HP has been moving to utilize version 2.0 of the Trusted Platform Module (TPM) Firmware on its newer products. The previous version of TPM is version 1.2. As there will be the possibility that customers have either upgraded or downgraded the version of TPM firmware they are using from what was originally installed on the system (or what was the default setting for that system), field engineers need to be able to adjust TPM settings when replacing a system board.

The purpose of this document is to provide an overview of how to determine if you need to change TPM firmware versions and the process to do so.

**Note:** The procedures described in this guide are for HP Commercial Notebooks, Desktops and RPOS only. HP Workstations will have the replacement system board set to the TPM firmware version of the system as it was ordered / requested.
Contents
HP TPM Strategy ........................................................................................................................................3
How to Determine the Required TPM Firmware Version ........................................................................6
New TPM Label on Replacement System Boards .................................................................................8
Process Overview ....................................................................................................................................9
Configuring TPM firmware - Notebooks ...............................................................................................11
Setting TPM Firmware Version - Desktops ............................................................................................15
**HP TPM Strategy**

HP is working to make the transition from TPM V1.2 to TPM V2.0 as smooth as possible. New systems introduced in 2016 and beyond will have the latest TPM V2.0 firmware as a default. In addition, replacement system boards for these products will be shipped with TPM set to V2.0. Older products or products that are currently shipping (sustaining) in 2016 will have TPM set to V1.2 as default and replacement system boards for those products will also have TPM set to V1.2. When the next generation of these products are introduced, they will begin using the TPM V2.0 firmware.

The following table summarizes the TPM firmware default options by operating system.

<table>
<thead>
<tr>
<th>Manufacture date</th>
<th>OS version</th>
<th>Default TPM firmware</th>
<th>TPM firmware can be configured to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPI before 7/28/16</td>
<td>Win 7 32/64-bit image</td>
<td>1.2</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>Win 10 image</td>
<td>1.2</td>
<td>2.0</td>
</tr>
<tr>
<td>NPI after 7/28/16</td>
<td>Win 7 32-bit image (only hybrid *)</td>
<td>1.2</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Win 7 64-bit image (only hybrid **)</td>
<td>1.2</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>Windows 10 Image</td>
<td>2.0</td>
<td>1.2</td>
</tr>
</tbody>
</table>

*Hybrid Platforms are Intel Skylake processor in a Kabylake chipset, or AMD Carrizo processor in Bristol Ridge chipset.*
Products Shipping with TPM V2.0 IN 2016

The following is a sample list of products that are shipping or scheduled to ship in 2016 with TPM firmware set to V2.0. Replacement system boards for these products will also be shipped with TPM set to V2.0. Customers may choose to downgrade to TPM V1.2 based upon their current operating system and organizational needs.

<table>
<thead>
<tr>
<th>Product</th>
<th>Launch</th>
<th>Shipped Default</th>
<th>Spare Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slice Elite HP Slice</td>
<td>8/22/2016</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>HP Elite 705 G3 SFF/MT</td>
<td>8/29/2016</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>Elite 705 G3 DM</td>
<td>8/29/2016</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>HP EliteBook Folio G1</td>
<td>3/18/2016</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>HP EliteBook Folio 1030 G1</td>
<td>5/20/2016</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>HP Elite X2 1012 G2</td>
<td>9/12/2016</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>HP ProBook 650/640 G2</td>
<td>1/6/2016</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>HP ProBook 655/645 G2</td>
<td>1/6/2016</td>
<td>2.0</td>
<td>2.0</td>
</tr>
</tbody>
</table>
Products Shipping with TPM V2.0 as an Option

Certain sustaining products (products currently shipping) provide the option of setting the TPM firmware to either V1.2 or V2.0 at the factory. The default setting for these products is TPM V1.2 and all system boards for these products are shipped with TPM set to V1.2. Customers may choose to configure the TPM to V2.0 on systems with the Windows 10 Operating Systems based upon their current operating system and organizational needs. The following table lists systems that support either TPM V1.2 or TPM V2.0.

<table>
<thead>
<tr>
<th>Product</th>
<th>Refresh Date / AV Available</th>
<th>Shipped Default</th>
<th>Spare Board</th>
<th>Option to be configured to TPM V2.0 from the Factory</th>
</tr>
</thead>
<tbody>
<tr>
<td>600 G2 SFF/MT/DM</td>
<td>5/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>600 G2 AiO T/NT</td>
<td>5/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>705 G2 SFF/MT/DM</td>
<td>5/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>705 G2 AiO T</td>
<td>5/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>800 G2 TWR/SFF/DM</td>
<td>5/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>800 G2 AiO</td>
<td>5/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>RP9 Model 9815/9818</td>
<td>5/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP EliteBook 1030</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP EliteBook Folio 1040 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ProBook 430 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ProBook 470 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ProBook 440 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ProBook 450 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ProBook 455 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ProBook 645 G2</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ProBook 645 G2</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP EliteBook 755 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP EliteBook 745 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP EliteBook 725 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP EliteBook 820 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP EliteBook 850 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP EliteBook 840/848 G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ProBook 650 G2</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ProBook 640 G2</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
<tr>
<td>HP ZBook 15u G3</td>
<td>9/1/2016</td>
<td>1.2</td>
<td>1.2</td>
<td>Yes</td>
</tr>
</tbody>
</table>
How to Determine the Required TPM Firmware Version

As a Field Engineer onsite, you must determine what TPM firmware version is required by the customer for the system board you are about to replace. There are multiple ways to determine which TPM firmware version is required:

Ask Your Customer

Most large commercial / enterprise accounts will know what TPM firmware version they are using for their systems, especially if the customer has changed the TPM firmware version after purchase or ordered a specific SKU with a unique TPM firmware version from the default version for that system.

Smaller customers may not know their TPM firmware version. These customers are less likely to have changed the firmware version or ordered a specific SKU with a unique TPM firmware version from the default version for that system. In this case, the replacement system board likely already includes the correct TPM firmware version.

Identify TPM Firmware Version from Current System Board

If you are able to boot the current system (or an identical system from the customer) and access the BIOS, you can determine the TPM firmware version of the current system board before you replace it. To determine the current TPM firmware version on a system, follow these steps:

1. Power on the computer and press F10 prior to OS boot.
3. View the TPM version of the current system board. The following graphic shows an example of a TPM configured to V1.2.
Look up the Unit in Serial Number Repository

If you have internet access, you can look up the system in the Serial Number Repository to see if the customer purchased a specific SKU with a unique TPM firmware version from the default setting for that system. Systems with the option of selecting the TPM firmware version will show up in the Serial Number Repository as a specific AV.

Operating System

While not 100% accurate, understanding what Operating System the customer is using can be useful in trying to determine if the TPM firmware needs to be changed. As a general rule, customers running Windows 7 Operating System will be using TPM V1.2. If the customer is running the Windows 10 operating system, there is a good chance that they will have moved to TPM V2.0.
New TPM Label on Replacement System Boards

To help facilitate the TPM configuration process, new system boards that feature the new HP Common Core BIOS will begin shipping with a label on the system board’s anti-static bag. The purpose of the label is to:

- Serve as a reminder to the field technician that the TPM Firmware on the system board they just received can be configured.
- Prompt the field technician to confirm TPM setting requirements on the current system under repair before installation of new system board.
- Provide links to obtain the detailed instruction to configure TPM.
- Identify the TPM firmware setting of the replacement system board.

Sample image of the new TPM Label to be found on replacement system boards that support the new HP Common core BIOS.

It is important to note that only system boards that support the new HP Common Core BIOS will feature the TPM labels. Older system boards will not feature the label and will not require the field technician to configure TPM.
Process Overview
As part of the system board replacement process, configuring the TPM firmware version should take place before Programming DMI, Committing ME (if applicable) and Locking the System Board. As always, the first step in the process will be to gather all of the appropriate information. A high-level overview of the process is outlined below:

TPM / DMI / Committing Process Flow
Update System BIOS

It is critical that you update the System BIOS to the most current version before attempting to change TPM settings.

Before you begin

Remember, you should ask the customer to do the following before performing any service procedures.

- Systems with BitLocker or other encryption should be unlocked before programming the DMI. Ask the customer to disable the encryption before service. If the customer is not able to do this prior to service, the customer will need to provide the recovery key.

- Remind the customer that with any system board replacement, the customer will need to use their recovery key to re-create the encryption key stored by the new TPM. This is the only way that the customer will be able to access their encrypted drive after system board replacement.

- BIOS passwords need to be cleared or provided prior to the service.
Configuring TPM firmware - Notebooks
To configure the TPM firmware version on commercial notebooks, use the UEFI TPM Update utility found on the DOS USB Key of your DMIFIT USB Keys. The TPM Update utility is included with DMIFIT V2.10. Follow the steps below to complete the procedure.

**Steps for Setting TPM using UEFI TPM Utility**

**Ensuring Boot Mode and Clear TPM**

1. Insert the DOS USB key into a USB 2.0 slot.
2. Power up the notebook.
3. Press F10 to enter HP Computer Setup.
5. Select Legacy Support Enabled and Secure Boot Disabled.

7. Select On next boot.

8. Press F10 to exit and select Save Changes.
Boot to DOS USB Key

1. Press F9 to access the boot options menu.
2. Select External USB Hard Drive (UEFI).

The system will automatically start the Commit ME utility and display a menu similar to the one below:

```
ME Firmware Type: Corporate/StdME
Discrete VGA Only: No.
Menu to commit the system as:
1 - vPro
2 - vPro w/RAID
3 - vPro w/PCIe
4 - vPro w/USB3.0
5 - vPro w/NFC support
6 - vPro w/SD support
7 - vPro w/SD + NFC support
8 - vPro w/SD + NFC + USB3.0
9 - vPro w/SD + NFC + USB3.0
10 - vPro w/SD + NFC + USB3.0
11 - vPro w/SD + NFC + USB3.0
12 - vPro w/SD + NFC + USB3.0
13 - vPro w/SD + NFC + USB3.0
14 - vPro w/SD + NFC + USB3.0
15 - vPro w/SD + NFC + USB3.0
16 - vPro w/SD + NFC + USB3.0

****All the files must be in folder \EFI\BOOT ****
Enter choice and press Enter
```

Run TPM Utility

1. At the prompt, type: TPM <enter>.

The tool will run and display a short menu indicating the current version of the TPM firmware and the option to upgrade to a later version (if required) or switch to an alternate version.

Important: Tool indicates current version of TPM on the system board.

Important: Tool provides a menu of options available and what to type to run each option.

Important: The file name to type to run the appropriate utility is shown here.
2. At the prompt, type the appropriate file name to run the corresponding utility. In the example above, you could type either of the following two commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>121to12.nsh</td>
<td>Update to latest version of TPM V1.2</td>
</tr>
<tr>
<td>121to20.nsh</td>
<td>Switch from TPM V1.2 to TPM V2.0</td>
</tr>
</tbody>
</table>

**Note:** Note that these menu options will change based upon your system. You should identify the action required and enter the corresponding command line as shown on your screen.

**Note:** If the system board is already configured with the latest version of TPM V1.2, you will not see the option to configure the latest version of TPM V1.2. You will only be presented the option to configure to V2.0.

For example, to switch from TPM V1.2 to TPM V2.0, type: **121to20.nsh<enter>**.

The utility will begin to configure the TPM firmware.

![Configuration Process](image)

After completion, the utility will confirm that the TPM firmware configuration was successful and the utility will return you to the prompt.

![Confirmation](image)

3. At the prompt, reboot the system.
Confirm TPM firmware version / TPM Enabled

1. Press F10 to access the HP Computer Setup utility.
2. Navigate to Security > TPM Embedded Security and verify the following settings:
   - TPM Specification Version should indicate the desired version of TPM.
   - TPM State box should be checked (if not, please check the TPM State box).

Important: Confirm that you are set to the version of TPM required by the customer.

Important: Confirm TPM is enabled by making sure there is a “✓” in the box.
Setting TPM Firmware Version - Desktops
To set the TPM firmware version on commercial desktops (in “Panic Mode”), use the UEFI TPM Utility found on the DOS USB Key of your DMIFIT V2.10 USB Keys. Follow the steps below to complete the procedure.

Steps for Setting TPM using UEFI TPM Utility

Ensuring Boot Mode / Clear TPM
1. Boot the system.
Upon startup, you should see the screen below indicating that the desktop system board is in “Panic Mode” (meaning the ME has been committed and the MPM lock command has been issued at the factory).

![Manufacturing Program Mode](image)

2. Press Y to enter the HP Computer Setup Utility.
5. Navigate to **Security > TPM Embedded Security > Clear TPM.**
6. Select **On next boot.**

![TPM Security Settings](image)

7. Press **F10** to exit and then **Save Changes.**
   
The system will reboot and return to the “Panic Mode” screen.

**Run TPM Utility**

1. Press the **Space Bar** to continue boot and immediately press the **Escape** key.
   
   This will take you to the Start-Up Menu.
2. Press **F9** for Boot Options Menu.
3. Select **External USB Hard Drive (UEFI).**
   
The system will display a status menu similar to the one below:

![Tpm Utility Menu](image)

4. At the prompt type: **TPM <enter>**.
   
The tool will run and display a short menu indicating the current version of the TPM firmware and the option to upgrade to the latest version (if required) or switch to the alternate version.
7. At the prompt, type the appropriate file name to run the corresponding utility. In the example above, you could type either of the following two commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>121to12.nsh</td>
<td>Update to latest version of TPM V1.2</td>
</tr>
<tr>
<td>121to20.nsh</td>
<td>Switch from TPM V1.2 to TPM V2.0 2.0</td>
</tr>
</tbody>
</table>

For example, to switch from TPM V1.2 to TPM V2.0, type: **121to20.nsh <enter>**.

The utility will begin to update the TPM Firmware.
After completion, the utility will confirm that the TPM firmware update was successful and the utility will return you to the prompt.

8. At the prompt, reboot the system. The system returns to the “Panic Mode” screen.

Confirm TPM firmware version / TPM Enabled

1. At “Panic Mode” screen, press Y to enter the HP Setup Utility.
2. Select Security > TPM Security and confirm the following TPM settings:
   - TPM Specification Version should indicated desired version of TPM.
   - TPM State box should be checked (if not, please check TPM State box).

21. Once the TPM settings are confirmed, you can proceed to program DMI Information under Main > Set Machine Unique Data.

As the system is still in panic mode, it should lock MPM once the correct system information has been entered.

Important: Confirm that you are set to the version of TPM required by the customer.

Important: Confirm TPM is enabled by making sure there is a “√” in the box.
After Setting TPM

Once you have selected the appropriate TPM setting, you can continue on with Programming DMI, Committing ME and locking the system board as required.