Intel® Management and Security Status Application

User's Guide

December 2011
Document Revision Version: 0.98
Firmware version: 6.2.x

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.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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.

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 the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/

Systems using Client Initiated Remote Access (CIRA) require wired LAN connectivity and may not be available in public hot spots or "click to accept" locations. For more information on CIRA visit http://www.intel.com/products/centrino2/vpro/index/htm.

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 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 © 2009-2011 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 5

2 System Requirements 7

3 Installation 9

3.1 Installing Microsoft* .NET Framework 9
3.2 Installing all SW Components 9

4 Using the Intel® Management and Security Status Application and Icon 15

4.1 General Tab 16
4.2 Intel® AMT Tab 19
4.2.1 Fast Call for Help 19
4.2.2 Support Session Status Section 20
4.2.3 System Defense State 21
4.3 Intel® Std Mgt Tab 23
4.3.1 Support Session Status Section 23
4.3.2 System Defense State 24
4.4 L3 Mgt Upgrade Tab 24
4.4.1 Fast Call for Help 24
4.4.2 Support Session Status Section 25
4.4.3 System Defense State 25
4.5 Intel® AT Tab 26
4.5.1 Intel® AT State 26
4.5.2 Intel® AT Registration 27
4.6 Advanced Tab 28
4.6.1 Intel® Management Engine 28
4.6.2 Secure Output Window Settings 29
4.6.3 Extended System Details 30
4.6.4 Network Information 31
4.7 Exiting the Application 32

5 Advanced Configuration 33

5.1 General tab Logo 33
5.2 Load on Start-Up Options 33
5.3 Load in Disabled State 33
5.4 Specifying the Delay Before the Intel® Management and Security Status Loads 34
5.5 Show Notification Option 34
5.6 Disabling the Intel® AT Tab 35
5.7 'Click here for more details' Link 35

6 Troubleshooting Intel® Management and Security Status Application 37

6.1 Error Message Appears upon Application Load 37
6.2 Working with Mutual Authentication on the Local Interface 37
6.3 'Information Unavailable' is Displayed instead of Technology Status 38
6.4 Client Initiated Remote Access Connection Failure 38

§

1 Introduction

This guide describes how to install and use the Intel® Management and Security Status application, an application that displays information about a platform's Intel® Active Management Technology (Intel® AMT), Intel® Standard Manageability, Level III Manageability Upgrade, Intel® Anti-Theft, Intel® Remote PC Assist (Intel® RPAT) services.

The Intel® Management and Security Status icon indicates whether Intel® AMT, Intel® Standard Manageability, Intel® RPAT, Level III Manageability Upgrade and Intel® Anti-Theft are running on the platform. The icon is located in the notification area. By default, each time Windows* starts, Intel® Management and Security Status application starts and the notification icon is displayed.

The Intel® Management and Security Status application has a separate version per every Intel® AMT generation (4.x, 5.x, 6.x). **This User Guide describes the Intel® Management and Security Status application for Intel® AMT generation 6.x.**

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® RPAT, Level III Manageability Upgrade or Intel® Standard Manageability is enabled on the platform. If the Intel® Management and Security Status application is started manually (via the Start menu), the icon is loaded even if none of these technologies is enabled, as long as all the drivers have been installed.

Note: The information displayed in the Intel® Management and Security Status application is not shown in real time. The data is refreshed at different intervals.

§

2 System Requirements

To enable installation and use of the Intel® Management and Security Status application, the following are required on the platform:

- Intel® 5 Series Express Chipset with Intel® AMT / Intel® Remote PC Assist Intel® Standard Manageability or Level III Manageability Upgrade
- Windows* XP / Windows Vista* / Windows 7* 32/64 bit versions
- Microsoft* .NET Framework 2.0, 3.5 or 4.0 (version 3.5 or above is preferred)
- The Intel® MEI driver.
- User Notification Service (UNS)
- Local Manageability Service (LMS)

Note: For Intel® AMT versions 6.x there is a bundled installation package for the following components: Intel® Management and Security Status application, Intel® MEI driver, LMS, UNS and SOL driver. Please see the Bring-up User Guide for more information.

§

3 Installation

The Intel® Management and Security Status application is automatically installed with the Management Engine components.

The installation process consists of two steps: Installing the Microsoft* .NET framework (a requirement for running the software); and installing the status application. The order of the steps is imperative (always install the framework before the Intel® AMT applications).

3.1 Installing Microsoft* .NET Framework

1. Download Microsoft* .NET Framework version 3.5 or higher (e.g. **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.

   Installing the version available in that location ensures that you are using a valid version required by the software package.
   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.

3.2 Installing all SW Components

The installer (**Setup.exe**) is located in the firmware kit at **Drivers\MEI_SOL_Installer** (and in the zip file at **Drivers\ME_IS** for the InstallShield version).
Note: The location and name of the installation program may be different, depending on the OEM's choice.

1. Double-click the installer to install the following components (**Note:** The location and name of the installation program may be different, depending on the OEM's choice):

    a. Intel® MEI

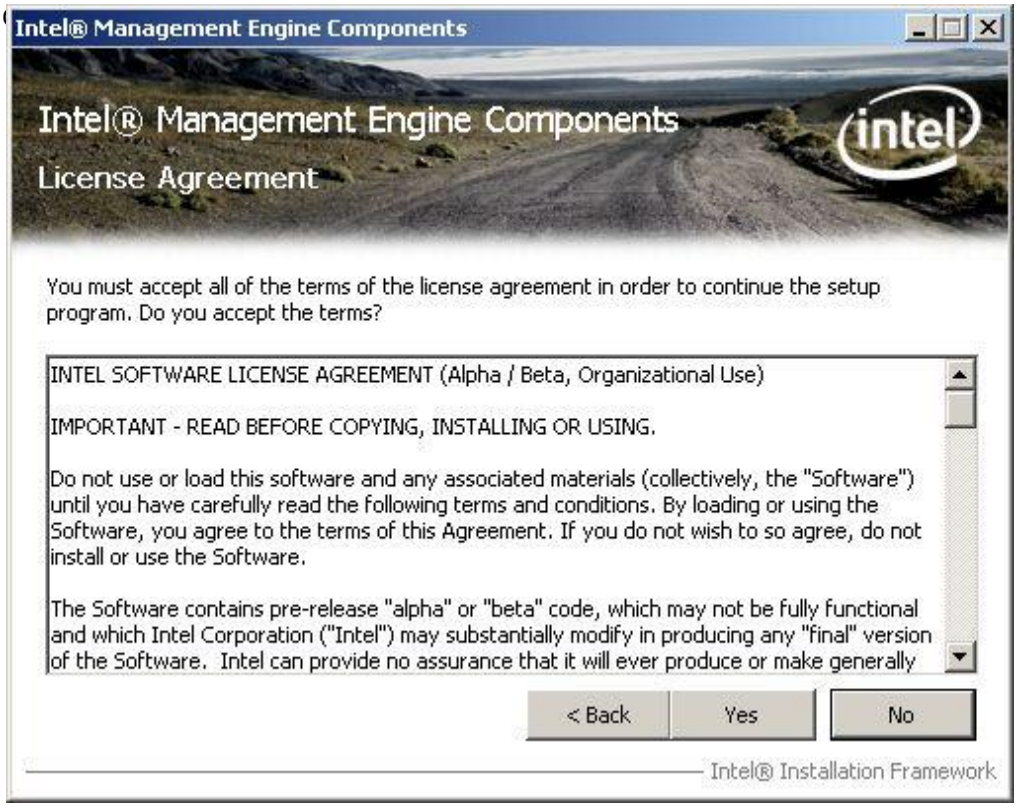
    b. SOL driver

    c. Local Manageability Service (LMS)

    d. User Notification Service (UNS)

    e. Intel® Management and Security Status application.

As a result the Welcome window opens.

2. 
Intel® Management Engine Components
Intel® Management Engine Components
License Agreement
You must accept all of the terms of the license agreement in order to continue the setup program. Do you accept the terms?
INTEL SOFTWARE LICENSE AGREEMENT (Alpha / Beta, Organizational Use)
IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING.
Do not use or load this software and 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.
The Software contains pre-release "alpha" or "beta" code, which may not be fully functional and which Intel Corporation ("Intel") may substantially modify in producing any "final" version of the Software. Intel can provide no assurance that it will ever produce or make generally
< Back
Yes
No
Intel® Installation Framework

3. Read the license conditions and click **Yes** to accept them.
   A Readme file displays system requirements and other information about the

4. Read the information in the Readme file and click **Next**. The installation begins, displaying its progress in the window.

5. When the installation is complete, click **Next** in the Setup Progress window, and click **Finish** in the **Setup is Complete** window.

§

4 Using the Intel® Management and Security Status Application and Icon

Whenever either Intel® AMT, Intel® RPAT, Intel® Standard Manageability or Level III Manageability Upgrade 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 UNS service is not running or the MEI driver is disabled or unavailable.)

To view the Intel® Management and Security Status application:

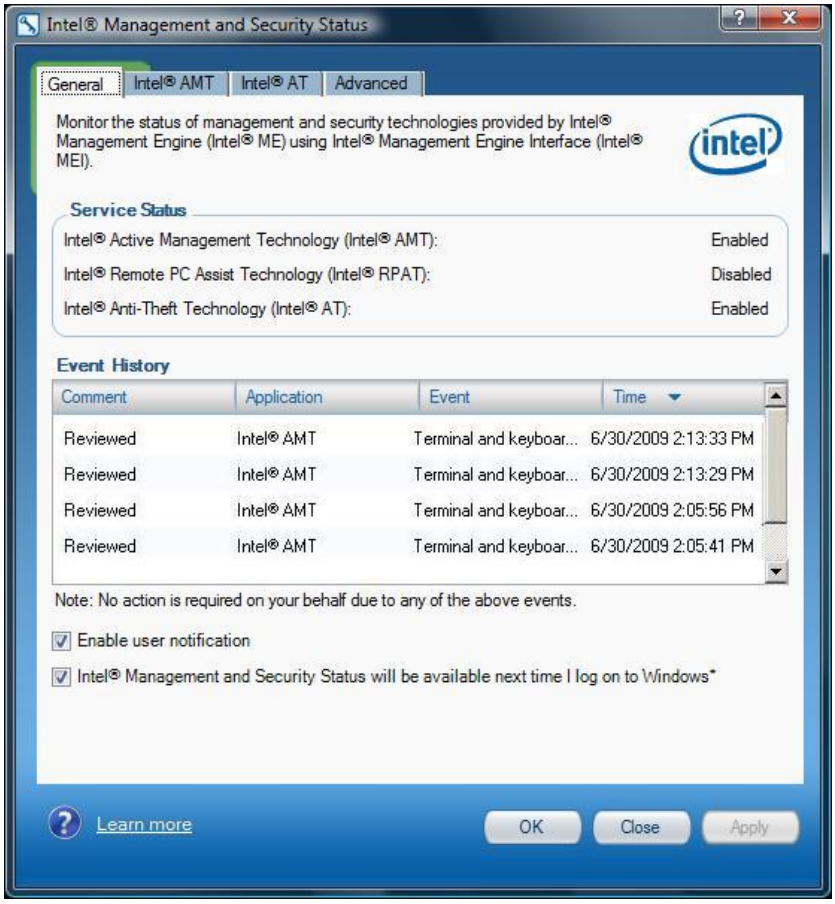
- Double-click the Intel® Management and Security Status icon, or
- Right-click or left-click the icon and choose **Open**, or
- Click **Start> All Programs>Intel>Intel® Management and Security Status> Intel® Management and Security Status**.

  Note: if your computer is set to Classic start menu - path will start with 'Programs' instead of 'All Programs'. In addition, settings presented above are the default – in case the user has changed the location during installation the path will be different.

The following sections describe the information available in the application's tabs. Information about the application is available also by clicking either the **Learn more** button or link.

4.1 General Tab

The **General** tab provides basic information about the Intel® AMT, Intel® Standard Manageability, Level III Manageability Upgrade, Intel® Anti-Theft, and Intel® RPAT status and events.



Events and some of their details are displayed in the **Event History** section. These can be sorted by clicking on the relevant column header.

The status of Intel® AMT, Intel® Standard Manageability, Level III Manageability Upgrade, Intel® Anti Theft or Intel® RPAT is displayed in the **Service Status** section depending on which technology is operational on the system. The tab displays information for either Intel® AMT, Intel® Standard Manageability, or Level III Manageability Upgrade. The status can be one of the following:

- **Intel® AMT**: Enabled / Disabled / Information unavailable

  When Intel® AMT status presents Enabled it means that the Intel® AMT technology is supported on the system. Intel® ME status (in the Advanced Tab) will give the user information on whether the Intel® ME is configured (hence Intel® AMT is functional and operating).

When Intel® AMT status presents Disabled it means that the Intel® AMT technology is not supported on the system or that Intel® AMT is disabled in MEBx.

Information unavailable: It is not known whether Intel® AMT technology is supported on the system. No Intel® AMT information is available. This can be for one of the following reasons: UNS service has stopped, or the MEI driver is disabled.

- **Intel Standard Manageability**: Enabled / Disabled / Information unavailable

  When Intel® Standard Manageability status presents Enabled it means that the Intel® Standard Manageability technology is supported on the system. Intel® ME status (in the Advanced Tab) will give the user information on whether the Intel® ME is configured (hence Intel® AMT is functional and operating).

  When Intel® Standard Manageability status presents Disabled it means that the Intel® Standard Manageability technology is not supported on the system.

  Information unavailable: It is not known whether Intel® Standard Manageability technology is supported on the system. No Intel® Standard Manageability information is available. This can be for one of the following reasons: UNS service has stopped, or the MEI driver is disabled.

- **Level III Manageability Upgrade**: Enabled / Disabled / Information unavailable

  When Level III Manageability Upgrade status presents Enabled it means that Level III Manageability Upgrade technology is supported on the system. Intel® ME status (in the Advanced Tab) will give the user information on whether the Intel® ME is configured (hence Level III Manageability Upgrade is functional and operating).

  When Level III Manageability Upgrade status presents Disabled it means that the Level III Manageability Upgrade technology is not supported on the system or that Level III Manageability Upgrade is disabled in MEBx.

  Information unavailable: It is not known whether Level III Manageability Upgrade technology is supported on the system. No Level III Manageability Upgrade information is available. This can be for one of the following reasons: UNS service has stopped, or the MEI driver is disabled.

  Intel® Anti-Theft: Enabled. This means that the Intel® Anti-Theft feature is supported on the platform (note that the feature becomes activated only after the platform has been enrolled with an Intel® Anti-Theft service provider). If Intel® Anti-Theft is not supported on the platform, no reference to it is displayed.
  Note: The information in this field shows the state of the platform when the Intel® Management and Security Status application was last launched.

- **Intel® RPAT**: Enabled / Disabled / Not Supported / Information unavailable

  When Intel® RPAT status shows **Enabled**, it means that that you can register with the Intel® RPAT service provider.

  When Intel® RPAT status shows **Disabled**, it means that Intel® AMT is active on the platform, allowing your IT personnel to remotely discover, heal and protect your computer.

  When Intel® RPAT status shows **Not Supported**, it means that your computer is not Intel® RPAT capable. For details, contact your hardware vendor.

Intel® Management and Security Status will be available next time I log on to Windows: Checking this box causes the Intel® Management and Security Status

application to be invoked, and the icon to be displayed, whenever you log on to Windows*.

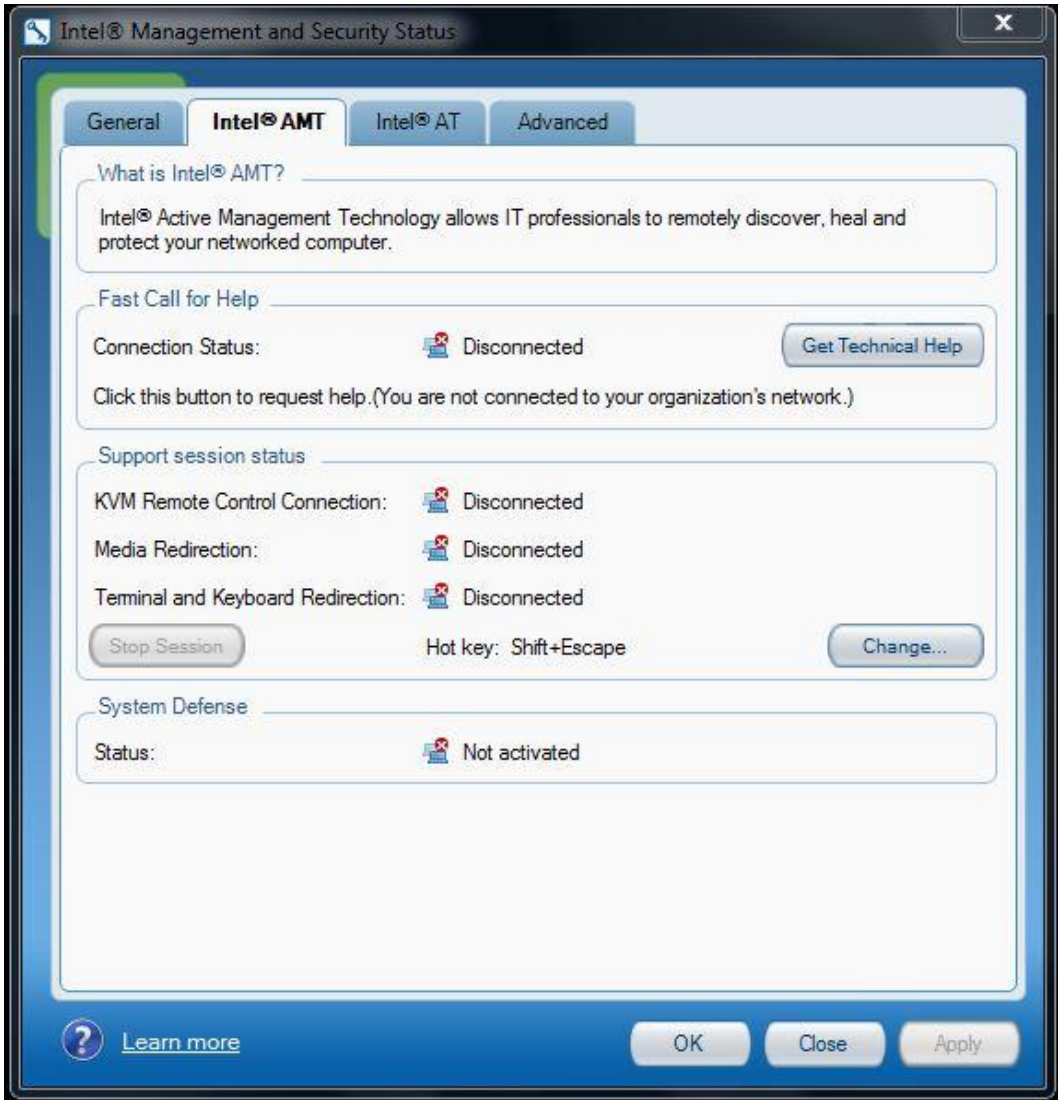
Note: The application does not load automatically with Windows* log-on if none of the technologies it displays (Intel® AMT, Intel® Standard Manageability, Intel® Anti-Theft, Level III Manageability Upgrade or Intel® RPAT) is enabled on the platform.

Enable user notification: This option will allow the user to enable or disable Intel® Management and Security Status icon from displaying important notifications in the notification area (for instance notification will be sent when one of the technologies is enabled or disabled).

4.2 Intel® AMT Tab

Note: This tab is displayed only if the platform supports Intel® AMT.

Click the **Intel® AMT** tab to display Intel® AMT information.



4.2.1 Fast Call for Help

The Fast Call for Help section provides CILA (Client Initiated Local Access) or CIRA (Client Initiated Remote Access) capabilities depending on whether the system is connected to the corporate network or not, respectively.

CIRA allows a user to connect the Intel® AMT system to the company's Information Technology network from an external internet connection. Click the **Get Technical Help** button to connect to your Information Technology network for system diagnostics and maintenance. The current connection status is displayed in this section as well.

CILA (Client Initiated Local Access) feature allows a user connected to the internal corporate network to send a support request to the IT administrator.

Note: The information displayed in the Intel® Management and Security Status application, including the Fast Call for Help section, is not shown in real time. The data is refreshed every time an event has arrived.

Note: When the user is connected as Guest account (in Windows*) the "Fast Call For Help" section will be grayed out. This was designed to prevent users outside of the organization to influence the organization network.

4.2.2 Support Session Status Section

The following information is provided:

- **Remote Control Connection**

  Indicates whether there is any open KVM (Keyboard, Video & Mouse) Remote Control session (Connected / Disconnected / Information unavailable).

  Note: When using server or mutual authentication, information is displayed only if a certificate exists.

  Click the Stop Session button to close an open Remote control session.

- **Media Redirection**

  Indicates whether there are any open IDE redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable

- **Terminal/Keyboard Redirection**

  Indicates whether there are any open terminal/keyboard redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable.

- **Stop Session**

  Click the Stop Session button to close any open KVM remote control session. If Host Based Configuration (aka HBC) is enabled, the Stop Session button will also close an open media redirection or terminal/keyboard redirection session. In cases where user consent is required for such a session, re-establishing the session will require renewal of user consent after clicking this button. (See more about HBC under Advanced Tab).

- **Hot key**

Indicates the hot key which could be used to close any open KVM remote control, media redirection, or terminal/keyboard redirection sessions (same effect as Stop Session button).

Click on the Change button to choose a different hot key for terminating an open session.

- **Prevent Access**

  This button will appear in cases where user consent is required for a remote support session to occur. In such cases, after the user will provide the required approval to the remote administrator and as long as the healing session hasn't begun, the user will see the Prevent Access button. This button enables the user to change his/her mind, as clicking on it will cancel user consent and disable the ability of the IT administrator to begin the remote session. During this time, the Hot Key will also serve as a means to cancel user consent. Once a remote support session has begun, the Prevent Access button will no longer be visible, and the Stop Session button will appear instead.

Note: User Consent, when required, will be granted to the administrator per session, by the user giving the administrator a one-time pass code which will appear on the Secure Output Window presented on the user's screen. See more about Secure Output Window and User Consent Policy under Advanced Tab - Secure Output Window Settings.

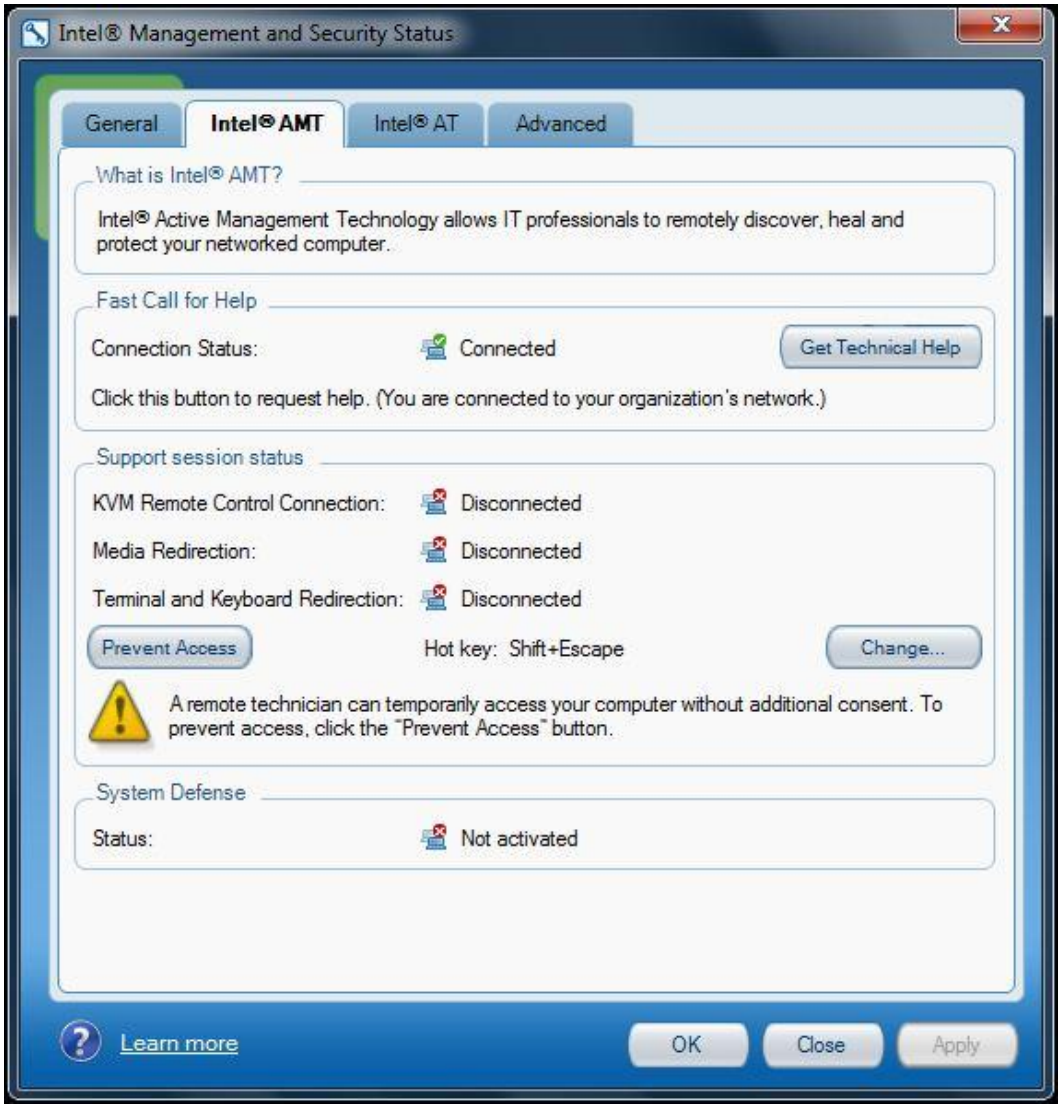
Intel® Management and Security Status Application Icon during support session

- The notification area tray icon appears animated as long as user consent or support session is active.
- Stop Session/ Prevent Access are available also thru clicking on the tray icon.

4.2.3 System Defense State

- **System Defense State**

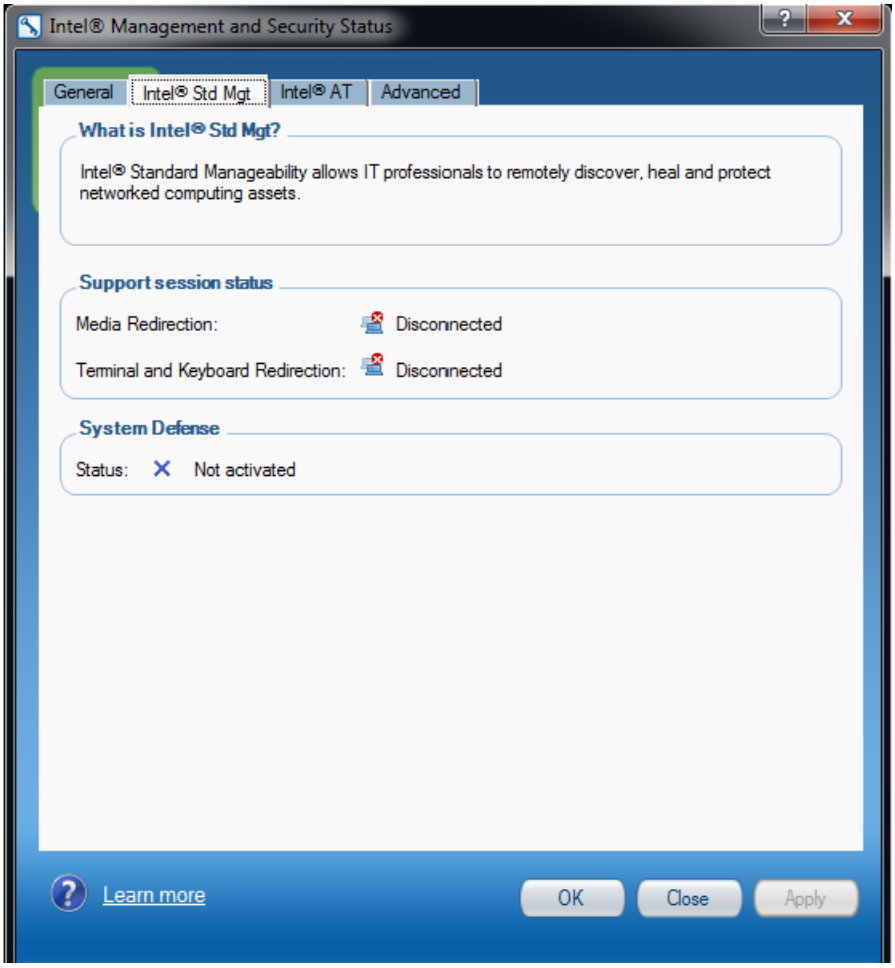
  Indicates whether System Defense policies are currently active.
  Possible values: Activated/Not activated/ Information unavailable.


Intel® Management and Security Status
General
Intel® AMT
Intel® AT
Advanced
What is Intel® AMT?
Intel® Active Management Technology allows IT professionals to remotely discover, heal and protect your networked computer.
Fast Call for Help
Connection Status:
Connected
Get Technical Help
Click this button to request help. (You are connected to your organization's network.)
Support session status
KVM Remote Control Connection:
Disconnected
Media Redirection:
Disconnected
Terminal and Keyboard Redirection:
Disconnected
Prevent Access
Hot key: Shift+Escape
Change...
A remote technician can temporarily access your computer without additional consent. To prevent access, click the "Prevent Access" button.
System Defense
Status:
Not activated
Learn more
OK
Close
Apply

4.3 Intel® Std Mgt Tab

Note: This tab is displayed only if the platform supports Intel® Standard Manageability.

Click the **Intel® Std Mgt** tab to display Intel® Standard Manageability information.



4.3.1 Support Session Status Section

The following information is provided:

- **Media Redirection**

  Indicates whether there are any open IDE redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable

- **Terminal and Keyboard Redirection**

  Indicates whether there are any open terminal/keyboard redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable.

4.3.2 System Defense State

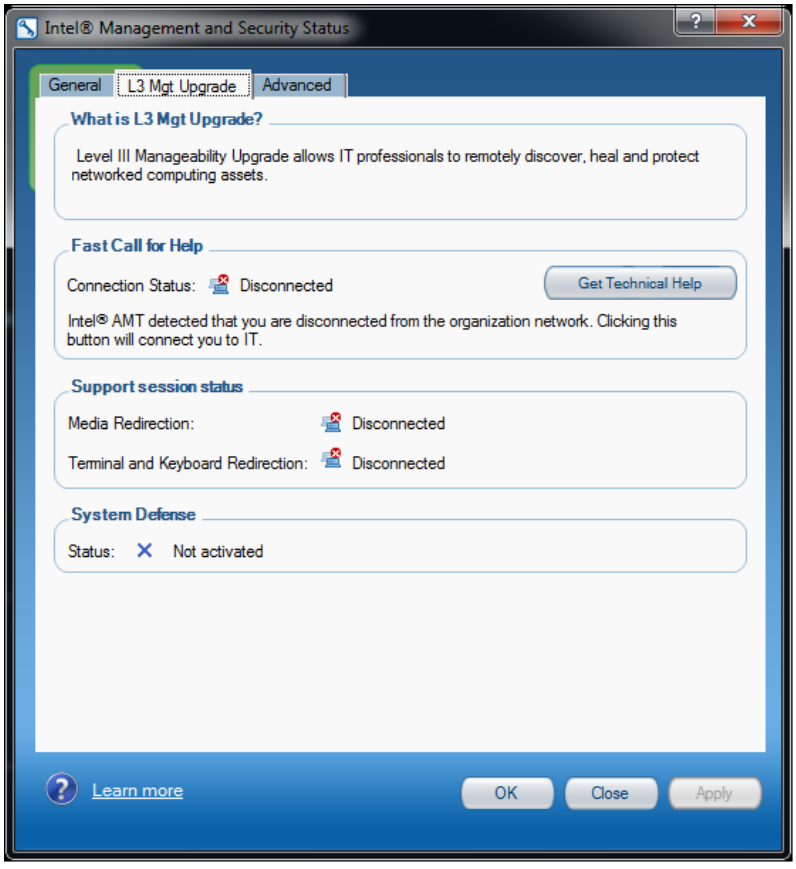
- **System Defense State**

  Indicates whether System Defense policies are currently active.
  Possible values: Activated/Not activated/ Information unavailable.

4.4 L3 Mgt Upgrade Tab

Note: This tab is displayed only if the platform supports Level III Manageability Upgrade.

Click the **L3 Mgt Upgrade** tab to display Level III Manageability Upgrade information.



4.4.1 Fast Call for Help

The Fast Call for Help section provides CILA (Client Initiated Local Access) or CIRA (Client Initiated Remote Access) capabilities depending on whether the system is connected to the corporate network or not, respectively.

CIRA allows a user to connect the Level III Manageability Upgrade system to the company's Information Technology network from an external internet connection.

Click the **Get Technical Help** button to connect to your Information Technology network for system diagnostics and maintenance. The current connection status is displayed in this section as well.

CILA (Client Initiated Local Access) feature allows a user connected to the internal corporate network to send a support request to the IT administrator.

Note: The information displayed in the Intel® Management and Security Status application, including the Fast Call for Help section, is not shown in real time. The data is refreshed every time an event has arrived.

Note: When the user is connected as Guest account (in Windows*) the "Fast Call For Help" section will be grayed out. This was designed to prevent users outside of the organization to influence the organization network.

4.4.2 Support Session Status Section

The following information is provided:

- **Media Redirection**

  Indicates whether there are any open IDE redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable

- **Terminal and Keyboard Redirection**

  Indicates whether there are any open terminal/keyboard redirection sessions.
  Possible values: Connected/ Disconnected/ Information unavailable.

4.4.3 System Defense State

- **System Defense State**

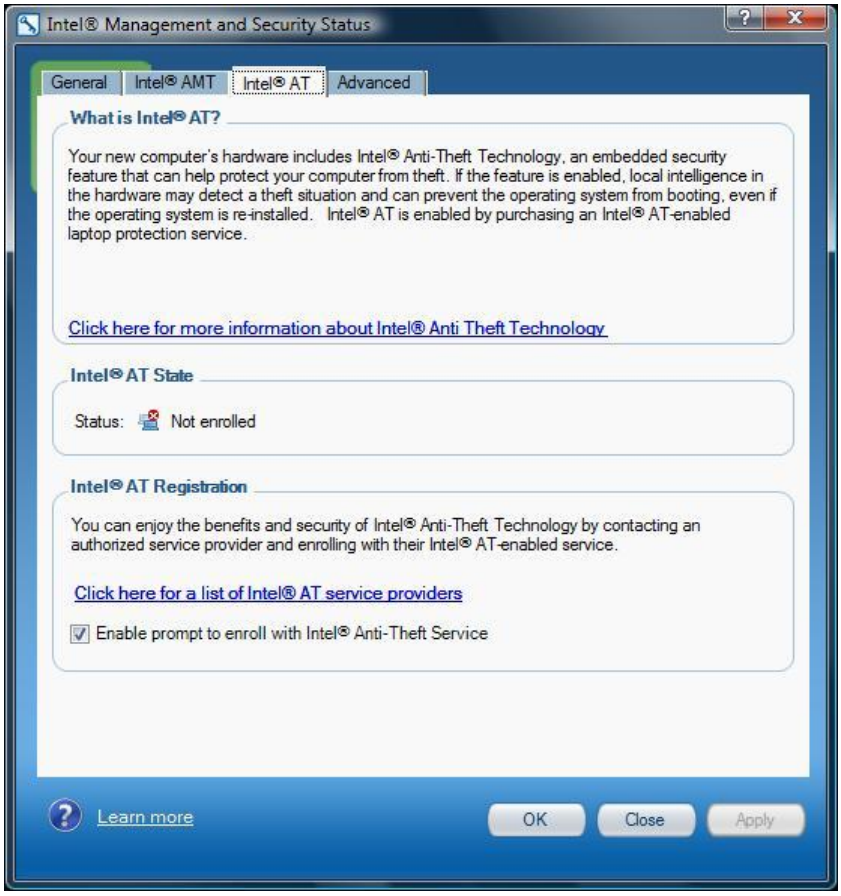
  Indicates whether System Defense is currently active.
  Possible values: Activated/Not activated/ Information unavailable.

4.5 Intel® AT Tab

Note: This tab is displayed only if the platform supports Intel® AT.

Click the Intel® AT tab to view Intel® Anti-Theft information.

Note: The information in this tab shows the state of the platform when the Intel® Management and Security Status application was last launched.



Clicking the link in the **What is Intel® AT** section connects you to an Intel site that provides you with information about Intel® Anti-Theft technology.

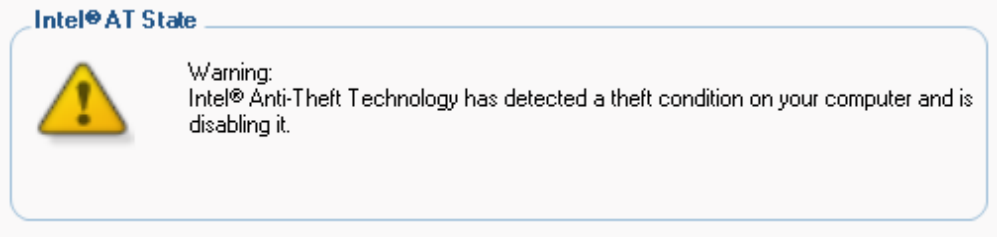
4.5.1 Intel® AT State

Provides the following information:

Enrolled: The platform has been enrolled with a service provider that is providing Intel® Anti-Theft protection for it.

Not Enrolled: The platform has not been enrolled with a service provider that is providing Intel® Anti-Theft protection.

Stolen: The Intel® Anti-Theft service provider has determined that the platform has been stolen, and has activated Intel® Anti-Theft to disable the platform. In this case, the following message is displayed:



4.5.2 Intel® AT Registration

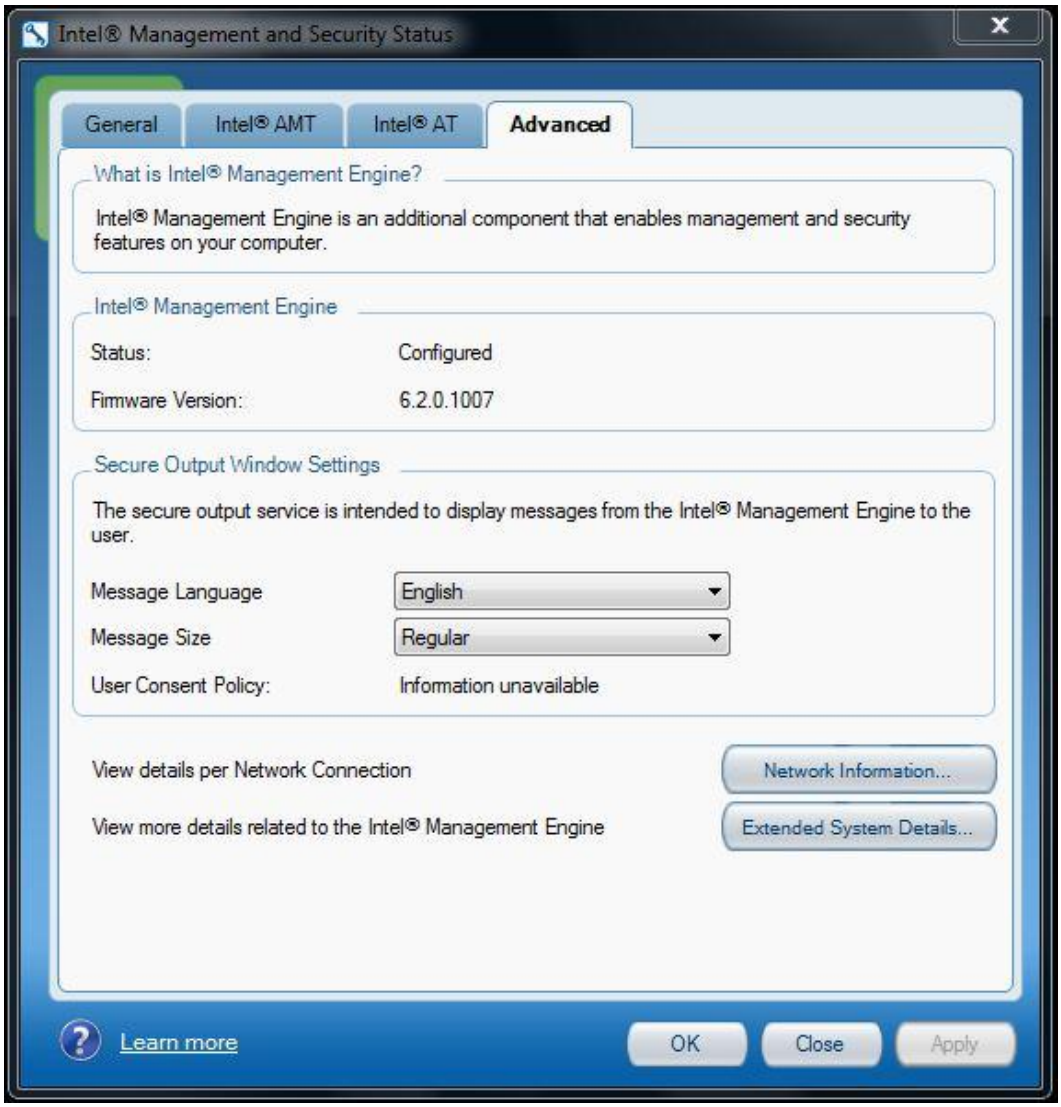
Note: This section is displayed only if the platform has not been enrolled with a service provider that is providing Intel® Anti-Theft protection.

Clicking the link in this section displays a list of Intel® AT service providers in your area and allows you to enroll with their Intel® AT service.

Enable prompt to enroll with Intel® Anti-Theft Service: If this box is checked, a balloon displaying an invitation to enroll with Intel® AT service is displayed every 5th time that the Intel® Management and Security Status application is started. If the platform has been enrolled with Intel® AT service, the balloon is not displayed.

4.6 Advanced Tab

Click the **Advanced** tab to view additional information.



4.6.1 Intel® Management Engine

The following information is provided:

- **Status**

  The operational status of Intel® ME
  Possible values: Configured / Unconfigured / Information unavailable.

- **Firmware Version**

The Intel® ME firmware version.
"Information Unavailable" will be displayed if the platform has no manageability or if the software has lost its connection to the firmware.

- **Control Mode (not present by default)**

  In 6.2.x firmware, "Host Based Configuration" (aka HBC) has been introduced, although disabled by default. There are two configuration modes for Intel® ME under HBC – Client Control Mode and Admin Control Mode. If the PC manufacturer has enabled HBC on the platform and the Intel® ME status is Configured, the relevant Control Mode will be shown.

4.6.2 Secure Output Window Settings

The following information is provided for the Secure Output feature, currently implemented in KVM (keyboard/video/mouse) redirection. If the machine has HBC enabled and has been configured in Client Control Mode, this is provided in IDE redirection and remote power operations as well.

- **Message Language**

  Specifies the language used by the Secure Output feature. Choose one of the listed languages.

- **Message Size**

  Specifies the window size of messages displayed by the Secure Output Feature. Choose one of the following: **Regular** or **Large**.

- **User Consent Policy**

  Specifies the policy for when the user's approval will be required in order to establish a remote support session by an IT administrator. User Consent will be granted to the administrator per session, by the user giving the administrator a one-time pass code which will appear on the Secure Output Window presented on the user's screen.

  Possible Policies are:

  User consent not required for any remote session

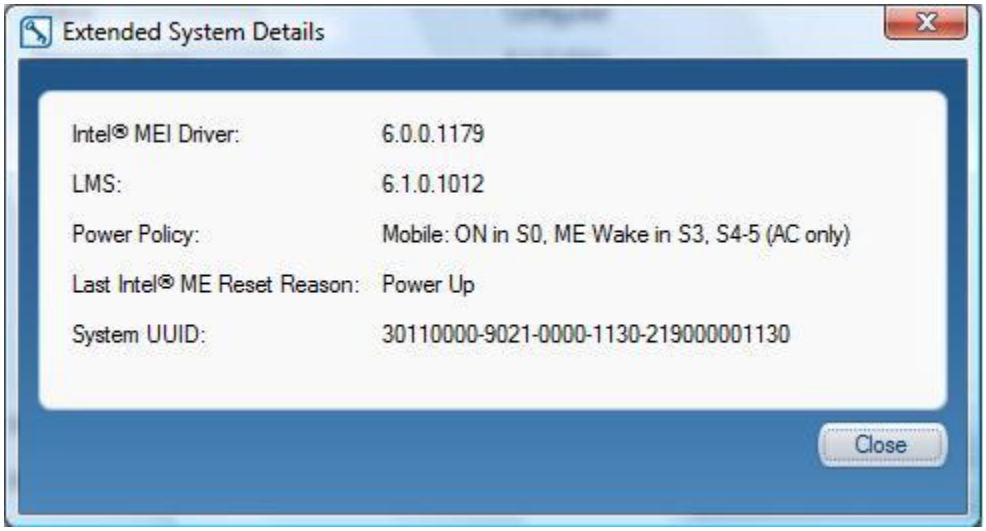
  User consent required for KVM session only

  User consent required for all remote sessions (i.e., KVM, IDE redirection, and remote power operation)

Note: If you are working in TLS mode but the local certificates are incorrect or missing, the KVM and Secure output information displayed by the Intel® Management and Security Status application is not up-to-date, and the secure output configuration cannot be changed.

4.6.3 Extended System Details

When you click Extended System Details, the following information is displayed:



- **Intel® MEI Driver**

  The version of the Intel® Manageability Engine Interface driver.

- **LMS**

  The version of the LMS service.

- **Power Policy**

  The power modes in which the Manageability Engine is available.
  States are: ON in S0, or any other power policy supported by the system.

- **Last Intel® ME Reset Reason**

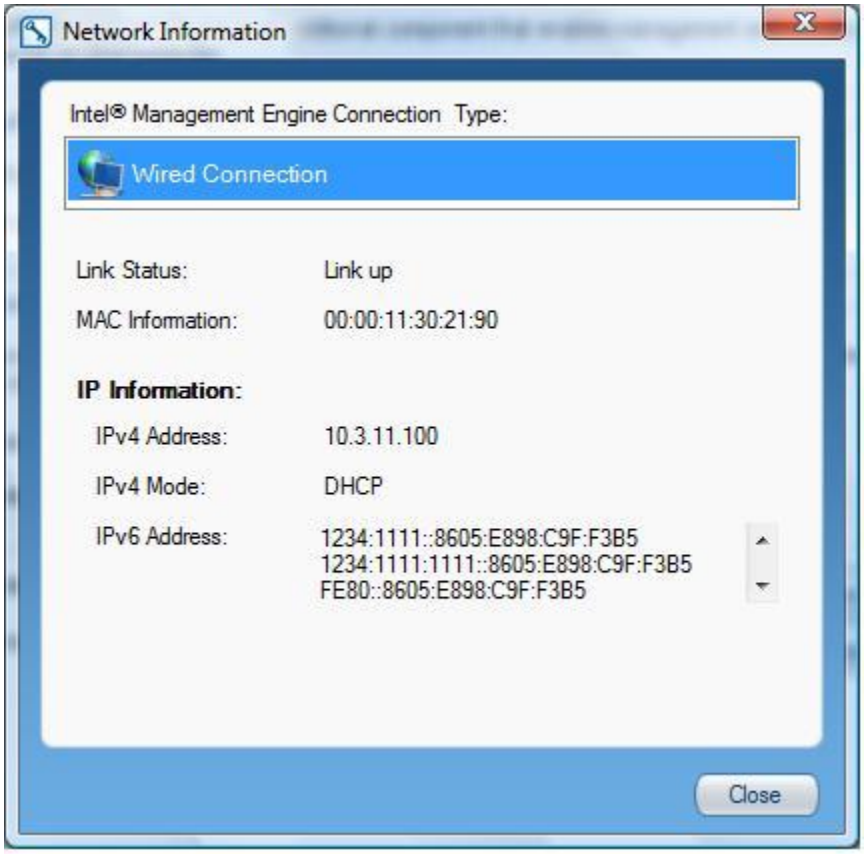
  Displays the reason that the Intel® ME was last reset.
  Possible values: Global System / FW reset / Power Up / Unknown cause / Information unavailable

- **System UUID**

  The current System Unique Universal Identification. Standard System UUID presentation, such as, 03000200-0400-0500-0006-000700080009.

4.6.4 Network Information

Click the **Network Information** button to display network details regarding Intel® ME wireless and wired connectivity.



In the **Connection Type** section, click either **Wireless Connection** or **Wired Connection** to display information on the following items for the selected interface:

- **Link Status**

  Whether the link is currently active.
  Possible values are: Link up/Link down/Information unavailable

- **MAC Information**

  XX:XX:XX:XX:XX:XX – e.g. 88:88:88:0A:88:87

- **IPv4 Address**

- **IPv4 Mode**

  Possible values: Static/DHCP/Information unavailable.

- **IPv6 address**

  If IPv6 addressing is enabled for the ME, the Intel® Management and Security Status application displays up to 6 IPv6 IP addresses configured for an ME network interface.

- **Configured for Wireless**

  (appears only for wireless connection)
  Possible values are: Wireless enabled / Wireless disabled / Information unavailable.

4.7 Exiting the Application

To exit the application, right click or left click on the Intel® Management and Security Status icon in the notification area and select **Exit**.

The following window is displayed.

Click **Yes** to automatically start the Intel® Management and Security Status application when you next log on.

§

5 Advanced Configuration

5.1 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**). The default logo will appear if the bitmap file is invalid or absent.

Note: The bitmap dimensions must be 62 (width) by 48 (height) or at the same proportions as 62 X 48. This is because the logo will be resized to match the logo size in the general tab.

5.2 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.

1. 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**.

2. 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.

5.3 Load in Disabled State

By default, Intel® Management and Security Status application will not load in case all ME technologies are disabled or required component is not functioning (referred as 'disabled state' in the following sections).

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'.

5.4 Specifying the Delay Before the Intel® Management and Security Status Loads

By default the Intel® Management and Security Status application starts loading 60 seconds 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 maximum allowed delay is 180 seconds.

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

IMSS "C:\Program Files\Common Files\Intel\Privacy Icon\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 (60 seconds). To cause the application to load without any delay, change the value of the **IMSS** key to
C:\Program Files\Common Files\Intel\Privacy Icon\PrivacyIconCLient.exe" -startup

5.5 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.

5.6 Disabling the Intel® AT Tab

By default, the Intel® AT tab is displayed if the platform supports Intel® AT. To disable Intel® AT on the platform, assign the value **1** to the **DisableAT** registry key in the **HKLM\SOFTWARE\Intel\PIcon\Setting** registry directory. (If this key is missing from the registry, create one with type DWORD.) If this is done, the Intel® AT tab is not displayed, no new balloon notifications are displayed, and no new Intel® AT events are displayed in the General tab.

5.7 '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 point 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, simply delete the value.

§

6 Troubleshooting Intel® Management and Security Status Application

6.1 Error Message Appears upon Application Load

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

To avoid this, install a suitable Microsoft* .NET framework – see Chapter 3 for more details.

6.2 Working with Mutual Authentication on the Local Interface

When an IT organization or the user has chosen to work with Mutual authentication on the local interface – they must set valid client certificate in the right directory for some commands to be sent to the FW, for example:

1. Stop Session (in the Support session status in the Intel® AMT tab).
2. Secure output window settings (in the Advanced tab).

All events from the FW will be presented normally without any dependence in the client certificate.

6.3 'Information Unavailable' is Displayed instead of Technology Status

The Intel® Management and Security Status icon relies on the User Notification Service, which is installed together with the Intel® Management and Security Status application, to obtain information concerning the status of the resident technologies. Please make sure that:

1. The User Notification Service is running and started automatically on Windows* startup. If it is not installed, please reinstall the drivers according to section 3.

2. The Local Manageability Service (LMS) is running and started automatically on Windows* startup. If it is not installed, please reinstall the drivers according to section 3.

3. The Intel® MEI driver is installed, enabled and functioning properly. Please review the Bring up Guide document for more information concerning this driver.

6.4 Client Initiated Remote Access Connection Failure

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

1. The User Notification Service is not running. It can be started through the Services pane in the Computer Management window. If it is not installed, please reinstall the drivers according to section 3.

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.

§