



Intel® Trusted Execution Engine Software

Installation and Configuration Guide

Supporting Intel® TXE firmware version: 4

April 2020

Revision 1.0



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm%20>

All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Intel® Active Management Technology requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup and configuration. For more information, visit Intel® Active Management Technology.

No system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) requires an enabled chipset, BIOS, firmware and software, and a subscription with a capable Service Provider. Consult your system manufacturer and Service Provider for availability and functionality. Service may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit <http://www.intel.com/go/anti-theft>.

No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd gen Intel® Core™ processor enabled chipset, firmware and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit <http://ipt.intel.com>.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel, Core, and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2017-2020 Intel Corporation. All rights reserved



IMPORTANT—READ BEFORE COPYING, INSTALLING OR USING.

Do not use or load this software or any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

LICENSE—Subject to the restrictions below, Intel Corporation ("Intel") grants you the following limited, revocable, non-exclusive, non-assignable, royalty-free copyright licenses in the Software.

The Software may contain the software and other property of third party suppliers, some of which may be identified in, and licensed in accordance with, the "license.txt" file or other text or file in the Software:

DEVELOPER TOOLS—including developer documentation, installation or development utilities, and other materials, including documentation. You may use, modify and copy them internally for the purposes of using the Software as herein licensed, but you may not distribute all or any portion of them.

RESTRICTIONS—You will make reasonable efforts to discontinue use of the Software licensed hereunder upon Intel's release of an update, upgrade or new version of the Software.

You shall not reverse-assemble, reverse-compile, or otherwise reverse-engineer all or any portion of the Software.

Use of the Software is also subject to the following limitations:

You,

- (1) are solely responsible to your customers for any update or support obligation or other liability which may arise from the distribution of your product(s)
- (ii) shall not make any statement that your product is "certified," or that its performance is guaranteed in any way by Intel
- (iii) shall not use Intel's name or trademarks to market your product without written permission
- (iv) shall prohibit disassembly and reverse engineering, and
- (v) shall indemnify, hold harmless, and defend Intel and its suppliers from and against any claims or lawsuits, including attorney's fees, that arise or result from your distribution of any product.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS—Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You will not remove, alter, deface or obscure any copyright notices in the Software. Intel may make changes to the Software or to items referenced therein at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITED MEDIA WARRANTY—If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

EXCLUSION OF OTHER WARRANTIES—EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel or its suppliers do not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained in the Software.

LIMITATION OF LIABILITY—IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.



Revision History

Revision Number	Description	Revision Date
1.0	• Initial Release	April 2020



Contents

1	Introduction	6
2	Software Components Overview	7
2.1	Intel® Trusted Execution Engine Interface (Intel® TXEI)	7
2.2	Intel® Dynamic Application Loader (Intel® DAL).....	7
2.3	Intel® Capability Licensing Services Client (iCLS Client)	7
2.4	Intel® Storage Proxy Driver (Intel® SPD)	7
3	Installer List.....	8
3.1	Intel® TXE SW Installer	8
3.2	Intel® TXE_SW_DCH	8
3.3	WindowsDriverPackages	8
4	System Requirements	9
5	Installing Intel® TXE Software Components.....	10
5.1	How to Install.....	10
5.1.1	Windows* 10 RS2 and before.....	10
5.1.2	Windows* 10 RS3 and beyond	11
5.2	Error Codes during Installation	13
5.3	Windows* PE.....	14
5.4	Firewall policy	14
6	Identifying Intel® TXE Software Components	15
7	Uninstalling Intel® TXE Software and Drivers.....	17



1 Introduction

This guide describes how to install, configure and troubleshoot the Intel® Trusted Execution Engine (Intel® TXE) software components.

For a list of software components, see *Software Components Overview*.





2 Software Components Overview

This section lists the software components supplied with the firmware kit and provides a short overview of each component.

To view the installer options, enter the following in a Command window:
SetupTXE.exe -? and the help dialog should appear.

2.1 Intel® Trusted Execution Engine Interface (Intel® TXEI)

This driver is the interface between the Intel® Trusted Execution Engine (Intel® TXE) firmware and the operating system. Drivers and applications on the host that wish to interact with Intel® TXE can use the Intel® TXEI host Windows* driver.

2.2 Intel® Dynamic Application Loader (Intel® DAL)

This is a service which exposes the host interface to usage of the Intel® Dynamic Application Loader infrastructure abilities, for loading/unloading signed applications to the Trusted Execution Environment and communicating with them. It will only be installed if the platform is Intel® Dynamic Application Loader capable.

2.3 Intel® Capability Licensing Services Client (iCLS Client)

Intel® Capability Licensing Services Client is a set of applications, services and dynamic libraries used to establish a trusted connection between FW and Intel's backend. It is responsible for:

- EPID group certificates provisioning to the FW
- Trusted Computing Base Recovery: EPID rekey
- Platform Trust Technology (firmware TPM) recertification
- Delivering assets to the FW (i.e. DRM keying material, signed permits)

2.4 Intel® Storage Proxy Driver (Intel® SPD)

Intel® Storage Proxy Driver is a host OS driver for UFS management. Intel® CSE and BIOS uses this proxy driver to perform the storage access during the Post OS boot scenario where storage head is owned by the OS storage driver.



3 ***Installer List***

This section describes the installation packages for the Intel® TXE software.

3.1 Intel® TXE SW Installer

This installation program is located at Installers folder and installs the Intel® TXE software components required for the platform on which you are installing, and installs only those components that match your platform's capabilities.

Following is a complete list of the components in the installer:

- Intel® Trusted Execution Engine Interface (Intel® TXE Interface) which is DC-compliant
- Intel® Dynamic Application Loader (Intel® DAL)
- Intel® Capability Licensing Service Client (iCLS Client)
- Intel® Storage Proxy Driver (Intel® SPD) which is DC-compliant

3.2 Intel® TXE_SW_DCH

This installation program installs the Intel® TXE software components required for the platform on which you are installing, and installs only those components that match your platform's capabilities.

Following is a complete list of the components in the installer:

- Intel® Trusted Execution Engine Interface (Intel® TXE Interface) driver which is DC-compliant
- Intel® Dynamic Application Loader (Intel® DAL) driver which is DC-compliant
- Intel® Capability Licensing Service Client (iCLS Client) driver which is DC-compliant
- Intel® Storage Proxy Driver (Intel® SPD) which is DC-compliant

3.3 WindowsDriverPackages

This package includes the drivers as UWD INF installer.

- TXEI: heci.inf in Installers\WindowsDriverPackages\TXEI
- iCLS: iclsClient.inf in Installers\WindowsDriverPackages\iCLS
- DAL: DAL.inf in Installers\WindowsDriverPackages\JHI\win10
- SPD: iclsClient.inf in Installers\WindowsDriverPackages\SPD
- OemExtension: OemExtension.inf in Installers\WindowsDriverPackages\OemExtension



4 *System Requirements*

To enable installation and use of the Intel® TXE software components, the following are required on the platform:

- Windows* 10.

§



5 Installing Intel® TXE Software Components

5.1 How to Install

5.1.1 Windows* 10 RS2 and before

The software installer **SetupTXE.exe** is located in the firmware kit in the **Installers** folder.

- 1) Double-click the installer to install the software components
- 2) Follow the steps in the installation wizard to complete the installation.
- 3) When the installation is complete, click **Next** in the *Setup Progress* window, then click **Finish** in the *Setup is Complete* window.

The software installer has command line options for specific installing configuration, under command line mode execute setupTXE.exe -? Will display the available options as follows:

-?

Displays this help dialog.

-b

Reboots the system without prompting after setup is complete, if reboot is required.

-dal

Installs only DAL.

-l <LCID>

Specifies the language of the setup dialogs.

-nodal

DAL will not be installed.

-notcs

TCS will not be installed.

-notxei

TXE driver will not be installed.

-overwrite

Ignores the overwrite warning.

-qn

Alternate silent mode.



-report <path>
Changes the default log path.

-s
Does not display any setup dialogs (silent install).

-tcs
Installs only TCS.

-txei
Installs only the TXE driver.

-ver
Displays driver versions.

The installation logs can be found at <user folder>\Intel\Logs.

5.1.2 Windows* 10 RS3 and beyond

The driver for TXEI , DAL, iCLS and SPD are provided as UWD INF installer. The component INFs are located in the firmware kit in the **Installers\WindowsDriverPackages** folder.

To install the drivers, right click on INF file, and click on install.

System manufacturers can take advantage of the components in **Installers\WindowsDriverPackages** to do offline injection e.g. via DISM. More information about DISM can be found at:

<https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/what-is-dism>

Note: TXEI driver is required to be installed before other drivers.

OemExtension is required to be installed along with installation of JHI or iCLS drivers.

The following devices will be shown in the device manager if the according drivers are installed on compatible devices:

TXEI: System devices \ Intel(R) Trusted Execution Engine Interface

DAL: Software components \ Intel(R) Dynamic Application Loader Host Interface

iCLS: Software components \ Intel(R) iCLS Client

SPD : System devices \ Intel(R) Trusted Execution Engine Storage Proxy Device



User may use installer **SetupTXE.exe** located in the firmware kit in the **Installers\TXE_SW_DCH** folder to install drivers required for the platform on which you are installing, and install only those components that match your platform's capabilities.

- 1) Double-click the installer to install the software components
- 2) Follow the steps in the installation wizard to complete the installation.
- 3) When the installation is complete, click **Next** in the *Setup Progress* window, then click **Finish** in the *Setup is Complete* window.

The software installer has command line options for specific installing configuration, under command line mode execute setupTXE.exe -? will display the available options as follows:

-?

Displays this help dialog.

-b

Reboots the system without prompting after setup is complete, if reboot is required.

-dal

Installs only DAL.

-l <LCID>

Specifies the language of the setup dialogs.

-nodal

DAL will not be installed.

-notcs

TCS will not be installed.

-notxei

TXE driver will not be installed.

-overwrite

Ignores the overwrite warning.

-qn

Alternate silent mode.

-report <path>

Changes the default log path.

-s

Does not display any setup dialogs (silent install).

-tcs

Installs only TCS.

-txei



Installs only the TXE driver.

-ver
Displays driver versions.

The installation logs can be found at <user folder>\Intel\Logs.

5.2 Error Codes during Installation

Error code	Error String	Description
0	ERROR_SUCCESS	Operation was successful and a reboot is not needed. Use of the -b switch will not cause a reboot in this case.
1602	ERROR_INSTALL_USEREXIT	One of: <ul style="list-style-type: none"> The user canceled the operation Setup was run silently but a downgrade was detected and the -overwrite switch was not used.
1603	ERROR_INSTALL_FAILURE	General failure code. The error could have been an unanticipated error or one of the expected errors such as: <ul style="list-style-type: none"> Not admin No device matches OS requirement not met .NET requirement not met
1633	ERROR_INSTALL_PLATFORM_UNSUPPORTED	Architectures not supported
1641	ERROR_SUCCESS_REBOOT_INITIATED	A system reboot has been initiated either by the user choosing to "reboot now" or the -b switch was used in silent mode and setup requires a reboot. Note that depending on the OS and platform speed, the calling process may never get this code due to it being terminated as part of the shutdown procedure.
3010	ERROR_SUCCESS_REBOOT_REQUIRED	Successful, but a reboot is required to complete the process.

Note that the installer may return other error codes in cases where an application or other process called returns one. The error code returned will be passed through.



5.3 Windows* PE

The Intel® TXEI driver can be installed on Windows* PE OS, and this is primarily used during manufacturing, when attempting to run Windows*-based manufacturing line tools.

When running the Intel® TXEI driver on Windows* PE 3 (based on Windows* 7), it is necessary to ensure that the KMDF 1.11 coininstallers are added to the Windows* PE image build, using the DISM command.

More information can be found at:

<http://msdn.microsoft.com/en-us/library/windows/hardware/ff544208%28v=vs.85%29.aspx>

The required coininstallers can be found at:

<http://msdn.microsoft.com/en-US/windows/hardware/br259104>

5.4 Firewall policy

To use DAL, applications need to be able to communicate with the DAL service over a network interface. The following traffic must not be blocked:

- Incoming traffic
 - From: Localhost
 - To process: jhi_service.exe
 - Port: Any





6 Identifying Intel® TXE Software Components

Once the Intel® TXE software stack is installed on a system, the contents of that kit can be identified via a single Software Package Version (SPV) marker. The Single Package Versioning feature provides one unique version identifier for a package (i.e. anything that is updated in the package iterates the version number). This SPV is useful for systems which need to identify and manage installations such as Software Inventory Control applications used in large IT organizations.

Each Intel® TXE Software Installer package contains a file called the 'mup.xml' which can be used to identify the SPV. The mup.xml describes the following information:
Example:

```
<fullpackageidentifier>

  <registrykeys>

    <registrykey componentID="103288">

      <displayName>HKEY_LOCAL_MACHINE\SOFTWARE\ManageableUpdatePackage\Intel\TXE\Display
</displayName>

      <displayValue>Intel(R) Trusted Execution Engine</displayValue>

<name>HKEY_LOCAL_MACHINE\SOFTWARE\ManageableUpdatePackage\Intel\TXE\Version</name>

      <value> yyww.4.nn.bbbb</value>

    </registrykey>

  </registrykeys>

</fullpackageidentifier>
```

The 'fullpackageidentifier' section points out where to look for the package version and what it should be in order to be the latest. The 'DisplayVersion' and {GUID} above are found Microsoft® Windows® registry in the locations below:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{GUID}\DisplayVersion

Typical release version numbering is as follows, yyww.mm.nn.bbbb where:

- yy – Build year
- ww – Build WorkWeek
- mm – Major version
- nn – Minor version
- bbbb – Build number



Identifying Intel® TXE Software Components

Service name for DAL or iCLS can be found in Services tab in task manager or services in Microsoft Management Console:

DAL: jhi_service / Intel(R) Dynamic Application Loader Host Interface Service

iCLS: SocketHeciServer.exe / Intel(R) Capability Licensing Service TCP IP Interface

TPMProvisioningService.exe / Intel(R) TPM Provisioning Service





7 *Uninstalling Intel® TXE Software and Drivers*

If you are installing TXE SW using SetupTXE.exe, uninstall the software via the Windows Control Panel:

- Double-click Intel® Trusted Execution Engine Components to uninstall the Intel® TXE software components.
- The uninstall welcome window opens.
- Click **Next**. Uninstall will be performed.
- After uninstall operations are completed, click **Next** to reach the uninstall completion window.
- Restart is required for changes to take effect. Click **Finish** to end the uninstall.

If you are installing the inf drivers manually – from the WindowsDriverPackages folder, you should uninstall them manually from device manager

- Right click the device name in device manger and choose **uninstall**

Note: If some system dlls have been removed between the installation and uninstallation of the Intel® TXE software, the uninstallation may fail. This has been noted, for example, when uninstalling Microsoft* Visual C.

Note: Don't manually uninstall TXE SW components via device manager if you are installing TXE SW using SetupTXE.exe.