



Intel® Converged Security Engine 15.40 Software

Installation and Configuration Guide

Supporting Intel® CSE firmware version: 15.40

January 2021

Revision 1.11

Intel Confidential



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.

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 © 2021 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,

- (0) 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
0.7	<ul style="list-style-type: none">Initial Release.	August 2019
0.8	<ul style="list-style-type: none">Update revision number.	November 2019
0.85	<ul style="list-style-type: none">Updated the Installer List to align with the current software components in EHL Intel® CSE 15.40 kits.Updated OS SupportFixed Typos.	March 2020
1.0	<ul style="list-style-type: none">Aligned revision number to 1.0	April 2020
1.1	<ul style="list-style-type: none">Replace Intel® ICLS with Intel® TCSAdd description: Intel® DAL also known as JHIAdded reference for Yocto* Getting Started Guide	August 2020
1.11	<ul style="list-style-type: none">Removed Intel® SPD driverRemoved Intel® TCS driver	January 2021



Contents

1	Introduction	6
	1.1 System Requirements	6
2	Software Components Overview	7
	2.1 Intel® Management Engine Interface (Intel® MEI)	7
	2.2 Intel® Dynamic Application Loader (Intel® DAL).....	7
3	Installer List.....	8
	3.1 ME_SW_DCH Installer	8
	3.2 WindowsDriverPackages	8
4	Installing Intel® CSE Software Components	9
	4.1 Using ME_SW_DCH SW Installer	9
	4.1.1 Logs	10
	4.2 Using UWD INF Installer	10
	4.3 Error Codes during Installation	11
	4.4 Windows* OS for Manufacturing	11
	4.5 Firewall policy	12
5	Identifying Intel® CSE Software Components	13
6	Uninstalling Intel® CSE Software	15



1 Introduction

This guide describes how to install, configure and troubleshoot the Intel® Converged Security Engine (Intel® CSE) software components in Windows* OS.

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

Important Note: For details on the OS configuration and EHL Intel® CSE SW components supported over Linux*, refer to Yocto* Getting Started Guide.

- Document ID [616424](#) . Refer to Chapters 5 and 6.

1.1 System Requirements

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

Windows* 10 RS5 (64Bit) or beyond





2 **Software Components Overview**

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

2.1 **Intel® Management Engine Interface (Intel® MEI)**

This driver is the interface between the Intel® Converged Security Engine (Intel® CSE) firmware and the operating system. Drivers and applications on the host that wish to interact with Intel® CSE can use the Intel® MEI host Windows* driver.

2.2 **Intel® Dynamic Application Loader (Intel® DAL)**

Also known as JHI. 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.





3 Installer List

This section describes the installation packages for the Intel® CSE 15.40 software.

- For installation instruction, refer to Chapter 4 Installing Intel® CSE Software Components.
- For an overview of the SW components, refer to Chapter 2 Software Components Overview.

3.1 ME_SW_DCH Installer

This installation program installs the Intel® CSE software components required for Elkhart Lake, where:

- The installed Intel® CSE software components are Declarative and Componentized (DC) compliant.
- The installer installs only those components that match the platform's capabilities.

See the list below defining the drivers installed:

- Intel® Management Engine Interface (Intel® ME Interface) driver.
- Intel® Dynamic Application Loader (Intel® DAL) driver.

The following table describes the components that are installed for the different platform capabilities:

If the platform includes this capability....	These software components are installed
Intel® Dynamic Application Loader	Intel® MEI driver, Intel® DAL service
PAVP	Intel® MEI driver
None of the above	Intel® MEI driver

3.2 WindowsDriverPackages

This package includes the drivers as Universal Windows* Driver (UWD) INF.

- For Intel® MEI driver, find the **heci.inf**
 - Path: Installers\WindowsDriverPackages\MEI\win10\
- For Intel® DAL, find the **DAL.inf**
 - Path: Installers\WindowsDriverPackages\JHI\win10\





4 Installing Intel® CSE Software Components

4.1 Using ME_SW_DCH SW Installer

The software installer **SetupME.exe** is located in the firmware kit in the **Installers\ME_SW_DCH** folder.

- 1) Double -click the installer to install the software components
- 2) Follow the installation wizard screens.
- 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 also has a command line mode for installing specific configurations. Execute SetupME.exe -? Under command line mode to see all available options as follows:

-?

Displays this help dialog.

-b

Reboots the system without prompting after setup is complete.

-l <LCID>

Specifies the language of the setup dialogs.

-nodrv

Does not install the driver.

-overwrite

Ignores the overwrite warning.

-p <path>

Changes default directory location for application files.

-report <path>

Changes the default log path.

-s

Does not display any setup dialogs (silent install).

-ver

Displays driver versions.

-drvonly

Installs drivers only.



-meidalonly

Installs Intel® Management Engine Interface and Intel® Dynamic Application Loader.

-preinst

Installs all drivers even if hardware is not present.

-tcs

Installs only TCS.

4.1.1 Logs

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

4.2 Using UWD INF Installer

The component INFs are located in the firmware kit under the **Installers\WindowsDriverPackages** folder. See Section 3.2 for more details.

To install the drivers, right click on INF file, and click on install. Note that Intel® MEI driver is required to be installed before other drivers.

After the installation, there will be devices shown in the device manager as follows:

- MEI: System devices \ Intel(R) Management Engine Interface
- DAL: Software components \ Intel(R) Dynamic Application Loader Host Interface

System manufacturers can take advantage of the components in this folder 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>



4.3 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
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.

4.4 Windows* OS for Manufacturing

The Intel® MEI driver can be installed on Windows* 10 IoT Enterprise 64-bit OS, this is primarily used during manufacturing, when attempting to run Windows* based manufacturing line tools.



4.5 Firewall policy

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

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





5 Identifying Intel® CSE Software Components

Once the Intel® CSE software stack is installed on a system, the contents that kit can be identified via a single Software Package Version (SPV) marker. The Software 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® CSE Software Installer package contains a file called the 'mup.xml' which can be used to identify the SPV.

Example:

```
<fullpackageidentifier>

    <msis>
        <msi componentID="100950">
            <identifyingnumber>{1CEAC85D-2590-4760-800F-
8DE5E91F3700}</identifyingnumber>
            <upgradecode>{1CEAC85D-2590-4760-800F-
8DE5E91F3700}</upgradecode>
            <version>yyww.15.40.bbbb</version>
        </msi>
    </msis>
</fullpackageidentifier>
```

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

- yy – Build year
- ww – Build WorkWeek
- mm – Major version, set as 15 for EHL Intel® CSE 15.40
- nn – Minor version, set as 40 for EHL Intel® CSE 15.40
- bbbb – Build number

E.g. If the FW kit that was built on WW09'19 is: 15.40.0.xxxx, the SW kit will be: 1909.15.40.bbbb



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 under Microsoft* Windows* registry in the locations below:

Win64:

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

Service name for DAL or TCS 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
- TCS: SocketHeciServer.exe / Intel(R) Capability Licensing Service TCP IP Interface
- TPMProvisioningService.exe / Intel(R) TPM Provisioning Service





6 Uninstalling Intel® CSE Software

If users installed the Intel® CSE SW from the installer (the SetupME.exe under ME_SW_DCH folder), they should follow these steps in the Windows* Control Panel to uninstall the SW:

Double-click "Intel® Management Engine Components" item to uninstall the Intel® CSE 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 may be required for changes to take effect. Click **Finish** to end the uninstall.

If users installed the INF drivers manually – from the WindowsDriverPackages folder, they should uninstall them manually from the device manager

Note: Please be aware that users should not uninstall Intel® CSE SW components manually from the device manager if they have used the Intel® CSE SW installer.

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

For the extension INF driver(TCS and DAL)

1. Before uninstalling an extension driver, the user must first uninstall the base driver (Intel® MEI). Next, run PnPUtil on the extension INF.
2. Run pnputil /enum-drivers, search original name of the extension INF driver and get the published Name
3. Run pnputil /delete-driver <published name> /uninstall

