

Intel® Converged Security and Management Engine Software

Installation and Configuration Guide

Supporting Intel® CSME firmware version: 10 and above

August 2018

Revision 2.1

Intel Confidential



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

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

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

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

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

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

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

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

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 © 2018 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
0.7	<ul style="list-style-type: none">• Initial Release	December 2016
0.8	<ul style="list-style-type: none">• Updated supported FW versions• Updated OS support• Updated LMS Registry Configuration Parameters	May 2017
0.81	<ul style="list-style-type: none">• Add note that CNL /CFL not supporting WIN7 OS	June 2017
0.9	<ul style="list-style-type: none">• Add -ioc installation feature in IOC description• revise system requirements• add iCLS client in section 3.1	August 2017
0.91	<ul style="list-style-type: none">• Added description for iCLS Client in section 2.8	October 2017
0.92	<ul style="list-style-type: none">• Change the full name definition of iCLS	October 2017
1.0	<ul style="list-style-type: none">• Section 8.4 : change location of ShowUserNotification• Section 9.1 : change location of LMS registry key• Remove the description of specifying Delay before IMSS Loads	December 2017
1.1	<ul style="list-style-type: none">• Remove Intel® AMT NAC Posture Plug-in , Intel® AMT NAP Plug-in and Intel® Identity Protection Technology (Intel® IPT)• Add section 6.6 for support of Windows* 10 RS3 and beyond• Add description of setupME.exe command line option	April 2018
1.2	<ul style="list-style-type: none">• Add description about release version numbering in section 7	April 2018
1.3	<ul style="list-style-type: none">• Add LMS and JHI INF in section 6.6	April 2018
1.4	<ul style="list-style-type: none">• Add OemExtension INF and driver description in section 6.6	April 2018
1.5	<ul style="list-style-type: none">• Add Firewall policy in section 6.7• Add PartialFWUImagePath limitation in section 9.1	May 2018
1.6	<ul style="list-style-type: none">• Add Windows 7 support in section 4	May 2018
1.7	<ul style="list-style-type: none">• Add -noIMSS option of setupme.exe	May 2018
1.8	<ul style="list-style-type: none">• Add installation of IMSS APPX in section 6• Add uninstall steps for extension INF drivers in section 10	July 2018
1.9	<ul style="list-style-type: none">• Section 5: .NET framework is required for Windows 7 only• Update content in section 6.1	August 2018
2.0	<ul style="list-style-type: none">• Add warning for user who chooses to use -p flag in section 6.1.1• Add identification for LMS, JHI, iCLS in section 7• Add more description about IMSS APPX in section 6.1.3	August 2018



Revision Number	Description	Revision Date
2.1	<ul style="list-style-type: none">•Add skipstartmenu in the options of setupme.exe in section 6.1.1•Add more note about UWP drivers in section 6.1.2	August 2018



Contents

1	Introduction	8
2	Software Components Overview	9
2.1	Intel® Management Engine Interface (Intel® MEI)	9
2.2	Serial Over LAN (SOL) Driver	9
2.3	Local Manageability Service (LMS)	9
2.4	Intel® CSME WMI Provider	10
2.5	Intel® Management and Security Status Application	10
2.6	Intel® Dynamic Application Loader (Intel® DAL)	11
2.7	Intel® Online Connect (IOC)	11
2.8	Intel® Capability Licensing Services Client (iCLS Client)	11
3	Installer List	12
3.1	Intel® ME_SW_MSI	12
3.2	Intel® MEI-Only Installer	13
4	System Requirements	14
5	Installing Microsoft* .NET Framework	15
6	Installing Intel® CSME Software Components	16
6.1	How to Install	16
6.1.1	Windows* 10 RS2 and before	16
6.1.2	Windows* 10 RS3 and beyond	17
6.1.3	IMSS APPX	20
6.2	Error Codes during Installation	21
6.3	Windows* 7	22
6.4	Windows* 8.x and Beyond	23
6.5	Windows* PE	23
6.6	Firewall policy	23
7	Identifying Intel® CSME Software Components	25
8	Advanced Configuration of Intel® Management and Security Status Application	27
8.1	General Tab Logo	27
8.2	Load on Start-Up Options	27
8.3	Load in Disabled State	27
8.4	Show Notification Option	28
8.5	Disabling the Intel® AT Tab	28
8.6	"Click Here for More Details" Link	28
9	Configuring LMS	29
9.1	LMS Registry Configuration Parameters	29
9.2	Intel® PROSet/Wireless Software Adapter Switching Override	30
10	Uninstalling Intel® CSME Software and Drivers	32
11	Troubleshooting Intel® Management and Security Status Application	33
11.1	Error Message when Intel® Management and Security Status Application Loads	33



11.2	"Information Unavailable" Displayed instead of Status	33
11.3	Client Initiated Remote Access Connection Failure.....	34
11.4	Grayed-Out Notification Icon	34



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*.

The Intel® CSME software installer has a separate version for each Intel® CSME generation. The installers provided with each version also supports earlier platforms, so, for example, the installers provided with 9.x also supports Intel® CSME 8.x platforms. Due to Intel CSME SW backwards compatibility requirement, the CSME 12 software supports any OS supported since Intel® ME 10 and onwards.

§



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:
MEISetup.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 (SOL) Driver

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 Local Manageability Service (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

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)

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. It is not available over Windows Server* 2003, Windows Server* 2008, Windows Server* 2012 or Windows Server* 2016.

2.7 Intel® Online Connect (IOC)

This Software is an enhancement to Intel® IPT which implements a [FIDO](#) UAF and U2F-compliant authentication framework client solution in support of secure online authentication for consumer services as a means to seamlessly on-board Windows* based PC client devices to FIDO solutions available now such as banking and payments. This software will only be installed on CSME 11.x firmware and Win 10 based platforms. This software consists of 2 services running in Session 0 context in Delayed-Start mode:

- IOC Access Service - a local webserver implementation that allows plugin and extension less communication from the browser hosted IOC JS module to the IOC Client. It comprises of a Windows service and a network filter driver that channels REST calls from the IOC JS module to the IOC Client.
- IOC Client - a Windows service which combines the implementation of the FIDO UAF Client and Authenticator Specific Module (ASM).

Intel® IOC is not installed by CSME SW installer anymore. In order to install IOC , use standalone Intel® Online Connect package available in VIP.

2.8 Intel® Capability Licensing Services Client (iCLS Client)

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

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



3 Installer List

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

3.1 Intel® ME_SW_MSI

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:

- Intel® Management Engine Interface (Intel® ME Interface)
- Serial Over LAN (SOL) driver
- Local Manageability Service (LMS)
- Intel® CSME WMI provider
- Intel® Management and Security Status application
- Intel® Dynamic Application Loader (Intel® DAL)
- Intel® Capability Licensing Service Client (iCLS Client)

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® iCLS, Intel® LMS, Intel® CSME WMI provider, Plug-ins, Intel® Management and Security Status application	On systems that do not have hardware to support Intel® AMT or Intel® Standard Manageability, the Installer would quit directly.
Intel® Dynamic Application Loader	Intel® MEI driver, SOL driver, Intel® DAL service, Intel® iCLS, Intel® LMS, Intel® CSME WMI provider, Plug-ins	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
PAVP	Intel® MEI driver, SOL driver, Intel® iCLS, Intel LMS, Intel® CSME WMI provider, Plug-ins	N/A
None of the above	Intel® MEI driver	N/A



3.2 Intel® MEI-Only Installer

This package installs the Intel® MEI driver only.





4 *System Requirements*

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

- Windows* 7 / Windows* 8 / Windows* 8.1 / Windows* 10 / Windows Server* 2008 64 bit versions / Windows Server* 2008 R2 / Windows Server* 2012 / Windows Server* 2016 – Latest Service Packs.
- Microsoft* .NET Framework: version 3.5 or above, required if the Intel® Management and Security Status application is installed on the platform.





5 *Installing Microsoft* .NET Framework*

If Intel® AMT, Intel® SBA or Intel® Standard Manageability are included on the platform, the installer installs the Intel® Management and Security Status application.

Note: Intel® SBA is not supported on Canon Lake platform.

Before installing the Intel® Management and Security Status application, installation of Microsoft* .NET framework is required for Windows* 7.

1. Download, for instance, Microsoft* .NET Framework 3.5 (**dotnetfx35.exe**) from Microsoft's* website. One link to the installer application is:
<http://download.microsoft.com/download/6/0/f/60fc5854-3cb8-4892-b6db-bd4f42510f28/dotnetfx35.exe>.

The downloading process may take several minutes.
Double-click the downloaded application.

2. The installer extracts the contents and displays the **Supplemental License Terms** screen.
3. Read the license content and select the **Accept** option to proceed with the installation.
4. When the installer finishes, press the **Finish** button.





6 Installing Intel® CSME Software Components

6.1 How to Install

6.1.1 Windows* 10 RS2 and before

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

There is also a version of the installer that installs only the MEI driver, and not the other software components. It is called **MEISetup.exe**, and is located located at **Installers\MEI-Only Installer MSI**.

Note: The components installed are subject to the platform's capabilities.

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

The software installer also have 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.

-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.
- noIMSS
Does not install Intel® Management and Security Status.
- meidalonly
Installs Intel® Management Engine Interface, Intel® Dynamic Application Loader, and Intel® Identity Protection Technology (Intel® IPT) components only.
- preinst
Installs all drivers even if hardware is not present.
- tcs
Installs only TCS.
- skipstartmenu
Does not add the Intel® IMSS shortcut to the Start menu

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

6.1.2 Windows* 10 RS3 and beyond

The driver for MEI , SOL, LMS, JHI and iCLS 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 this folder do offline injection e.g. via DISM. More information about DISM can be found at:

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

Note that MEI and SOL drivers are required to be installed before other drivers.

MEI: heci.inf in Installers\WindowsDriverPackages\MEI\win10

SOL: mesrl.inf in Installers\WindowsDriverPackages\SOL

iCLS: iclsClient.inf in Installers\WindowsDriverPackages\iclsClientUWD



LMS: LMS.inf in Installers\WindowsDriverPackages\LMS

JHI: DAL.inf in Installers\WindowsDriverPackages\JHI\win10

OemExtension: OemExtension.inf in Installers\WindowsDriverPackages\OemExtension

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

There are devices shown in the device manager as following:

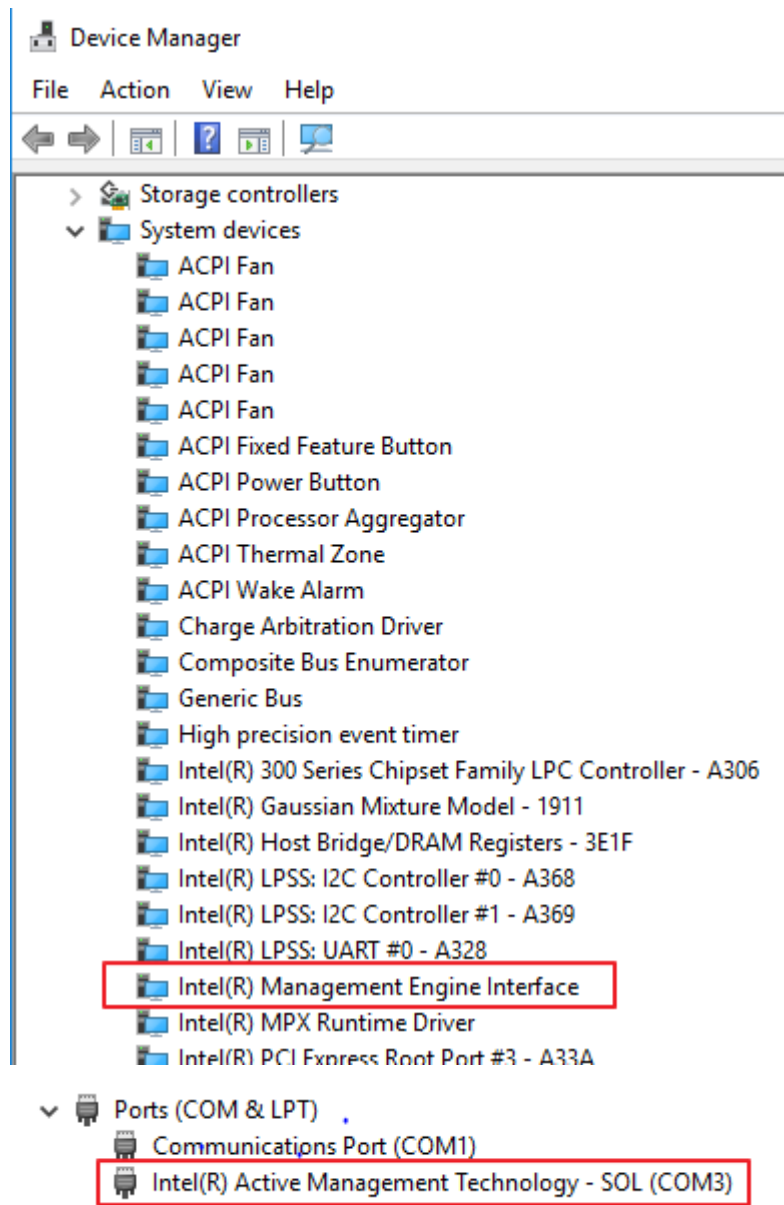
MEI: System devices \ Intel(R) Management Engine Interface

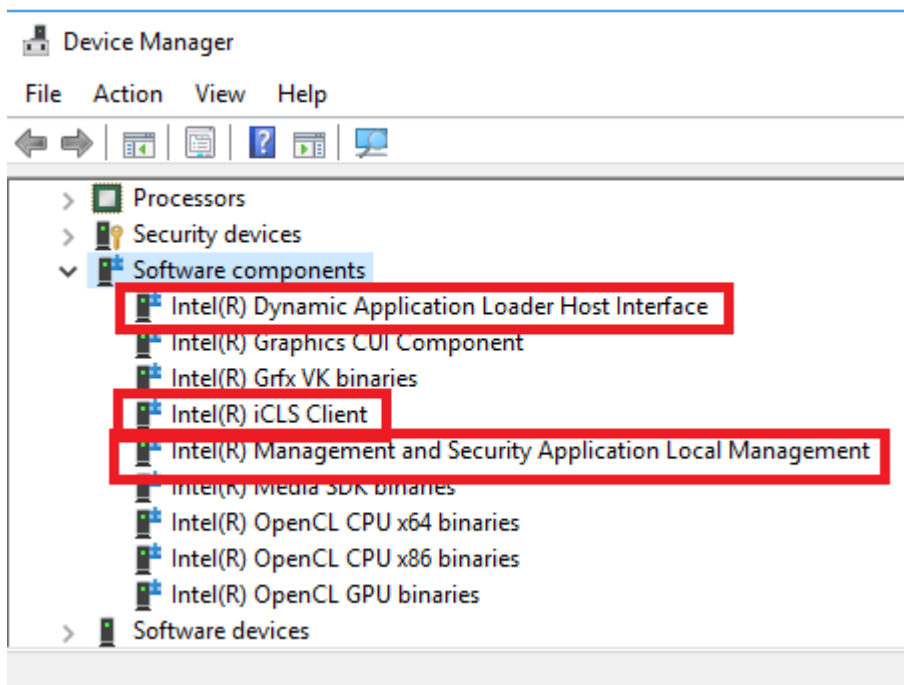
SOL: Ports(COM & LPT) \ Intel(R) Active Management Technology - SOL

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

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

iCLS: Software components \ Intel(R) iCLS Client



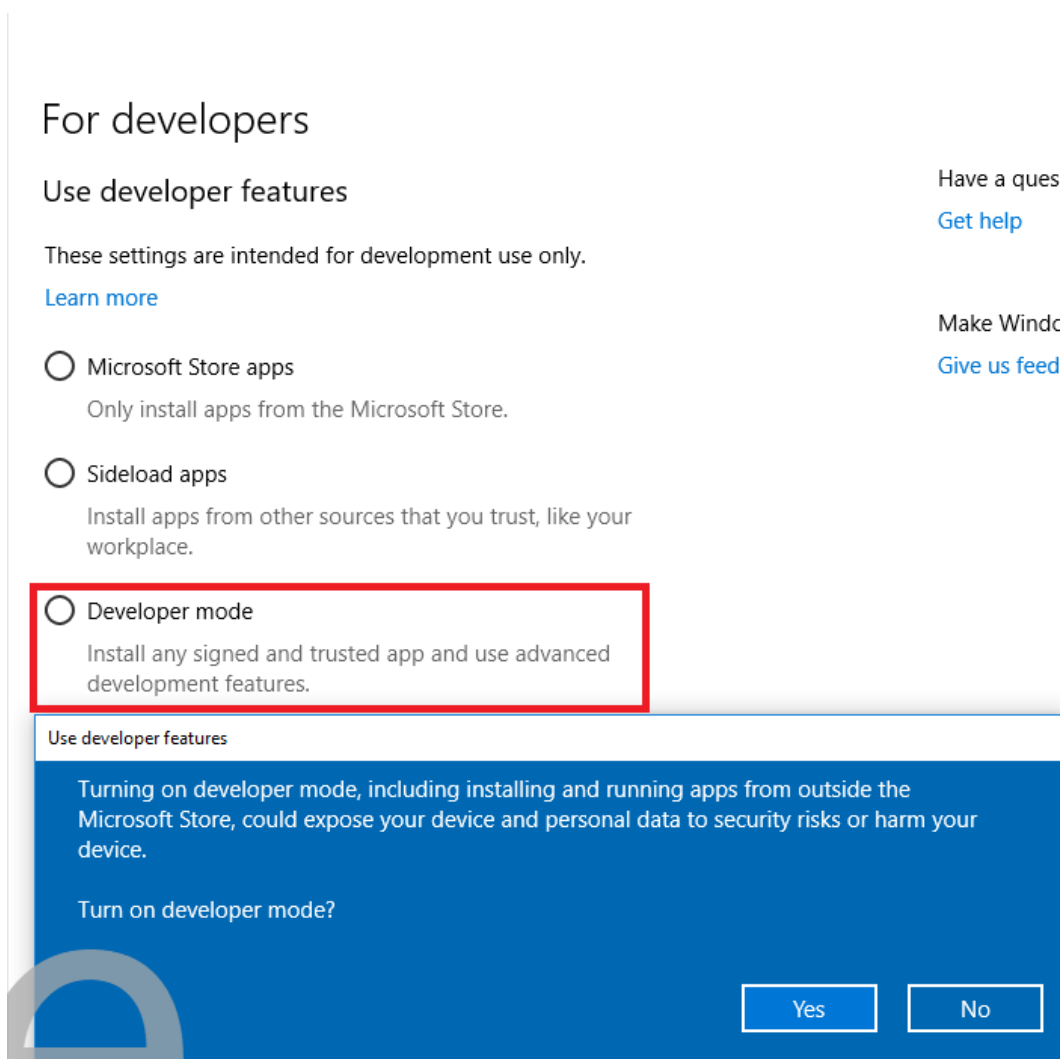


6.1.3 IMSS APPX

IMSS APPX is located in the firmware kit in the **Installers\WindowsDriverPackages\IMSS** folder.

To install IMSS APPX, follow the steps as below:

- 1.install the certificate by Clicking certificate file in Installers\WindowsDriverPackages\ folder(e.g. PrivacyIconClientPackagingProject_1.0.19.0_AnyCPU.cer)
- 2.run Add-AppDevPackage.ps1 with power shell. During execution, The following window will be pop up. Click and turn on developer mode to acquire a developer license, then continue with power shell by choosing [Y]Yes.



6.2 Error Codes during Installation

Error code	Error String	Description
0	ERROR_SUCCESS	Operation was successful and a reboot is not needed. Use of the -b switch will not cause a reboot in this case.
1602	ERROR_INSTALL_USEREXIT	One of: <ul style="list-style-type: none"> The user canceled the operation Setup was run silently but a downgrade was detected and the -overwrite switch was not used.



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">• Not admin• No device matches• OS requirement not met• .NET requirement not met
1633	ERROR_INSTALL_PLATFORM_UNSUPPORTED	Architectures not supported
1641	ERROR_SUCCESS_REBOOT_INITIATED	A system reboot has been initiated either by the user choosing to "reboot now" or the -b switch was used in silent mode and setup requires a reboot. Note that depending on the OS and platform speed, the calling process may never get this code due to it being terminated as part of the shutdown procedure.
3010	ERROR_SUCCESS_REBOOT_REQUIRED	Successful, but a reboot is required to complete the process.

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

6.3 Windows* 7

Note: Windows* 7 is not supported in Cannon Lake/ Coffee Lake Platforms. It is in the Installer for backward compatibility.

To run Intel® MEI driver on Windows*7, the following Microsoft security update must be installed:

- KB2921916
- KB3033929
- KB3123479
- KB3035131

When the Intel® Management and Security Status application is installed on a Windows* 7 operating system, it may need to install the Microsoft* KMDF Co-installer which is not present by default on these systems. In these cases, the installation of the KMDF Co-installer will prompt the user for a restart of the system at the end of the installation process.

Note that if the KMDF Co-installer was already present on the system (due to some other installation installing it, or Microsoft* Windows Update downloading it), no restart will be required.



When Local Manageability Service (LMS) is installed on a Windows* 7 operating system, system need to have the updated root certificates in order to allow LMS service to start.

The required certificates are contained in:

- x86: Update for Root Certificates for Windows 7 [November 2013] (KB931125)
- x64: Update for Root Certificates for Windows 7 for x64-based Systems [November 2013] (KB931125)
- Certificates can be found in <http://catalog.update.microsoft.com/v7/site/Search.aspx?q=root%20certificate%20update>

6.4 Windows* 8.x and Beyond

When the Intel® Management and Security Status application is installed on a Windows* 8 or 8.1 operating system, a Windows* tile is placed on the start screen. This tile is used by the Intel® Management and Security Status application to post Toast* notifications to the Windows* UI.

This tile may be removed by an System manufacturers before the platform is shipped. It will be re-created by the Intel® Management and Security Status application if Intel® Active Management Technology (Intel® AMT) is provisioned on the platform.

6.5 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>

6.6 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



Installing Intel® CSME Software Components

- Port: Any





7 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.12.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:

Win32:

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

Win64:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\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, set as 12 for ME12
- nn – Minor version
- bbbb – Build number

E.g. If the FW kit that was built on WW09'18 is: 12.0.0.xxxx, the SW kit will be: 1809.12.0.bbbb

Service name for LMS, JHI or iCLS 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

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

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

TPMProvisioningService.exe / Intel(R) TPM Provisioning Service

If LMS, JHI or iCLS is installed via installer **SetupME.exe**, the components file location is C:\Program Files (x86)\Intel\Intel(R) Management Engine Components

If LMS, JHI or iCLS is installed via **UWD INF installer**, the components file locations are different from that installed by setupme.exe:

LMS.exe and related files : %SystemRoot%\Intel\Intel(R) Management Engine Components\LMS

Jhi_service.exe and related files: %SystemRoot%\system32\

iCLS: %SystemRoot%\system32\Intel\iCLS Client

§



8 Advanced Configuration of Intel® Management and Security Status Application

8.1 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.

8.2 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.

8.3 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".

8.4 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.

8.5 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.

8.6 "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.

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.



9 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:

9.1 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

9.2 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.





10 Uninstalling Intel® CSME Software and Drivers

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.

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.

For the extension INF driver(LMS, iCLS , JHI and oemextension)

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



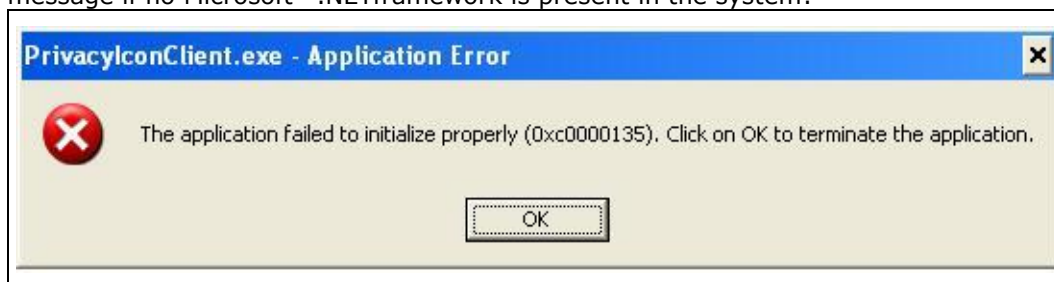


11 Troubleshooting Intel® Management and Security Status Application

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

Microsoft* .NET applications fail when executed in an environment that has no Microsoft* .NET framework 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* .NET framework is present in the system:



If this happens, install Microsoft* .NET Framework version 3.5 or above and then re-open the application.

11.2 "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.



11.3 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.

11.4 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.

