

Intel® Converged Security and Management Engine Software

Installation and Configuration Guide

Supporting Intel® CSME firmware version: 11.8, 12, 13, 14, 15, 16, 16.1, 18, 19, 20

June 2023

Revision 1.3



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 © 2023 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	<ul style="list-style-type: none">initial release	August 2022
1.1	<ul style="list-style-type: none">Add requirement of Intel® SOL LMS Extension for Intel® LMSUpdate description in section 10.1Update description for uninstallationUpdate Intel® DAL: deprecated after Meteor Lake platform running ME18.	October 2022
1.2	<ul style="list-style-type: none">Update copyright year to 2023Remove support of Windows* 7 / Windows* 8 / Windows* 8.1 / Windows Server* 2008 R2 64-bit versions	January 2023
1.3	<ul style="list-style-type: none">add support of pre-PV systemsadd the installation steps for the test version of Intel® MSS	June 2023



Contents

1	Introduction	7
2	Software Components Overview	8
2.1	Intel® Management Engine Interface (Intel® MEI) Driver	8
2.2	Serial Over LAN (SOL) Driver	8
2.3	Intel® Local Manageability Service (Intel® LMS)	8
2.4	Intel® CSME WMI Provider	9
2.5	Intel® Management and Security Status (Intel® MSS) Application	9
2.6	Intel® Dynamic Application Loader (Intel® DAL)	10
2.7	Intel® Trusted Connect Service (Intel® TCS)	10
2.8	Intel® Wireless Manageability (Wiman) driver	10
3	Installer List	11
3.1	Legacy	11
3.2	Main_DCH	12
3.3	Drivers	12
4	System Requirements	14
5	Installing Intel® CSME Software Components	15
5.1	How to Install	15
5.1.1	Windows* 10 RS2 and before	15
5.1.2	Windows* 10 RS3 and beyond	16
5.1.3	Intel® MSS	20
5.2	Error Codes during Installation	22
5.3	Windows* PE	23
5.4	Firewall policy	23
6	Identifying Intel® CSME Software Components	24
7	Advanced Configuration of Intel® Management and Security Status Application	26
7.1	General Tab Logo	26
7.2	Load on Start-Up Options	26
7.3	Load in Disabled State	27
7.4	Show Notification Option	27
7.5	Disabling the Intel® AT Tab	27
7.6	"Click Here for More Details" Link	27
8	Configuring Intel® LMS	29
8.1	LMS Registry Configuration Parameters	29
8.2	Intel® PROSet/Wireless Software Adapter Switching Override	30
9	Uninstalling Intel® CSME Software and Drivers	32
10	Troubleshooting	33
10.1	Error Message when Intel® Management and Security Status Application Loads	33
10.2	"Information Unavailable" Displayed instead of Status	34
10.3	Client Initiated Remote Access Connection Failure	34



10.4	Grayed-Out Notification Icon	34
10.5	Redundant software components in device manager	34



1 Introduction

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

This guide provides comprehensive information about various systems, including both existing sustaining platforms and new platforms that have not yet undergone production validation (PV).





2 **Software Components Overview**

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

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

This host 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 driver.

2.2 **Serial Over LAN (SOL) Driver**

This host 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.

After Windows* 10 RS3 or later with Intel® MEI driver 2124.100.0.1096 or newer, Intel® SOL LMS Extension is required along with Intel® LMS. Intel® LMS will be functional only if Intel® SOL device exists and Intel® SOL LMS extension INF is installed.



2.4 Intel® CSME WMI Provider

This provider enables ISV and IT administrators to perform Intel® AMT discovery and configuration operations using WMI technology. The 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 Intel® LMS events and receives them via WMI events.

Following are the main functionalities implemented in the 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 provider is implemented as a DLL (MeProv.dll) and operates as part of Windows* WMI service.

The provider has switched to INF installation support. Refer to section 5 for more detail of installing method.

2.5 Intel® Management and Security Status (Intel® MSS) Application

This 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 (Intel® AT) services. The application indicates whether Intel® AMT, Intel® SBA, Intel® AT and Intel® Standard Manageability are running on the platform.

When the 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 Intel® LMS is not running or Intel® MEI driver is disabled or unavailable.

If the application starts automatically because 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 application starts manually (via the Start menu or file manager), the icon is loaded even if none of these technologies exists.

The information displayed in the 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 Intel® JHI. This is a service which exposes the host interface to usage of the Intel® DAL 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® DAL capable.

This service is deprecated after Meteor Lake platform running ME18.

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)
- License distribution for Extended Platform Service (EPS) (only available in some platforms)

Depending on platform type detected by Intel® MEI the appropriate SW component is enumerated:

- Support TCB-R Only (Component – SWC\VENDOR_INTEL_COMPONENT_ICLSCLIENT) and run TCB-R Transactions.
- Support EPS Only (Component SWC\VENDOR_INTEL_COMPONENT_ICLSCLIENT_ES_ONLY) and run EPS Transaction.
- Support both TCB-R & EPS (both components should be installed)

Detail refers to TA#[734356](#).

2.8 Intel® Wireless Manageability (Wiman) driver

This driver includes CSME-related flows which once were in Windows* WIFI driver. This driver is capable of filtering OS request, especially System-state and device power state queries and transitions. In addition, this driver is 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.

Wiman is only present and functional on Corporate sku FW image for Coffee Lake platform and above.

To comply with Microsoft* DC requirement, Wiman extension INF is required to be installed along with installation of Wiman driver. Wiman is functional only if Wiman extension INF is installed.



3 *Installer List*

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

3.1 *Legacy*

The installation program in this folder 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.

Note: This installer only supports for sustaining platforms including Intel® Coffee Lake and older platforms on Windows* 10.

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

- Intel® Management Engine Interface (Intel® MEI) driver
- Serial Over LAN (SOL) driver
- Intel® Local Manageability Service (Intel® LMS)
- Intel® CSME WMI provider
- Intel® Management and Security Status application (Intel® MSS)
- Intel® Dynamic Application Loader (Intel® DAL)
- Intel® Trusted Connect Service (Intel® TCS)
- Intel® Wireless Manageability (Wiman) 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® AMT, Intel® SBA, Intel® Standard Manageability	Intel® MEI driver, SOL driver, Intel® TCS, Intel® LMS, Intel® CSME WMI provider, Wiman ⁽¹⁾ driver, Intel® DAL ⁽²⁾
Intel® Dynamic Application Loader	Intel® MEI driver, Intel® DAL ⁽²⁾
None of the above	Intel® MEI driver, Intel® TCS, Intel® CSME WMI provider

- (1) Wiman is only installed and functional on corporate sku FW image for Coffee Lake platform and above.
- (2) 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.



3.2 Main_DCH

The installation program in this folder installs the Intel® CSME software components which are compliant with Microsoft DC requirement. The installation program 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® MEI) driver
- Serial Over LAN (SOL) driver
- Intel® Local Manageability Service (Intel® LMS)
- Intel® CSME WMI provider
- Intel® Dynamic Application Loader (Intel® DAL)
- Intel® Trusted Connect Service (Intel® TCS)
- Intel® Wireless Manageability (Wiman) driver

Note: Intel® MSS application is not installed by this installer. For installation of Intel® MSS please refer to section 5.1.3.

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® AMT, Intel® SBA, Intel® Standard Manageability	Intel® MEI driver, SOL driver, Intel® TCS ⁽¹⁾ , Intel® LMS, Intel® CSME WMI provider, Wiman ⁽²⁾ driver, Intel® DAL ⁽³⁾
Intel® Dynamic Application Loader	Intel® MEI driver, Intel® DAL ⁽³⁾
None of the above	Intel® MEI driver, Intel® TCS ⁽¹⁾ , Intel® CSME WMI provider

- (1) Depending on platform type, Intel® TCS may be not installed by Intel® CSME SW installer. Detail refers to TA#[734356](#).
- (2) Wiman is only installed and functional on corporate sku FW image for Coffee Lake platform and above.
- (3) 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. Note that Intel® DAL is deprecated after Meteor Lake platform running ME18.

3.3 Drivers

This package includes the INF installers for Intel® CSME software components and Intel® MSS APPX package.

- Intel® MEI: heci.inf in Drivers\MEI\



- Intel® SOL: mesrl.inf in Drivers\SOL (only available in corporate sku)
- Intel® TCS: iclsClient.inf in Drivers\ICLS
- Intel® LMS: LMS.inf in Drivers\LMS (only available in corporate sku)
- Intel® DAL: DAL.inf in Drivers\JHI\win10
- Intel® MSS APPX: Drivers\IMSS (only available in corporate sku)
- Wiman driver: Drivers\WiMan (only available in corporate sku)
- Wiman extension: Drivers\wiman_wlan_extension (only available in corporate sku)
- Intel® CSME WMI Provider: MEWMIProv.inf in Drivers\WMIPProvider
- Intel® MSS HSA extension: ImssHsaExtension.inf in Drivers\IMSS_HSA_EXTENSION (only available in corporate sku)
- Intel® SOL LMS Extension: SOLLMSExtension.inf in SW\Drivers\SOL_LMS_Extension (only available in corporate sku)

Note: the driver INF in the SW kit for pre-PV platforms are Microsoft pre-production signed drivers. The prerequisites and provisioning Steps for systems that require enabling Secure Boot can be found at the following link:
<https://learn.microsoft.com/en-us/windows-hardware/drivers/install/preproduction-driver-signing-and-install>



4 *System Requirements*

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

- Windows* 10 / Windows* 11 / Windows Server* 2012 64 bit versions / Windows Server* 2012 R2 64 bit versions / Windows Server* 2016 64 bit versions / Windows Server* 2019.
- Microsoft* .NET Framework: version 4.8 or above.
- Microsoft* Visual C++ 2015 Redistributable: released with Intel® MSS APPX and required for Intel® MSS application.





5 Installing Intel® CSME Software Components

5.1 How to Install

5.1.1 Windows* 10 RS2 and before

For the systems running Windows* 10 RS2 or older, use the installer **SetupME.exe** in **Legacy** folder.

Note: The components installed are subject to the 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 installer has command line options 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.

Note: with this parameter, the installer will install Intel® MSS anyway. If Intel® MSS is not required, please add -noimss to skip it.

-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.
- noIMSS
Does not install Intel® MSS.
- meidalonly
Installs Intel® Management Engine Interface, Intel® Dynamic Application Loader only.
- preinst
Installs all drivers even if hardware is not present.
- tcs
Installs only Intel® TCS.
- skipstartmenu
Does not add the Intel® MSS shortcut to the Start menu
- nowiman
Does not install Wireless Manageability
- wmionly
Install and register only Intel® CSME WMI Provider.

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

5.1.2 Windows* 10 RS3 and beyond

To comply with Microsoft DC requirement, it is recommended to use the INF installers in **Drivers** folder.

Users or system manufacturers should follow the list in section 3.3 to install required software components.

To install them, right click on INF file, and click on install.

System manufacturers can do offline injection via DISM. More information about DISM can be found at:

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



Intel® MEI driver and SOL driver are recommended to be installed before other drivers/components.

Wiman Extension is required along with Wiman driver. Wiman will be functional only if Wiman extension INF is installed.

SOL LMS Extension is required along with SOL device and Intel® LMS. Intel® LMS will be functional only if SOL device exists and SOL LMS extension INF is installed.

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

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

Note: The MEI driver INF in Drivers\MEI\win10 is signed for Windows* 10 RS5 and later, while the MEI driver INF in Drivers\MEI\win8 is signed for windows* 8.1 and later. Refer to DOC#618680 in RDC for more detail.

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

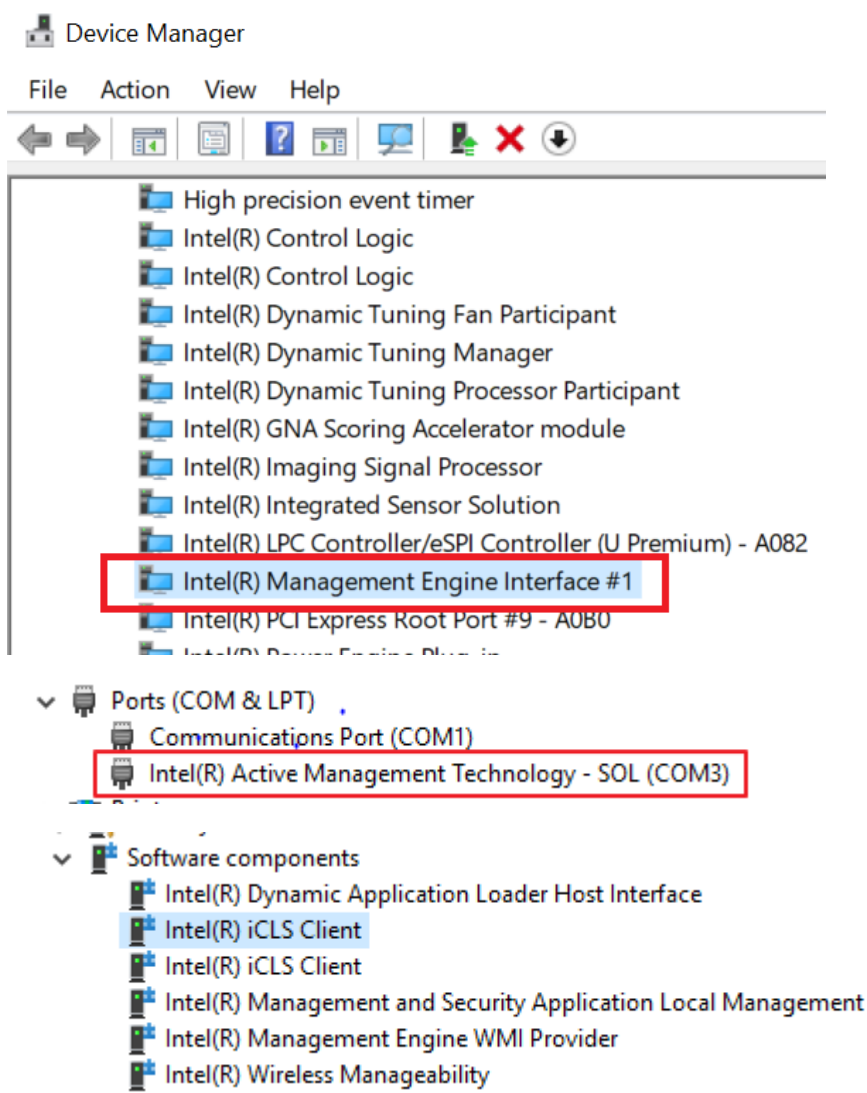
Intel® DAL: Software components \ Intel(R) Dynamic Application Loader Host Interface

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

Intel® TCS: Software components \ Intel(R) iCLS Client

Wiman: Software components \ Intel(R) Wireless Manageability

Intel® CSME WMI Provider: Software components \ Intel(R) Management Engine WMI Provider



User may use installer SetupME.exe in the **Main_DCH** folder to facilitate the installation:

- 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.

Note: The installer SetupME.exe may not be forward compatible with update of Windows* OS and may fail due to new update of Windows patches. Consult Intel for more detail and issues.

The installer SetupME.exe has command line options 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 Intel® TCS.

-nowiman

Does not install Intel® Wireless Manageability

-wmionly

Install and register only Intel® CSME WMI Provider.



To get the debug log for the installer, users can execute the installation using the command line with the parameter "-report <path>". The installation logs can be found at <user folder>\Intel\Logs.










5.1.3 Intel® MSS

Intel® MSS is for Intel® AMT systems only, it is not required to be installed on NON Intel® AMT systems.

User may download and install Intel® MSS from Microsoft* store, or install IMSS_HSA_EXTENSION INF, which will pull Intel® MSS from Microsoft* store and install Intel® MSS in the background when SOL device and internet connection exist.

Intel® MSS APPX installation package is for pre-install, and the installation package is in the Drivers\IMSS folder.

For pre-PV platforms, there may be a test version of IMSS installation package which has postfix _Test added in the folder name and the folder structure looks like:

	Add-AppDevPackage.resources	12
	Dependencies	12
	TelemetryDependencies	12
	Add-AppDevPackage.ps1	12
	Install.ps1	12
	PrivacyIconClientPackagingProject_2250.0.14.0_x64.appxsym	12
	PrivacyIconClientPackagingProject_2250.0.14.0_x86.appxsym	12
	PrivacyIconClientPackagingProject_2250.0.14.0_x86_x64.appxbundle	12
	PrivacyIconClientPackagingProject_2250.0.14.0_x86_x64.cer	12

To install test version of Intel® MSS, follow the steps as below:

1.allow power shell script execute without signing

PowerShell

Apply the following settings to execute PowerShell scripts.

☒ Change execution policy to allow local PowerShell scripts to run without signing. Require signing for remote scripts. [Show settings](#)

Apply

2.execute PrivacyIconClientPackagingProject_xxx.cer



3.run install.ps1 with power shell. During execution, The following window will be pop up. Turn on developer mode, and continue with power shell by choosing [Y]Yes.

For developers

These settings are intended for development use only.

[Learn more](#)

Developer Mode

Install apps from any source, including loose files.

☒ On

Device Portal

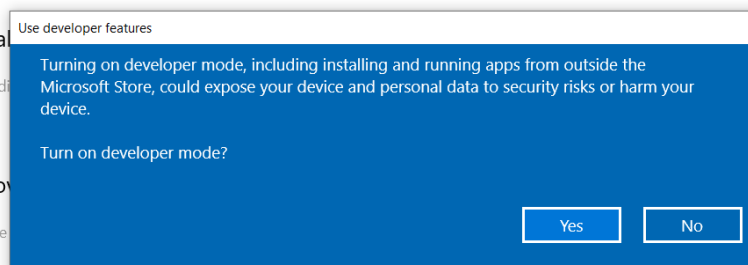
Turn on remote debugging

☐ Off

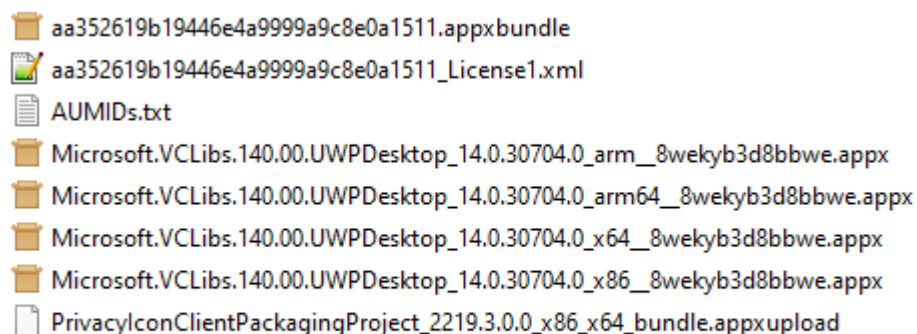
Device discovery

Make your device discoverable

☐ Off



For MSFT signed version of Intel® MSS installation package, the folder structure looks like:



System manufacturers may use DISM to install MSFT signed version of Intel® MSS APPX. Refer to <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/preinstall-apps-using-dism> for more detail.

Microsoft Visual C++ 2015 Redistributable is released with Intel® MSS APPX and may be installed with Intel® MSS APPX using DISM.

the example DISM command for pre-install OS as below:

```
Dism /Image:c:\test\offline /Add-ProvisionedAppxPackage /PackagePath:<pre-install kit Folder Path>\< Intel® MSS APPX appxbundle file> /LicensePath:<pre-install kit
```



Folder Path>\< Intel® MSS APPX License xml file> /DependencyPackagePath: :<pre-install kit Folder Path>\Microsoft.VCLibs_xxx_<OS sku>_xxx.appx

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>\< Intel® MSS APPX appxbundle file> /LicensePath:<pre-install kit Folder Path>\< Intel® MSS APPX License xml file> /DependencyPackagePath: :<pre-install kit Folder Path>\Microsoft.VCLibs_xxx_<OS sku>_xxx.appx /region=all
```

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 operationSetup 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 adminNo device matchesOS 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® 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>

5.4 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® CSME Software Components

Once the Intel® CSME software stack is installed by the installer SetupME.exe, the contents of the 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.BR.BUILD.PFU</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.BR.BUILD.PFU where:

- YY – Build year
- WW – Build WorkWeek
- BR: branch indication number
- BUILD: 4 digits at most
- PFU: indicate PFU was modified. Increased integer.

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

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

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

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



TPMProvisioningService.exe / Intel(R) TPM Provisioning Service

If Intel® LMS, Intel® DAL or Intel® TCS are installed via installer SetupME.exe in Legacy folder, the components file location is

C:\Program Files (x86)\Intel\Intel(R) Management Engine Components.





7 Advanced Configuration of Intel® Management and Security Status Application

Note: This section is only for legacy MSS and not applicable for Intel® MSS APPX. please refer to Intel® MSS user guide for Intel® MSS APPX.

7.1 General Tab Logo

The logo displayed in the general tab can be substituted in order to match the visual identity of the computer supplier. For example, a particular manufacturer may prefer to display the company's logo.

To change the logo, add a bitmap file called **oemlogo.bmp** to the Intel® Management and Security Status application folder (located at **Program Files\ Intel\ Intel® Management Engine Components\IMSS**, or at **Program Files (x86)\ Intel\ Intel® Management Engine Components\IMSS** for 64-bit operating systems). The default logo will appear if the bitmap file is invalid or missing.

Note: The bitmap dimensions should be 62 (width) by 48 (height) and size of file no larger than 8 KB. If the image file shall exceed 8 KB, the logo may not be well visible. If the bitmap dimensions are smaller than 62x48, the logo image will be centered into its designated area.

7.2 Load on Start-Up Options

By default, Intel® Management and Security Status application loads on Windows* startup. A user can uncheck the **Intel® Management and Security Status will be available next time I log on to Windows*** check box to prevent it from happening.

To disable application load on startup for all users, add a value named **AppAutoStartDefaultVal** with value **0** to the following registry location **HKLM\SOFTWARE\Intel\PIcon\Setting**.

To return to the default behavior, change the data of the same value to **1**, or delete the value.

Note: The application will still be available from the Start Menu, regardless of the value in this registry key.

Note: The user selection overrides system values in the registry key.



7.3 Load in Disabled State

By default, Intel® Management and Security Status application will not load in case all Intel CSME technologies are permanently disabled or not present on the platform.

To enable application load in “disabled state” add a value named **AutoStartInDisabled** with value **1** to the following registry location **HKLM\SOFTWARE\Intel\PIcon\Setting**.

To return to the default behavior, change the data of the same value to **0**, or delete the value.

Note: The application will still be available from the Start Menu, regardless of the value in this registry key.

Note: The user selection overrides system values in the registry key. Meaning that in case the user will uncheck the Intel® Management and Security Status will be available next time I log on to Windows check box the application will not load in “disabled state”.

7.4 Show Notification Option

By default, Enable User Notification check box in the Intel® Management and Security Status application – General tab is checked.

To change the default behavior, add a value named **ShowUserNotification** with value **0** to the following registry location **HKEY_CURRENT_USER\SOFTWARE\Intel\PIcon\Setting**.

To return to the default behavior, change the data of the same value to **1**, or delete the value. The user selection overrides system values in the registry key.

7.5 Disabling the Intel® AT Tab

By default, the Intel® AT tab is displayed if the platform supports Intel® AT. To disable Intel® AT tab in Intel® Management and Security Status application, assign the value **1** to the **DisableAT** registry key in the **HKLM\SOFTWARE\Intel\PIcon\Setting** registry directory. A DWORD key should be created upon missing such key. Applying this setting will hide the Intel® AT tab starting at the next time the application starts.

7.6 “Click Here for More Details” Link

By default, clicking the “**Click here for more details**” inside the **Learn More** dialog will direct the user to the official Intel Corporation - Privacy website.

The link pointed to by the “**Click here for more details**” text inside the **Learn more** dialog can be modified to link to a page of the manufacturer's choice.



Advanced Configuration of Intel® Management and Security Status Application

To perform this change, add a value named **HelpURL** with the URL of your choice (e.g. <http://www.intel.com/>) to the **HKLM\SOFTWARE\Intel\PIcon\Setting** key in the registry. To return to the default behavior, delete the value.





8 Configuring Intel® LMS

Intel® 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. Intel® 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:

8.1 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 Intel® LMS will function as required without their existence. All changes to registry keys are noted at Intel® LMS startup only. To force the changes to be noted, restart Intel® LMS.

AllowFlashUpdate: Allows Intel® LMS to invoke Partial FW Updates. This is a DWORD Value. Setting value to 0 will prohibit Intel® 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 Intel® 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

8.2 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

OverrideProsetAdapterSwitching: This registry key is relevant for Windows* 7 only. Adding OverrideProsetAdapterSwitching key as a DWORD and setting the value to 0 will disable the Intel® PROSet/Wireless Software Adapter Switching override feature in the Intel® CSME firmware. Setting the value to 1 will enable the Intel® PROSet/Wireless Software Adapter Switching override feature in the Intel® CSME firmware.

Adapter Switching notifications to Intel® CSME firmware from Intel® PROSet/Wireless Software are only available systems running Windows* 7. For more information about the Adapter Switching feature, consult the Intel® PROSet/Wireless Software user guide.

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.





9 Uninstalling Intel® CSME Software and Drivers

If you are installing Intel® CSME software using any installer – in Legacy or Main_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 may be required for changes to take effect. Click **Finish** to end the uninstall.

If you are installing the inf drivers manually – from the Drivers folder, you should uninstall them manually:

- Right click the device name in device manger and choose **uninstall**
- Or use pnputil command to 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 Intel® CSME software components via device manager if you installed them using installer SetupME.exe.

Installation of Wiman includes Wiman driver and Wiman_extension. Therefore, when uninstalling Wiman manually from device manager it will uninstall only the WiMan driver. User then need to uninstall manually (with pnputil command) the Wiman_extension that is shown in device manager as "Generic Software Component".

There are 3 different Wiman's (WiMan-WiFi for Canon Lake/Coffee Lake/Whisky Lake, WiManH for Comet Lake/Tiger Lake, WiManHu for Alder Lake and above). When user uses the NIC that is relevant for Canon Lake/Coffee Lake/Whisky Lake on upper platform version he will get the WiMan-WiFi as hidden device in device manager, and the WiMan-WiFi will be as a "zombie".

If users installing SOL LMS extension INF want to downgrade Intel® CSME software, the existing Intel® CSME software including SOL LMS extension INF should be removed firstly.

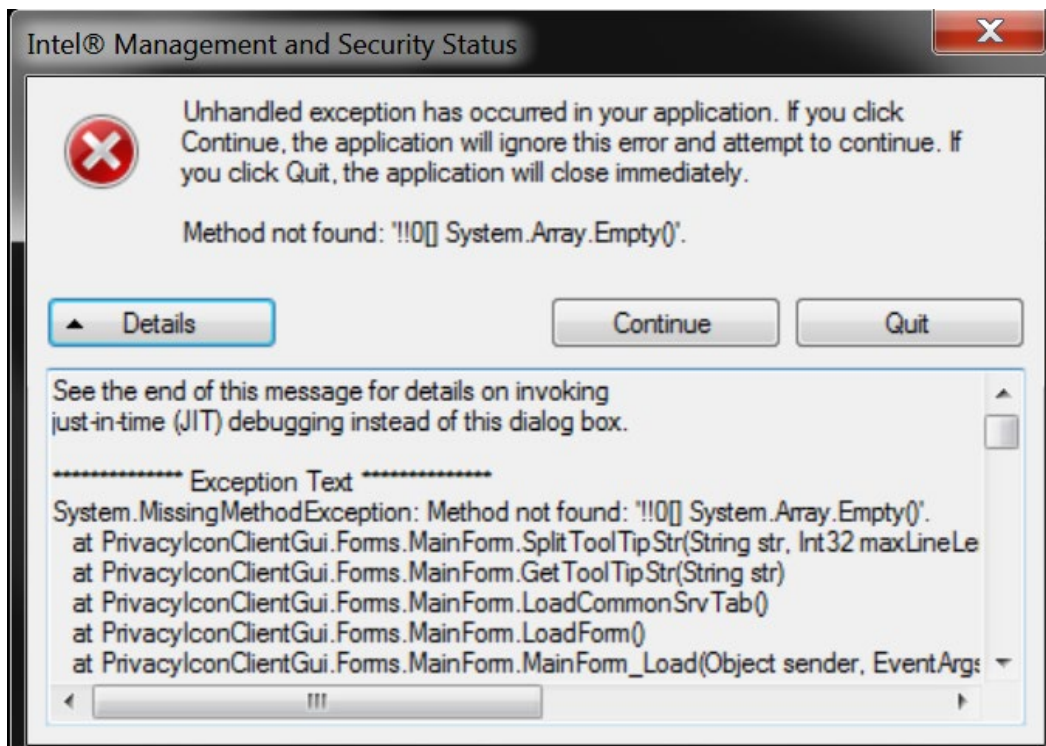
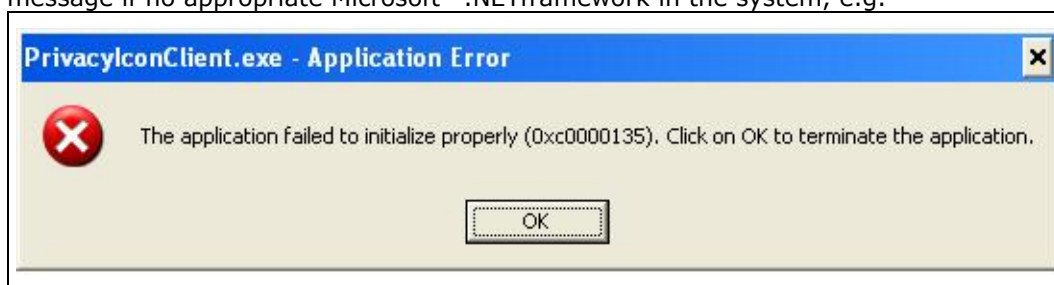
SOL and Intel® LMS device must be removed before SOL LMS extension INF is uninstalled.

10 Troubleshooting

10.1 Error Message when Intel® Management and Security Status Application Loads

Intel® MSS will fail when executing in an environment without appropriate Microsoft* .NET framework. Microsoft* does not provide a safeguard mechanism in such conditions.

The Intel® Management and Security Status application will display unspecific error message if no appropriate Microsoft* .NETframework in the system, e.g.



If these kinds of issues happen, check the installed Microsoft* .NET Framework. The required version refers to section 4.



10.2 “Information Unavailable” Displayed instead of Status

The service status of Intel® Active Management Technology or Intel® Standard Manageability in the General tab of Intel® MSS depends on which technology is operational on the system.

If “Information Unavailable” displays on the systems supporting Intel® Active Management Technology or Intel® Standard Manageability, Check that:

1. Intel® Active Management Technology or Intel® Standard Manageability is functioning properly in Intel® CSME firmware.
2. Intel® LMS is installed, running normally and starts automatically on Windows* startup.
3. Intel® MEI driver is installed, enabled and functioning properly.

10.3 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.

10.4 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® MSS application is running, the Intel® MSS 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.

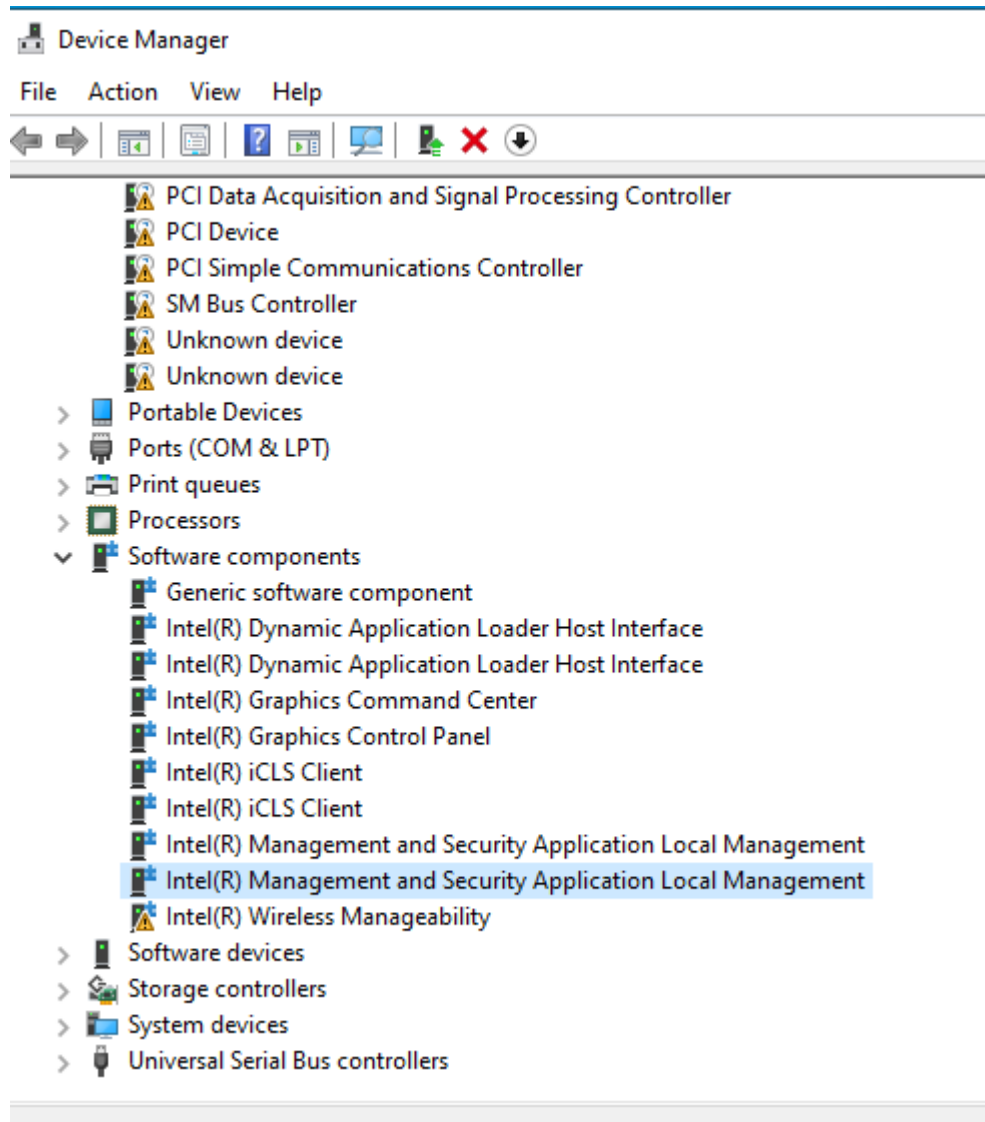
Note: The icon will also be gray if Intel® LMS service is not running or the Intel® MEI driver is disabled or unavailable.

10.5 Redundant software components in device manager

After Intel® MEI driver 1931.14.0.1323, the functionality of add components is migrated from oemextension INF to Intel® MEI driver. For the system on which the



legacy OEM extension INF has been installed (and not removed), user will see redundant software components in device manager after Intel® MEI driver is installed/updated with version 1931.14.0.1323 or later.



This symptom doesn't impact the functionality of Intel® TCS, Intel® DAL and Intel® LMS. If user still wants to remove these duplicate components from device manager, user may remove oemextension INF via pnputil command.

S