

# **Intel® Converged Security and Management Engine Software**

**Installation and Configuration Guide**

---

***Supporting Intel® CSME firmware version: 15***

***January 2021***

***Revision 1.8***



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 2<sup>nd</sup> 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 © 2017-2021 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,

- (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
0.3	<ul style="list-style-type: none"><li>• Initial Release</li></ul>	April 2018
0.5	<ul style="list-style-type: none"><li>• Updated Tiger Lake and Intel® CSME References</li></ul>	February 2019
0.7	<ul style="list-style-type: none"><li>• Updated Tiger Lake and Intel® CSME References</li></ul>	February 2019
0.8	<ul style="list-style-type: none"><li>• Update backward supporting platform</li></ul>	May 2019
1.0	<ul style="list-style-type: none"><li>• Remove IPT in –meidalonly in section 6.1.1</li><li>• Remove Intel® Online Connect (IOC)</li><li>• Remove OEM extension INF since the function has been migrated to MEI driver, update in section 3.4 and 6.1.2</li><li>• Add WIFI driver requirement for Wiman driver in section 6.1.2</li><li>• Add Note in section 6.1.2 : MEI driver folder layout change in \Installers\WindowsDriverPackages\MEI</li></ul>	November 2019
1.1	<ul style="list-style-type: none"><li>• Update copyright year to 2020</li><li>• Update section 1</li><li>• Remove section ME_SW_MSI</li><li>• Remove support of Win7 / Win 8 in section 4 and section 6</li><li>• Remove section : Installing Microsoft* .NET Framework</li><li>• Update section : How to Install</li><li>• Remove section : Advanced Configuration of Intel® Management and Security Status Application</li><li>• Update description of installer option -b in section 5.1</li></ul>	April 2020
1.2	<ul style="list-style-type: none"><li>• Update description of MEI device in section 2.1: add HECI3 for ME15</li></ul>	June 2020
1.3	<ul style="list-style-type: none"><li>• Replace Intel® iCLS with Intel® TCS</li><li>• Add description: Intel® DAL also known as JHI</li></ul>	July 2020
1.4	<ul style="list-style-type: none"><li>• Update description of MEI device in section 2.1: remove HECI3</li><li>• Add flag -wmionly in section 5.1</li></ul>	September 2020
1.5	<ul style="list-style-type: none"><li>• Change the display name of MEI device in section 5.1</li></ul>	September 2020
1.6	<ul style="list-style-type: none"><li>• Add description about installation of Intel® TCS in section 2.7</li><li>• Revise LMS, TCS and DAL description in section 3.2</li><li>• Update the table for different platform capabilities in section 3.2</li></ul>	October 2020
1.7	<ul style="list-style-type: none"><li>• Update copyright year to 2021</li><li>• Update supporting OS in section 4</li></ul>	December 2020



Revision Number	Description	Revision Date
1.8	<ul style="list-style-type: none"><li>• Add description about requirement of Intel® Wiman in section 2.8</li></ul>	January 2021



# Contents

---

1	Introduction .....	7
2	Software Components Overview .....	8
2.1	Intel® Management Engine Interface (Intel® MEI) .....	8
2.2	Serial Over LAN Driver (SOL) .....	8
2.3	Intel® Local Manageability Service (Intel® LMS) .....	8
2.4	Intel® CSME WMI Provider .....	9
2.5	Intel® Management and Security Status Application (IMSS) .....	9
2.6	Intel® Dynamic Application Loader (Intel® DAL) .....	10
2.7	Intel® Trusted Connect Service (Intel® TCS) .....	10
2.8	Intel® Wireless Management (Intel® Wiman) .....	10
3	Installer List .....	11
3.1	Intel® MEI-Only Installer .....	11
3.2	Intel® ME_SW_DCH .....	11
3.3	WindowsDriverPackages .....	12
4	System Requirements .....	13
5	Installing Intel® CSME Software Components .....	14
5.1	How to Install .....	14
5.2	IMSS .....	17
5.3	Error Codes during Installation .....	17
5.4	Windows* PE .....	18
5.5	Firewall policy .....	18
6	Identifying Intel® CSME Software Components .....	20
7	Configuring LMS .....	22
7.1	LMS Registry Configuration Parameters .....	22
7.2	Intel® PROSet/Wireless Software Adapter Switching Override .....	23
8	Uninstalling Intel® CSME Software and Drivers .....	25
9	Troubleshooting Intel® Management and Security Status Application .....	26
9.1	Error Message when Intel® Management and Security Status Application Loads .....	26
9.2	"Information Unavailable" Displayed instead of Status .....	27
9.3	Client Initiated Remote Access Connection Failure .....	27
9.4	Grayed-Out Notification Icon .....	28



# ***1 Introduction***

---

This guide describes how to install, configure and troubleshoot the Intel® Converged Security and Management Engine (Intel® CSME) 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.

**Note:** Applications and drivers are installed based on the system's specific hardware and firmware features. For example, if none of the following technologies: Intel® Active Management Technology (Intel® AMT), Intel® Small Business Advatage (Intel® SBA), or Intel® Standard Manageability exists on the system, the Intel® Management and Security Status application will not be installed.

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

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

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

### 2.2 Serial Over LAN Driver (SOL)

This driver enables the remote display of managed client's user interface through management console and emulates serial communication over standard network connection. This driver supports systems with one of the following technologies: Intel® AMT, Intel® Standard Manageability.

### 2.3 Intel® Local Manageability Service (Intel® LMS)

This service enables local applications running on Intel® AMT, Intel® SBA or Intel® Standard Manageability supported devices to use common SOAP and WS-Management functionality that is available to remote applications. It listens to the Intel® CSME IANA (Internet Assigned Names Authority) ports and routes all traffic to the firmware through the Intel® MEI.

It also provides Intel® CSME with various host operation abilities. For instance, it enables Intel® CSME technologies to write user notifications to the local host OS event log for the purpose of notifying end users of predefined events, such as when support personnel connect remotely to the platform for a healing session. Intel provides documentation on how ISVs can extract these events from the event log for use in their applications.





## 2.4 Intel® CSME WMI Provider

The Intel® CSME WMI provider enables ISV and IT administrators to perform Intel® AMT discovery and configuration operations using WMI technology. The Intel® CSME WMI provider complements the existing WS-Management API by abstracting low-level Intel® MEI operations through WMI. In addition, the provider enables the user to subscribe to LMS events and receive them via WMI events.

Following are the main functionalities implemented in the Intel® CSME WMI provider:

- Discovery of Intel® CSME and Intel® AMT related attributes, such as firmware version and provisioning state.
- Local activation operation, performed as part of Remote Configuration.
- Hardware events.

The Intel® CSME WMI provider is implemented as a DLL (MeProv.dll) and operates as part of Windows\* WMI service. The provider is installed as part of the kit.

## 2.5 Intel® Management and Security Status Application (IMSS)

This application is a Microsoft\* Windows\* application that displays information about a platform's Intel® Active Management Technology (Intel® AMT), Intel® Small Business Advantage (Intel® SBA), Intel® Standard Manageability, and Intel® Anti-Theft services. The Intel® Management and Security Status application indicates whether Intel® AMT, Intel® SBA, Intel® AT and Intel® Standard Manageability are running on the platform. The application is installed and executed as part of the Intel® CSME SW installation program.

When Intel® Management and Security Status application is running on the platform, an icon is displayed in the notification area. Clicking the icon opens the application.

By default, the icon is loaded and displayed every time Windows\* starts. The icon will be gray if the Intel® Management and Security Application Local Management Service is not running or the Intel® Management Engine Interface (Intel® MEI) driver is disabled or unavailable.

**Note:** If the Intel® Management and Security Status application starts automatically as a result of the user logging on to Windows\*, the icon will be loaded to the notification area only if Intel® AMT, Intel® SBA or Intel® Standard Manageability exists on the system. If the Intel® Management and Security Status application is started manually (via the Start menu or file manager), the icon is loaded even if none of these technologies exists.

**Note:** The information displayed in the Intel® Management and Security Status application is refreshed at pre-defined intervals. The application dynamically hides tabs that are not relevant. For example, on platforms that do not support Intel® AT, the Intel® AT tab is hidden.



## **2.6 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.

## **2.7 Intel® Trusted Connect Service (Intel® TCS)**

Also known as Intel® Capability Licensing Services (Intel® iCLS). It 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)

Intel® TCS is only installed and functional on systems which don't support On-Die Certificate Authority (ODCA).

## **2.8 Intel® Wireless Management (Intel® Wiman)**

This driver includes CSME-related flows which once were in Windows WIFI driver. This driver is placed on the WLAN device stack and will be capable of filtering OS request, especially System-state and device power state queries and transitions. In addition this driver will be capable of filtering WDI - IHV requests and notifications, filtering and diverting Tx and Rx data traffic to CSME, injecting CSME data traffic to WLAN Tx path.

Intel® Wiman driver is only present and functional on Intel® Vpro system for coffee lake platform and above.



## 3 Installer List

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

### 3.1 Intel® MEI-Only Installer

This package installs the Intel® MEI driver only.

### 3.2 Intel® ME\_SW\_DCH

This installation program installs the Intel® CSME 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® Management Engine Interface (Intel® ME Interface) driver which is DC-compliant
- Serial Over LAN (SOL) driver which is DC-compliant
- Local Manageability Service (LMS) which is DC-compliant
- Intel® CSME WMI provider
- Intel® Dynamic Application Loader (Intel® DAL) which is DC-compliant
- Intel® Trusted Connect Service (Intel® TCS) which is DC-compliant
- Intel® Wireless Management (Intel® Wiman) which is DC-compliant

**Note:** IMSS APPX will not be installed by DCH installer. For installation of IMSS APPX please refer to section 5.2.

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	Comments
Intel® AMT, Intel® SBA, Intel® Standard Manageability	Intel® MEI driver, SOL driver, Intel® DAL service, Intel® TCS, Intel® LMS, Intel® CSME WMI provider, Intel® Wiman	Intel® Wiman driver is only installed and functional on Intel® Vpro system for coffee lake platform and above.  Intel® TCS is only installed and functional on systems which don't support On-Die Certificate Authority (ODCA)



<b>If the platform includes this capability....</b>	<b>These software components are installed</b>	<b>Comments</b>
Intel® Dynamic Application Loader	Intel® MEI driver, Intel® DAL service, Intel® LMS, Intel® CSME WMI provider	The Installer provides the option to install only Intel® MEI driver and Intel® DAL service by running the installer with the following flag: setup.exe -meidalonly. LMS is installed along with WMI provider and only used by WMI provider.
PAVP	Intel® MEI driver, Intel® LMS, Intel® CSME WMI provider	LMS is installed along with WMI provider and only used by WMI provider
None of the above	Intel® MEI driver, Intel® TCS	Intel® TCS is only installed and functional on systems which don't support On-Die Certificate Authority (ODCA)

### 3.3 WindowsDriverPackages

This package includes the drivers as UWD INF installer and IMSS APPX package.

- MEI: heci.inf in Installers\WindowsDriverPackages\MEI
- SOL: mesrl.inf in Installers\WindowsDriverPackages\SOL (only available in corporate sku)
- TCS: iclsClient.inf in Installers\WindowsDriverPackages\ICLS
- LMS: LMS.inf in Installers\WindowsDriverPackages\LMS (only available in corporate sku)
- DAL: DAL.inf in Installers\WindowsDriverPackages\JHI\win10
- IMSS APPX: Installers\WindowsDriverPackages\IMSS (only available in corporate sku)
- Wiman driver: Installers\WindowsDriverPackages\WiMan (only available in corporate sku)
- Wiman extension: Installers\WindowsDriverPackages\wiman\_wlan\_extension (only available in corporate sku)

## §



## **4      *System Requirements***

---

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

- Windows\* 10 / Windows Server\* 2019.
- Microsoft\* .NET Framework: version 4.6.2 or above, required if the Intel® Management and Security Status application is installed on the platform.
- Microsoft Visual C++ 2015 Redistributable: version 14.0.26905.0 or above, required if the Intel® Management and Security Status application is installed on the platform.





## 5 Installing Intel® CSME Software Components

---

### 5.1 How to Install

The driver for MEI , SOL, LMS, DAL , TCS and Wiman 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 the **Installers\WindowsDriverPackages** 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>

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

Wiman Extension is required to be installed along with installation of wiman driver.

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

MEI: System devices \ Intel(R) Management Engine Interface #1

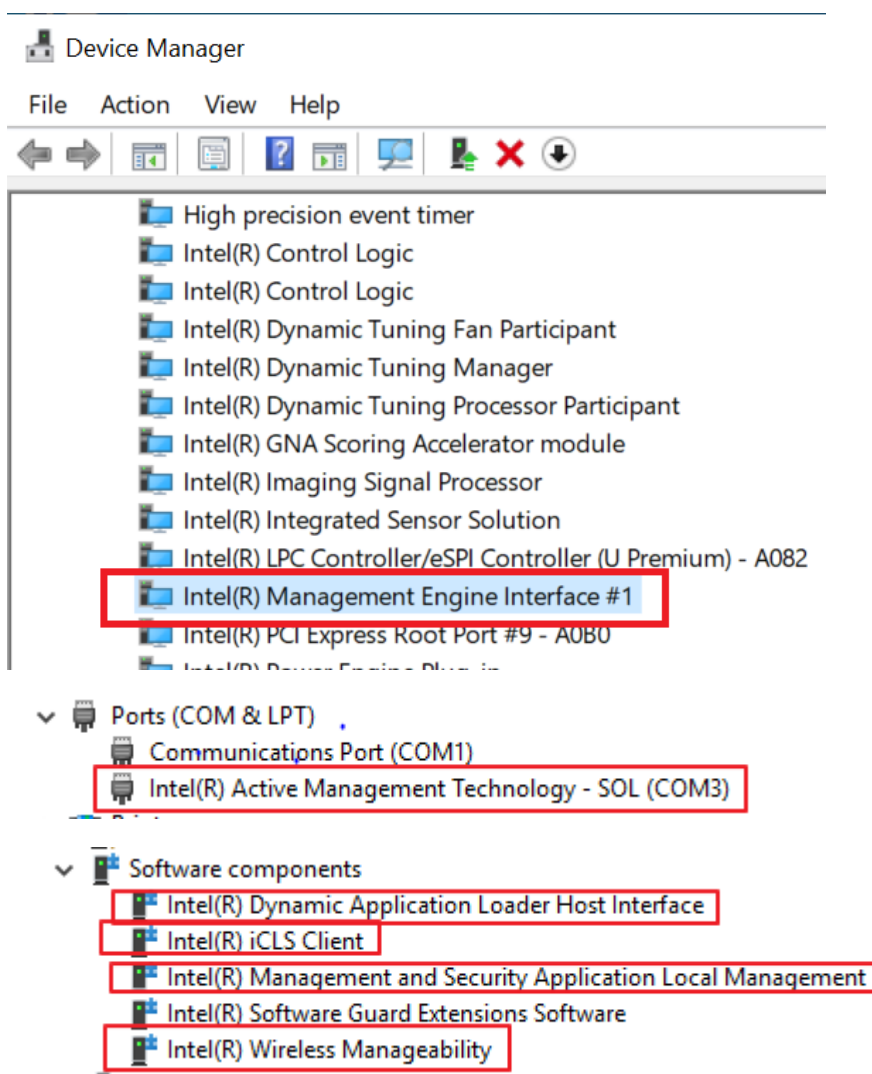
SOL: Ports(COM & LPT) \ Intel(R) Active Management Technology - SOL

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

LMS: Software components \ Intel(R) Management and Security Application Local Management

TCS: Software components \ Intel(R) iCLS Client

Wiman : Software components \ Intel(R) Wireless Manageability



User may use installer **SetupME.exe** located in the firmware kit in the **Installers\ME\_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 option for specific installing configuration, under command line mode execute setupME.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.

-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.

**Warning** : User who chooses to use -p flag must make sure the destination directory is a secure folder (write access by admin). Otherwise it can lead to a security issue.

-report <path>

Changes the default log path.

-s

Does not display any setup dialogs (silent install).

-ver

Displays driver versions.

-drvonly

Installs drivers only.

-meidonly

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

-preinst

Installs all drivers even if hardware is not present.

-tcs

Installs only TCS.

-nowiman

Does not install Intel® Wireless Management

-wmionly

Install and register only WMI Provider.

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





## 5.2 IMSS

Note: IMSS is for AMT system only, it is not required to be installed on NON AMT system.

User may download IMSS from Microsoft store.

IMSS APPX for pre-install is located in the firmware kit in the **Installers\WindowsDriverPackages\IMSS** folder.

DISM is required to install IMSS APPX. Refer to <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/preinstall-apps-using-dism> for more detail.

For the OS without Microsoft Visual C++ 2015 Redistributable 14.0.26905.0 or later(e.g. fresh OS or pre-install OS without windows update), the DependencyPackagePath is required for installing Microsoft Visual C++ 2015 Redistributable along with IMSS APPX

the example command for pre-install OS as below:

```
Dism /Image:c:\test\offline /Add-ProvisionedAppxPackage /PackagePath:<pre-install kit Folder Path>\<IMSS APPX appxbundle file> /LicensePath:<pre-install kit Folder Path>\<IMSS APPX License xml file> /DependencyPackagePath: :<pre-install kit Folder Path>\Microsoft.VCLibs_xxx_<OS sku>_xxx.appx /region=all
```

where c:\test\offline is the folder where you mounted the WIM image

<pre-install kit Folder Path> is the folder where the package is extracted to

the example DISM command for running OS as below:

```
Dism /online /Add-ProvisionedAppxPackage /PackagePath:<pre-install kit Folder Path>\<IMSS APPX appxbundle file> /LicensePath:<pre-install kit Folder Path>\<IMSS APPX License xml file> /DependencyPackagePath: :<pre-install kit Folder Path>\Microsoft.VCLibs_xxx_<OS sku>_xxx.appx /region=all
```

## 5.3 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	<p>One of:</p> <ul style="list-style-type: none"> <li>The user canceled the operation</li> <li>Setup was run silently but a downgrade was detected and the -overwrite switch was not used.</li> </ul>



Error code	Error String	Description
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"><li>• Not admin</li><li>• No device matches</li><li>• OS requirement not met</li><li>• .NET requirement not met</li></ul>
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.

## 5.4 Windows\* PE

The Intel® MEI 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® MEI 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>

## 5.5 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

**S**



## 6 Identifying Intel® CSME Software Components

---

Once the Intel® CSME software stack is installed on a system, the contents 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® CSME 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>
  <msis>
    <msi componentID="100950">
      <identifyingnumber>{1CEAC85D-2590-4760-800F-
8DE5E91F3700}</identifyingnumber>
      <upgradecode>{1CEAC85D-2590-4760-800F-8DE5E91F3700}</upgradecode>

      <version>yyww.mm.nn.bbbb</version>
    </msi>
  </msis>
</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

E.g. If the FW kit that was built on WW35'20 is: 15.0.0.xxxx, the SW kit will be: 2035.15.0.bbbb

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

LMS: LMS / Intel(R) Management and Security Application Local Management Service

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





## 7 Configuring LMS

---

LMS is able to write user notifications to the local host OS event log for the purpose of notifying end users of predefined events, such as when critical System Defense policies are applied by the Intel® CSME firmware. LMS also has additional functionalities, such as synchronizing the network configuration information between the host and the firmware. Intel provides documentation on how the ISV can extract these events from the event log for use in their application.

LMS.exe is installed along with the other software components. Note the following installation circumstances:

### 7.1 LMS Registry Configuration Parameters

User can add the following registry keys under **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LMS\IntelAMTUNS**:

**Note:** The following keys are not mandatory and LMS will function as required without their existence. All changes to registry keys are noted at LMS startup only. To force the changes to be noted, restart LMS.

**AllowFlashUpdate:** Allows LMS to invoke Partial FW Updates. This is a DWORD Value. Setting value to 0 will prohibit LMS from invoking Partial FW Update, while setting value to 1 allows Partial FW Update by LMS. Default behavior (i.e. no value) is Partial FW Update allowed.

**Note:** Partial Firmware Update is a feature new from Intel® ME 8 that allows update of specific sections of Intel ME, without requiring a system reset.

**Note:** Disabling Partial FW Update will eliminate the user's ability to change the user consent language and to replace the wireless adapter type without affecting Intel® AMT functionality over wireless LAN.

**PartialFWUIImagePath:** A custom path to the update partitions file, including the filename (using absolute or relative path), e.g. **C:\<path>\pfwupdateimg.bin**. Default is the LMS.exe path.

Note :The path can't point to a network shared folder. It must point to a local folder.

You can configure the following parameters in the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Intel\IntelAMTUNS\ConfigData** registry key:

The following Registry keys could be added for configuring which events will be shown in Event Log. This is a DWORD Value. Setting value to 0 will prevent the event from appearing, while setting value to 1 will cause the relevant event to appear. Note that the settings only take effect when LMS is (re)started.



Registry Key	Event Log event
NETWORK_TRAFFIC_TX_CEASED	Security policy invoked. Some or all network traffic (TX) was stopped
NETWORK_CONNECTIVITY_TX_REDUCED	Security policy invoked. TX Network connectivity was reduced
NETWORK_TRAFFIC_RX_CEASED	Security policy invoked. Some or all network traffic (RX) was stopped
NETWORK_CONNECTIVITY_RX_REDUCED	Security policy invoked. RX Network connectivity was reduced
WLAN_WIRELESS_PROFILE_STATE_CHANGED	WLAN Wireless Profile sync enablement state changed WLAN interface
WLAN_SESSION_ESTABLISHED	Control preference for WLAN interface assigned to Intel(R) Converged Security and Management Engine. Intel(R) CSME will take control of WLAN interface when it is able
WLAN_SESSION_ENDED	Preference for WLAN interface assigned to operating system. Operating system will take control of WLAN interface when it is able
REMOTE_SOL_STARTED	A remote Serial Over LAN session was established
REMOTE_SOL_ENDED	Remote Serial Over LAN session finished. User control was restored
REMOTE_IDER_STARTED	A remote IDE-Redirection session was established. For platforms supporting USB-Redirection instead of IDE-Redirection, remote USB-Redirection session was established.
REMOTE_IDER_ENDED	Remote IDE-Redirection session finished. User control was restored. For platforms supporting USB-Redirection instead of IDE-Redirection, Remote USB-Redirection session finished. User control was restored

## 7.2 Intel® PROSet/Wireless Software Adapter Switching Override

The Intel® CSME firmware configuration of the Intel® PROSet/Wireless Software Adapter Switching override is disabled by default. However, on systems without Intel® LAN support (as defined by hardware configuration settings), it is enabled by default. When enabled, and when Adapter Switching is active (as notified by Intel® PROSet/Wireless Software to Intel® CSME firmware), the Intel® CSME firmware will configure the WLAN to override the Host software RF-Kill and establish its own wireless connection when wireless Intel® AMT is configured. When Adapter Switching



is inactive or if the Host WLAN driver is healthy, the Intel® CSME firmware will not configure the WLAN to override the Host software RF-Kill, nor establish its own wireless connection.

Users wishing to override the default setting in Intel® CSME firmware may add the following registry key under:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Intel\IntelAMTUNS**

The Intel® PROSet/Wireless Software Adapter Switching override feature in Intel® CSME firmware is available only on systems with Intel® AMT 11.6 or later.







## 8 *Uninstalling Intel® CSME Software and Drivers*

---

If you are installing CSME SW using any installer – ME\_SW\_MSI or ME\_SW\_DCH, uninstall the software via the Windows Control Panel:

- Double-click Intel® Management Engine Components to uninstall the Intel® CSME 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® CSME software, the uninstallation may fail. This has been noted, for example, when uninstalling Microsoft\* Visual C.

**Note:** Don't manually uninstall ME SW components via device manager if you are installing CSME SW using installer



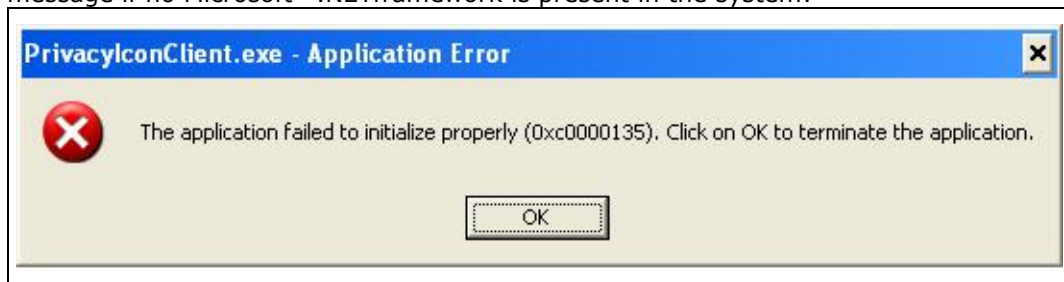
## **9     *Troubleshooting Intel® Management and Security Status Application***

---

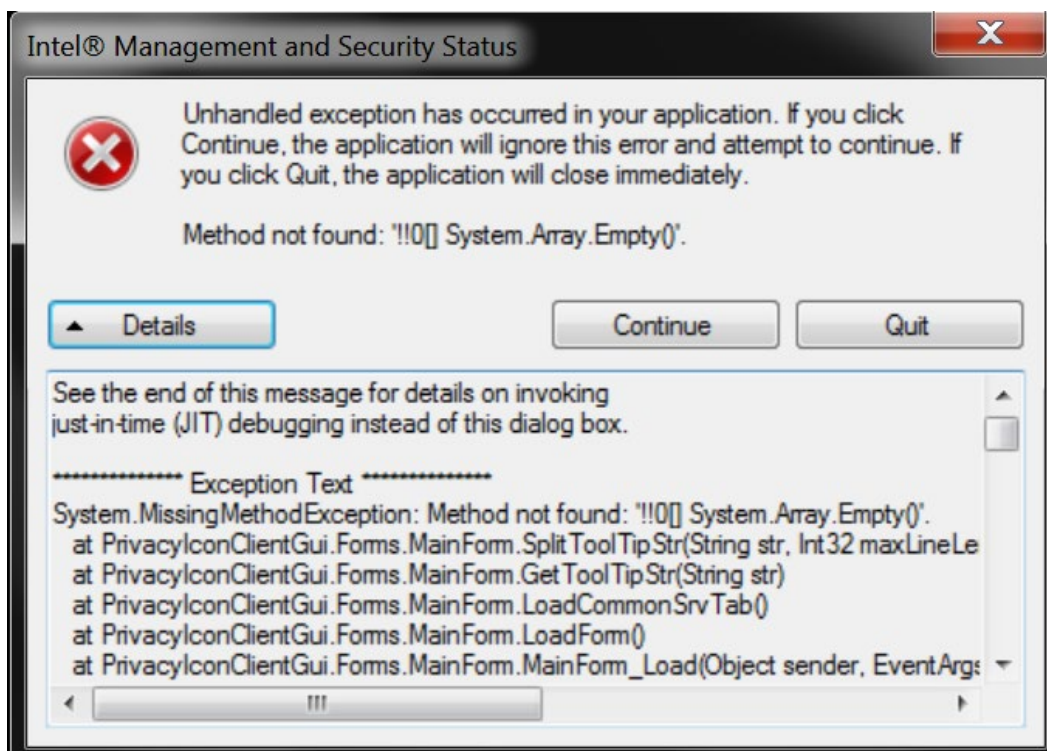
### **9.1     Error Message when Intel® Management and Security Status Application Loads**

Microsoft\* .NETapplications fail when executed in an environment that has no Microsoft\* .NETframework installed. Microsoft\* does not provide a safeguard mechanism in such conditions.

The Intel® Management and Security Status application will display the following error message if no Microsoft\* .NETframework is present in the system:



The Intel® Management and Security Status application will display the following error message if no Microsoft\* .NETframework version is not 4.6.2 or above:



If these happen, install Microsoft\* .NET Framework version 4.6.2 or above and then re-open the application.

## 9.2 “Information Unavailable” Displayed instead of Status

The **General** tab provides basic information about the Intel® AMT, Intel® SBA, Intel® Standard Manageability, and Intel® Anti-Theft Technology status and events.

The Intel® Management and Security Status icon relies on the Local Management Service, which is installed together with the Intel® Management and Security Status application, to obtain information about the status of the resident technologies. Make sure that:

1. The Local Manageability Service (LMS) is running and starts automatically on Windows\* startup. If LMS is not installed, reinstall the software components.
2. The Intel® MEI driver is installed, enabled and functioning properly. Review the Bring-Up Guide document for more information concerning this driver.

## 9.3 Client Initiated Remote Access Connection Failure

Failure to connect to the Information Technology network can be caused by the following:




1. The Local Management Service is not running. It can be started through the Services pane in the Computer Management window. If it is not installed, reinstall the software components.
2. The network cable is disconnected, or the network connection is not configured properly.

If the actions above do not resolve the problem, it is recommended to contact your Information Technology department.

## 9.4 Grayed-Out Notification Icon

Whenever either Intel® AMT, Intel® SBA or Intel® Standard Manageability is enabled, Intel® Management and Security Status icon is loaded into the notification area when Windows\* starts. It can also be started by clicking **Start> All Programs\Intel\Intel® Management and Security Status\ Intel® Management and Security Status**.

While the Intel® Management and Security Status application is running, the Intel® Management and Security Status icon is visible in the notification area.  This icon will appear blue if any one of the aforementioned technologies is enabled on the computer. In any other case, the icon will appear gray.

**Note:** The icon will also be gray if the LMS service is not running or the Intel® MEI driver is disabled or unavailable.