

Intel® Management Engine Software

Installation and Configuration Guide

March 2015

Document Revision Version: 1.2
Supporting Intel® ME firmware version: 8 and above

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 © 2015 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,

(i) 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.



Contents

1 Introduction 6

2 Software Components Overview 7
- 2.1 Intel® Management Engine Interface (Intel® MEI) 7
- 2.2 Serial Over LAN (SOL) Driver 7
- 2.3 Intel Local Manageability Service (LMS) 7
- 2.4 Intel® ME WMI Provider 8
- 2.5 Intel® Management and Security Status Application 8
- 2.6 Intel® AMT NAC Posture Plug-in 9
- 2.7 Intel® AMT NAP Plug-in 9
- 2.8 Intel® Dynamic Application Loader (Intel® DAL) 9
- 2.9 Intel® Identity Protection Technology (Intel® IPT) 9
- 2.10 Intel® Update Manager 9
- 2.11 Intel® Security Assist (Intel® SA) 9
- 2.12 Intel® Technology Access (Intel® TA) 10

3 Installer List 11
- 3.1 Intel® ME_SW_MSI 11
- 3.2 Intel® MEI-Only Installer 12

4 System Requirements 13

5 Installing Microsoft* .NET Framework 14

6 Installing Intel® ME Software Components 15
- 6.1 How to Install 15
- 6.2 Error Codes During Installation 15
- 6.3 Windows* 7 16
- 6.4 Windows* 8 and 8.1 and Beyond 16
- 6.5 Windows* PE 17

7 Identifying Intel® ME Software Components 18

8 Advanced Configuration of the Intel® Management and Security Status Application 19
- 8.1 General Tab Logo 19
- 8.2 Load on Start-Up Options 19
- 8.3 Load in Disabled State 19
- 8.4 Specifying the Delay Before the Intel® Management and Security Status Application Loads 20
- 8.5 Show Notification Option 21
- 8.6 Disabling the Intel® AT Tab 21
- 8.7 ”Click Here for More Details” Link 21

9 Configuring the LMS 22
- 9.1 LMS Registry Configuration Parameters 22

10 Uninstalling the Intel® ME Software 25

11 Troubleshooting Intel® Management and Security Status Application 26



11.1 Error Message when Intel® Management and Security Status Application Loads 26
11.2 ”Information Unavailable” Displayed Instead of Status 26
11.3 Client Initiated Remote Access Connection Failure..... 27
11.4 Grayed-Out Notification Icon 27



1 Introduction

This guide describes how to install, configure and troubleshoot the Intel® Management Engine (Intel® ME) software components.

For a list of software components, see *Software Components Overview* (Section 2).

The Intel® ME software installer has a separate version for each Intel® ME generation (6.x, 7.x, 8.x, 9.x, 10.x etc.). The installers provided with each version also supports earlier platforms, so, for example, the installers provided with 9.x also supports Intel® ME 8.x platforms.

§



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 Technology (Intel® SBT), 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: **setup.exe -?** and the help dialog should appear.

2.1 Intel® Management Engine Interface (Intel® MEI)

This driver is the interface between the Intel® Management Engine (Intel® ME) firmware and the operating system. Drivers and applications on the host that wish to interact with Intel® ME 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 Intel Local Manageability Service (LMS)

This service enables local applications running on Intel® AMT, Intel® SBT 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® ME IANA (Internet Assigned Names Authority) ports and routes all traffic to the firmware through the Intel® MEI.

It also provides Intel® ME with various host operation abilities. For instance, it enables Intel® ME 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® ME WMI Provider

The Intel® ME WMI provider enables ISV and IT administrators to perform Intel® AMT discovery and configuration operations using WMI technology. The Intel® ME 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® ME WMI provider:

- Discovery of Intel® ME 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® ME 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 Technology (Intel® SBT), Intel® Standard Manageability, and Intel® Anti-Theft services. The Intel® Management and Security Status application indicates whether Intel® AMT, Intel® SBT, Intel® AT and Intel® Standard Manageability are running on the platform. The application is installed and executed as part of the Intel® ME 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® SBT 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® AMT NAC Posture Plug-in

This is an application that allows a Cisco* Trusted agent to start its authentication process in order to retrieve a posture from the Intel® AMT firmware for the purpose of providing the Intel® AMT posture to the NAC backend.

This application is only installed on Intel® ME generations before 9.0.

2.7 Intel® AMT NAP Plug-in

This is an application that enables authentication from the Intel® AMT firmware to a Microsoft* Network Access Protection (NAP) backend.

2.8 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 applications 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, or Windows Server* 2012.

2.9 Intel® Identity Protection Technology (Intel® IPT)

This software contains the components and APIs required for ISV applications to utilize Intel® IPT abilities (i.e. One Time Password and True Cove). 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, or Windows Server* 2012.

2.10 Intel® Update Manager

This software is required for Intel® Update Manager. It will be installed only if the feature is enabled on the system. The Intel® Update Manager will periodically check for critical updates to the Intel ME Firmware and will offer the user to initiate installation of update if available.

2.11 Intel® Security Assist (Intel® SA)

This is a software that utilizes Intel platform hardware to provide security functionality. It is designed to help the security built into Intel platforms by providing users with additional features, functionality, and recommendations. Enhancements will be discussed with Intel customers before they are implemented and released as an update to the initial release.



2.12 Intel® Technology Access (Intel® TA)

Intel® Technology Access is a mechanism that exposes various platform capabilities as a web service to browser applications. It is designed to give standardized access to the capabilities. Enhancements will be discussed with Intel customers before they are implemented and released as an update to the initial release. Any known issues will be documented within the Intel® Technology Access independent installer package, which is available to customers for downloading on VIP.

§



3 Installer List

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

3.1 Intel® ME_SW_MSI

This installation program installs the Intel® ME 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® ME WMI provider
- Intel® Active Management Technology NAC Posture Plug-in
- Intel® Active Management Technology NAP Plug-inIntel® Management and Security Status application
- Intel® Dynamic Application Loader (Intel® DAL)
- Intel® Identity Protection Technology (Intel® IPT)
- Intel® Update Manager
- Intel® Management Engine Service
- Intel® Security Assist (Intel® SA)
- Intel® Technology Access (Intel® TA)

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® SBT, Intel® Standard Manageability	Intel® MEI driver, SOL driver, LMS, Intel® ME 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 SOL driver will not be installed.

If the platform includes this capability….	These software components are installed	Comments
Intel® Dynamic Application Loader	Intel® MEI driver, Intel® DAL service, Intel® IPT Client Middleware	The Installer provides the option to install only Intel® MEI driver, Intel® DAL service and Intel® IPT Client Middleware by running the installer with the following flag: setup.exe –meidalonly
PAVP	Intel® MEI driver, LMS	Intel® ME WMI provider is not installed on 1.5 MB SKU
None of the above	Intel® MEI driver	

If the Intel® Update Manger feature is enabled on the system, the following components are installed as well, regardless of the platform capabilities: Intel® Update Manager and Intel® Management Engine Service.

3.2 Intel® MEI-Only Installer

This package installs the Intel® MEI driver only. This is available on the 5 MB SKU only.

§



4 System Requirements

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

- Windows* XP / Windows* 7 / Windows* 8 / Windows* 8.1 and beyond / Windows Server* 2003 / Windows Server* 2008 32/64 bit versions / Windows Server* 2008 R2 / Windows Server* 2012 – 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.

Note: If working with Windows* XP, one may consider adding the EnableSignCheck key to the Registry to avoid the possibility of LMS performance issues. See more details under LMS Registry Configuration Parameters.

Note: Windows* Server Core installation is not supported.

§

5 Installing Microsoft* .NET Framework

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

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

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® ME Software Components

6.1 How to Install

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

For 1.5MB skus, the installer **SetupME.exe**, is in **Installers\ME_SW_MSI**.

For 5MB skus, the installer **SetupME.exe**, is, as appropriate, in **Installers\ME_SW_MSI\PreProduction** or **Installers\ME_SW_MSI\Production**.
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 installation log can be found at "C:\Intel\Logs\IntelAMT.log"

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: • The user canceled the operation • Setup was run silently but a downgrade was detected and the –overwrite switch was not used.
1603	ERROR_INSTALL_FAILURE	General failure code. The error could have been an unanticipated error or one of the expected errors such as: • Not admin • No device matches • OS requirement not met • .NET requirement not met

Error code	Error String	Description
1633	ERROR_INSTALL_PLATFORM_UNSUPPORTED	A device check revealed no matching devices to INF's in the setup.
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

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 and 8.1 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 OEM 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 coinstallers 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 coinstallers can be found at:

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

§

7 Identifying Intel® ME Software Components

Once the Intel® ME 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® Management Engine 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>
<identifyingnumber>{65153EA5-8B6E-43B6-857B-C6E4FC25798A}</identifyingnumber>
<version>7.1.40.1161</version>
<upgradecode>{65153EA5-8B6E-43B6-857B-C6E4FC25798A}</upgradecode>
</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

§



8 Advanced Configuration of the 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® ME 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 Specifying the Delay Before the Intel® Management and Security Status Application Loads

By default the Intel® Management and Security Status application starts loading 3 minutes after the user logs on. If you need the Intel® Management and Security Status application to load later because of other applications loading at log-on time, you can increase this period by changing the value of the **IMSS** registry key in the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** branch (this branch is correct for 32-bit operating systems; for 64-bit operating systems the location of the key in the registry is **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run).** The timeout could be set to be shorter or longer, ranging from 1 second to a maximum of 180 seconds.

For example, to cause a delay of 90 seconds before the Intel® Management and Security Status application loads, change the **IMSS** registry key’s value to the following:

“C:\Program Files\Intel\Intel® Management Engine Components\IMSS\PIconStartup.exe” 90

Note: The lowest value you can enter here is 1. If you enter the value 0, the Intel® Management and Security Status application will load after the default period (3 minutes). To cause the Intel® Management and Security Status application to load without any delay, change the value of the IMSS key to:

“C:\Program Files\Intel\Intel® Management Engine Components\IMSS\PrivacyIconCLient.exe” -startup

(For 64-bit systems, **“C:\Program Files (x86)\ Intel\ Intel® Management Engine Components\IMSS\PrivacyIconCLient.exe” –startup)**

(These are the default installation locations; you can choose a different location during installation).



8.5 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 **HKLM\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.

8.6 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.

8.7 ”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 the 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® ME 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.

The LMS also provides NAC (via a plug-in) and NAP functionality. To enable NAP, see the installation note below.

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\SOFTWARE\Intel\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.

EnableSignCheck: This registry key is relevant to Windows* XP only. It enables or disables DLL signature checking by LMS. With Operating Systems other than Windows* XP, signature checking will always be enabled. With Windows* XP, adding the EnableSignCheck key as a DWORD value and setting its value to 0 will disable the signature checks. Setting its value to 1 will enable the signature checks. Default behavior (i.e. no value) is signature checking enabled even when in Windows* XP.

Starting with Intel® ME 8.0, LMS loads a series of dynamic software libraries (DLLs) per need. When loading a DLL, LMS by default will check for a valid signature, for security purposes. On Windows* XP, the DLL signature checking may impact the performance of LMS. A significant performance issue may be experienced if the machine is not connected to the Internet. Disabling the signature checking, by adding the EnableSignCheck key and setting its value to 0, may improve LMS performance in Windows* XP in the stated above network situation, but is not recommended from a security standpoint.

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 new feature of Intel® ME 8 that allows an 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.

PartialFWUImagePath: 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.

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) Management Engine. Intel(R) ME 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.

Registry Key	Event Log event
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



10 Uninstalling the Intel® ME Software

Uninstall the software via the Windows Control Panel.

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

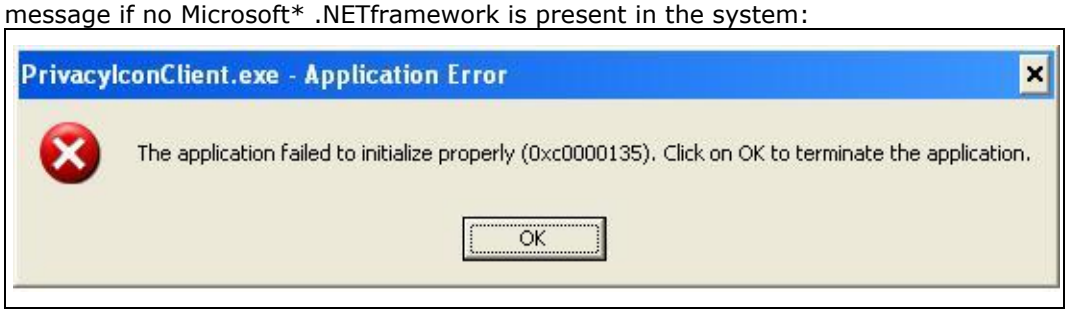
§

11 Troubleshooting Intel® Management and Security Status Application

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

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

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



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® SBT, 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. Please 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. Please 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 don't resolve the problem, it is recommended to contact your Information Technology department.

11.4 Grayed-Out Notification Icon

Whenever either Intel® AMT, Intel® SBT 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.

§