How to Clear TPM HW on HP Personal Systems

Version: 6

Release Date: 18 October 2017

There are several methods to clear TPM HW on HP Personal Systems, depending on the system model. This document is only intended to provide instructions on how to clear TPM HW using the different methods. Note: Clearing the TPM will remove any keys previously generated by the TPM.

It is strongly recommended that you follow all instructions from software vendors for disabling or suspending TPM protections within the applications prior to using these Clear TPM instructions. It is also recommended backup your data and the TPM data in the event that TPM protected data becomes unavailable after clearing the TPM if you did not properly suspend or disable the protection.

On some HP systems, you may be required to take additional preparations to disable or suspend HW or BIOS features that use TPM protection, for example, Intel® Trusted Execution Technology (TXT) or Intel® Software Guard Extensions (SGX).

WARNING! HP strongly recommends backing up all data before performing this procedure. Errors or mistakes during the process can render the hard drive inaccessible and can result in loss of data stored on the hard drive. HP is not responsible for loss of data that might occur during the procedure.

Preparations before Clearing TPM

Caution: Failure to properly prepare your system before clearing the TPM may cause data protected by a TPM key to become unavailable. Before using any of the clear TPM instructions, be sure to follow all recommended preparations to disable or suspend software or system features that depend on the TPM protections.

- Make sure all applications that use the TPM have been disabled or suspended.
- Make sure all TPM protected data has been properly backed up.
- Disable or suspend system features that use TPM in BIOS Setup.

For additional information and precautions to clearing your TPM, see section 6 “Clear TPM” of the following Microsoft advisory:

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV170012

Disable System Features in HP BIOS Setup or HP BiosConfigurationUtility (BCU)

If your system supports Intel® TXT or Intel® SGX, suspend or disable applications that use these features, then set the BIOS settings to disable in preparation for clearing the TPM.

For systems that support Intel® TXT, the feature setting can be found in BIOS Setup (F10) or the HP Public WMI utility HP BiosConfigurationUtility (BCU). Depending on the platform model, the feature may be presented as follows:

Trusted Execution Technology (TXT)
*Disable
Enable

For systems that support Intel® SGX, the feature setting can be found in BIOS Setup (F10) or the HP Public WMI utility HP BiosConfigurationUtility (BCU). Depending on the platform model, the feature may be presented as follows:

Intel Software Guard Extensions (SGX) *Disable Enable	Intel Software Guard Extensions (SGX) *Disable Enable Software control

For further information, see the BIOS (UEFI) Setup Guide for you specific system.

There are two methods to Clear TPM. Of the two, HP recommends using Clear TPM Method for Customers using Microsoft Windows.

1. Clear TPM Method for Customers using Microsoft Windows

Customers using Microsoft Windows 10 / 8 / 7 on the latest HP products are recommended to follow the Clear TPM instructions provided on the following Microsoft website (using TPM.MSC or PowerShell Clear-TPM):

https://docs.microsoft.com/en-us/windows/device-security/tpm/initialize-and-configure-ownership-of-the-tpm#clear-all-the-keys-from-the-tpm

Note: On some HP systems, the BIOS (UEFI) may prompt for PPI (Physical Presence) when requesting to clear the TPM via Windows TPM.MSC. Users must accept the change to complete clearing the TPM. Do not accept the clear TPM PPI if the request is from an unknown source, contact your administrator.

Note: On some HP systems, to clear the TPM via Windows TPM.MSC, additional settings must be configured in BIOS Setup (or BCU).

Reset of TPM from OS	Reset of Embedded Security Device through OS
*Enable	Disabled
Disable	*Enabled

2. Clear TPM Method using BIOS Setup

Depending on your system model, the specific instructions and setting names may vary from the general process described below.

> **Caution:** Failure to properly prepare your system before clearing the TPM may cause data protected by a TPM key to become unavailable. Before using any of the clear TPM instructions, be sure to follow all recommended preparations to disable or suspend software or system features that depend on the TPM protections.

1. Turn on or restart the system.
2. During BIOS POST, press F10 to enter BIOS setup.
3. Go to the Security page.
4. Set Clear TPM as ‘On next boot’.
   Note: Alternate settings may include:
   - Clear TPM as ‘Yes’
   - Reset to Factory Settings as ‘Reset’
   - TPM Set to Factory Defaults as ‘Yes’

   Note: Some platforms may require ‘BIOS Admin Password’ or ‘Setup Password’ to be configured prior to accessing the Clear TPM setting. Refer to the Computer User’s Guide or BIOS (UEFI) Setup Guide for your specific model for more details.

5. Save changes and exit F10.
   Note: After saving the change and exiting F10, the system will restart and may display the following message or similar message, depending on system model:

```
A configuration change was requested to clear
this computer's TPM (Trusted Platform Module)

"WARNING: Clearing erases information stored on the TPM."
"You will lose all created keys and access to data encrypted by these keys. "

Press F1 = Accept
Press F2 = Reject
```

Note: For older HP Elite Desktops, Workstations, Thin Clients, and Retail systems, BIOS does not prompt for the PPI (Physical Presence) when clearing the TPM via BIOS Setup.

6. Press F1 to accept.
   Note: The system may turn off for a few seconds, then automatically turn back on. The TPM has been cleared.

After the TPM has been cleared during BIOS POST, additional steps may be required to re-enable the TPM. For TPM2.0, no additional actions are required. For TPM1.2, use the following steps to re-enable the TPM.

1. Turn on or restart the system.
2. During BIOS POST, press F10 to enter BIOS setup.
3. Go to the Security page.
4. Set TPM State as ‘Enable’ (check the TPM State).
   Note: Alternate settings may include:
   - Embedded Security Device State as ‘Enable’ (check the box)
   - Embedded Security Device as ‘Enabled’
5. Save changes and exit F10.
   Note: After saving the change and exiting F10, the system will restart and may display below message:

```
A configuration change was requested to enable
this computer's TPM (Trusted Platform Module)

Press F1 = Accept
Press F2 = Reject
```

   Note: For older HP Elite Desktops, Workstations, Thin Clients, and Retail systems, BIOS does not prompt for the PPI (Physical Presence) when enabling the TPM (Embedded Security Device) via BIOS Setup.

7. Press F1 to accept.
   Note: The system may turn off for a few seconds, then automatically turn back on. The TPM has been enabled and is ready for use.

HP Inc. shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither HP or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice. HP Inc. and the names of HP products referenced herein are trademarks of HP Inc. in the United States and other countries. Other product and company names mentioned herein may be trademarks of their respective owners.