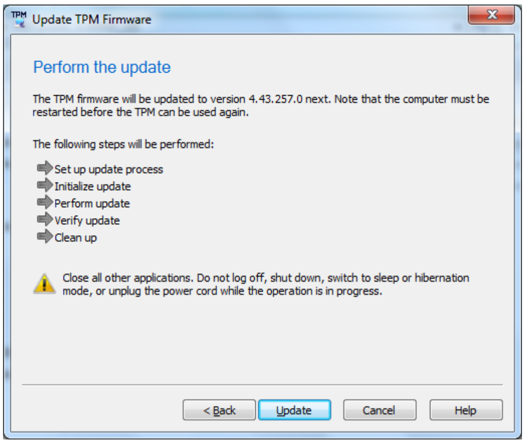
Update TPM Firmware

Select Owner Password Backup File

The Owner Password is required to perform the firmware update.

Owner Password File:

14. Choose “Update” to start firmware update.



Update TPM Firmware

Perform the update

The TPM firmware will be updated to version 4.43.257.0 next. Note that the computer must be restarted before the TPM can be used again.

The following steps will be performed:

- Set up update process
- Initialize update
- Perform update
- Verify update
- Clean up

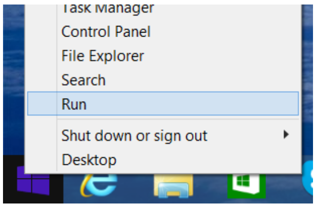
Close all other applications. Do not log off, shut down, switch to sleep or hibernation mode, or unplug the power cord while the operation is in progress.

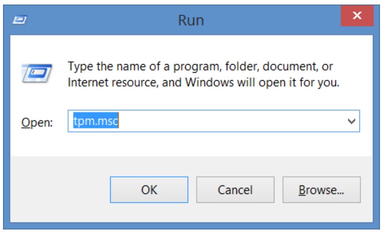
WARNING

- On Windows 7, the firmware update may take up to 10 minutes. Do NOT turn off the computer until the update completes.

4.2. Windows 8.1, Windows 10 version 1507 and 1511

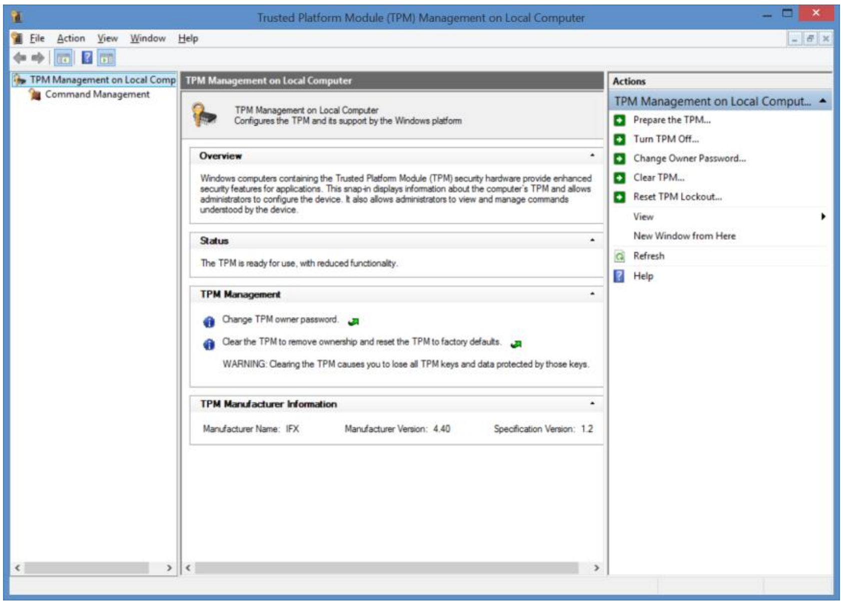
1. Right click Start Menu and choose “Run”. Run “tpm.msc” from “Run”. (Type “tpm.msc” at “Open”.) “Trusted Platform Module (TPM) Management on Local Computer” appears.





Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: tpm.msc



TPM Management on Local Computer

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status

The TPM is ready for use, with reduced functionality.

TPM Management

Change TPM owner password.

Clear the TPM to remove ownership and reset the TPM to factory defaults.

WARNING: Clearing the TPM causes you to lose all TPM keys and data protected by those keys.

TPM Manufacturer Information

Manufacturer Name: IFX   Manufacturer Version: 4.40   Specification Version: 1.2

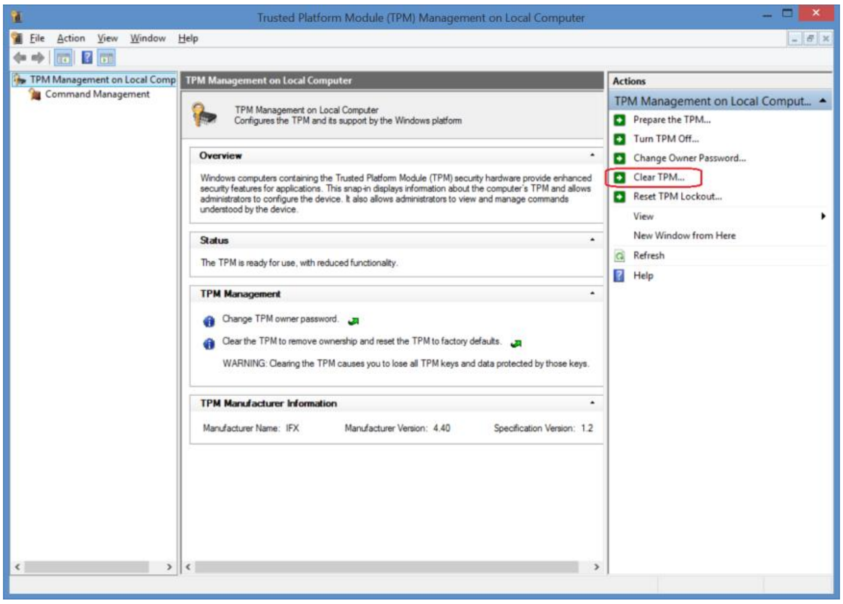
2. To confirm whether the TPM firmware is subject to update, clarify “Manufacturer Name” and “Specification Version” are “IFX” and “1.2”, and “Manufacturer Version” are shown in Table 1.

3. In case you have the TPM Owner Password or the TPM Owner Password Backup File, proceed to 7.
   In case both the TPM Owner Password and the TPM Owner Password Backup File are not found, you need to clear the TPM.

WARNING

- Before starting update, it is strongly recommended to backup the computer.
- In case your drive was encrypted by BitLocker, it blocks the TPM firmware update. Before starting the firmware update, “Suspend protection” of BitLocker.
- In case clearing the TPM, it resets the TPM to factory defaults. It will lose every created keys and data protected by those keys. Clearing the TPM may cause you to be prompted for your BitLocker recovery key, or re-setting PIN, in case using these features.

4. On “Trusted Platform Module (TPM) Management on Local Computer”, choose “Clear TPM…” from “Actions”.


Trusted Platform Module (TPM) Management on Local Computer
File Action View Window Help
TPM Management on Local Comp
Command Management
TPM Management on Local Computer
Actions
TPM Management on Local Comput...
Prepare the TPM...
Turn TPM Off...
Change Owner Password...
Clear TPM...
Reset TPM Lockout...
View
New Window from Here
Refresh
Help

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status

The TPM is ready for use, with reduced functionality.

TPM Management

Change TPM owner password.

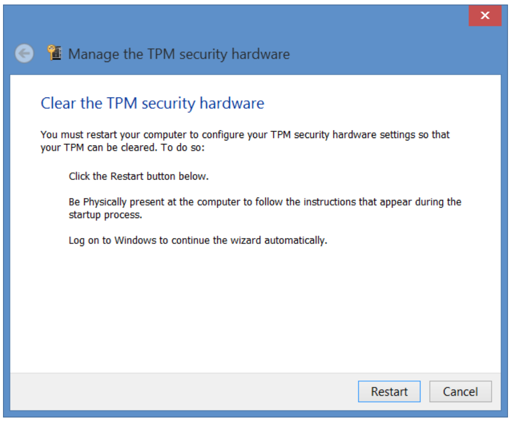
Clear the TPM to remove ownership and reset the TPM to factory defaults.

WARNING: Clearing the TPM causes you to lose all TPM keys and data protected by those keys.

TPM Manufacturer Information

Manufacturer Name: IFX   Manufacturer Version: 4.40   Specification Version: 1.2

5. The following screen appears. Choose “Restart” to restart the computer.



Manage the TPM security hardware

Clear the TPM security hardware

You must restart your computer to configure your TPM security hardware settings so that your TPM can be cleared. To do so:

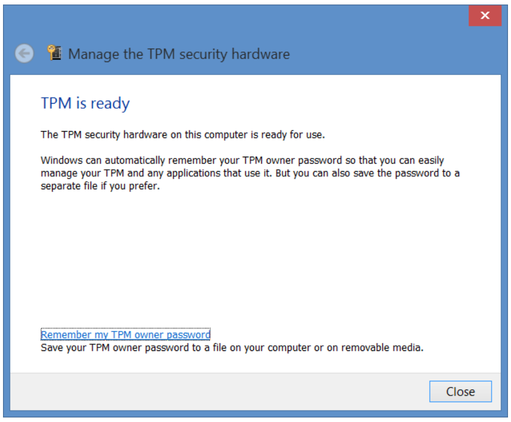
Click the Restart button below.

Be Physically present at the computer to follow the instructions that appear during the startup process.

Log on to Windows to continue the wizard automatically.

After restart, BIOS warning message may appear. Press [F11] to clear TPM and proceed.

6. After restart, the following screen appears. Choose “Remember my TPM owner password”, and choose location to save the TPM Owner Password. USB memory is recommended.



Manage the TPM security hardware

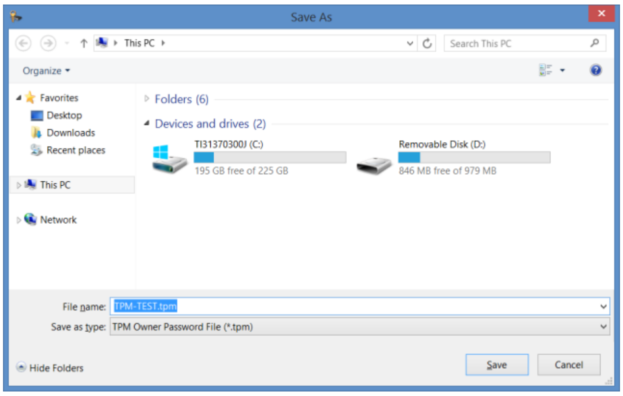
TPM is ready

The TPM security hardware on this computer is ready for use.

Windows can automatically remember your TPM owner password so that you can easily manage your TPM and any applications that use it. But you can also save the password to a separate file if you prefer.

Remember my TPM owner password

Save your TPM owner password to a file on your computer or on removable media.

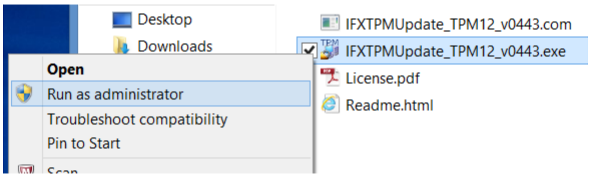


File name: TPM-TEST.tpm

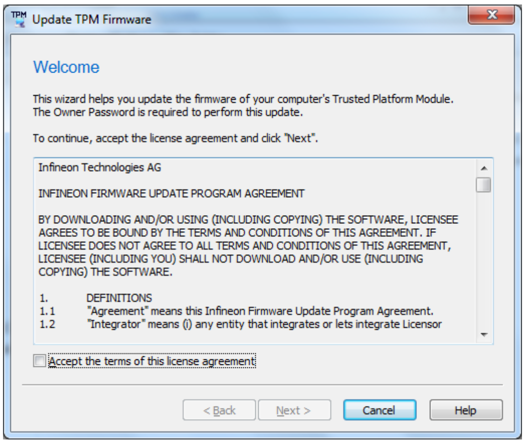
Save as type: TPM Owner Password File (*.tpm)

After saving the password, choose “Close” on “Manage the TPM security hardware”.

7. Right click Firmware Update Tool in Table 1 corresponds to Manufacturer Version, choose “Run as administrator”.


Desktop
Downloads
Open
Run as administrator
Troubleshoot compatibility
Pin to Start
Scan
IFXTPMUpdate_TPM12_v0443.com
IFXTPMUpdate_TPM12_v0443.exe
License.pdf
Readme.html

The following screen appears.



Welcome

This wizard helps you update the firmware of your computer's Trusted Platform Module.
The Owner Password is required to perform this update.

To continue, accept the license agreement and click "Next".

Infineon Technologies AG

INFINEON FIRMWARE UPDATE PROGRAM AGREEMENT

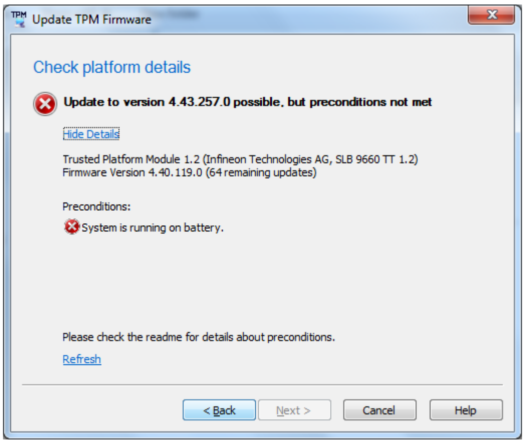
BY DOWNLOADING AND/OR USING (INCLUDING COPYING) THE SOFTWARE, LICENSEE AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF LICENSEE DOES NOT AGREE TO ALL TERMS AND CONDITIONS OF THIS AGREEMENT, LICENSEE (INCLUDING YOU) SHALL NOT DOWNLOAD AND/OR USE (INCLUDING COPYING) THE SOFTWARE.

1. DEFINITIONS
1.1 "Agreement" means this Infineon Firmware Update Program Agreement.
1.2 "Integrator" means (i) any entity that integrates or lets integrate Licensor

□ Accept the terms of this license agreement

8. Check “Accept the terms of this license agreement”, and choose “Next”.

In case AC adapter is not plugged, the following screen appears. Plug the AC adapter and choose “Back” to return previous screen once.



Check platform details

Update to version 4.43.257.0 possible, but preconditions not met

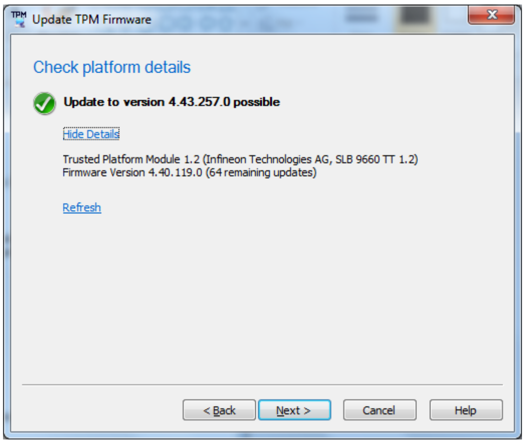
Hide Details

Trusted Platform Module 1.2 (Infineon Technologies AG, SLB 9660 TT 1.2)
Firmware Version 4.40.119.0 (64 remaining updates)

Preconditions:
System is running on battery.

Please check the readme for details about preconditions.
Refresh

9. The following screen appears. Check platform details and choose “Next”.



Check platform details

Update to version 4.43.257.0 possible

Hide Details

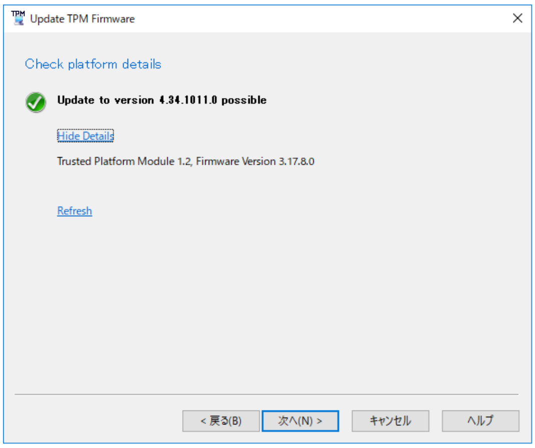
Trusted Platform Module 1.2 (Infineon Technologies AG, SLB 9660 TT 1.2)
Firmware Version 4.40.119.0 (64 remaining updates)

Refresh

TPM Owner Password is not queried.

WARNING

- In case Manufacturer Version is 3.17 or 3.19, it is not a subject to firmware update, the following screen can appear. In the case, choose “Cancel” to cancel firmware update. Even if you choose “Next”, firmware update is not executed.



Check platform details

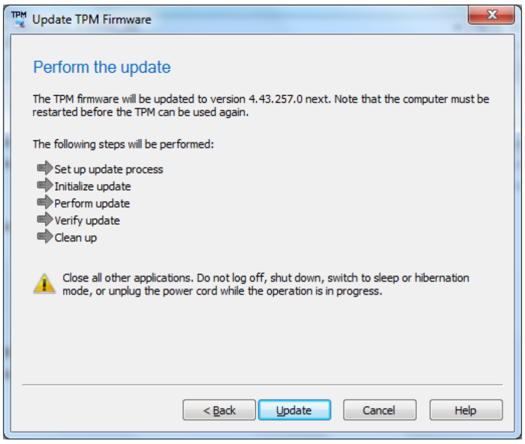
Update to version 4.34.1011.0 possible

Hide Details

Trusted Platform Module 1.2, Firmware Version 3.17.8.0

Refresh

10. Choose “Update” to start firmware update.



Perform the update

The TPM firmware will be updated to version 4.43.257.0 next. Note that the computer must be restarted before the TPM can be used again.

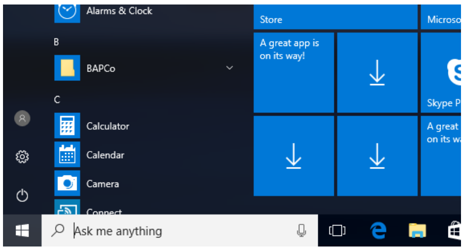
The following steps will be performed:

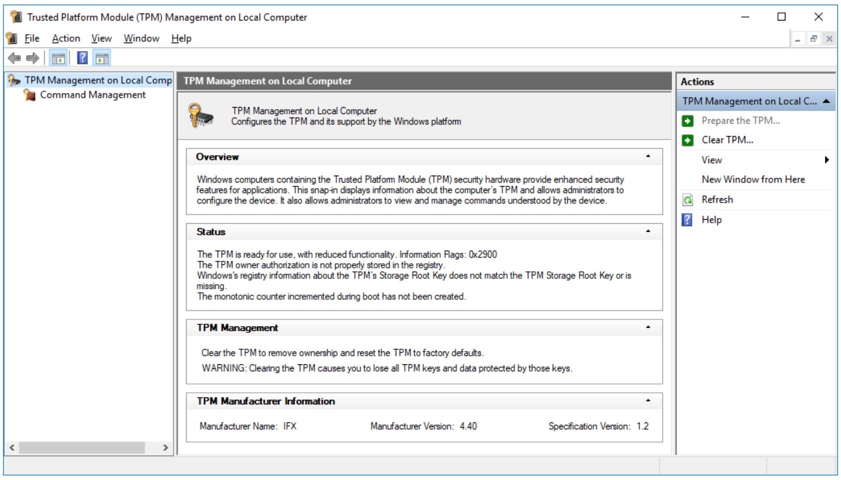
- Set up update process
- Initialize update
- Perform update
- Verify update
- Clean up

Close all other applications. Do not log off, shut down, switch to sleep or hibernation mode, or unplug the power cord while the operation is in progress.

4.3. Windows 10 version 1607 (Anniversary Update) and after

1. Run “tpm.msc” from Start Menu. (Type “tpm.msc” at “Search programs and files”.) “Trusted Platform Module (TPM) Management on Local Computer” appears.




Trusted Platform Module (TPM) Management on Local Computer
File Action View Window Help
TPM Management on Local Comp
Command Management
TPM Management on Local Computer
Actions
TPM Management on Local C...
Prepare the TPM...
Clear TPM...
View
New Window from Here
Refresh
Help

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status

The TPM is ready for use, with reduced functionality. Information Flags: 0x2900
The TPM owner authorization is not properly stored in the registry.
Windows's registry information about the TPM's Storage Root Key does not match the TPM Storage Root Key or is missing.
The monotonic counter incremented during boot has not been created.

TPM Management

Clear the TPM to remove ownership and reset the TPM to factory defaults.
WARNING: Clearing the TPM causes you to lose all TPM keys and data protected by those keys.

TPM Manufacturer Information

Manufacturer Name: IFX Manufacturer Version: 4.40 Specification Version: 1.2

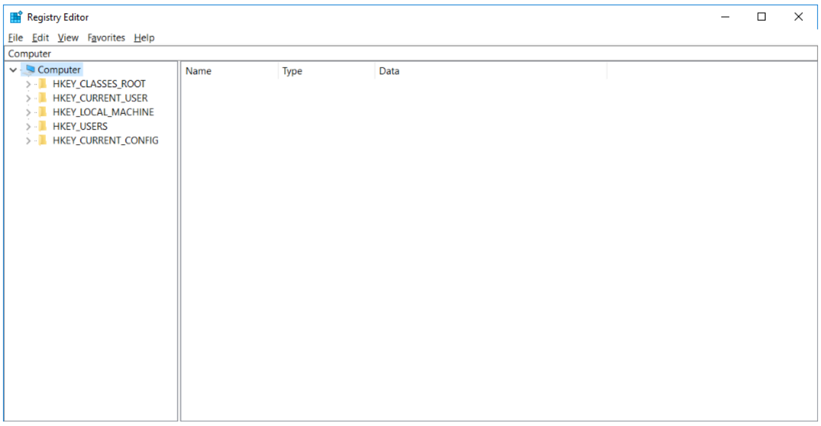
2. To confirm whether the TPM firmware is subject to update, clarify “Manufacturer Name” and “Specification Version” are “IFX” and “1.2”, and “Manufacturer Version” are shown in Table 1.

3. In case you have the TPM Owner Password or the TPM Owner Password Backup File, proceed to 10.
   In case both the TPM Owner Password and the TPM Owner Password Backup File are not found, you need to clear the TPM.

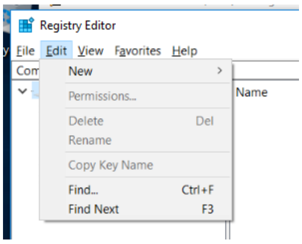
WARNING

- Before starting update, it is strongly recommended to backup the computer.
- In case your drive was encrypted by BitLocker, it blocks the TPM firmware update. Before starting the firmware update, “Suspend protection” of BitLocker.
- In case clearing the TPM, it resets the TPM to factory defaults　It will lose every created keys and data protected by those keys.　Clearing the TPM may cause you to be prompted for your BitLocker recovery key, or re-setting PIN, in case using these features.

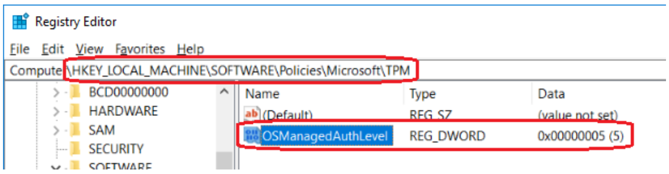
4. Run “regedit” from Start Menu.　(Type “regedit” at “Search programs and files”.) “Registry Editor” appears.



5. Clarify registry key [HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥TPM] OSManagedAuthLevel, and record original key data.　Choose “Edit” – “Find…”.



Type “OSManagedAuthLevel” at “Find what”, then press “Find Next”.　The following screen appears after a while.

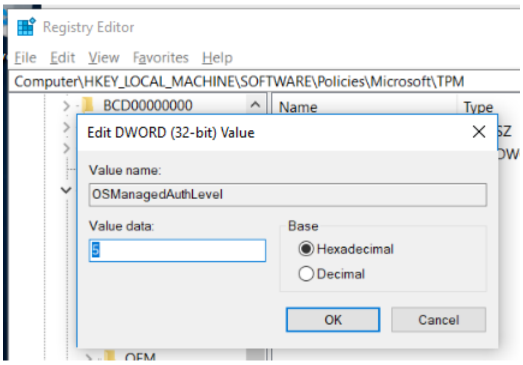


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\TPM

Name	Type	Data
(Default)	REG_SZ	(value not set)
OSManagedAuthLevel	REG_DWORD	0x00000005 (5)

Clarify upper text shows “HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥TPM”, and lower left text shows “OSManagedAuthLevel”, and take a note for the data. (In this screenshot case, “5”.) After updating the firmware, this register key shall be restored, so do not miss to take a note.

6. Double click “OSManagedAuthLevel”. The following screen appears.



Registry Editor

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\TPM

Edit DWORD (32-bit) Value

Value name:
OSManagedAuthLevel

Value data:
5

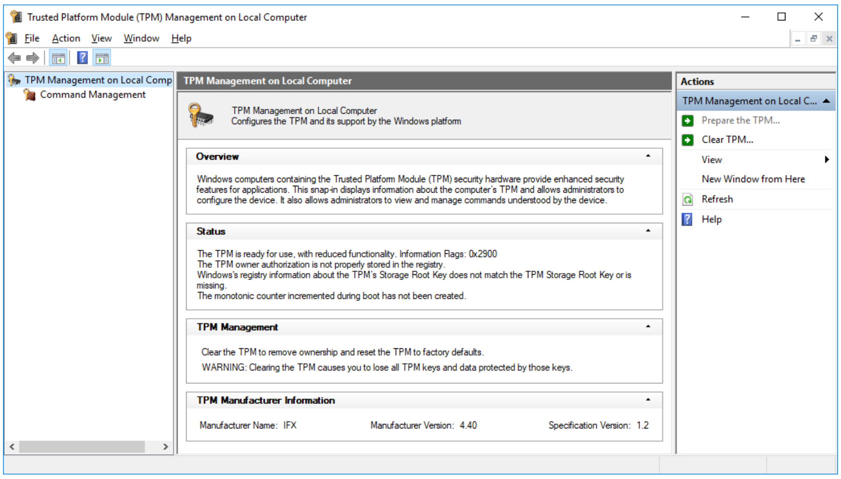
Base
● Hexadecimal
○ Decimal

7. Change “Value data” as 4, and press “OK”.

8. Run “tpm.msc” from Start Menu, and choose “Clear TPM…” from “Actions”.

WARNING

- Before starting update, it is strongly recommended to backup the computer.
- In case your drive was encrypted by BitLocker, it blocks the TPM firmware update. Before starting the firmware update, “Suspend protection” of BitLocker.
- In case clearing the TPM, it resets the TPM to factory defaults. It will lose every created keys and data protected by those keys. Clearing the TPM may cause you to be prompted for your BitLocker recovery key, or re-setting PIN, in case using these features.



Trusted Platform Module (TPM) Management on Local Computer

TPM Management on Local Computer

TPM Management on Local Computer
Configures the TPM and its support by the Windows platform

Overview

Windows computers containing the Trusted Platform Module (TPM) security hardware provide enhanced security features for applications. This snap-in displays information about the computer's TPM and allows administrators to configure the device. It also allows administrators to view and manage commands understood by the device.

Status

The TPM is ready for use, with reduced functionality. Information Flags: 0x2900
The TPM owner authorization is not properly stored in the registry.
Windows's registry information about the TPM's Storage Root Key does not match the TPM Storage Root Key or is missing.
The monotonic counter incremented during boot has not been created.

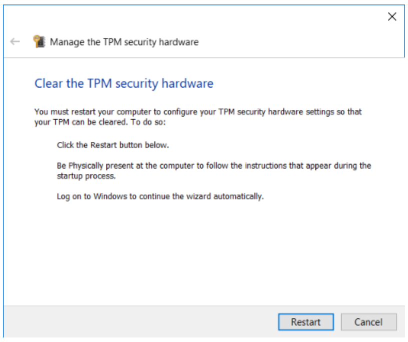
TPM Management

Clear the TPM to remove ownership and reset the TPM to factory defaults.
WARNING: Clearing the TPM causes you to lose all TPM keys and data protected by those keys.

TPM Manufacturer Information

Manufacturer Name: IFX Manufacturer Version: 4.40 Specification Version: 1.2

9. The following screen appears. Choose “Restart” to restart the computer.



Manage the TPM security hardware

Clear the TPM security hardware

You must restart your computer to configure your TPM security hardware settings so that your TPM can be cleared. To do so:

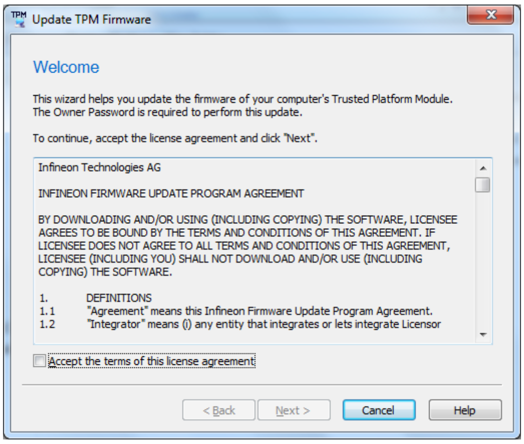
Click the Restart button below.

Be Physically present at the computer to follow the instructions that appear during the startup process.

Log on to Windows to continue the wizard automatically.

After restart, BIOS warning message may appear. Press [F11] to clear TPM and proceed.

10. Right click Firmware Update Tool in Table 1 corresponds to Manufacturer Version, choose “Run as administrator”. The following screen appears.



Update TPM Firmware

Welcome

This wizard helps you update the firmware of your computer's Trusted Platform Module. The Owner Password is required to perform this update.

To continue, accept the license agreement and click "Next".

Infineon Technologies AG

INFINEON FIRMWARE UPDATE PROGRAM AGREEMENT

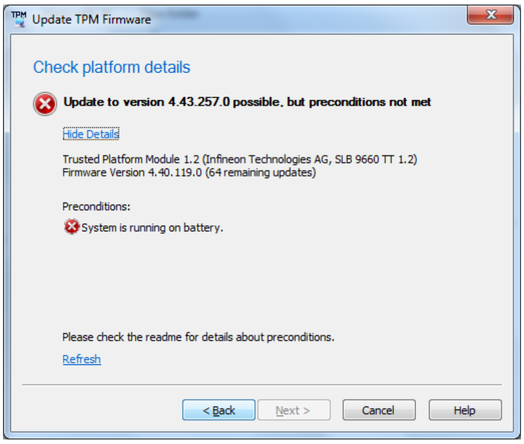
BY DOWNLOADING AND/OR USING (INCLUDING COPYING) THE SOFTWARE, LICENSEE AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF LICENSEE DOES NOT AGREE TO ALL TERMS AND CONDITIONS OF THIS AGREEMENT, LICENSEE (INCLUDING YOU) SHALL NOT DOWNLOAD AND/OR USE (INCLUDING COPYING) THE SOFTWARE.

1. DEFINITIONS
1.1 "Agreement" means this Infineon Firmware Update Program Agreement.
1.2 "Integrator" means (i) any entity that integrates or lets integrate Licensor

□ Accept the terms of this license agreement

11. Check “Accept the terms of this license agreement”, and choose “Next”.

In case AC adapter is not plugged, the following screen appears. Plug the AC adapter and choose “Back” to return previous screen once.



Update TPM Firmware

Check platform details

Update to version 4.43.257.0 possible, but preconditions not met

Hide Details

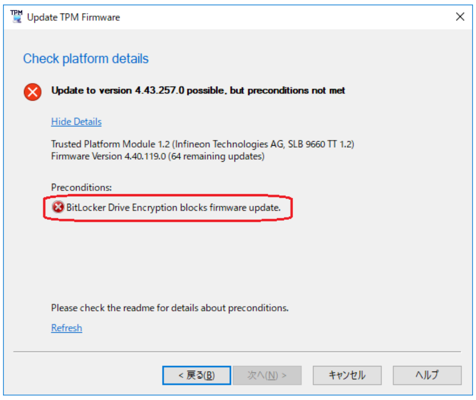
Trusted Platform Module 1.2 (Infineon Technologies AG, SLB 9660 TT 1.2)
Firmware Version 4.40.119.0 (64 remaining updates)

Preconditions:
System is running on battery.

Please check the readme for details about preconditions.

Refresh

In case the following screen appears (Preconditions shows “BitLocker Drive Encryption blocks firmware update”), BitLocker is turned on. Press “Cancel” to cancel the firmware update, and “Suspend protection of” BitLocker, then go back to 10.



Update TPM Firmware

Check platform details

Update to version 4.43.257.0 possible, but preconditions not met

Hide Details

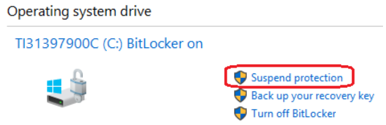
Trusted Platform Module 1.2 (Infineon Technologies AG, SLB 9660 TT 1.2)
Firmware Version 4.40.119.0 (64 remaining updates)

Preconditions:

BitLocker Drive Encryption blocks firmware update.

Please check the readme for details about preconditions.

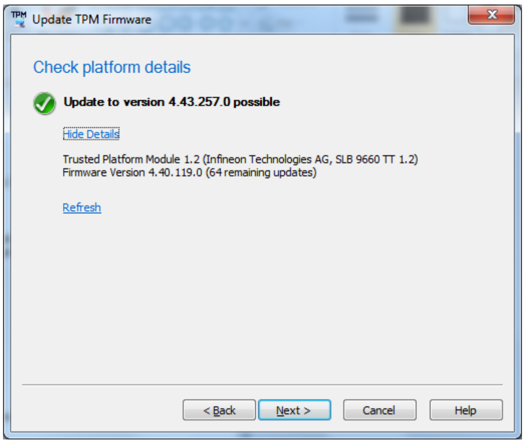
Refresh



Operating system drive

TI31397900C (C:) BitLocker on

12. The following screen appears. Check platform details and choose “Next”.



Update TPM Firmware

Check platform details

Update to version 4.43.257.0 possible

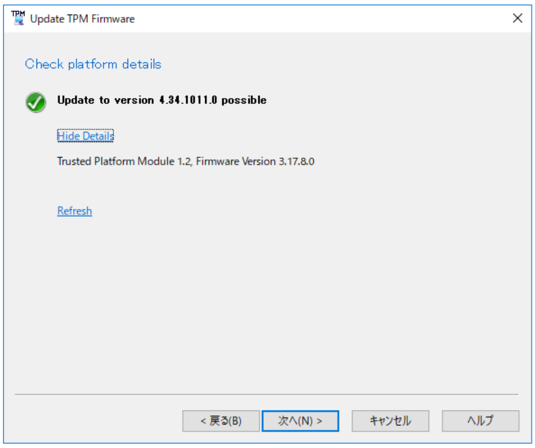
Hide Details

Trusted Platform Module 1.2 (Infineon Technologies AG, SLB 9660 TT 1.2)
Firmware Version 4.40.119.0 (64 remaining updates)

Refresh

WARNING

- In case Manufacturer Version is 3.17 or 3.19, it is not a subject to firmware update, the following screen can appear. In the case, choose “Cancel” to cancel firmware update. Even if you choose “Next”, firmware update is not executed.



Update TPM Firmware

Check platform details

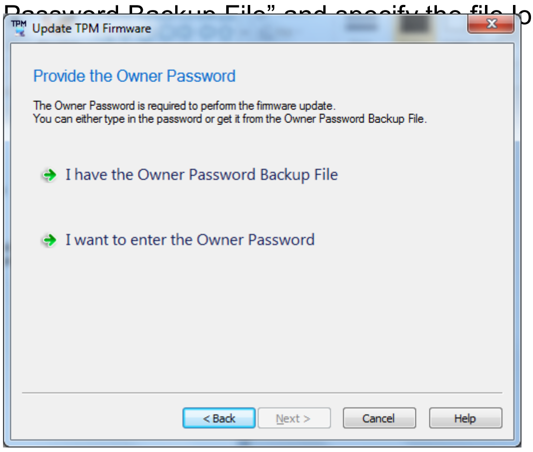
Update to version 4.34.1011.0 possible

Hide Details

Trusted Platform Module 1.2, Firmware Version 3.17.8.0

Refresh

13. In case the following screen appears, provide the Owner Password. In case does not appears, skip to 14. In case having the Owner Password as the Owner Password Backup File, choose “I have the Owner Password Backup File” and specify the file location by pressing “Browse...”.

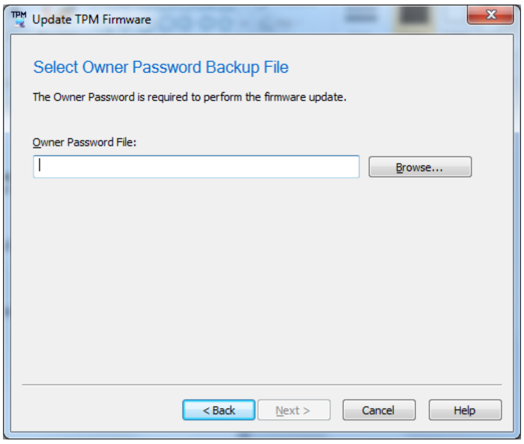


Provide the Owner Password

The Owner Password is required to perfom the fimware update.
You can either type in the password or get it from the Owner Password Backup File.

I have the Owner Password Backup File

I want to enter the Owner Password

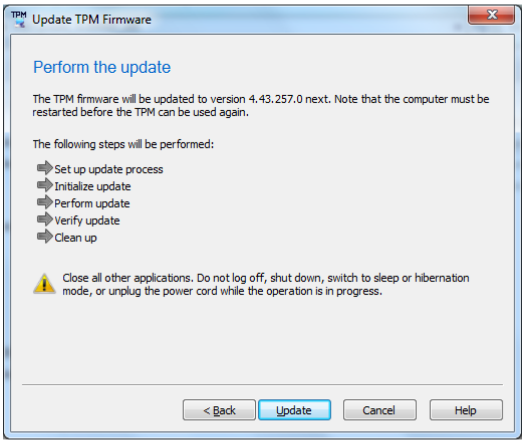


Select Owner Password Backup File

The Owner Password is required to perform the firmware update.

Owner Password File:

14. Choose “Update” to start firmware update.



Perform the update

The TPM firmware will be updated to version 4.43.257.0 next. Note that the computer must be restarted before the TPM can be used again.

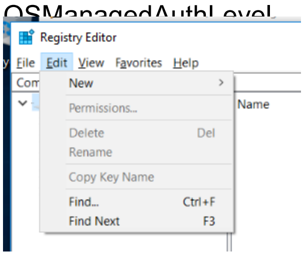
The following steps will be performed:

- Set up update process
- Initialize update
- Perform update
- Verify update
- Clean up

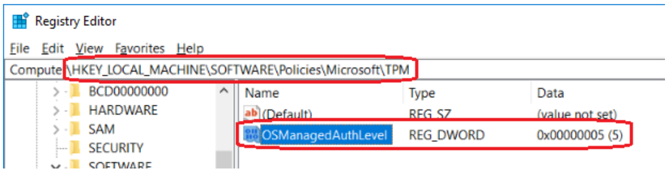
Close all other applications. Do not log off, shut down, switch to sleep or hibernation mode, or unplug the power cord while the operation is in progress.

15. Run “regedit” from Start Menu. (Type “regedit” at “Search programs and files”.) “Registry Editor” appears.

16. Search registry key [HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥TPM] OSManagedAuthLevel. Choose “Edit” – “Find…”.



Type “OSManagedAuthLevel” at “Find what”, then press “Find Next”. The following screen appears after a while.

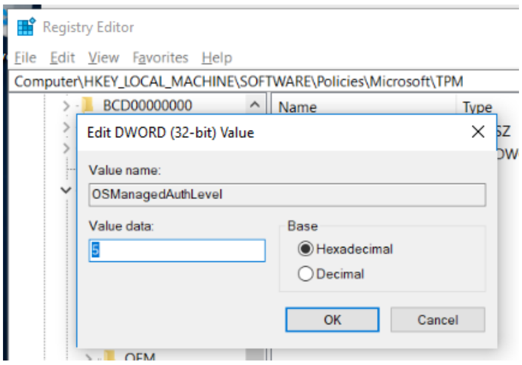


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\TPM

Name	Type	Data
(Default)	REG_SZ	(value not set)
OSManagedAuthLevel	REG_DWORD	0x00000005 (5)

Clarify upper text shows “HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥TPM”, and lower left text shows “OSManagedAuthLevel”.

17. Double click “OSManagedAuthLevel”. The following screen appears.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\TPM

Value name: OSManagedAuthLevel

Value data: 5

Base
● Hexadecimal
○ Decimal

18. Change “Value data” as data noted at 5, and press “OK”.

(End of Document)